Blockchain Article Citations

This document is a compilation of blockchain documents (I find interesting) pertaining mostly to health care but also to:

- Electronic Health Records (and Interoperability), Health Systems, or Health Advocacy
- Clinical Trials
- Security, Encryption, Software Engineering
- Identity Management
- Legal or Regulatory considerations
- Business and Community management

The citations are nearly exclusively comprised of the following reference types:

- Journal articles (traditional and electronic)
- Books and Book Sections (traditional, electronic, edited)
- Conference Papers
- Conference Proceedings
- Government Documents, such as Bills, Hearings, Reports, Regulations, and Statutes
- Theses

Some Magazine Articles, (Company) Reports, or Unpublished Work were also included in this listing if they contributed unique perspective—even if not peer reviewed.

Reference Format


Disclaimers

- Citation information was downloaded from the publisher whenever possible, but it was necessary to use discretion to determine the correct ‘Reference Type’ and to manually augment several details or correct inaccuracies. It is not feasible to identify all of the publisher’s inaccuracies.
- Journal Abbreviations were manually obtained from PubMed or http://www.journalabbr.com/ and other internet sources.
- For Conference Papers and Conference Proceedings, it was also necessary to manually look up the conference location, dates, and publisher—requiring up to 30-45 minutes of searching per Conference article. Different websites provides slightly different information and I used discretion to add as much information as I could find; however, it is not feasible to obtain all information.
- The Abstract was copied and pasted from the Abstract section of the article whenever available; otherwise, the first few paragraphs were provided. I corrected obvious publisher spelling errors whenever identified, but I did not modify unconventional capitalizations, punctuations, or spellings.
- Website locations are considered part of the formal citation for electronic articles and books. For other types of articles, I created a separate listing as a courtesy so the reader can find the article.

Contact Information
Citations


Reference Type: Journal Article
Available from: https://www.mdpi.com/2073-8994/11/6/774

Abstract: The Internet of Things (IoT) makes our lives much easier, more valuable, and less stressful due to the development of many applications around us including smart cities, smart cars, and smart grids, offering endless services and solutions. Protecting IoT data of such applications at rest either on the objects or in the cloud is an indispensable requirement for achieving a symmetry in the handling and protection of the IoT, as we do with data created by persons and applications. This is because unauthorised access to such data may lead to harmful consequences such as linkage attacks, loss of privacy, and data manipulation. Such undesired implications may jeopardise the existence of IoT applications if protection measures are not taken, and they stem from two main factors. One is that IoT objects have limited capabilities in terms of memory capacity, battery life, and computational power that hamper the direct implementation of conventional Internet security solutions without some modifications (e.g., traditional symmetric algorithms). Another factor is the absence of widely accepted IoT security and privacy guidelines for IoT data at rest and their appropriate countermeasures, which would help IoT stakeholders (e.g., developers, manufacturers) to develop secure IoT systems and therefore enhance IoT security and privacy by design. Toward this end, we first briefly describe the main IoT security goals and identify IoT stakeholders. Moreover, we briefly discuss the most well-known data protection frameworks (e.g., General Data Protection Regulation (GDPR), Health Insurance Portability (HIPAA)). Second, we highlight potential attacks and threats against data at rest and show their violated security goals (e.g., confidentiality and integrity). Third, we review a list of protection measures by which our proposed guidelines can be accomplished. Fourth, we propose a framework of security and privacy guidelines for IoT data at rest that can be utilised to enhance IoT security and privacy by design and establish a symmetry with the protection of user-created data. Our framework also presents the link between the suggested guidelines, mitigation techniques, and attacks. Moreover, we state those IoT stakeholders (e.g., manufacturers, developers) who will benefit most from these guidelines. Finally, we suggest several open issues requiring further investigation in the future, and we also discuss the limitations of our suggested framework.


Reference Type: Electronic Article

Abstract: Achieving government’s goals for cannabis regulation requires legal cannabis to be a cheaper, more attractive consumer alternative compared to the illegal market. This goal may be undermined by the costs and disadvantages of traditional regulatory management.

A Canada wide, real-time blockchain tracking system appears to be a viable technical solution architecture.

A permissioned blockchain network could be tested alongside traditional tracking. This investment, if proven effective, could reduce regulatory costs for government and red tape for business, helping to achieve Governments’ objectives to:
1) Enhance public safety by ensuring quality and monitoring product sales
2) Undermine illegal markets to reduce crime and prevent product diversion


Reference Type: Journal Article
Available from: https://www.mdpi.com/2227-9032/7/2/56

Abstract: Since blockchain was introduced through Bitcoin, research has been ongoing to extend its applications to non-financial use cases. Healthcare is one industry in which blockchain is expected to have significant impacts. Research in this area is relatively new but growing rapidly; so, health informatics researchers and practitioners are always struggling to keep pace with research progress in
This paper reports on a systematic review of the ongoing research in the application of blockchain technology in healthcare. The research methodology is based on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) guidelines and a systematic mapping study process, in which a well-designed search protocol is used to search four scientific databases, to identify, extract and analyze all relevant publications. The review shows that a number of studies have proposed different use cases for the application of blockchain in healthcare; however, there is a lack of adequate prototype implementations and studies to characterize the effectiveness of these proposed use cases. The review further highlights the state-of-the-art in the development of blockchain applications for healthcare, their limitations and the areas for future research. To this end, therefore, there is still the need for more research to better understand, characterize and evaluate the utility of blockchain in healthcare.


Reference Type: Journal Article
Available from: http://www.eurekaselect.com/172892/article Subscription required to view

Abstract: BACKGROUND: The promising eventual fate of blockchain in healthcare has a lot more extensive horizon. The blockchain is a novel structure that gives another design to storage and trade of data among different members of a particular network. In case of a hospital, blockchain takes into consideration for the creation of better treatment structure by the expert doctor in order to arrange the meeting based on a symptom of patients throughout the world by the electronic system. The blockchain technology is crucial for biomedical and human services applications as social insurance has turned out to be a standout amongst the most essential rising application areas of the blockchain distributed ledger technology. RESULT: By and large, blockchain is treated as a conveyed record to store social insurance related information for allocation, trading, dissecting, footage, and affirming purposes among accomplices. The advantage of blockchain databases versus traditional dispersed databases is that they are decentralized, permanent and perfected with advanced digital payment frameworks and hash chain occasion structure. The blockchain code is unlocked resource and can be utilized, altered and customized by its clients. CONCLUSION: Now a day, blockchain is expected to be almost universally adopted across medical organizations around the world. The purpose of this review article is to comprehend the current explore subjects, difficulties and future headings in regards to blockchain innovation from the specialized perspective in the health care system.


Reference Type: Journal Article
Available from: https://www.nature.com/articles/550043e

Abstract: Blockchain technology is helping to meet sustainability challenges for example in renewable energy and conservation. Food security could also benefit from the technology’s transparency, relatively low transaction costs and instantaneous application. Blockchain assignment of unique digital identifiers to food products would make them traceable through supply chains, along with their growth conditions, batch numbers and expiry dates. This would help to prevent food waste, allow consumers to work out the ecological footprint of their food, and guide the distribution of surplus food to those who need it. This shared and immutable register of foods and transactions would prevent fraud and enable source identification of food-borne illness. And as digital technologies are increasingly used to manage farms, blockchain will promote sharing of on-farm data.


Reference Type: Conference Paper

Abstract: Digital world has produced efficiencies, new innovative products, and close customer relationships globally by the effective use of mobile, IoT (Internet of Things), social media, analytics and cloud technology to generate models for better decisions. Blockchain is recently introduced and revolutionizing the digital world bringing a new perspective to security, resiliency and efficiency of systems. While initially popularized by Bitcoin, Blockchain is much more than a foundation for crypto currency. It offers a secure way to exchange any kind of good, service, or transaction. Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. To address these challenges, Blockchain will enable more agile value chains, faster
product innovations, closer customer relationships, and quicker integration with the IoT and cloud technology. Further Blockchain provides a lower cost of trade with a trusted contract monitored without intervention from third parties who may not add direct value. It facilitates smart contracts, engagements, and agreements with inherent, robust cyber security features. This paper is an effort to break the ground for presenting and demonstrating the use of Blockchain technology in multiple industrial applications. A healthcare industry application, Healthchain, is formalized and developed on the foundation of Blockchain using IBM Blockchain initiative. The concepts are transferable to a wide range of industries as finance, government and manufacturing where security, scalability and efficiency must meet.


Reference Type: Conference Paper

Abstract: Healthcare data are grabbing the interest of cyber attackers in recent years. Annihilating consequences of healthcare data could be alleviated through decentralization. A peer to peer (P2P) network enables the property of decentralization, where different parties can store and run computation while keeping the sensitive health data private. Blockchain technology leverages decentralized or distributed process, which ensures the accountability and integrity of its use. This paper presents a patient centric healthcare data management system by using Blockchain as storage to attain privacy. Pseudonymity is ensured by using the cryptographic functions to protect patient’s data.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/18/10/3561

Abstract: Resource consumption in residential areas requires novel contributions in the field of consumer information management and collaborative mechanisms for the exchange of resources, in order to optimize the overall consumption of the community. We propose an authorization system to facilitate access to consumer information and resource trading, based on blockchain technology. Our proposal is oriented to the Smart communities, an evolution of Community Energy Management Systems, in which communities are involved in the monitoring and coordination of resource consumption. The proposed environment allows a more reliable management of monitoring and authorization functions, with secure data access and storage and delegation of controller functions among householders. We provide the definition of virtual assets for energy and water resource sharing as an auction, which encourages the optimization of global consumption and saves resources. The proposed solution is implemented and validated in application scenarios that demonstrate the suitability of the defined consensus mechanism, trustworthiness in the level of provided security for resource monitoring and delegation and reduction on resource consumption by the resource trading contribution.


Reference Type: Journal Article
Available from: https://www.jacr.org/article/S1546-1440(18)31282-1/fulltext

Abstract: The medical device industry is undergoing rapid change as innovation accelerates, new business models emerge, and artificial intelligence and the Internet of Things create disruptive possibilities in health care. On the innovation front, global annual patent applications related to medical devices have tripled in 10 years, and technology cycle times have halved in just 5 years. Connectivity has exploded-by 2021, the world will have more than three times as many smart connected devices as people-and more and more medical devices and processes contain integrated sensors. In this article, we report on recent McKinsey (McKinsey & Company, New York, New York) work to map start-ups and trends shaping the future of medical imaging. We identify technology clusters with prospects of future growth, look at some of their cutting-edge practices, and consider what the implications may be for our specialty.

Reference Type: Conference Paper

Abstract: Blockchains as a technology emerged to facilitate money exchange transactions and eliminate the need for a trusted third party to notarize and verify such transactions as well as protect data security and privacy. New structures of Blockchains have been designed to accommodate the need for this technology in other fields such as e-health, tourism and energy. This paper is concerned with the use of Blockchains in managing and sharing electronic health and medical records to allow patients, hospitals, clinics, and other medical stakeholder to share data amongst themselves, and increase interoperability. The selection of the Blockchains used architecture depends on the entities participating in the constructed chain network. Although the use of Blockchains may reduce redundancy and provide caregivers with consistent records about their patients, it still comes with few challenges which could infringe patients' privacy, or potentially compromise the whole network of stakeholders. In this paper, we investigate different Blockchains structures, look at existing challenges and provide possible solutions. We focus on challenges that may expose patients' privacy and the resiliency of Blockchains to possible attacks.

Al-Nemrat A, Houari Boumediene University of Sciences and Technology, IEEE, editors. Identity theft on e-government/e-governance digital forensics [abstract]. 2018 International Symposium on Programming and Systems (ISPS); 2018 Apr 24-26; Algiers, Algeria. IEEE.

Reference Type: Conference Proceedings

Abstract: In the context of the rapid technological progress, the cyber-threats become a serious challenge that requires immediate and continuous action. As cybercrime poses a permanent and increasing threat, governments, corporate and individual users of the cyber-space are constantly struggling to ensure an acceptable level of security over their assets. Maliciousness on the cyber-space spans identity theft, fraud, and system intrusions. This is due to the benefits of cyberspace-low entry barriers, user anonymity, and spatial and temporal separation between users, make it a fertile field for deception and fraud. Numerous, supervised and unsupervised, techniques have been proposed and used to identify fraudulent transactions and activities that deviate from regular patterns of behaviour. For instance, neural networks and genetic algorithms were used to detect credit card fraud in a dataset covering 13 months and 50 million credit card transactions. Unsupervised methods, such as clustering analysis, have been used to identify financial fraud or to filter fake online product reviews and ratings on e-commerce websites. Blockchain technology has demonstrated its feasibility and relevance in e-commerce. Its use is now being extended to new areas, related to electronic government. The technology appears to be the most appropriate in areas that require storage and processing of large amounts of protected data. The question is what can blockchain technology do and not do to fight malicious online activity?


Reference Type: Journal Article

Abstract: The blockchain technology has reached a great boom in the health sector, due to its importance to overcome interoperability and security challenges of the EHR and EMR systems in eHealth. The main objective of this work is to show a review of the existing research works in the literature, referring to the new blockchain technology applied in ehealth and exposing the possible research lines and trends in which this technology can be focused. The search for blockchain studies in eHealth field was carried out in the following databases: IEEE Xplore, Google Scholar, Science Direct, PubMed, Web of Science and ResearchGate from 2010 to the present. Different search criteria were established such as: “Blockchain” AND (“eHealth” OR “EHR” OR “electronic health records” OR “medicine”) selecting the papers considered of most interest. A total of 84 publications on blockchain in eHealth were found, of which 18 have been identified as relevant works, 5.56% correspond to the year 2016, 22.22% to 2017 and 72.22% to 2018. Many of the publications found show how this technology is being developed and applied in the health sector and the benefits it provides. The new blockchain technology applied in eHealth identifies new ways to share the distributed view of health data and promotes the advancement of precision medicine, improving health and preventing diseases.

Reference Type: Conference Proceedings

Available from: https://dl.acm.org/citation.cfm?id=3144733 Subscription required to view.

Abstract: Our data is now more valuable than ever. The uncontrolled growth of internet-centered services has led us to accept many compromises about how we share it. In the era of Internet of Things, smart devices are collecting personal data continuously. Now, more than ever, we are in need of privacy-preserving applications where users are always in control of their sensitive data. Previous work focuses on the preservation of privacy on datasets possibly collected during clinical trials. In contrast, here we focus on the preservation of privacy during the preliminary recruiting phase of a clinical trial. Our solution is the first where a) user's data are not stored in any public database and remain in the user's private space during the whole recruiting phase and b) at the same time the Clinical Research Institute is assured that it is acquiring useful and authentic data. We provide a proof-of-concept implementation and study its performance based on a real-world evaluation.


Reference Type: Conference Paper


Abstract: Our personal data is now more valuable than ever. The uncontrolled growth of internet-centered services has led us to accept many compromises about how we share it. In the era of Internet of Things, personal data is collected continuously. Now, more than ever, we are in need of privacy-preserving applications where users always retain control of their personal data. In this paper, we present a secure way to control the flow of personal data in the specific case of the recruitment of participants for clinical trials. We take special care to protect the interests of both parties: the individual can keep its data private until an agreement is reached, and the Clinical Research Institute can be assured that it is acquiring useful and authentic data. We provide a proof-of-concept implementation and study its performance based on a real-world evaluation.


Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/PMC6308650/ Subscription required to view.

Abstract: In the era of the Internet of Things (IoT), drug developers can potentially access a wealth of real-world, participant-generated data that enable better insights and streamlined clinical trial processes. Protection of confidential data is of primary interest when it comes to health data, as medical condition influences daily, professional, and social life. Current approaches in digital trials entail that private user data are provisioned to the trial investigator that is considered a trusted party. The aim of this paper is to present the technical requirements and the research challenges to secure the flow and control of personal data and to protect the interests of all the involved parties during the first phases of a clinical trial, namely the characterization of the potential patients and their possible recruitment. The proposed architecture will let the individuals keep their data private during these phases while providing a useful sketch of their data to the investigator. Proof-of-concept implementations are evaluated in terms of performances achieved in real-world environments.


Reference Type: Journal Article


Abstract: The ongoing discussion regarding blockchain technologies is focused primarily on cryptocurrencies, but blockchain features and functionalities have developed beyond financial instruments. As the technologies provide new functionalities, the associated value proposition changes
This study explores the relationship between blockchain technologies and their underlying value drivers. Four identified distinct blockchain stages of increased maturity are analyzed and discussed. This covers the evolutionary technology types focused on transactions, smart contracts, decentralized applications, and the introduction of artificial intelligence supporting decentralized decision making. In addition, we address management issues around appropriate blockchain adoption using a blockchain value driver-focused framework that gives decision-makers actionable questions and recommendations. We provide practitioners with a method for assessing suitable blockchain adoption that addresses the specific value creation associated with a given organizational strategy. For academics, we critically identify and assess the characteristics of the blockchain stages and their strategy implications and provide a structured approach conceptualizing blockchain technology evolution.


Reference Type: Journal Article
Available from: https://www.ahajournals.org/doi/full/10.1161/CIRCOUTCOMES.117.003800

Abstract: Blockchain technology has gained substantial attention in recent years with increased interest in several diverse fields, including the healthcare industry. Blockchain offers a secure, distributed database that can operate without a central authority or administrator. Blockchain uses a distributed, peer-to-peer network to make a continuous, growing list of ordered records called blocks to form a digital ledger. Each transaction, represented in a cryptographically signed block, is then automatically validated by the network itself. Blockchain has also garnered interest as a platform to improve the authenticity and transparency of healthcare data through many use cases, from maintaining permissions in electronic health records (EHR) to streamlining claims processing. In this article, we describe the basics of blockchain and illustrate current and future applications of this technology within the healthcare industry.


Reference Type: Journal Article

Abstract: Cryptocurrency applications of distributed ledger methods such as blockchains are now well established, but their implications for more general topics are just beginning to be appreciated. Beyond applications in finance and banking, new applications are emerging in supply chain management, manufacturing, agricultural product tracking, advertising verification, Internet of Things, healthcare, and the pharmaceutical industry, among others.


Reference Type: Journal Article

Abstract: Food security can benefit from the technology's transparency, relatively low transaction costs and instantaneous applications. A blockchain is a distributed database of records in the form of encrypted blocks, or a public ledger of all transactions or digital events that have been executed and shared among participating parties and can be verified at any time in the future. Generally, the robust and decentralized functionality of the blockchain is used for global financial systems, but it can easily be expanded to contracts and operations such as tracking of the global supply chain. In the precision agriculture context, Information and Communications Technology can be further implemented with a blockchain infrastructure to enable new farm systems and e-agriculture schemes. The purpose of this review is to show a panorama of the scientific studies (enriched by a terms mapping analysis) on the use of blockchain in the agri-food sector, from both an entirely computational and an applicable point of view. As evidenced by the network analysis, the reviewed studies mainly focused on software aspects (e.g., the architecture and smart contracts). However, some aspects regarding the different blockchain knots (computers always connected to the blockchain network) having the role to store and distribute an updated copy of each block in a food supply chain, result of crucial importance. These technologies appear very promising and rich of great potential showing a good flexibility for applications in several sectors but still immature and hard to apply due to their complexity. This article is protected by copyright. All rights reserved.

Blockchain, the underlying technology that powers cryptocurrencies such as Bitcoin and Ethereum, is gaining so much attention from different industry stakeholders, governments and research communities. Its application is extending beyond cryptocurrencies and has been exploited in different domains such as finance, E-commerce, Internet of Things (IoT), healthcare, and governance. Some key attributes of the technology are decentralization, immutability, security and transparency. This paper aims to describe how permissioned Blockchain can be applied to a specific educational use case - decentralized verification of academic credentials. The proposed Blockchain-based solution, named ‘CredenceLedger’, is a system that stores compact data proofs of digital academic credentials in Blockchain ledger that are easily verifiable for education stakeholders and interested third party organizations.

---


Abstract: The first commercial transaction with the first cryptocurrency in 2010 marked the start of a revolution in transactions. Blockchain and cryptocurrencies will dramatically transform how we do transactions, just as the Internet revolutionized how we communicate. Currently, more than 2,000 cryptocurrencies are quoted on the market, and many more are being launched in initial coin offerings for use as an exchange method in a specific business ecosystem or as rights to assets or liabilities. As an emerging fintech, cryptocurrencies open up many opportunities, but they also pose significant challenges and limitations. This paper analyzes the key factors for the successful development of a cryptocurrency from a consumer-behavior perspective. Using a technology acceptance theoretical framework, we test a model able to explain almost 85% of the intention to use cryptocurrencies. Surprisingly, risk was not a significant factor. This could be because most of the respondents considered operating with cryptocurrencies to be risky; the lack of variability in their responses to the questions about perceived risk would explain this lack of explanatory power. However, willingness to manage cryptocurrency risk could be a precondition for adoption. The performance expectancy for a given cryptocurrency was the most important factor for its success. The research was conducted in Spain with college-educated adults with basic knowledge of the Internet.

---


Abstract: Internet protocols permit a single machine to masquerade as many, allowing an adversary to appear to control more nodes than it actually does. The possibility of such Sybil attacks has been taken to mean that distributed algorithms that tolerate only a fixed fraction of faulty nodes are not useful in peer-to-peer systems unless identities can be verified externally. The present work argues against this assumption by presenting practical algorithms for the distributed computing problem of Byzantine agreement that defend against Sybil attacks by using moderately hard puzzles as a pricing scheme for identities. Though our algorithms do not prevent Sybil attacks entirely, they solve Byzantine agreement (and some useful variants) when the limited fraction of nodes that can fail is replaced by a limited fraction of the total computational power. These results suggest that Byzantine agreement and similar tools from the distributed computing literature are likely to help solve the problem of adversarial behavior by components of peer-to-peer systems.

---


Abstract: The most fundamental purpose of blockchain technology is to enable persistent, consistent,
distributed storage of information. Increasingly common are authentication systems that leverage this property to allow users to carry their personal data on a device while a hash of this data is signed by a trusted authority and then put on a blockchain to be compared against. For instance, in 2015, MIT introduced a schema for the publication of their academic certificates based on this principle. In this work, we propose a way for users to obtain assured identities based on face-to-face proofing that can then be validated against a record on a blockchain. Moreover, in order to provide anonymity, instead of storing a hash, we make use of a scheme of Brands to store a commitment against which one can perform zero-knowledge proofs of identity. We also enforce the confidentiality of the underlying data by letting users control a secret of their own. We show how our schema can be implemented on Bitcoin’s blockchain and how to save bandwidth by grouping commitments using Merkle trees to minimize the number of Bitcoin transactions that need to be sent. Finally, we describe a system in which users can gain access to services thanks to the identity records of our proposal.

References:


Baars DS. Towards self-sovereign identity using blockchain technology [Master's Thesis]: University of Twente; 2016.
of these identities is very important. Surveys show that people often use the identity management systems they don't want to use. They don't have full control over their information, have no way to know what is shared with other parties and are dependent on trusted parties when logging into websites. Blockchain technology is used as a basis for a secure and transparent distributed ledger for the Bitcoin cryptocurrency. Its decentralized, public and immutable properties solve the double spending problem and allow all participants in the network to read the transaction history, help in the validation process and pay and receive Bitcoin. Cryptographically complex math ensures that everyone can do transactions with everyone without the need for a trusted third party. Next to financial transactions, this also holds for other claims. Entities can put claims on a decentralized ledger by digitally signing it, which allows any other entity to verify that these claims are made by that specific entity. This allows authorities like governments to make claims about individuals, which can be combined with other claims to create a very strong claim about someone. Because both the claimant and the claimee can be verified, this allows entities like mortgage lenders to outsource their Customer Due Diligence (CDD) processes. In this research we will explore the possibility of self-sovereign identity, where you are in control of your digital identity. We started with a desk research on currently available identity management solutions. We concluded that in most systems, the end-user is not able to store their own data. Currently only one decentralized system is available, but has not gained wide adoption yet. A case study has been performed on a solution which allows the exchange of KYC attributes, resulting from thorough Customer Due Diligence (CDD) as is often performed when opening a bank account. These attributes can be used by other entities, like insurance companies and mortgage lenders to make their on-boarding process easier for customers, since they don't need to supply copies of the same documentation all over again. Also, the companies themselves could outsource their Customer Due Diligence (CDD) this way to lower costs and make fewer errors. Although the idea is very interesting, the studied solution did not meet the expectations. At the time the company behind the solution was very small and the process to improve very complex. The solution was also proprietary, creating dependence on the vendor, which heightens the adoption barrier. Because of the lessons learned from the case study, the results of the literature research and the desk research, we designed an architecture for a Decentralized Identity Management System (DIMS) using the concept of claim-based identity and blockchain technology. To lower adoption barriers and create a self-sustaining ecosystem, it will be developed on a public blockchain and source code will be made open-source. The solution will be privacy-friendly by using privacy-enhancing techniques and storing only claims about one's identity. We also provide a solution to allow retrieval of more sensitive data, and made it as modular as possible to make integration within existing IT architecture easier. The Decentralized Identity Management System (DIMS) can be useful in a wide range of use cases, like proving your age when buying liquor at the supermarket or applying for a health insurance where you get a student discount if you can show you are enrolled at a university. This shows that our work resulted in a solid foundation for self-sovereign identity using blockchain technology.


Reference Type: Report


Abstract: Since the introduction of Bitcoin[Nak09] in 2009, and the multiple computer science and electronic cash innovations it brought, there has been great interest in the potential of decentralized cryptocurrencies. At the same time, implementation changes to the consensus critical parts of Bitcoin must necessarily be handled very conservatively. As a result, Bitcoin has greater difficulty than other Internet protocols in adapting to new demands and accommodating new innovation. We propose a new technology, pegged sidechains, which enables bitcoins and other ledger assets to be transferred between multiple blockchains. This gives users access to new and innovative cryptocurrency systems using the assets they already own. By reusing Bitcoin’s currency, these systems can more easily interoperate with each other and with Bitcoin, avoiding the liquidity shortages and market fluctuations associated with new currencies. Since sidechains are separate systems, technical and economic innovation is not hindered. Despite bidirectional transferability between Bitcoin and pegged sidechains, they are isolated: in the case of a cryptographic break (or malicious design) in a sidechain, the damage is entirely confined to the sidechain itself. This paper lays out pegged sidechains, their implementation requirements, and the work needed to fully benefit from the future of interconnected blockchains.


Reference Type: Conference Paper


Abstract: Recently, Blockchain is considered as one of the main powerful techniques in security and privacy domains. It is considered as the promised security concept for replacing the current third parties trusting solutions. This could be achieved by mixing some cryptography techniques, consensus algorithms alongside with some peer-to-peer communication protocols. In this paper, to meet the requirement of distributed structure in the eHealth Records (EHRs) system, we propose a novel protocol to achieve a perfect privacy preserving for the patient namely Pseudonym Based Encryption with
Different Authorities (PBE-DA) by applying the concept of Blockchain on the healthcare communication entities in an e-health platform. Therefore, PBE-DA will be used to help the patient anonymously to access, check or update his sensitive data on EHRs system. Moreover, we analyzed not only the public blockchain tier between the different EHRs cloud provider but also another Blockchain tier between the patient sensors (IoT devices used to do some patient measurements) and the patient system as a gateway for the whole healthcare platform.


Reference Type: Journal Article

Abstract: Internet of Things (IoT) are being adopted for industrial and manufacturing applications such as manufacturing automation, remote machine diagnostics, prognostic health management of industrial machines and supply chain management. Cloud-Based Manufacturing is a recent on-demand model of manufacturing that is leveraging IoT technologies. While Cloud-Based Manufacturing enables on-demand access to manufacturing resources, a trusted intermediary is required for transactions between the users who wish to avail manufacturing services. We present a decentralized, peer-to-peer platform called BPIIoT for Industrial Internet of Things based on the Block chain technology. With the use of Blockchain technology, the BPIIoT platform enables peers in a decentralized, trustless, peer-to-peer network to interact with each other without the need for a trusted intermediary.


Reference Type: Report

Abstract: With more consumers demanding a greater say in how their health is managed, life sciences and healthcare companies are increasingly adopting a patient-centric business model. In response to this paradigm shift, enterprises will need to reimagine how they receive regulatory approval for new products while meeting local and global regulatory requirements and gain access to information that can be shared rapidly with the patients and caregivers. Regulatory affairs (RA) is one of the most critical areas within the life sciences domain and is the gateway for acquiring product approvals. Regulatory process are subject to changes and adoption due to the ever changing updates to regulation as well as the new and emerging regulations. This causes several challenges – traceability and global visibility of the process, are the submissions being done as per the current or the earlier regulations, are we current on the latest labelling requirements, and are the products being shipped to that country in conformance with the submission made there in?

Equally important is that the entire organization and external consumers (such as clinical research organization (CRO), institutional review board (IRB), patients, and contract manufacturing organization (CMO) in the ecosystem have the most relevant and current data or information sets are the regulatory data like CMC coming from the several stakeholders consistent? This becomes a complicated affair when a globally distributed network of affiliates are responsible for managing a significant volume of critical product information.


Reference Type: Journal Article
Available from: http://ebooks.iospress.nl/publication/51706 Subscription required to view.

Abstract: One of the major problems that a national health system face is the lack of a unified clinical data management. In Greece, the critical and sensitive medical data generated during a patient lifetime are fragmented in one or more hospitals and healthcare services are not characterized by a ‘continuity’ factor. There is not the appropriate technological and administrative infrastructure for a unified patient medical history, prescriptions, laboratory tests or therapeutic plan. Technological, administrative and economic factors have led to this situation. We propose the integration and implementation of a blockchain network as a complementary technology to the existing information systems, so reliable and effective information management could be provided by a healthcare organization or the national healthcare system. Blockchain technology could be implemented as a bridge that can provide information systems interoperability within a hospital or between different hospitals.
Banga R, Juneja M. Clinical trials on blockchain. In PhUSE EU Connect; 2018 Nov 4-7; Frankfurt, Germany. Kent, United Kingdom: PhUSE; 2018.

Reference Type: Conference Paper

Abstract: The objective of this paper is to demonstrate how blockchain technology can be used to optimize the clinical trial workflow. We will demonstrate how pharmaceutical companies and other clinical trial participants (such as CROs, regulatory agencies) can collect and store subjects' data and analysis results in a secure, distributed manner and introduce a sample use case and technical architecture used for implementation of a blockchain based Clinical Trial Management Solution. We will demonstrate this concept using Hyperledger Fabric, an open source enterprise blockchain hosted by the Linux Foundation.

-------------------------------------------------------


Reference Type: Journal Article

Abstract: This paper discusses the dynamics of intraday prices of 12 cryptocurrencies during the past months' boom and bust. The importance of this study lies in the extended coverage of the cryptoworld, accounting for more than 90% of the total daily turnover. By using the complexity-entropy causality plane, we could discriminate three different dynamics in the data set. Whereas most of the cryptocurrencies follow a similar pattern, there are two currencies (ETC and ETH) that exhibit a more persistent stochastic dynamics, and two other currencies (DASH and XEM) whose behavior is closer to a random walk. Consequently, similar financial assets, using blockchain technology, are differentiated by market participants.

-------------------------------------------------------


Reference Type: Magazine Article

Abstract: The potential for blockchain to transform health care is very much a future prospect in 2019. But there are ways the technology can be applied today that can begin to pave the way to such a future.

Over the past few years, the healthcare industry has seen a rise in understanding of the timestamped, distributed-register technology blockchain and how it might, over time, affect the complex relationship between commerce and care. Healthcare leaders are beginning to have a realistic grasp of blockchain's potential and how it might transform the industry.

-------------------------------------------------------


Reference Type: Conference Proceedings

Abstract: In this paper, we present the applications of blockchain technology in healthcare. Furthermore, we evaluate the choice and deployment of Blockchain technology in such applications, review the advantages and disadvantages of such an approach. We review the Estonian system, which is the first blockchain-based health system at the national level, in detail and discuss its ramifications to Turkey. This paper is one of the first papers in this domain and, to the best of authors' knowledge, the first in Turkish.

-------------------------------------------------------

Blockchain technology stands to improve governance of the environment and of renewable energy. It could also facilitate peer-to-peer fundraising donations to transform nature conservation, which is drastically underfunded.

Cryptocurrency transactions are instant and transparent. They do not require bank accounts and international exchange fees are small. Donations can be sent directly to individuals or projects worldwide, rather than being collected, pooled and distributed by organizations. This encourages donors because the blockchain tracks the impact of donations.

By removing funding barriers, anyone can do conservation work — from restoring urban ecology to preventing conflicts between humans and wildlife. With a greater number and variety of conservationists and natural spaces, such small participatory efforts will be amplified through social networks.

Peer-to-peer conservation will not solve issues such as the ivory trade, could enable fraudulent or counterproductive projects, and may result in a bias towards flagship species. Yet it can still make an important contribution.


Abstract: The pharmaceutical industry is in the midst of transformation as a result of confounding demands to accelerate time to market, increase patient centricity and reduce the development and validation costs for new drugs. This chapter explores how the mistrust that exists between clinical trial stakeholders can affect this transformation and identifies areas where distributed ledger technology, aka blockchain, could help. We present how pharmaceutical and other industry consortiums such as PHUSE and IEEE, as well as individual companies, are advancing the concept of blockchain from thought exercises and white papers to pilots, prototypes and beyond. In conclusion, we review our lessons learned from early stage blockchain projects, identify where blockchain can provide the most value and provide a roadmap for standard clinical trial use.


Abstract: There are several areas of healthcare and well-being that could be enhanced using blockchain technologies. These include device tracking, clinical trials, pharmaceutical tracing, and health insurance. Within device tracking, hospitals can trace their asset within a blockchain infrastructure, including through the complete lifecycle of a device. The information gathered can then be used to improve patient safety and provide after-market analysis to improve efficiency savings. This paper outlines recent work within the areas of pharmaceutical traceability, data sharing, clinical trials, and device tracking.


Abstract: Dear Editor, We recently read with great interest a paper published in your journal entitled “Big data and targeted machine learning in action to assist medical decision in the ICU” by Pirracchio et al. It is an extremely precise analysis of the most recent developments in the fields of big data, technology, and statistics. These innovations can lead to increasingly tailored health treatment; real-time processing of data might also allow their application in time-dependent medical specialisations, such as in the case of perioperative medicine and intensive care.
next, traceable back to what’s called the Genesis block, a.k.a. the first block in the chain ever created. Each link in the chain verifies the network are confident of their data’s authenticity within the encrypted chains. The shared ledger structure makes blockchain ideal for storing permanent records. Because of this, authorized members of a public key encryption to protect information. Once entries are created on the chain, they are immutable, today, public blockchain technology (i.e. Bitcoin) is a secure P2P (peer-to-peer) ledger system that uses management for healthcare records, making it ideal for a new interoperability standard. As it stands, Blockchain protocols in clinical trials: transparency and traceability of consent. F1000Res. 2018;6:66. Epub 2018 Feb 1.

Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676196/

Abstract: Clinical trial consent for protocols and their revisions should be transparent for patients and traceable for stakeholders. Our goal is to implement a process allowing for collection of patients’ informed consent, which is bound to protocol revisions, storing and tracking the consent in a secure, un falsifiable and publicly verifiable way, and enabling the sharing of this information in real time. For that, we build a consent workflow using a trending technology called Blockchain. This is a distributed technology that brings a built-in layer of transparency and traceability. From a more general and prospective point of view, we believe Blockchain technology brings a paradigmatical shift to the entire clinical research field. We designed a Proof-of-Concept protocol consisting of time-stamping each step of the patient’s consent collection using Blockchain, thus archiving and historicising the consent through cryptographic validation in a securely un falsifiable and transparent way. For each protocol revision, consent was sought again. We obtained a single document, in an open format, that accounted for the whole consent collection process: a time-stamped consent status regarding each version of the protocol. This document cannot be corrupted and can be checked on any dedicated public website. It should be considered a robust proof of data. However, in a live clinical trial, the authentication system should be strengthened to remove the need for third parties, here trial stakeholders, and give participative control to the peer users. In the future, the complex data flow of a clinical trial could be tracked by using Blockchain, which core functionality, named Smart Contract, could help prevent clinical trial events not occurring in the correct chronological order, for example including patients before they consented or analysing case report form data before freezing the database. Globally, Blockchain could help with reliability, security, transparency and could be a consistent step toward reproducibility.


Reference from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5517794/

Abstract: Reproducibility, data sharing, personal data privacy concerns and patient enrolment in clinical trials are huge medical challenges for contemporary clinical research. A new technology, Blockchain, may be a key to addressing these challenges and should draw the attention of the whole clinical research community. Blockchain brings the Internet to its definitive decentralisation goal. The core principle of Blockchain is that any service relying on trusted third parties can be built in a transparent, decentralised, secure “trustless” manner at the top of the Blockchain (in fact, there is trust, but it is hardcoded in the Blockchain protocol via a complex cryptographic algorithm). Therefore, users have a high degree of control over and autonomy and trust of the data and its integrity. Blockchain allows for reaching a substantial level of historicity and inviolability of data for the whole document flow in a clinical trial. Hence, it ensures traceability, prevents a posteriori reconstruction and allows for securely automating the clinical trial through what are called Smart Contracts. At the same time, the technology ensures fine-grained control of the data, its security and its shareable parameters, for a single patient or group of patients or clinical trial stakeholders. In this commentary article, we explore the core functionalities of Blockchain applied to clinical trials and we illustrate concretely its general principle in the context of consent to a trial protocol. Trying to figure out the potential impact of Blockchain implementations in the setting of clinical trials will shed new light on how modern clinical trial methods could evolve and benefit from Blockchain technologies in order to tackle the aforementioned challenges.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676196/

Abstract: Data stored in a blockchain is immutable and available for access by separate parties. The excellent potential residing in this technology includes security, verification, and expanded data management for healthcare records, making it ideal for a new interoperability standard. As it stands today, public blockchain technology (i.e. Bitcoin) is a secure P2P (peer-to-peer) ledger system that uses public key encryption to protect information. Once entries are created on the chain, they are immutable, making blockchain ideal for storing permanent records. Because of this, authorized members of a network are confident of their data’s authenticity within the encrypted chains. The shared ledger structure provides an immutable audit trail for every transaction. In healthcare, organizations can create authenticated records and entries without needing a central authority. Each link in the chain verifies the next, traceable back to what’s called the Genesis block, a.k.a. the first block in the chain ever created.


Reference Type: Journal Article

Reference Type: Journal Article

Abstract: Telemedicine and blockchain technology share a core philosophy of empowering the individual. Blockchain solutions that focus on empowering patients and enhancing the workflows for the providers who treat them continue to make big headlines, as does enterprise investment and adoption of telehealth. Both models focus on direct-to-consumer health services, with a personalized care experience designed from the ground up to save time and money for everyone involved. The typical binding factor between the telehealth and HIT (health information technology) blockchain adoption is a patient centric, value-based care model. Therefore, it is as no coincidence that value-based care is at the center of the fastest growing (and operational) part of HIT blockchain adoption. For this reason, telehealth can demonstrate adoption synergies than most other lines of business in healthcare cannot.


Reference Type: Journal Article

Abstract: [FIRST FEW PARAGRAPHS] Two startup organisations that are committed to recycling expensive cancer drugs for re-use have been chosen by the US Food and Drug Administration (FDA) to form part of a consortium for a drug supply chain pilot project.

Following the enactment of the Drug Quality and Security Act in 2013, the FDA announced plans to launch a pilot programme intending to develop technologies for identifying and tracing prescription drugs, to enhance the safety and security of the drug supply chain.

RemediChain and Good Shepherd Pharmacy (both in Memphis, TN, USA) take unused cancer drugs and give them to patients who otherwise cannot afford them. The unused drugs are donated by cancer clinics and individuals no longer in need of them and are given to suitable patients in need across the USA.


Reference Type: Journal Article

Abstract: Data sharing, information exchange, knowledge acquisition and health intelligence are the basis of an efficient and effective evidence-based decision-making tool. A decentralized blockchain architecture is a flexible solution that can be adapted to institutional and managerial culture of organizations and services. Blockchain can play a fundamental role in enabling data sharing within a network and, to achieve that, this work defines the high-level resources necessary to apply this technology to Tuberculosis related issues. Thus, relying in open-source tools and in a collaborative development approach, we present a proposal of a blockchain based network, the TB Network, to underpin an initiative of sharing of Tuberculosis scientific, operational and epidemiologic data between several stakeholders across Brazilian cities.

Reference Type: Journal Article

Available from: https://repository.belmont.edu/lawreview/vol5/iss1/10/

Abstract: Part I highlights the inadequacies and inefficiencies of our Medicare payment system, focusing on the initiatives currently in place and the susceptibilities that persist. Part II offers a broad overview of the development, importance, features, and collateral technologies surrounding blockchain. Part III posits that Congress and HHS, through its various subsidiary agencies, should work in tandem with private stakeholders to create and/or implement a blockchain-based infrastructure to facilitate federal healthcare payments and support future growth of quality-based initiatives. This Note concludes with a recommendation for future agency research focusing on the viability and cost efficiency of a blockchain solution.


Reference Type: Electronic Article

Abstract: This paper expounds the latest main regulatory projects and industry-wide consultations in the United States (US), in the European Union (EU) and in the main economic countries where distributed ledgers (thereafter, “Blockchain”) regulations have been discussed, proposed and/or adopted.

In just a few years, the Blockchain has become a major topic for public decision-makers worldwide. As this disruptive and decentralized technology has emerged as a key business issue for start-ups and market participants, the central banks and financial regulators have changed, most notably in the US and in the EU, from an initial strong hostility to a more cautious and market-friendly position.

The paper extensively covers and compares the current regulatory trends in selected relevant countries on the various applications enabled or issues raised by the Blockchain technology (Bitcoin/virtual currencies/crypto-tokens, smart contracts, decentralized autonomous organization (“DAO”), initial coin offerings (“ICO”…)).

Three main regulatory items should be distinguished and will be analyzed separately thereafter:
(I) the virtual currencies regulation,
(II) the ICO (and crypto tokens) regulation, and
(III) the legal validity of Blockchain technology and smart contracts.


Reference Type: Electronic Book

Abstract: Blockchains are a remarkably transparent and decentralised way of recording lists of transactions. Their best-known use is for digital currencies such as Bitcoin, which announced blockchain technology to the world with a headline-grabbing 1000% increase in value in the course of a single month in 2013. This bubble quickly burst, but steady growth since 2015 means Bitcoins are currently valued higher than ever before.

There are many different ways of using blockchains to create new currencies. Hundreds of such currencies have been created with different features and aims. The way blockchain-based currency transactions create fast, cheap and secure public records means that they also can be used for many non-financial tasks, such as casting votes in elections or proving that a document existed at a specific time. Blockchains are particularly well suited to situations where it is necessary to know ownership histories. For example, they could help manage supply chains better, offer certainty that diamonds are ethically sourced, that clothes are not made in sweatshops and that champagne comes from Champagne. They could help finally resolve the problem of music and video piracy, while enabling digital media to be legitimately bought, sold, inherited and given away second-hand like books, vinyl and video tapes. They also present opportunities in all kinds of public services such as health and welfare payments and, at the frontier of blockchain development, are self-executing contracts paving the way for companies that run themselves without human intervention.

Blockchains shift some control over daily interactions with technology away from central elites, redistributing it among users. In doing so, they make systems more transparent and, perhaps, more democratic. That said, this will not probably not result in a revolution. Indeed, the governments and industry giants investing heavily in blockchain research and development are not trying to make
use the Byzantine agreement to remove unreliable users. Then, matrix factorization is employed to
matrix factorization (BMF). We develop a user verification approach based on homomorphic hash, and
etc., we propose a personalized QoS prediction method for web services that we call blockchain-based
blockchain with distributed ledger technology, distributed consensus mechanisms, encryption algorithms,
values submitted by unreliable users, leading to inaccurate predictions. To address this issue, inspired by
have been investigated in recent years. However, these approaches do not fully address untrustworthy QoS
high-quality service-oriented systems. To obtain accurate prediction results, many approaches have
been studied to address these problems, such as the use of homomorphic hash and distributed consensus
mechanisms. However, these approaches do not fully address untrustworthy QoS values submitted
by unreliable users, leading to inaccurate predictions. To address this issue, inspired by blockchain
distributed ledger technology, we propose a personalized QoS prediction method for web services that
we call blockchain-based matrix factorization (BMF). We develop a user verification approach based on
homomorphic hash, and use the Byzantine agreement to remove unreliable users. Then, matrix factorization is employed to

This report provides an accessible entry point for those in the European Parliament and beyond who are
interested in learning more about blockchain development and its potential impacts. In doing so, the aim
is to stimulate reflection and discussion of this complicated, controversial and fast-moving technology.
The report is non-sequential, so readers are invited to choose the sections that interest them and read
them in any order. The section immediately below presents an introduction to how blockchain technology
works. The subsequent eight sections each present two-page briefings about how it could be deployed in
various application areas, its potential impacts, and its implications for European policy. Finally, a
concluding section presents some overall remarks and potential responses to blockchain development.

Abstract: Personalized quality of service (QoS) prediction plays an important role in helping users build
accurate QoS predictions for web services. However, untrustworthy QoS values submitted by unreliable users
lead to inaccurate predictions. To address this issue, we propose a personalized QoS prediction method for web
services that we call blockchain-based matrix factorization (BMF). We develop a user verification approach based on
distributed ledger technology, distributed consensus mechanisms, encryption algorithms, etc., and use
the Byzantine agreement to remove unreliable users. Then, matrix factorization is employed to
dermine the QoS values of web services.

Cai W, Du X, Xu J. A personalized QoS prediction method for web services via blockchain-based matrix
Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/12/2749

Abstract: The on-demand digital healthcare ecosystem is on the near horizon. It has the potential to
extract a wealth of information from “big data” collected at the population level, to enhance preventive
and precision medicine at the patient level. This may improve efficiency and quality while decreasing cost
of healthcare delivered by professionals. However, there are still security and privacy issues that need to
be addressed before algorithms, data, and models can be mobilized safely at scale. In this paper we
discuss how blockchain technologies can play a key role in advancing electronic health, by
ensuring authenticity and integrity of data generated by wearable and embedded devices. We
demonstrate how the Masked Authenticated Messaging extension module of the IOTA protocol can be
used to securely share, store, and retrieve encrypted activity data using a tamper-proof distributed ledger.

Burchett C, Decker C, Wattenhofer R. Scalable funding of Bitcoin micropayment channel networks. R
Reference Type: Journal Article

Abstract: The Bitcoin network has scalability problems. To increase its transaction rate and speed,
micropayment channel networks have been proposed; however, these require to lock funds into specific
channels. Moreover, the available space in the blockchain does not allow scaling to a worldwide payment
system. We propose a new layer that sits in between the blockchain and the payment channels. The new
layer addresses the scalability problem by enabling trustless off-blockchain channel funding. It consists of
shared accounts of groups of nodes that flexibly create one-to-one channels for the payment network.
The new system allows rapid changes of the allocation of funds to channels and reduces the cost of
opening new channels. Instead of one blockchain transaction per channel, each user only needs one
transaction to enter a group of nodes-within the group the user can create arbitrarily many channels. For
a group of 20 users with 100 intra-group channels, the cost of the blockchain transactions is reduced by
90% compared to 100 regular micropayment channels opened on the blockchain. This can be increased
further to 96% if Bitcoin introduces Schnorr signatures with signature aggregation.

Cai W, Du X, Xu J. A personalized QoS prediction method for web services via blockchain-based matrix
Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/12/2749

Abstract: Personalized quality of service (QoS) prediction plays an important role in helping users build
high-quality service-oriented systems. To obtain accurate prediction results, many approaches have
been investigated in recent years. However, these approaches do not fully address untrustworthy QoS
values submitted by unreliable users, leading to inaccurate predictions. To address this issue, inspired by
blockchain with distributed ledger technology, distributed consensus mechanisms, encryption algorithms,
etc., we propose a personalized QoS prediction method for web services that we call blockchain-based
matrix factorization (BMF). We develop a user verification approach based on homomorphic hash, and
use the Byzantine agreement to remove unreliable users. Then, matrix factorization is employed to
improve the accuracy of predictions and we evaluate the proposed BMF on a real-world web services dataset. Experimental results show that the proposed method significantly outperforms existing approaches, making it much more effective than traditional techniques.


Reference Type: Journal Article

Abstract: The reputation system has been designed as an effective mechanism to reduce risks associated with online shopping for customers. However, it is vulnerable to rating fraud. Some raters may inject unfairly high or low ratings to the system so as to promote their own products or demote their competitors. Method: This study explores the rating fraud by differentiating the subjective fraud from objective fraud. Then it discusses the effectiveness of blockchain technology in objective fraud and its limitation in subjective fraud, especially the rating fraud. Lastly, it systematically analyzes the robustness of blockchain-based reputation systems in each type of rating fraud. Results: The detection of fraudulent raters is not easy since they can behave strategically to camouflage themselves. We explore the potential strengths and limitations of blockchain-based reputation systems under two attack goals: ballot-stuffing and bad-mouthing, and various attack models including constant attack, camouflage attack, whitewashing attack and sybil attack. Blockchain-based reputation systems are more robust against bad-mouthing than ballot-stuffing fraud. Conclusions: Blockchain technology provides new opportunities for redesigning the reputation system. Blockchain systems are very effective in preventing objective information fraud, such as loan application fraud, where fraudulent information is fact-based. However, their effectiveness is limited in subjective information fraud, such as rating fraud, where the ground-truth is not easily validated.


Reference Type: Journal Article

Abstract: The wide deployment of cloud-assisted electronic health (eHealth) systems has already shown great benefits in managing electronic health records (EHRs) for both medical institutions and patients. However, it also causes critical security concerns. Since once a medical institution generates and outsources the patients' EHRs to cloud servers, patients would not physically own their EHRs but the medical institution can access the EHRs as needed for diagnosing, it makes the EHRs integrity protection a formidable task, especially in the case that a medical malpractice occurs, where the medical institution may collude with the cloud server to tamper with the outsourced EHRs to hide the medical malpractice. Traditional cryptographic primitives for the purpose of data integrity protection cannot be directly adopted because they cannot ensure the security in the case of collusion between the cloud server and medical institution. In this paper, a secure cloud-assisted eHealth system is proposed to protect outsourced EHRs from illegal modification by using the blockchain technology (blockchain-based currencies, e.g., Ethereum). The key idea is that the EHRs only can be outsourced by authenticated participants and each operation on outsourcing EHRs is integrated into the public blockchain as a transaction. Since the blockchain-based currencies provide a tamper-proofing way to conduct transactions without a central authority, the EHRs cannot be modified after the corresponding transaction is recorded into the blockchain. Therefore, given outsourced EHRs, any participant can check their integrity by checking the corresponding transaction. Security analysis and performance evaluation demonstrate that the proposed system can provide a strong security guarantee with a high efficiency.


Reference Type: Conference Proceedings

Abstract: Enabled by mobile and wearable technology, personal health data delivers immense and increasing value for healthcare, benefiting both care providers and medical research. The secure and convenient sharing of personal health data is crucial to the improvement of the interaction and collaboration of the healthcare industry. Faced with the potential privacy issues and vulnerabilities existing in current personal health data storage and sharing systems, as well as the concept of self-
sovereign data ownership, we propose an innovative user-centric health data sharing solution by utilizing a decentralized and permissioned blockchain to protect privacy using channel formation scheme and enhance the identity management using the membership service supported by the blockchain. A mobile application is deployed to collect health data from personal wearable devices, manual input, and medical devices, and synchronize data to the cloud for data sharing with healthcare providers and health insurance companies. To preserve the integrity of health data, within each record, a proof of integrity and validation is permanently retrievable from cloud database and is anchored to the blockchain network. Moreover, for scalable and performance considerations, we adopt a tree-based data processing and batching method to handle large data sets of personal health data collected and uploaded by the mobile platform.


Reference Type: Electronic Article

Abstract: Technological advancements have proven to be indispensable for improving patient care, yet they continue to present a host of problems. One of the most pressing concerns is how to improve quality of care while controlling costs. Beyond clinical care, one plausible solution is to share patient information freely and efficiently. Hospitals and clinics may share data internally, but external information sharing remains an issue. Despite the digitization of medical records, there remains a lack of adequate computing infrastructure or unwillingness to share data among providers. Care quality often suffers as a result. Implementing a type of peer-to-peer distributed digital technology, known as a blockchain, to record and transmit transactional data could be a solution to these concerns. Originally, blockchain was developed to record cryptocurrency transactions. However, as blockchain technologies have matured and adopted across dissimilar industries, the feasibility of possible applications of blockchain technology in healthcare is getting more attention. This article explores possible opportunities of adoption of blockchain technology to improve patient data security, privacy, and care while outlining the challenges that practitioners may encounter.


Reference Type: Conference Paper


Abstract: Current supply chain is a linear economy model that directly or indirectly fulfills supply needs. But this model has some disadvantages, such as the relationships between the members of the supply chain or the lack of information for the consumer about the origin of the products. In this paper we propose a new model of supply chain via blockchain. This new model enables the concept of circular economy and eliminates many of the disadvantages of the current supply chain. In order to coordinate all the transactions that take place in the supply chain a multi-agent system is created for this paper.


Reference Type: Journal Article


Abstract: This work provides a systematic literature review of blockchain-based applications across multiple domains. The aim is to investigate the current state of blockchain technology and its applications and to highlight how specific characteristics of this disruptive technology can revolutionise “business-as-usual” practices. To this end, the theoretical underpinnings of numerous research papers published in high ranked scientific journals during the last decade, along with several reports from grey literature as a means of streamlining our assessment and capturing the continuously expanding blockchain domain, are included in this review. Based on a structured, systematic review and thematic content analysis of the discovered literature, we present a comprehensive classification of blockchain-enabled applications across diverse sectors such as supply chain, business, healthcare, IoT, privacy, and data management, and we establish key themes, trends and emerging areas for research. We also point to the shortcomings identified in the relevant literature, particularly limitations the blockchain technology presents and how these limitations spawn across different sectors and industries. Building on these findings, we identify various research gaps and future exploratory directions that are anticipated to be of significant value both for academics and practitioners.

Reference Type: Report

Abstract: The term “smart contract” has entered the public consciousness following the rise to mainstream awareness of virtual currencies and blockchain technology. However, this term is frequently misunderstood and used incorrectly, creating unnecessary and potentially harmful confusion surrounding the application of U.S. law to smart contracts, and prompting states to attempt to clarify their position through legislation. The purpose of this document is to provide a plain language explanation of smart contracts and how they fit within existing law, demonstrating that further state legislation is unnecessary to support the growth of this industry.


Reference Type: Report

Abstract: [FIRST TWO PARAGRAPHS] Smart contracts have come a long way in a short time. They will help to realize the many possibilities of distributed ledger technology (DLT). Certainty of outcome, automation of performance, and efficiencies in the streamlining of processes are reasons enough for smart contracts to be fundamental to the uptake of DLT. Their potential is now being actively considered and developed in sectors as diverse as Financial Services, Life Sciences and Healthcare, Technology and Telecoms, Transport, Energy, Infrastructure, Mining and Commodities. In Financial Services, for example, no one will be surprised to see smart contracts being used in areas such as securities clearing and settlement, collateral management, derivatives contracts, securities asset servicing, international money transfers, and perhaps even syndicated lending.

For many sectors it is the ability of smart contracts to be transformative in relation to existing business processes that is compelling. For others it is the potential of smart contracts to reduce execution risk (by making transfer of the relevant asset or instrument in question near to inevitable by virtue of automatic performance). As Chapter 3 of this white paper discusses, that may only achieve factual (that is, de facto) transfer. It may still be necessary, therefore, to apply established legal concepts and principles in order to determine whether transfer has been achieved at law (de jure).


Reference Type: Journal Article
Available from: https://journals.lww.com/ajpmr/Citation/2019/07000/The_Application_of_Blockchain_Technology_in_Stroke.17.aspx Subscription required to view.

Abstract: [FIRST PARAGRAPH] Blockchain has turned the conventional wisdom about data storage and management on its head. Instead of keeping transaction data in a centralized server, blockchain distributes the data to all users in the network and jointly manages them via a peer-to-peer network, thereby ensuring the safety, reliability, integrity, and transparency of data. Whereas all data are stored in a central server and only the central authority owns the data in a traditional centralized network, a decentralized network powered by blockchain distributes ledgers that contain all the data across all users' personal computers.1 Blockchain is hack-proof: hackers may attempt to alter or manipulate information contained in a blockchain network, but their attempts are futile when information is scattered across multiple individuals at once. Therefore, information is highly reliable and easy to track because it cannot be deleted or lost, and all transactions are transparent to everyone. Blockchain streamlines transaction processes and reduces time, saves costs for contract arbitration, and creates a new ecosystem of open-source service. The technology is expected to have huge social and economic ripple effects. Use of blockchain technology was originally confined to the financial sector but has now forayed into various nonfinancial industries such as logistics, distribution, energy, public service, and, in particular, health care, arousing much interest among healthcare professionals on its potential.2 Currently, medical data are stored in electronic medical record systems and are owned by hospitals, which hampers information-sharing between hospitals. Patients who visit other hospitals often have to retake the same medical tests and doctors often fail fully understand the patient's condition. In contrast, medical data that are distributed across a blockchain network are owned by patients rather than medical institutions. Blockchain technology, once implemented in medical data management, will give control over medical data back to patients themselves, allowing them to easily submit their digitized medical records directly to the clinic of their choice. This not only eliminates the need for repeated examinations
but also enables medical institutions to identify their patients quickly and easily using the information provided by the patients themselves. Medical practitioners can just focus on planning further examinations and the course of treatment.


Reference Type: Journal Article
Available from: https://www.mdpi.com/2504-2289/3/2/25
Abstract: Blockchain technology has an enormous scope to revamp the healthcare system in many ways as it improves the quality of healthcare by data sharing among all the participants, selective privacy and ensuring data safety. This paper explores the basics of blockchain, its applications, quality of experience and advantages in disease surveillance over the other widely used real-time and machine learning techniques. The other real-time surveillance systems lack scalability, security, interoperability, thus making blockchain as a choice for surveillance. Blockchain offers the capability of enhancing global health security and also can ensure the anonymity of patient data thereby aiding in healthcare research. The recent epidemics of re-emerging infections such as Ebola and Zika have raised many concerns regarding health security which resulted in strengthening the surveillance systems. We also discuss how blockchains can help in identifying the threats early and reporting them to health authorities for taking early preventive measures. Since the Global Health Security Agenda addresses global public health threats (both infectious and NCDs); strengthen the workforce and the systems; detect and respond rapidly and effectively to the disease threats; and elevate global health security as a priority. The blockchain has enormous potential to disrupt many current practices in traditional disease surveillance and health care research.


Reference Type: Journal Article
Abstract: We polled the Editorial Board of Genome Biology to ask where they see genomics going in the next few years. Here are some of their responses.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6711478/
Abstract: With the rise of technology, modern healthcare and biomedical sciences have largely shifted their content to cyberspace. This raises the challenges of accessibility and security of such data, and the solution may lie in a recent technology called blockchain. Blockchain is a public transaction ledger that offers two unique capabilities, immutability and decentralization of data, that make it stand out as an unparalleled technology in the spheres of healthcare and biomedicine.


Reference Type: Journal Article
Abstract: Data leakage in electronic health records (EHRs) could result in the compromise of patient privacy (e.g. medical conditions). Generally most data in EHRs remain unchanged once they are uploaded to the system; thus, blockchain can be potentially used to facilitate the sharing of such data. Different participating medical organizations and individuals (e.g. medical practitioners, hospitals, medical labs and insurance companies) can then access EHRs stored on the blockchain with a higher level of confidence. In this paper, a blockchain based searchable encryption scheme for EHRs is proposed. The index for EHRs is constructed through complex logic expressions and stored in the blockchain, so that a data user can utilize the expressions to search the index. As only the index is migrated to the blockchain to facilitate propagation, the data owners have full control over who can see their EHRs data. The use of
blockchain technology ensures the integrity, anti-tampering, and traceability of EHRs' index. Finally, the performance of the proposed scheme is evaluated from two aspects, namely in terms of the overhead for extracting the document IDs from EHRs and the overhead associated with conducting transactions on smart contract in Ethereum.


Reference Type: Journal Article

Abstract: Accurate and complete medical data are one valuable asset for patients. Privacy protection and the secure storage of medical data are crucial issues during medical services. Secure storage and making full use of personal medical records has always been a concern for the general population. The emergence of blockchain technology brings a new idea to solve this problem. As a hash chain with the characteristics of decentralization, verifiability and immutability, blockchain technology can be used to securely store personal medical data. In this paper, we design a storage scheme to manage personal medical data based on blockchain and cloud storage. Furthermore, a service framework for sharing medical records is described. In addition, the characteristics of the medical blockchain are presented and analyzed through a comparison with traditional systems. The proposed storage and sharing scheme does not depend on any third-party and no single party has absolute power to affect the processing.


Reference Type: Journal Article

Abstract: While the healthcare industry is undergoing disruptive digital transformation, data breaches involving health information are not usually the result of integration of new technologies. Based on published industry reports, fundamental security safeguards are still considered to be lacking with many documented data breaches occurring as the result of device and equipment theft, human error, hacking, ransomware attacks and misuse. Health information is considered to be one of the most attractive targets for cybercriminals due to its inherent sensitivity, but digital investigations of incidents involving health information are often constrained by the lack of the necessary infrastructure forensic readiness. Following the analysis of healthcare data breach causes and threats, we describe the associated digital forensic readiness challenges in the context of the most significant incident causes. With specific focus on privilege misuse, we present a conceptual architecture for forensic audit logging to assist with capture of the relevant digital artefacts in support of possible future digital investigations.


Reference Type: Electronic Article
Abstract: Blockchain technology has become almost as famous for incidents involving security breaches as for its innovative potential. We shed light on the prevalence and nature of these incidents through a database structured using the STIX format. Apart from OPSEC-related incidents, we find that the nature of many incidents is specific to blockchain technology. Two categories stand out: smart contracts, and techno-economic protocol incentives. For smart contracts, we propose to use recent advances in software testing to find flaws before deployment. For protocols, we propose the PRESTO framework that allows us to compare different protocols within a five-dimensional framework.


Reference Type: Journal Article

Abstract: Growing understanding of the influence of social determinants of health (SDH) on healthcare costs and outcomes for low income populations is leading State Medicaid agencies to consider incorporating SDH into their program design. This paper explores states’ current approaches to SDH.

Reference Type: Journal Article

Abstract: The cost of conducting multi-site clinical trials has significantly increased over time, with site monitoring, data management, and amendments being key drivers. Clinical trial data management approaches typically rely on a central database, and require manual efforts to encode and maintain data capture and reporting requirements. To reduce the administrative burden, time, and effort of ensuring data integrity and privacy in multi-site trials, we propose a novel data management framework based on permissioned blockchain technology. We demonstrate how our framework, which uses smart contracts and private channels, enables confidential data communication, protocol enforcement, and an automated audit trail. We compare this framework with the traditional data management approach and evaluate its effectiveness in satisfying the major requirements of multi-site clinical trials. We show that our framework ensures enforcement of IRB-related regulatory requirements across multiple sites and stakeholders.


Reference Type: Journal Article

Abstract: Recent changes to the Common Rule, which govern Institutional Review Boards (IRB), require implementing new policies to strengthen research protocols involving human subjects. A major challenge in implementing such policies is an inability to automatically and consistently meet these ethical rules while securing sensitive information collected during the study. In this paper, we propose a novel framework, based on blockchain technology, to enforce IRB regulations on data collection. We demonstrate how to design smart contracts and a ledger to meet the requirements of an IRB protocol, including subject recruitment, informed consent management, secondary data sharing, monitoring risks, and generating automated assessments for continuous review. Furthermore, we show how we can employ the immutable transaction log in the blockchain to embed security in research activities by detecting malicious activities and robustly tracking subject involvement. We evaluate our approach by assessing its ability to enforce IRB guidelines in different types of human subjects studies, including a genomic study, a drug trial, and a wearable sensor monitoring study.


Reference Type: Journal Article

Abstract: Introduction: Patients with diabetes often generate large amounts of data specifically related to the disease and to their general health. Cross-institutional sharing of patient health care data is complex, and as a consequence, data are not always available to the health care provider treating the patient. Accommodating this challenge could lead to better clinical effectiveness and improve clinical research. This work aims to present an approach for a blockchain-based platform for sharing health care data. The approach considers privacy concerns, data sharing, and patients as the center for governing their own data.

Methods: The concept of this blockchain-based platform consists of using the NEM multi-signature blockchain contracts for access control of data management and the sharing and encryption of data to allow privacy and control of health care data. The architecture is built around cryptography, tokens, and multi-signature contracts. The multi-signature contract enables several entities to administrate the activity of an account and control the assets of one account. Multi-signature generates a contract that assigns the rights and powers of a certain account to other accounts; this contract can be edited to allow or remove entities.

Discussion: Using blockchain could lead to improvements in diabetes data management. In the coming years, this technology should be implemented in existing small-scale diabetes health care system to explore its real-world benefits and challenges.

Conclusion: This new approach could potentially lead to more efficient sharing of data between institutions and utilization of new types of data and research possibilities.

Reference Type: Journal Article

Abstract: Big Data are radically changing biomedical research. The unprecedented advances in automated collection of large-scale molecular and clinical data pose major challenges to data analysis and interpretation, calling for the development of new computational approaches. The creation of powerful systems for the effective use of biomedical Big Data in Personalized Medicine (a.k.a. Precision Medicine) will require significant scientific and technical developments, including infrastructure, engineering, project and financial management. We review here how the evolution of data-driven methods offers the possibility to address many of these problems, guiding the formulation of hypotheses on systems functioning and the generation of mechanistic models, and facilitating the design of clinical procedures in Personalized Medicine.

Reference Type: Electronic Article
Abstract: This article describes how blockchain technologies can be used in the context of Public Health Surveillance through decentralized sharing of genomic data. A brief analysis of why blockchain technologies are needed in public health is presented together with a distinction between public and private blockchains. Finally, a proposal for a network of blockchains, using the Cosmos framework, together with decentralized storage systems like IPFS and BigchainDB, is included to address the issues of interoperability in the health sector.

Reference Type: Electronic Article
Abstract: Background: Effective supply chain management is a challenge in every sector, but in healthcare there is added complexity and risk as a compromised supply chain in healthcare can directly impact patient safety and health outcomes. One potential solution for improving security, integrity, data provenance, and functionality of the health supply chain is blockchain technology.

Objectives: Provide an overview of the opportunities and challenges associated with blockchain adoption and deployment for the health supply chain, with a focus on the pharmaceutical supply, medical device and supplies, Internet of Healthy Things (IoHT), and public health sectors.

Methods: A narrative review was conducted of the academic literature, grey literature, and industry publications, in addition to identifying and characterizing select stakeholders engaged in exploring blockchain solutions for the health supply chain.

Results: Critical challenges in protecting the integrity of the health supply chain appear well suited for adoption of blockchain technology. Use cases are emerging, including using blockchain to combat counterfeit medicines, securing medical devices, optimizing functionality of IoHT, and improving the public health supply chain. Despite these clear opportunities, most blockchain initiatives remain in proof-of-concept or pilot phase.

Conclusion: Blockchain technology has the unrealized promise to help improve the health supply chain, but further study, evaluation and alignment with policy mechanisms is needed.

Reference Type: Journal Article
Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0164603
Abstract: In January 3, 2009, Satoshi Nakamoto gave rise to the "Bitcoin Blockchain", creating the first block of the chain hashing on his computer's central processing unit (CPU). Since then, the hash calculations to mine Bitcoin have been getting more and more complex, and consequently the mining hardware evolved to adapt to this increasing difficulty. Three generations of mining hardware have followed the CPU's generation. They are GPU's, FPGA's and ASIC's generations. This work presents an agent-based artificial market model of the Bitcoin mining process and of the Bitcoin transactions. The goal of this work is to model the economy of the mining process, starting from GPU's generation, the first
with economic significance. The model reproduces some "stylized facts" found in real-time price series and some core aspects of the mining business. In particular, the computational experiments performed can reproduce the unit root property, the fat tail phenomenon and the volatility clustering of Bitcoin price series. In addition, under proper assumptions, they can reproduce the generation of Bitcoins, the hashing capability, the power consumption, and the mining hardware and electrical energy expenditures of the Bitcoin network.


Reference Type: Electronic Article

Abstract: Disease surveillance, especially for infectious diseases, is a complex and inefficient process. Here we propose an optimized, blockchain-based monitoring and reporting system which can achieve all the desired features of an ideal surveillance system while maintaining costs down and being transparent and robust. We describe the technical specifications of such a system and discuss possibilities for its implementation. Together with a token based incentive system, it is possible to rewards data quality as well as build a marketplace for data analysis which will help finance the surveillance system. Finally, the impact of the adoption of distributed ledger technology for disease surveillance is discussed.


Reference Type: Journal Article


Abstract: We present a decentralised solution for managing scientific communication, based on distributed ledger technologies, also called blockchains. The proposed system aims to solve incentive problems displayed by traditional systems in scientific communication and publication. A minimal working model is presented, defining roles, processes, and expected results from the novel system. The proposed solution is viable, given the current status of blockchain technology, and should lead to a rethinking of current practices and their consequences for scientific communication.


Reference Type: Electronic Article

Abstract: Over the past decade, there have been many innovations in new payment and care delivery models and technology, from telemedicine to artificial intelligence (AI) to blockchain. These innovations, however, must be used in tandem to drive real change. We review each of these innovations and propose a model for how they can be combined to be greater than the sum of their parts. In doing so, we can create a global, decentralized health system that truly puts patient care at the center, while supporting and further enabling the clinicians who make this care possible, to deliver higher quality care at a fraction of the cost.


Reference Type: Journal Article

Available from: https://www.internationaljournalofcardiology.com/article/S0167-5273(19)31652-3/fulltext
Subscription required to view.

Abstract: The connection between health literacy and health outcomes includes access and utilization of healthcare services, patient/provider interaction and self-care. Digital approaches can be designed to simplify or expand on a concept, test for understanding, and do not have a time constraint. New technologies, such as artificial intelligence and machine learning, virtual and augmented reality, and blockchain can move the role of technology beyond data collection to a more integrated system. Rather than being a passive participant, digital solutions provide the opportunity for the individual to be an active participant in their health. These solutions can be delivered in a way that builds or enhances the individual's belief that the plan will be successful and more confidence that they can stick with it, while giving the patient a greater voice and empowering them to be active participants in their care, they can develop their decision
making and shared decision making skills. The first step in our health literacy instructional model is to address the emotional state of the person. Once the emotional state has been addressed, and an engagement strategy has been deployed the final phase is the delivery of an educational solution. While a clear definition of health literacy and an instructional model are important, further research must be done to continually determine more effective ways to incorporate health technology in the process of improving health outcomes.


Reference Type: Journal Article

Abstract: Purpose: The purpose of this article is to clarify current and widespread misconceptions about the properties of blockchain technologies and to describe challenges and avenues for correct and trustworthy design and implementation of distributed ledger system (DLS) or Technology (DLT). Design/methodology/approach: The authors contrast the properties of a blockchain with desired, however emergent, properties of a DLS, which is a complex and distributed system. They point out and justify, with facts and analysis, current misconceptions about the blockchain and DLSs. They describe challenges that these systems will need to address and possible solution avenues for achieving trustworthiness. Findings: Many of the statements that have appeared on the internet, news and academic articles, such as immutable ledger and exact copies, may be misleading. These are desired emergent properties of a complex system, not assured properties. It is well-known within the distributed systems and critical software community that it is extremely hard to prove that a complex system correctly and completely implements emergent properties. Further research and development for trustworthy DLS design and implementation is needed, both practical and theoretical. Research limitations/implications: This is the first known published attempt at describing current misconceptions about blockchain technologies. Further collaborative work, discussions, potential solutions, evaluations, resulting publications and verified reference implementations are needed to ensure DLTs are safe, secure, and trustworthy. Practical implications: Interdisciplinary teams with members from academia, business and industry, and from disciplines such as business, entrepreneurship, theoretical and practical computer science, cybersecurity, finance, mathematics and statistics, must be formed. Such teams must collaborate with the objective of developing strategies and techniques for ensuring the correctness and security of future DLSs in which our society may become dependent. Originality value: The value and originality of this article is twofold: the disproving, through fact collection and systematic analysis, of current misconceptions about the properties of the blockchain and DLSs, and the discussion of challenges to achieving adequate trustworthiness along with the proposal of general avenues for possible solutions.


Reference Type: Journal Article

Abstract: A blockchain is essentially a distributed database of records, or public ledger of all transactions or digital events that have been executed and shared among participating parties. Each transaction in the public ledger is verified by consensus of a majority of the participants in the system. Once entered, information can never be erased. The blockchain contains a certain and verifiable record of every single transaction ever made. Bitcoin, the decentralized peer-to-peer digital currency, is the most popular example that uses blockchain technology. The digital currency bitcoin itself is highly controversial but the underlying blockchain technology has worked flawlessly and found wide range of applications in both financial and non-financial world.

The main hypothesis is that the blockchain establishes a system of creating a distributed consensus in the digital online world. This allows participating entities to know for certain that a digital event happened by creating an irrefutable record in a public ledger. It opens the door for developing a democratic open and scalable digital economy from a centralized one. There are tremendous opportunities in this disruptive technology, and the revolution in this space has just begun.

This white paper describes blockchain technology and some compelling specific applications in both financial and non-financial sector. We then look at the challenges ahead and business opportunities in this fundamental technology that is all set to revolutionize our digital world.

Culver K. Blockchain technologies: a whitepaper discussing how the claims process can be improved. ONC/NIST Use of Blockchain for Healthcare and Research Workshop; 2016 Sep 26-27; Gaithersburg,
Abstract: The healthcare industry suffers from an inability to clearly communicate costs in a timely and easy-to-understand format. This problem is a symptom of interoperability issues and complex agreements between providers, patients, health plans/payers and government regulators. These agreements are encoded in legal language with the intent of being defensible in court. However, the focus on legal enforceability, instead of understandability, creates problems resulting in hundreds of billions of dollars spent annually to administer an inefficient, outdated and complex process for adjudicating and paying health plan claims. The process results in errors and often leaves the patient unclear on how much they need to pay. If these agreements were instead translated into computer code (smart contracts) leveraging Blockchain technologies, the claim process would not only be interoperable, but also drive standardization, research and innovation. Transparency and trust can be injected into the process when both the logic and the data driving these decisions is stored permanently and made available to all stakeholders through a peer-to-peer distributed database like blockchain. The result will be a paradigm shift toward interoperability and transparency, enhancing the speed and accuracy of cost reporting to patients. This paper discusses how smart contracts, blockchain and other technologies can be combined into a platform that enables drastic improvements to the healthcare experience for all stakeholders.


are executed with secure transactions. We describe HCLS use cases that can leverage these facets of blockchain, including: patient consent and health data exchange, outcome-based contracts, next-generation clinical trials, supply chain traceability, and payments and claims transactions. We then describe a blockchain based architecture and platform for enabling these use cases. Finally, we outline a realization of this architecture in a case study and outline further research topics in this domain.


Reference Type: Journal Article
Available from: https://jbba.scholasticahq.com/article/4451-e-voting-on-the-blockchain

Abstract: Building a secure electronic voting system is a difficult task. The US Pentagon dropped their proposed online voting system which would have given overseas military personnel the opportunity to vote in the elections in 2005, citing the inability to ensure the legitimacy of votes as the reason. There is however a new cry in the wild to deploy a voting blockchain. The blockchain serves as a public ledger of transactions which cannot be reversed. The all-important consensus of transaction (i.e. legitimate votes) is achieved through ‘miners’ agreeing to validate new records being added. Whenever a new insertion is to be made e.g. votes, then a new transaction record is created by a voter adding details of their cast vote to the blockchain. Should it be deemed a valid transaction then the new vote is added to the end of the blockchain and remains there forever. What is neat about this solution is the fact that no centralized authority is needed to approve the votes but rather a majority consensus. Here everyone agrees on the final tally as they can count the votes themselves & because of the blockchain audit trail, anyone can verify that no votes were tampered with and no illegitimate votes were inserted. This paper discusses the application of blockchain to voting.


Reference Type: Electronic Article
Abstract: Blockchain technology has the potential to transform healthcare delivery by facilitating data sharing between providers and electronic health record (EHR) systems. However, significant roadblocks stand in the way of widespread implementation of this technology across the healthcare industry. Our blockchain-based data-sharing solution addresses two of the most critical challenges associated with using blockchain for health data sharing: protecting sensitive health information and deploying and installing blockchain software across diverse hospital environments. Since transparency is a fundamental feature of blockchain, we enabled user- and group-based secret sharing by adding purpose-built software that leverages a collection of well-established cryptographic algorithms. To streamline deployment, we built a containerized solution that guarantees portability, simplifies installation, and reduces overhead maintenance costs associated with administration. To ensure ease of implementation in a hospital system, we designed our blockchain solution using a distributed microservices architecture that allows us to encapsulate core functions of our system into isolated services that can be scaled independently based on the requirements of a particular hospital system deployment. As part of this architecture, we built core components for securely handling cryptographic secrets, interacting with blockchain nodes, facilitating large file sharing, enabling secondary-index based lookups, and integrating external business logic that governs how users interact with Smart Contracts. The innovative design of our blockchain solution, which addresses critical data security, deployment, and installation challenges, provides the healthcare community with a unique approach that has the power to connect providers while protecting sensitive data.


Reference Type: Electronic Article
Abstract: Data privacy refers to ensuring that users keep control over access to information, whereas data accessibility refers to ensuring that information access is unconstrained. Conflicts between privacy and accessibility of data are natural to occur, and healthcare is a domain in which they are particularly relevant. In the present article, we discuss how blockchain technology, and smart contracts, could help in some typical scenarios related to data access, data management and data interoperability for the specific healthcare domain. We then propose the implementation of a large-scale information architecture to access Electronic Health Records (EHRs) based on Smart Contracts as information mediators. Our main contribution is the framing of data privacy and accessibility issues in healthcare and the proposal of an integrated blockchain based architecture.

Reference Type: Journal Article


Abstract: Despite an increased focus on the security of electronic health records and an effort by large cities around the globe to pursue smart city infrastructure, the private information of patients is subject to data breaches on a regular basis. Previous efforts to combat this have resulted in data being mostly inaccessible to patients. Existing record management systems struggle with balancing data privacy and the need for patients and providers to regularly interact with data. Blockchain technology is an emerging technology that enables data sharing in a decentralized and transactional fashion. Blockchain technology can be leveraged in the healthcare domain to achieve the delicate balance between privacy and accessibility of electronic health records. In this paper, we propose a blockchain-based framework for secure, interoperable, and efficient access to medical records by patients, providers, and third parties, while preserving the privacy of patients' sensitive information. Our framework, named Ancile, utilizes smart contracts in an Ethereum-based blockchain for heightened access control and obfuscation of data, and employs advanced cryptographic techniques for further security. The goals of this paper are to analyze how Ancile would interact with the different needs of patients, providers, and third parties, and to understand how the framework could address longstanding privacy and security concerns in the healthcare industry.


Reference Type: Electronic Article

Abstract: The governance of data used for biomedical research and clinical trials is an important requirement for generating accurate results. To improve the visibility of data quality and analysis, we developed TrialChain, a blockchain-based platform that can be used to validate data integrity from large, biomedical research studies. We implemented a private blockchain using the MultiChain platform and integrated it with a data science platform deployed within a large research center. An administrative web application was built with Python to manage the platform, which was built with a microservice architecture using Docker. The TrialChain platform was integrated during data acquisition into our existing data science platform. Using NiFi, data were hashed and logged within the local blockchain infrastructure. To provide public validation, the local blockchain state was periodically synchronized to the public Ethereum network. The use of a combined private/public blockchain platform allows for both public validation of results while maintaining additional security and lower cost for blockchain transactions. Original data and modifications due to downstream analysis can be logged within TrialChain and data assets or results can be rapidly validated when needed using API calls to the platform. The TrialChain platform provides a data governance solution to audit the acquisition and analysis of biomedical research data. The platform provides cryptographic assurance of data authenticity and can also be used to document data analysis.


Reference Type: Journal Article


Abstract: Since the passage of the Sarbanes-Oxley Act, IS professionals are facing even greater challenges to meet raised expectations to provide accurate, visible, and timely information while ensuring their company’s information assets are secure. This article presents an IT governance framework for responding to these challenges.


Reference Type: Journal Article
Abstract: Exponential growth of the impact of information technology innovation is an indispensable part of today's industry. Blockchain technology has identified itself as an efficiency booster and service optimization for financial industries. Yet non-financial venues have gained little benefit from this new major horizon, Blockchain technology. It offers a secure way to exchange any kind of good, service, or transaction. Industrial growth increasingly depends on trusted partnerships; but increasing regulation, cybercrime and fraud are inhibiting expansion. Blockchain enables more agile value chains, faster product innovations, closer customer relationships, and faster integration with the Internet of Things (IoT) and cloud technology. Now with Cloud and Blockchain technologies providing high computing power and network capabilities, cognitive systems are available tools to deepen the relationship between humans and the world. Many problems that have been with our society for a long time can be solved. Cognitive systems are the tools to accomplish that ambitious goal. This study is continuing our effort on surveying the applicability of Blockchain technology innovation in non-finance (non-bitcoin). The study concluded with discussing opportunities and challenges of the application of two intra-horizons of Blockchain technology, Cognitive Computing and Healthcare.


Reference Type: Conference Proceedings

Abstract: Blockchain technology is rapidly gaining traction in healthcare industry as one of the most exciting technological developments. In particular, blockchain technology presents numerous opportunities for healthcare industry such as reduced transaction costs, increased transparency for regulatory reporting, efficient healthcare data management and healthcare records universality. In the context of smart health, blockchain may provide distinct benefits, particularly from a context-aware perspective where efficient and personalised solutions may be provided to citizens and the society in general. In this article, we portray the symbiotic relationship between blockchain and smart health. Among others, we identify and analyse three individual streams of possible synergies. In addition, we discuss several challenges for actually implementing blockchain-based applications in the healthcare industry along with several opportunities for future research directions.


Reference Type: Journal Article

Abstract: The report starts with an overview of the blockchain security system and then highlights the specific security threats and summarizes them. We review with some comments and possible research direction. This survey, we examines the security issues of blockchain model related technologies and their applications. The blockchain is considered a still growing like the internet in 1990. It has the potential to disrupt so many technology areas in the future. But as a new underdeveloped field, it is suffering many setbacks mostly resulting from the security area. Its security concerns coming not only from distributed/decentralized computing issue or Cryptography algorithm issue, from some unexpected field too. Here, in this paper, we tried to classify the security concerns for the blockchain based on our survey from recent research papers. We also tried to show which way blockchain development trends are going.


Reference Type: Electronic Article
Abstract: “Code is law” refers to the idea that, with the advent of digital technology, code has progressively established itself as the predominant way to regulate the behavior of Internet users. Yet, while computer code can enforce rules more efficiently than legal code, it also comes with a series of limitations, mostly because it is difficult to transpose the ambiguity and flexibility of legal rules into a formalized language which can be interpreted by a machine. With the advent of blockchain technology and associated smart contracts, code is assuming an even stronger role in regulating people's
interactions over the Internet, as many contractual transactions get transposed into smart contract code. In this paper, we describe the shift from the traditional notion of "code is law" (i.e. code having the effect of law) to the new conception of "law is code" (i.e. law being defined as code).


Reference Type: Journal Article

Abstract: Blockchain technology has unprotected its immense adaptability in hot off the press years as a departure from the norm of super convenience store sectors. In which sought ways in incorporating its abilities directed toward their operations. While so far most of the focus has been on the financial service industry, several projects in other service-related areas such as healthcare start showing innumerable change. Numerous starting points for Blockchain technology in the healthcare industry are the focus of this paper. With examples for a person in the street healthcare powers that be, user-oriented medical scan and abused substance counterfeiting in the pharmaceutical section, this tells aims to repeat possible influences, goals and potentials installed to this on a tear technology.


Reference Type: Journal Article

Abstract: Managing information has been troublesome for the sprawling US health care industry. Every doctor, medical office, hospital, pharmacy, therapist and insurance company needs different pieces of data to properly care for patients. Electronic health records are scattered across multiple systems which are unable to communicate with each other. Furthermore, records are not always up-to-date, and some remain in paper form in filing cabinets.

There might be a way, however, toward a health care system where patients have accurate and updated records that are secure against tampering or snooping, with data that can be shared quickly and easily with any provider who needs it: blockchain.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/14/3119

Abstract: The industrial control systems are facing an increasing number of sophisticated cyber attacks that can have very dangerous consequences on humans and their environments. In order to deal with these issues, novel technologies and approaches should be adopted. In this paper, we focus on the security of commands in industrial IoT against forged commands and misrouting of commands. To this end, we propose a security architecture that integrates the Blockchain and the Software-defined network (SDN) technologies. The proposed security architecture is composed of: (a) an intrusion detection system, namely RSL-KNN, which combines the Random Subspace Learning (RSL) and K-Nearest Neighbor (KNN) to defend against the forged commands, which target the industrial control process, and (b) a Blockchain-based Integrity Checking System (BICS), which can prevent the misrouting attack, which tampers with the OpenFlow rules of the SDN-enabled industrial IoT systems. We test the proposed security solution on an Industrial Control System Cyber attack Dataset and on an experimental platform combining software-defined networking and blockchain technologies. The evaluation results demonstrate the effectiveness and efficiency of the proposed security solution.


Reference Type: Report
Abstract: RAND Europe was commissioned by the British Standards Institution (BSI) in January 2017 to carry out a rapid scoping study to examine the potential role of standards in supporting Distributed Ledger Technologies (DLT)/Blockchain. The current document, intended for dissemination to interested parties, aims to serve as an overview of the study, which was conducted over a 6-week period. A more comprehensive report, with more detailed results of the analysis and findings and complete descriptions of the methods, was also submitted to the BSI.

DLT/Blockchain refers to a type of database which is spread over multiple locations (i.e. a distributed database) and which can be used like a digital ledger to record and manage transactions. Although the technology is at a relatively early stage of adoption and significant challenges remain, it is becoming apparent that DLT/Blockchain holds the potential for major opportunities across several sectors. Furthermore, standardization efforts related to DLT/Blockchain have recently gathered momentum with the setting up of the International Organization for Standardization (shortened to ISO) technical committee on Blockchain and electronic DLT.

In this report, we present an overview of the current landscape of DLT/Blockchain developments and closely examine the issues that are central to the development of DLT/Blockchain. We articulate a set of areas for further consideration by DLT/Blockchain stakeholders regarding the potential role of standardization. Rather than providing a definitive list of topics, the aim of the study is to provoke further discussion across the DLT/Blockchain community about the potential role of standards in supporting the development and adoption of the technology. We carried out the research using a mixed methods approach involving a focused review of the literature, in-depth interviews with stakeholders from public and private organizations, and an internal workshop. Although the study is primarily intended to inform the BSI’s approach towards developing a standards strategy in relation to DLT/Blockchain, it is also likely to be of relevance to stakeholders in the DLT/Blockchain community, including policymakers, industry, other standards organizations (national and international), and academia.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8389459 Subscription required to view

Abstract: Blockchain and Internet of things are the most promising and upcoming technologies. Blockchain is a distributed, peer to peer database forming a chain between multiple blocks of data. The Internet of things works on a similar paradigm where multiple devices are connected to the internet forming a network of networks. Combined together they offer solutions for various problems, especially in the field of healthcare where quick reporting of data or results is of utmost importance. Recent studies have proven that delays in providing healthcare are directly linked to patient confidence and chances of
recovery. An unreliable storage of health records has only aggravated the problem. Our paper aims to provide a solution for these issues by proposing a Blockchain-Internet of things model where a bio-sensor measures and collects real time data with respect to a patient's medical status and stores it in the blockchain. In this way quick reporting and tamper proof storage of data occurs. By deploying a smart contract the final hospital bill can be calculated along with insurance coverage. This would negate the need of third party providers and create a transparent system. Our paper also proposes the use of Inter planetary file system to store discharged patients records thus reducing the load on the actual blockchain. Overall this will surely benefit patients and doctors alike by creating a safe and transparent environment along with quick response to a patient's need.


Abstract: This work proposes to exploit blockchain technology to define Access Control systems that guarantee the auditability of access control policies evaluation. The key idea of our proposal is to codify attribute-based Access Control policies as smart contracts and deploy them on a blockchain, hence transforming the policy evaluation process into a completely distributed smart contract execution. Not only the policies, but also the attributes required for their evaluation are managed by smart contracts deployed on the blockchain. The auditability property derives from the immutability and transparency properties of blockchain technology. This paper not only presents the proposed Access Control system in general, but also its application to the innovative reference scenario where the resources to be protected are themselves smart contracts. To prove the feasibility of our approach, we present a reference implementation exploiting XACML policies and Solidity written smart contracts deployed on the Ethereum blockchain. Finally, we evaluate the system performances through a set of experimental results, and we
discuss the advantages and drawbacks of our proposal.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6372466/

Abstract: Objectives: This pilot study aimed to provide an overview of the potential for blockchain technology in the healthcare system. The review covers technological topics from storing medical records in blockchains through patient personal data ownership and mobile apps for patient outreach.
Methods: We performed a preliminary survey to fill the gap that exists between purely technically focused manuscripts about blockchains, on the one hand, and the literature that is mostly concerned with marketing discussions about their expected economic impact on the other hand.
Results: The findings show that new digital platforms based on blockchains are emerging to enabling fast, simple, and seamless interaction between data providers, including patients themselves.
Conclusions: We provide a conceptual understanding of the technical foundations of the potential for blockchain technology in healthcare, which is necessary to understand specific blockchain applications, evaluate business cases such as blockchain startups, or follow the discussion about its expected economic impacts.


Reference Type: Electronic Article
Abstract: While Edward Lloyd is largely credited with commercializing the insurance industry, with the creation of his namesake firm, Lloyd’s, over 330 years ago, the original concept of spreading risk (or “mutualizing”) goes back even further. Hundreds of years before Lloyd’s was formed, Chinese merchants would spread their valuable cargo across multiple vessels, with each one carrying an equal share of another merchant’s goods. In this manner, no single loss would be catastrophic. This spread of risk, of course, also prevented a merchant from absconding with his ship’s goods and never reuniting with the other traders; he’d have too much to lose. In effect, they all had skin in the game, which remains one of the most elusive elements of modern finance. Both then and in 1686, when Lloyd’s was born in a London coffee house, the global insurance industry was a business of utmost good faith, as it remains today.

Thus a trust and efficiency engine like blockchain technology has the potential to drive radical change in the insurance industry while improving transparency and outcomes across the entire value chain. Intermediaries or “trust brokers” do not have to be written out of the equation — or disintermediated — as many blockchain enthusiasts argue. Rather, they can become early adopters of the technology. Admittedly, this shift will be hardest on the established monoliths in the industry, for it will require uncomfortable transparency and price corrections in their business models. This will be toughest on the portions of the industry that are the least differentiated, where consumers often decide based on price: auto, life, and homeowner’s insurance. However, even these commodity offerings can find ways to innovate and survive.


Reference Type: Electronic Article
Abstract: The Internet of Things (IoT) is experiencing exponential growth in research and industry, but it still suffers from privacy and security vulnerabilities. Conventional security and privacy approaches tend to be inapplicable for IoT, mainly due to its decentralized topology and the resource-constraints of the majority of its devices. BlockChain (BC) that underpin the cryptocurrency Bitcoin have been recently used to provide security and privacy in peer-to-peer networks with similar topologies to IoT. However, BCs are computationally expensive and involve high bandwidth overhead and delays, which are not suitable for IoT devices. This position paper proposes a new secure, private, and lightweight architecture for IoT, based on BC technology that eliminates the overhead of BC while maintaining most of its security and privacy benefits. The described method is investigated on a smart home application as a representative case study for broader IoT applications. The proposed architecture is hierarchical, and consists of smart homes, an overlay network and cloud storages coordinating data transactions with BC to provide privacy and security. Our design uses different types of BC’s depending on where in the network hierarchy a transaction occurs, and uses distributed trust methods to ensure a decentralized topology. Qualitative evaluation of the architecture under common threat models highlights its effectiveness in providing security and privacy for IoT applications.
Abstract: Blockchain is a distributed, immutable ledger technology introduced as the enabling mechanism to support cryptocurrencies. Blockchain solutions are currently being proposed to address divergent problems in different domains. This paper presents a scoping review of the scientific literature to map the current research area of blockchain applications in the biomedical domain. The goal is to identify biomedical problems treated with blockchain technology, the level of maturity of respective approaches, types of biomedical data considered, blockchain features and functionalities exploited and blockchain technology frameworks used. The study follows the PRISMA-ScR methodology. Literature search was conducted on August 2018 and the systematic selection process identified 47 research articles for detailed study. Our findings show that the field is still in its infancy, with the majority of studies in the conceptual or architectural design phase; only one study reports real world demonstration and evaluation. Research is greatly focused on integration, integrity and access control of health records and related patient data. However, other diverse and interesting applications are emerging, addressing medical research, clinical trials, medicines supply chain, and medical insurance.


Abstract: Usually, medical information including physical examination results and treatment of patients is stored in the hospital's centralized database. Although sophisticated access control strategy is adopted, it is still high-risk to expose patients' privacy in complex network environment. Moreover, a practical service platform is missed to share this kind of information under patients' authentication. To solve these problem, we elaborate an efficient and secure medical information service platform based on distributed cloud and blockchain technology, simultaneously guarantee security and confidentiality by hierarchical identity-based broadcast encryption system. Within our proposed framework, medical data are stored on distributed cloud after encryption. An incentive mechanism is designed to encourage customers and miners to maintain the platform. It shows that our platform is safe and effective in practice.


Abstract: Electronic medical records (EMRs) are critical, highly sensitive private information in healthcare, and need to be frequently shared among peers. Blockchain provides a shared, immutable and transparent history of all the transactions to build applications with trust, accountability and transparency. This provides a unique opportunity to develop a secure and trustable EMR data management and sharing system using blockchain. In this paper, we present our perspectives on blockchain based healthcare data management, in particular, for EMR data sharing between healthcare providers and for research studies. We propose a framework on managing and sharing EMR data for cancer patient care. In collaboration with Stony Brook University Hospital, we implemented our framework in a prototype that ensures privacy, security, availability, and fine-grained access control over EMR data. The proposed work can significantly reduce the turnaround time for EMR sharing, improve decision making for medical care, and reduce the overall cost.
Abstract: Blockchain is a technological concept which evolves from the first cryptocurrency, Bitcoin, and disrupts constantly enlarging areas of economy. The concept of blockchain is developing, and while the future of Bitcoin remains unclear (as it is for the most elements of the economy) it is evident that the blockchain holds enormous potential for large-scale improvements. However, being a technology that could decrease significance many of today’s large global corporations, institutions and power structures which have keen interest in preserving established hierarchies, its potential could well remain unexploited. This paper aims to introduce and present the concept of blockchain and its current applications in logistics and supply networks. Blockchain technology promises overpowering trust issues and allowing trustless, secure and authenticated system of logistics and supply chain information exchange in supply networks. The new implementations within supply chain are shifting from blockchain to a wider notion of distributed ledger technologies. Paper presents description and rationale behind current and possible future applications of blockchain in logistics and supply chain.

Reference Type: Conference Paper

Abstract: Distributed Ledger Technology (DLT) has been proposed as a new way to incorporate decentralization into a wide range of digital infrastructures. Applications of DLT to digital identity are increasing in prevalence, with a recent survey reporting that 55% of DLT technologies in development track digital identity. However, while proofs of concept, open source software, and new ideas are readily available, it is still unclear the extent to which DLT can play a role to underpin new forms of digital identity. In this position paper, we situate this fast-moving application domain into the broader challenges faced in digital identity, with the aim to highlight the socio-technical nature of the challenge at hand, and to propose directions for future research.

Reference Type: Journal Article

Abstract: The emergence of distributed ledger technology (DLT) based on a blockchain data structure has given rise to new approaches to identity management that aim to upend dominant approaches to providing and consuming digital identities. These new approaches to identity management (IdM) propose to enhance de-centralization, transparency, and user control in transactions that involve identity information; however, given the historical challenge to design IdM, can these new DLT-based schemes deliver on their lofty goals? We introduce the emerging landscape of DLT-based IdM and evaluate three representative proposals—uPort, ShoCard, and Sovrin—using the analytic lens of a seminal framework that characterizes the nature of successful IdM schemes.

Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/2/326

Abstract: Medical care has become one of the most indispensable parts of human lives, leading to a dramatic increase in medical big data. To streamline the diagnosis and treatment process, healthcare professionals are now adopting Internet of Things (IoT)-based wearable technology. Recent years have witnessed billions of sensors, devices, and vehicles being connected through the Internet. One such technology—remote patient monitoring—is common nowadays for the treatment and care of patients. However, these technologies also pose grave privacy risks and security concerns about the data transfer and the logging of data transactions. These security and privacy problems of medical data could result from a delay in treatment progress, even endangering the patient’s life. We propose the use of a blockchain to provide secure management and analysis of healthcare big data. However, blockchains are computationally expensive, demand high bandwidth and extra computational power, and are therefore not completely suitable for most resource-constrained IoT devices meant for smart cities. In this work, we try to resolve the above-mentioned issues of using blockchain with IoT devices. We propose a novel framework of modified blockchain models suitable for IoT devices that rely on their distributed nature and other additional privacy and security properties of the network. These additional privacy and security properties in our model are based on advanced cryptographic primitives. The solutions given here make
IoT application data and transactions more secure and anonymous over a blockchain-based network.

Reference Type: Journal Article
Abstract: Cryptocurrency investigations have centered almost entirely around the transfer of value "money" or a cryptocurrency asset. The use of cryptocurrency for illicit purposes, especially Bitcoin, is well documented both in academic writing, media reporting and even film documentaries. The infamous SilkRoad marketplace in addition to the millions of dollars spent within dark markets on drugs, guns and assassinations have grabbed the headlines. This paper looks at how blockchain is creating new areas of investigation that are yet to be explored in detail. This scenario-based research examines the hosting of stolen data (P.I.I) personal identifiable information on a distributed blockchain host where the data is also accessible. The platform used is based on Ethereum infrastructure but demonstrates just one available platform that poses the paradigm. The paper examines the considerations through the lens of an incident responder / cyber investigator, forensics examiner and data controller. The scenario highlights distinct differences in considerations from a traditional response compared to dealing with the immutable and unstoppable distributed technology. The paper concludes that more is needed to be done to understand digital forensics in the blockchain era and the need to develop beyond track and trace in the cryptocurrency investigative toolbox. The discussion also brings forth how data retention and GDPR requires consideration when applying it blockchain systems.

Reference Type: Conference Paper
Abstract: Conceptually, the blockchain is a distributed database containing records of transactions that are shared among participating members. Each transaction is confirmed by the consensus of a majority of the members, making fraudulent transactions unable to pass collective confirmation. Once a record is created and accepted by the blockchain, it can never be altered or disappear. Nowadays the blockchain technology is considered as the most significant invention after the Internet. If the latter connects people to realize on-line business processes, the former could decide the trust problem by peer-to-peer networking and public-key cryptography. The purpose of this paper is to consider on distinct use cases at the all-pervasive impact of the blockchain technology and look at this as an inalienable part of our daily life.

Reference Type: Conference Proceedings
Available from: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf
Abstract: A long-standing focus on compliance has traditionally constrained development of fundamental design changes for Electronic Health Records (EHRs). We now face a critical need for such innovation, as personalization and data science prompt patients to engage in the details of their healthcare and restore agency over their medical data. In this paper, we propose MedRec: a novel, decentralized record management system to handle EHRs, using blockchain technology. Our system gives patients a comprehensive, immutable log and easy access to their medical information across providers and treatment sites. Leveraging unique blockchain properties, MedRec manages authentication, confidentiality, accountability and data sharing—crucial considerations when handling sensitive information. A modular design integrates with providers' existing, local data storage solutions, facilitating interoperability and making our system convenient and adaptable. We incentivize medical stakeholders (researchers, public health authorities, etc.) to participate in the network as blockchain "miners". This provides them with access to aggregate, anonymized data as mining rewards, in return for sustaining and securing the network via Proof of Work. MedRec thus enables the emergence of data economics, supplying big data to empower researchers while engaging patients and providers in the choice to release metadata. The purpose of this paper is to expose, in preparation for field tests, a working prototype through which we analyze and discuss our approach and the potential for blockchain in health IT and research.

Reference Type: Conference Proceedings


Abstract: In this paper, we present the applications of blockchain technology in healthcare. Furthermore, we evaluate the choice and deployment of Blockchain technology in such applications, review the advantages and disadvantages of such an approach. We review the Estonian system, which is the first blockchain-based health system at the national level, in detail and discuss its ramifications to Turkey. This paper is one of the first papers in this domain and, to the best of authors' knowledge, the first in Turkish.


Reference Type: Journal Article


Abstract: The cryptocurrency market surpassed the barrier of $100 billion market capitalization in June 2017, after months of steady growth. Despite its increasing relevance in the financial world, a comprehensive analysis of the whole system is still lacking, as most studies have focused exclusively on the behaviour of one (Bitcoin) or few cryptocurrencies. Here, we consider the history of the entire market and analyse the behaviour of 1469 cryptocurrencies introduced between April 2013 and May 2017. We reveal that, while new cryptocurrencies appear and disappear continuously and their market capitalization is increasing (super-)exponentially, several statistical properties of the market have been stable for years. These include the number of active cryptocurrencies, market share distribution and the turnover of cryptocurrencies. Adopting an ecological perspective, we show that the so-called neutral model of evolution is able to reproduce a number of key empirical observations, despite its simplicity and the assumption of no selective advantage of one cryptocurrency over another. Our results shed light on the properties of the cryptocurrency market and establish a first formal link between ecological modelling and the study of this growing system. We anticipate they will spark further research in this direction.


Reference Type: Journal Article


Abstract: Electronic government (e-government) uses information and communication technologies to deliver public services to individuals and organisations effectively, efficiently and transparently. E-government is one of the most complex systems which needs to be distributed, secured and privacy- preserved, and the failure of these can be very costly both economically and socially. Most of the existing e-government systems such as websites and electronic identity management systems (eIDs) are centralized at duplicated servers and databases. A centralized management and validation system may suffer from a single point of failure and make the system a target to cyber attacks such as malware, denial of service attacks (DoS), and distributed denial of service attacks (DDoS). The blockchain technology enables the implementation of highly secure and privacy-preserving decentralized systems where transactions are not under the control of any third party organizations. Using the blockchain technology, exiting data and new data are stored in a sealed compartment of blocks (i.e., ledger) distributed across the network in a verifiable and immutable way. Information security and privacy are enhanced by the blockchain technology in which data are encrypted and distributed across the entire network. This paper proposes a framework of a decentralized e-government peer-to-peer (p2p) system using the blockchain technology, which can ensure both information security and privacy while simultaneously increasing the trust of the public sectors. In addition, a prototype of the proposed system is presented, with the support of a theoretical and qualitative analysis of the security and privacy implications of such system.


Reference Type: Conference Proceedings
Abstract: Data mining is the process of knowledge discovery in databases (centralized or distributed); it consists of different tasks associated with them different algorithms. Nowadays the scenario of one centralized database that maintains all the data is difficult to achieve due to different reasons including physical, geographical restrictions and size of the data itself. One approach to solve this problem is distributed databases where different partities have horizontal or vertical partitions of the data. The data is normally maintained by more than one organization, each of which aims at keeping its information stored in the databases private, thus, privacy-preserving techniques and protocols are designed to perform data mining on distributed data when privacy is highly concerned. Cluster analysis is a frequently used data mining task which aims at decomposing or partitioning a usually multivariate data set into groups such that the data objects in one group are the most similar to each other. It has an important role in different fields such as bio-informatics, marketing, machine learning, climate and healthcare. In this paper we introduce a novel clustering algorithm that was designed with the goal of enabling a privacy preserving version of it, along with sub-protocols for secure computations, to handle the clustering of vertically partitioned data among different healthcare data providers.

Reference Type: Journal Article

Abstract: Medline started in 1971 with 22 users who had access to 236 indexed journals and almost 150,000 indexed papers on which some 70,000 searches were performed. By 2016, celebrating Medline's 45th anniversary, these numbers had grown exponentially to a staggering 601 million users having access to over 22 million papers published in 5618 Journals on which some 2.8 billion PubMed searches were performed. Annual growth is well over 800,000 papers and this is testimony to a medical research industry that has grown beyond recognition and perhaps human measure in just the life span of a surgical career. If we assume a normal distribution of mean scientific quality of all papers available on PubMed than well over 500,000 papers (approximately 2.5%) are characterised by over 2 standard deviations difference to the left side of the mean scientific quality. With increasing scientific output we have seen proportional growth of papers aggregating and analysing data in systematic reviews and meta-analyses but also of papers analysing basic flaws and biases of the medical research industry. Poor quality medical research has been a perennial issue and perhaps it is time to accept that less is more.

Reference Type: Journal Article
Available from: https://timreview.ca/article/1111

Abstract: Health services must balance patient care with information privacy, access, and completeness. The massive scale of the healthcare industry also amplifies the importance of cost control. The promise of blockchain technology in health services, combined with application layers built atop it, is to be a mechanism that provides utmost privacy while ensuring that appropriate users can easily add to and access a permanent record of information. Blockchains, also called distributed ledgers, enable a combination of cost reduction and increased accessibility to information by connecting stakeholders directly without requirements for third-party brokers, potentially giving better results at lower costs. New ventures are looking to apply blockchain technology to solve real-world problems, including efforts to track public health, centralize research data, monitor and fulfill prescriptions, lower administrative overheads, and organize patient data from an increasing number of inputs. Here, concrete examples of the application of blockchain technology in the health sector are described, touching on near-term promise and challenges.

Reference Type: Journal Article
Available from: https://www.jmir.org/2019/6/e14184/

Abstract: BACKGROUND: Nowadays, a number of mechanisms and tools are being used by health care organizations and physicians to electronically exchange the personal health information of patients. The main objectives of different methods of health information exchange (HIE) are to reduce health care costs, minimize medical errors, and improve the coordination of interorganizational information exchange
The challenge for a privacy standard. In: Wu Y, Min G, Georgalas N, IEEE International Conference on Internet of Things, editors. 2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); June 21-23; Exeter, United Kingdom. IEEE International Conference on Internet of Things; 2017. p. 727-34.

Reference Type: Conference Paper

Abstract: The IoT is innovative and important phenomenon prone to several services and applications, but it should consider the legal issues related to data protection law. However, should be taken into account the legal issues related to the data protection and privacy law. Technological solutions are welcome, but it is necessary, before developing applications, to consider the risks which we cannot dismiss. Personal data is a value. In this context is fundamental to evaluate the legal issues and prevent them, adapting in each project the privacy by design approach. Regarding the privacy and security risks, there are some issues with potential consequences for data security and liability. The IoT system allows us to transfer data on the Internet, including personal data. In this context, it is important to consider the new European General Data Protection Regulation (GDPR) - already in force from 24 May 2016 - that will be applicable on 25 May 2018. The GDPR introduces Data Protection Impact Assessment (DPIA), data breach notification and very hard administrative fines in respect of infringements of the Regulation. A correct law analysis allows evaluating risks preventing the wrong usage of personal data. The IoT ecosystem is evolving quickly, developing several applications in different sectors. The main topics for the last time are Big Data and the blockchain. People are paying attention to the latest one because of its potential concrete use for services and applications, increasing the security measures to guarantee a secure system. However, it is equally important to analyse the legal issues related to them. Everyone has the right to the protection of personal data concerning him or her. In this context, we cannot dismiss to guarantee an adequate protection of personal data designing any application. The contribution describes the main legal issues related to privacy and data protection especially regarding the blockchain, focusing on the Privacy by Design approach, according to the GDPR. Furthermore, I resolutely believe that is
possible to develop a worldwide privacy standard framework that organisations can use for their data protection activities.


Abstract: Digital medicine, digital research and artificial intelligence (AI) have the power to transform the field of diabetes with continuous and no-burden remote monitoring of patients’ symptoms, physiological data, behaviours, and social and environmental contexts through the use of wearables, sensors and smartphone technologies. Moreover, data generated online and by digital technologies—which the authors suggest be grouped under the term ‘digitosome’—constitute, through the quantity and variety of information they represent, a powerful potential for identifying new digital markers and patterns of risk that, ultimately, when combined with clinical data, can improve diabetes management and quality of life, and also prevent diabetes-related complications. Moving from a world in which patients are characterized by only a few recent measurements of fasting glucose levels and glycated haemoglobin to a world where patients, healthcare professionals and research scientists can consider various key parameters at thousands of time points simultaneously will profoundly change the way diabetes is prevented, managed and characterized in patients living with diabetes, as well as how it is scientifically researched. Indeed, the present review looks at how the digitization of diabetes can impact all fields of diabetes—its prevention, management, technology and research—and how it can complement, but not replace, what is usually done in traditional clinical settings. Such a profound shift is a genuine game changer that should be embraced by all, as it can provide solid research results transferable to patients, improve general health literacy, and provide tools to facilitate the everyday decision-making process by both healthcare professionals and patients living with diabetes.


Abstract: With the development of electronic information technology, electronic medical records (EMRs) have been a common way to store the patients' data in hospitals. They are stored in different hospitals' databases, even for the same patient. Therefore, it is difficult to construct a summarized EMR for one patient from multiple hospital databases due to the security and privacy concerns. Meanwhile, current EMRs systems lack a standard data management and sharing policy, making it difficult for pharmaceutical scientists to develop precise medicines based on data obtained under different policies. To solve the above problems, we proposed a blockchain-based information management system, MedBlock, to handle patients' information. In this scheme, the distributed ledger of MedBlock allows the efficient EMRs access and EMRs retrieval. The improved consensus mechanism achieves consensus of EMRs without large energy consumption and network congestion. In addition, MedBlock also exhibits high information security combining the customized access control protocols and symmetric cryptography. MedBlock can play an important role in the sensitive medical information sharing.


Abstract: Bitcoins were conceptualized in 2008, which revolutionized the digital transfers of value within payment systems (Nakamoto, 2008). The advent of digital currencies revealed problems concerning anonymity embedded in bitcoins, consequently raising money laundering concerns. Regulators and law enforcement agencies struggle with addressing the money laundering issues inherent with bitcoin and digital currencies (Ajello, 2025). In response to these threats, agencies have issued various opinions regarding defining digital currencies within a financial framework. Regulator opinions concerning the applicability of bitcoins existing as currency, property, a commodity and commodity money contradict each other. Moreover, prosecutorial agencies attempt to fit digital currency exchangers under the regulations pertinent to money service businesses (MSB) (Mandjee, 2015; Sonderegger, 2015). This project provided an analysis of scholarly material, government publications, case law, and current trade information to examine a solution to the problem of money laundering through digital currency. This project revealed a need for a clear definition of bitcoin and digital currency within the context of U.S. laws
and regulation to assist with investigations concerning illicit uses of digital currency. Furthermore, a need exists for new U.S. legislation specific to digital currency, which addresses money laundering and terrorist finance risks. Research revealed that digital currency regulations should mirror MSB regulations to curb peer-to-peer digital currency exchanges (Kirby, 2014). Additionally, FinCEN’s purview with financial crimes provides a unique position to assist law enforcement with digital currency investigations (FinCEN, 2014). A need exists for FinCEN to develop a blockchain analysis tool for law enforcement agencies and to assist with complex digital currency investigations (DHS, 2014).

Reference Type: Journal Article
Available from: https://www.nature.com/articles/d41586-018-07449-z/
Abstract: By 2025, up to 10% of global gross domestic product is likely to be stored on blockchains. A blockchain is a digital tool that uses cryptography techniques to protect information from unauthorized changes. It lies at the root of the Bitcoin cryptocurrency. Blockchain-related products are used everywhere from finance and manufacturing to health care, in a market worth more than US$150 billion.

When information is money, data security, transparency and accountability are crucial. A blockchain is a secure digital record, or ledger. It is maintained collectively by users around the globe, rather than by one central administration. Decisions such as whether to add an entry (or block) to the ledger are based on consensus — so personal trust doesn’t come into it. Any party inside or outside the network can check the integrity of the ledger by making a simple calculation.

But within a decade, quantum computers will be able to break a blockchain’s cryptographic codes. Here we highlight how quantum technology makes blockchains vulnerable — and how it could render them more secure.

Reference Type: Journal Article
Abstract: Blockchain, as a decentralized and distributed public ledger technology in peer-to-peer network, has received considerable attention recently. It applies a linked block structure to verify and store data, and applies the trusted consensus mechanism to synchronize changes in data, which makes it possible to create a tamper-proof digital platform for storing and sharing data. It is believed that blockchain can be utilized in diverse Internet interactive systems (e.g., Internet of Things, supply chain systems, identity management, and so on). However, there are some privacy challenges that may hinder the applications of blockchain. The goal of this survey is to provide some insights into the privacy issues associated with blockchain. We analyze the privacy threats in blockchain and discuss existing cryptographic defense mechanisms, i.e., anonymity and transaction privacy preservation. Furthermore, we summarize some typical implementations of privacy preservation mechanisms in blockchain and explore future research challenges that still need to be addressed in order to preserve privacy when blockchain is used.

Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/10/2394
Abstract: Industry 4.0 has paved the way for a world where smart factories will automate and upgrade many processes through the use of some of the latest emerging technologies. One of such technologies is Unmanned Aerial Vehicles (UAVs), which have evolved a great deal in the last years in terms of technology (e.g., control units, sensors, UAV frames) and have significantly reduced their cost. UAVs can help industry in automatable and tedious tasks, like the ones performed on a regular basis for determining the inventory and for preserving item traceability. In such tasks, especially when it comes from untrusted third parties, it is essential to determine whether the collected information is valid or true. Likewise, ensuring data trustworthiness is a key issue in order to leverage Big Data analytics to supply chain efficiency and effectiveness. In such a case, blockchain, another Industry 4.0 technology that has become very popular in other fields like finance, has the potential to provide a higher level of transparency, security, trust and efficiency in the supply chain and enable the use of smart contracts.
Thus, in this paper, we present the design and evaluation of a UAV-based system aimed at automating inventory tasks and keeping the traceability of industrial items attached to Radio-Frequency Identification (RFID) tags. To confront current shortcomings, such a system is developed under a versatile, modular and scalable architecture aimed to reinforce cyber security and decentralization while fostering external audits and big data analytics. Therefore, the system uses a blockchain and a distributed ledger to store certain inventory data collected by UAVs, validate them, ensure their trustworthiness and make them available to the interested parties. In order to show the performance of the proposed system, different tests were performed in a real industrial warehouse, concluding that the system is able to obtain the inventory data really fast in comparison to traditional manual tasks, while being also able to estimate the position of the items when hovering over them thanks to their tag's signal strength. In addition, the performance of the proposed blockchain-based architecture was evaluated in different scenarios.


Reference Type: Journal Article

Abstract: The paradigm of Internet of Things (IoT) is paving the way for a world, where many of our daily objects will be interconnected and will interact with their environment in order to collect information and automate certain tasks. Such a vision requires, among other things, seamless authentication, data privacy, security, robustness against attacks, easy deployment, and self-maintenance. Such features can be brought by blockchain, a technology born with a cryptocurrency called Bitcoin. In this paper, a thorough review on how to adapt blockchain to the specific needs of IoT in order to develop Blockchain-based IoT (BioT) applications is presented. After describing the basics of blockchain, the most relevant BioT applications are described with the objective of emphasizing how blockchain can impact traditional cloud-centered IoT applications. Then, the current challenges and possible optimizations are detailed regarding many aspects that affect the design, development, and deployment of a BioT application. Finally, some recommendations are enumerated with the aim of guiding future BioT researchers and developers on some of the issues that will have to be tackled before deploying the next generation of BioT applications.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/15/3319

Abstract: Diabetes patients suffer from abnormal blood glucose levels, which can cause diverse health disorders that affect their kidneys, heart and vision. Due to these conditions, diabetes patients have traditionally checked blood glucose levels through Self-Monitoring of Blood Glucose (SMBG) techniques, like prick their fingers multiple times per day. Such techniques involve a number of drawbacks that can be solved by using a device called Continuous Glucose Monitor (CGM), which can measure blood glucose levels continuously throughout the day without having to prick the patient when carrying out every measurement. This article details the design and implementation of a system that enhances commercial CGMs by adding Internet of Things (IoT) capabilities to them that allow for monitoring patients remotely and, thus, warning them about potentially dangerous situations. The proposed system makes use of smartphones to collect blood glucose values from CGMs and then sends them either to a remote cloud or to distributed fog computing nodes. Moreover, in order to exchange reliable, trustworthy and cybersecure data with medical scientists, doctors and caretakers, the system includes the deployment of a decentralized storage system that receives, processes and stores the collected data. Furthermore, in order to motivate users to add new data to the system, an incentive system based on a digital cryptocurrency named GlucoCoin was devised. Such a system makes use of a blockchain that is able to execute smart contracts in order to automate CGM sensor purchases or to reward the users that contribute to the system by providing their own data. Thanks to all the previously mentioned technologies, the proposed system enables patient data crowdsourcing and the development of novel mobile health (mHealth) applications for diagnosing, monitoring, studying and taking public health actions that can help to advance in the control of the disease and raise global awareness on the increasing prevalence of diabetes.


Reference Type: Journal Article
Abstract: This is the first work to introduce the use of blockchain technology for the electronic traceability of wood from standing tree to final user. Infotracing integrates the information related to the product quality with those related to the traceability (physical and digital documents (Radio Frequency IDentification-RFID-architecture)) within an online information system whose steps (transactions) can be made safe to evidence of alteration through the blockchain. This is a decentralized and distributed ledger that keeps records of digital transactions in such a way that makes them accessible and visible to multiple participants in a network while keeping them secure without the need of a centralized certification organism. This work implements a blockchain architecture within the wood chain electronic traceability. The infotracing system is based on RFID sensors and open source technology. The entire forest wood supply chain was simulated from standing trees to the final product passing through tree cutting and sawmill process. Different kinds of Internet of Things (IoT) open source devices and tags were used, and a specific app aiming the forest operations was engineered to collect and store in a centralized database information (e.g., species, date, position, dendrometric and commercial information).


Reference Type: Journal Article

Abstract: This article examines data protection on blockchains and other forms of distributed ledger technology. Whereas the General Data Protection Regulation was fashioned for centralised methods of data collection, storage and processing, blockchains decentralise each of these processes. We engage with the resulting tensions in the below analysis.


Reference Type: Journal Article

Abstract: The increasing demand for Android mobile devices and blockchain has motivated malware creators to develop mobile malware to compromise the blockchain. Although the blockchain is secure, attackers have managed to gain access into the blockchain as legal users, thereby comprising important and crucial information. Examples of mobile malware include root exploit, botnets, and Trojans and root exploit is one of the most dangerous malware. It compromises the operating system kernel in order to gain root privileges which are then used by attackers to bypass the security mechanisms, to gain complete control of the operating system, to install other possible types of malware to the devices, and finally, to steal victims’ private keys linked to the blockchain. For the purpose of maximizing the security of the blockchain-based medical data management (BMDM), it is crucial to investigate the novel features and approaches contained in root exploit malware. This study proposes to use the bio-inspired method of practical swarm optimization (PSO) which automatically select the exclusive features that contain the novel android debug bridge (ADB). This study also adopts boosting (adaboost, realadaboost, logitboost, and multiboost) to enhance the machine learning prediction that detects unknown root exploit, and scrutinized three categories of features including (1) system command, (2) directory path and (3) code-based. The evaluation gathered from this study suggests a marked accuracy value of 93% with Logitboost in the simulation. Logitboost also helped to predicted all the root exploit samples in our developed system, the root exploit detection system (RODS).


Reference Type: Conference Paper

Abstract: This paper describes the use of blockchain technology as a data provider in Internet of Things (IoT) applications. Blockchain is a novel technology, which has gained a lot of attention in the last years, mainly due to its use as a backbone for cryptocurrencies. The main purpose of blockchain technology is to provide anonymous transactions between participants, over a peer-to-peer network, using a decentralized distributed ledger. The goal of this novel approach is to eliminate any 3<sup>rd</sup> party involvement.
party validation and replace the trust of a central authority for transaction validation with cryptographic proof. While most applications of the blockchain revolve around cryptocurrencies, the blockchain can be used in many other fields, such as finance, distributed data storage, health and medicine, automation, etc. By creating an open, decentralized network, the blockchain can be used to develop decentralized applications and enable data access and sharing on a much higher level than the common implementations of client-server architectures which are in use today. In this paper, we will present a proof of concept method for field devices to store and share data using a distributed ledger built on the IOTA tangle, as well as provide means of access to the data which can be used in IoT and decentralized applications.

Francisco K., Swanson D. The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics. 2018;2(1). Epub 2018 Jan 5.

Abstract: Blockchain technology, popularized by Bitcoin cryptocurrency, is characterized as an open-source, decentralized, distributed database for storing transaction information. Rather than relying on centralized intermediaries (e.g., banks) this technology allows two parties to transact directly using duplicate, linked ledgers called blockchains. This makes transactions considerably more transparent than those provided by centralized systems. As a result, transactions are executed without relying on explicit trust of a third party, but on the distributed trust based on the consensus of the network (i.e., other blockchain users). Applying this technology to improve supply chain transparency has many possibilities. Every product has a long and storied history. However, much of this history is presently obscured. Often, when negative practices are exposed, they quickly escalate to scandalous, and financially crippling proportions. There are many recent examples, such as the exposure of child labor upstream in the manufacturing process and the unethical use of rainforest resources. Blockchain may bring supply chain transparency to a new level, but presently academic and managerial adoption of blockchain technologies is limited by our understanding. To address this issue, this research uses the Unified Theory of Acceptance and Use of Technology (UTAUT) and the concept of technology innovation adoption as a foundational framework for supply chain traceability. A conceptual model is developed and the research culminates with supply chain implications of blockchain that are inspired by theory and literature review.


Abstract: Many Internet services require the registration of an account before permitting use of their services. Over time, many Internet users end up with a multitude of accounts with separated identities. A solution to this problem is offered by single-sign-on (SSO) providers, where a user can create a single identity and use this identity for multiple services. However it requires the user to trust the SSO provider. When the provider blocks access to the identities the users lose access to their subscribed services. To avoid this problem, we propose DecentID, a completely decentralized identity storage system that does not require a centralized trusted third party. Instead, a public blockchain is used as trust anchor. Identities can be created and used for different services. Each service can only read the identity attributes disclosed for it without being able to read attributes the user wants to keep secret.
an open, public, distributed, and secure digital registry where information transactions are secured and have a clear origin, explicit pathways, and concrete value. Health professions education based on blockchain will potentially allow improved tracking of content and the individuals who create it, quantify educational impact on multiple generations of learners, and build a relative value of educational interventions. Furthermore, institutions adopting blockchain technology would be able to provide certification and credentialing of healthcare professionals with no intermediaries. There is potential for blockchain to significantly change the future of health professions education and radically transform how patients, professionals, educators, and learners interact around safe, valid, and accountable information.


Reference Type: Electronic Article
Abstract: Publishing reproducible analyses is a long-standing and widespread challenge for the scientific community, funding bodies and publishers. Although a definitive solution is still elusive, the problem is recognized to affect all disciplines and lead to a critical system inefficiency. Here, we propose a blockchain-based approach to enhance scientific reproducibility, with a focus on life science studies and precision medicine. While the interest of encoding permanently into an immutable ledger all the study key information—incorporating endpoints, data and metadata, protocols, analytical methods and all findings—has been already highlighted, here we apply the blockchain approach to solve the issue of rewarding time and expertise of scientists that commit to verify reproducibility. Our mechanism builds a trustless ecosystem of researchers, funding bodies and publishers cooperating to guarantee digital and permanent access to information and reproducible results. As a natural byproduct, a procedure to quantify scientists’ and institutions’ reputation for ranking purposes is obtained.


Reference Type: Electronic Article
Abstract: Associating the health-related records and transactions of patients with their numerous “identities” as they interact with different healthcare providers, payers, pharmacy benefit managers and other entities is an expensive and complex problem. With many years of experience addressing this issue in different healthcare systems and Health Information Exchanges (HIEs), it is apparent that there is now a compelling and relatively straightforward technical solution for this problem. Presented here is a broadly feasible and technically compelling argument for a blockchain-based approach to addressing these issues. At the same time, challenges ahead and potential strategies to address them are discussed.

Gallersdörfer USS. Analysis of use cases of blockchain technology in legal transactions [Master’s Thesis]: Technical University of Munich; 2017.

Reference Type: Thesis
Available from: https://wwwmatthes.in.tum.de/file/1i46ejaad8w5j/Sebis-Public-Website/-/Master-s-Thesis-Ulrich-Gallersdoerfer/170508%20Gallersdoerfer%20MT.pdf

Abstract: The interest in blockchain technology of enterprises and startups is rising. The technology itself, up today mostly found in cryptocurrencies, promises to be a decentralized platform for storing data or transferring assets preventing any manipulation. The decentralized database cuts out a trusted third party (TTP), guaranteeing the integrity only with its underlying cryptographic promises. While cryptocurrencies clearly benefit from this technology, it is difficult to see the benefits and usages of this technology in other areas of interest. Varying industries are researching the potentials behind blockchain, proposing a range of different use case scenarios.

We give an insight into the technology itself behind cryptocurrencies and explain in detail, how the functionality of Blockchain is established and how it is set up. Upon that knowledge, different views describing the blockchain architecture are created, giving an overview about the technical layers, the roles, and its life cycle. The different views allow users and developers to comprehensively access the technology. Additionally, a blockchain ontology is created, explaining connections between single components within the network.

Furthermore, this thesis provides an overview of different use cases and proposes a topology. In this topology, use cases are classified in categories, showing the potentials of Blockchain technology. Additionally, we give a detailed description of existing parameters for the blockchain, explaining which influence they have on the overall network. With this, a mapping is facilitated between these categories and the different parameters, giving a detailed overview about the blockchain and its potentials. It informs about all varying abilities and enables decision makers to properly find and select use cases within this
In interviews with over 15 experts from different companies, an insight is given into the recent developments in this technology and the advancements of it.

Additionally, we prototypically implemented a use case, enabling lawyers to collaboratively create a contract in which all changes are recorded on a Blockchain. Thereby, Blockchain is effectively used to prevent manipulation of content or attribution to authors.


Reference Type: Journal Article
Available from: https://www.nature.com/articles/nm0418-378 Subscription required to view.

Abstract: [FIRST FEW PARAGRAPHS] Lucy Ojomoko eyes her selfie. She is young, tall and slender, and her dark hair is pulled back in a ponytail. She clicks ‘upload’ and waits. Her picture is soon accepted to the system she helped to create, and five LifePounds are deposited in her online account.

While she waits for the LifePounds to deposit, she clicks through to add her current health information—height, weight, blood pressure, resting pulse—and adds updated data in these fields. More sensitive information, like blood tests or pictures of her skin, face, back or chest, earn more LifePounds. The company says that their digital currency can eventually be traded for discounts on health tests or products like toothpaste and shampoo—and exchanged for cold, hard cash. The LifePound is a brand of cryptocurrency, a new form of digital currency that operates without a bank. The government, as well as private companies and drug developers aiming to develop drugs and antiaging products, can buy the data linked to the currency through the Longenesis marketplace.


Reference Type: Journal Article
Available from: http://ul.qucosa.de/api/qucosa%3A32042/attachment/ATT-0/

Abstract: Compliance with data protection requirements is always a tricky business and even more intricate when it comes to cutting-edge technologies such as distributed ledger technology (DLT), better known as Block Chain Technology (BCT). These difficulties increase even more when the personal data concerned is accorded a special level of protection, as is the case with health data. The following article aims to describe and analyze the legal issues associated with this scenario. The focus here is on the European Union's (EU) General Data Protection Regulation (GDPR), which took effect on May 25, 2018. Furthermore, the functionality of BCT and its possible fields of application in healthcare will be outlined.

Gatteschi V, Lamberti F, Demartini C, Pranteda C, Santamaria V. To blockchain or not to blockchain: that is the question. IT Prof. 2018;20(2):62-74. Epub 2018 Apr 16.

Reference Type: Journal Article

Abstract: Blockchain has been considered a breakthrough technology—but does your company need it? In this article, the authors discuss the advantages and disadvantages of blockchain technology using examples from the insurance sector, which can be generalized and applied to other sectors.

Gebremedhin TA. Blockchain as a technology to facilitate privacy and better health record management. The University of Bergen: Western Norway University of Applied Science; 2018.

Reference Type: Thesis
Available from: http://bora.uib.no/handle/1956/19621

Abstract: Fear of stigmatization and discrimination from colleagues, friends and family drives patients with various type of mental health problems away from a traditional face-to-face therapy and enforces them to look for an alternative treatment methods. Internet-based mental health therapy helps patients to get their needed therapies and support from healthcare professional and peers, or as a part of automated online form of therapy. Conducting Internet based therapy anonymously is vital for the patient privacy. However, lack of trust, access permission, ownership control and traceability undermines patient safety and security. Blockchain technology is an innovative technology initially designed for a cryptocurrency.
However, with the introduction of programming blockchain and smart contracts, the technology has extended its importance to other areas for developing decentralized application (DApp), such as mental health related information management, which is the primary focus of this thesis. Privacy and security are very crucial for patient safety and to preserve patient’s medical history from adversaries. Sharing of private medical information online between the patient and their respective provider contains sensitive information that can easily be compromised if a proper security measure is not put in place. Blockchain is consensus-based peer-to-peer distributed ledger technology that stores and maintains an updated copy of all transactions within the network. It makes trust more transparent and traceable by keeping auditable-logs of all transactions in the form of blocks. In this thesis, Blockchain and its underlying technology are studied, and a prototype has been developed to explore the potential of the blockchain technology. Furthermore, we explore alternative distributed ledger technologies and their respective security models such as consensus protocols, cryptographic techniques, privacy and scalability. The prototype was proposed based on Ethereum blockchain.


Reference Type: Conference Paper

Available from: http://ebooks.iospress.nl/publication/52057

Abstract: Security, privacy, transparency, consent, and data sharing are major challenges that healthcare institutions must address today. The explosion of the Internet of Things (IoT), the enactment of the General Data Protection Regulation (GDPR), the growing trend of patients self-managing their diseases, and the eagerness of patients to share their self-collected health data with primary and secondary health organisations further increase the complexity of these challenges. Smart contracts, based on blockchain technology, can be a legitimate approach for addressing these challenges. Smart contracts define rules and penalties in an agreement, enforce those rules, and render them irrevocable. This paper presents a state-of-the-art review (as of May 2018) of the possible usages of smart contracts in healthcare and focuses on data sharing between patients, doctors, and institutions.


Reference Type: Journal Article


Abstract: The Drug Supply Chain Security Act (DSCSA) and similar global regulations were designed to help protect the integrity of the medication supply chain by gathering data at each step of a medication’s journey. While the focus is on the “Approved Drug” supply chain, there has been little conversation or focus on the clinical drug supply chain. Blockchain technology has the potential to positively impact clinical trial supply chains by improving the traceability of medications from active pharmaceutical ingredient (API) to patient, while facilitating the gathering of patient-level data in a HIPAA-compliant manner. This is done by having patients and other individuals participating in the network record data to the blockchain, which then moves that information to the appropriate system and groups with access to
Abstract: Blockchain is a disruptive technology with the potential to have a significant impact on business models and industries, similar to the adoption of Internet. Blockchain promotes distributed, open, inclusive, immutable, and secure architectural approaches, instead of centralized, hidden, exclusive, and alterable alternatives. The adoption of blockchain in the healthcare domain offers promising solutions for securing communications among stakeholders, efficient delivery of clinical reports, and integrating various kinds of private health records of individuals on a secure infrastructure. Accordingly, the main aim of this study is to propose a holistic blockchain structure covering all stakeholders in the healthcare domain and to analyse opportunities and challenges by presenting an integrated blockchain architecture. The comprehensive view of blockchain based healthcare system consists of services as follows: personal medical health record storage and access, personal genomic data storage and access, inventory tracking and buy-sell mechanism, health research commons, health document notary services, doctor services, digital health wallet, peer-to-peer insurance. The opportunities of using blockchain in the healthcare domain are considered with respect to several viewpoints such as transparency, accountability, decentralization, record accuracy, secure transactions, interoperability, lower costs, collaboration, agility, individualized care with specialized treatment, improved diagnosis methods, risk of insurance contract, prevention of counterfeit drugs and improved quality of medical research. Challenges associated with the implementation of blockchain in the healthcare domain are also highlighted, such as governance, lack of legacy, privacy, sustainability, scalability, adoption of participation, and cost of operations.


Reference Type: Report

Abstract: Patient-related outcome measures (PROMs), which focus on outcomes that are directly related to the patient, have taken on added importance and significance over the past several years. This is due, in part, to the increased attention focused on the patient experience of care and to provide a patient-focused assessment on the burden and impact of disease. PROMs can include symptoms and other aspects of health—related quality of life indicators such as physical or social function, treatment adherence, and satisfaction with treatment. They can also facilitate more accurate patient-physician communication in terms of the burden of treatment-related morbidities by providing a more detailed and complete evaluation of treatments for specific conditions, such as cancer or multiple sclerosis.


Reference Type: Journal Article

Abstract: Interoperability in healthcare has traditionally been focused around data exchange between business entities, for example, different hospital systems. However, there has been a recent push towards interoperability, in which health data exchange is patient-mediated and patient-driven. Patient-centered interoperability, however, brings with it new challenges and requirements around security and privacy, technology, incentives, and governance that must be addressed for this type of data sharing to succeed at scale. In this paper, we look at how blockchain technology might facilitate this transition through five mechanisms: (1) digital access rules, (2) data aggregation, (3) data liquidity, (4) patient identity, and (5) data immutability. We then look at barriers to blockchain-enabled patient-driven interoperability, specifically clinical data transaction volume, privacy and security, patient engagement, and incentives. We conclude by noting that while patient-driving interoperability is an exciting trend in healthcare, given these challenges, it remains to be seen whether blockchain can facilitate the transition.
from institution-centric to patient-centric data sharing.

Greenberger M. Block what? The unrealized potential of blockchain in healthcare. Nurs Manage. 2019;50 (5).

Reference Type: Journal Article
Available from: https://journals.lww.com/nursingmanagement/Fulltext/2019/05000/Block_what___The_unrealized_potential_of_blockchain.3.aspx Subscription required to view

Abstract: Merging technology is a constant—just like change—in industries like healthcare where scenarios shift at a moment’s notice. Healthcare leaders recognize that innovations and novel ways of addressing today’s healthcare challenges continue to be developed yet understand that new solutions can bring unintended consequences. And clinicians are used to the latest technologies entering the marketplace and being advertised as the answer to complicated problems. Alternatively, disruptive technology is a fresh way of solving old problems. Blockchain is one such technology that’s quietly challenging the way businesses and individuals think about accessing and sharing information among different stakeholders. But why should we care about blockchain in healthcare?


Reference Type: Journal Article

Abstract: As Internet of Things (IoT) devices and other remote patient monitoring systems increase in popularity, security concerns about the transfer and logging of data transactions arise. In order to handle the protected health information (PHI) generated by these devices, we propose utilizing blockchain-based smart contracts to facilitate secure analysis and management of medical sensors. Using a private blockchain based on the Ethereum protocol, we created a system where the sensors communicate with a smart device that calls smart contracts and writes records of all events on the blockchain. This smart contract system would support real-time patient monitoring and medical interventions by sending notifications to patients and medical professionals, while also maintaining a secure record of who has initiated these activities. This would resolve many security vulnerabilities associated with remote patient monitoring and automate the delivery of notifications to all involved parties in a HIPAA compliant manner.


Reference Type: Electronic Article

Abstract: In the years since the first human genome was sequenced at a cost of over $3 billion, technological advancements have driven the price below $1,000, making personal genome sequencing affordable to many people. Personal genome sequencing has the potential to enable better disease prevention, more accurate diagnoses, and personalized therapies. Furthermore, sequencing costs, data privacy concerns, regulatory restrictions, and technical challenges impede the growth of genomic data and hinder data sharing. In this article, we propose that these challenges can be addressed by combining decentralized system design, privacy-preserving technologies, and an equitable compensation model in a platform that vests control over data with individual owners; ensures transparency and privacy; facilitates regulatory compliance; minimizes expensive data transfers; and shifts the sequencing costs from consumers, patients, and biobanks to researchers in industry and academia. We exemplify this by describing the implementation of Nebula, a distributed genomic data generation, sharing, and analysis platform.

Gropper A. Powering the physician-patient relationship with HIE of One Blockchain Health IT. ONC/NIST Use of Blockchain for Healthcare and Research Workshop; 2016 Sep 26-27; Gaithersburg, MD. National Institute of Standards Technology.
Abstract: Physicians steer treatment together with patients and are responsible for the vast majority of decisions, and therefore expenditures, in healthcare. Yet the technology that mediates the physician-patient relationship today is not directly purchased or controlled by either the physicians or the patients. Electronic health records and health information exchange technology are sold as strategic assets to institutions, typically very large businesses, that currently have incentives to maximize institutional growth. We seek a better balance of institutional needs with the needs of physicians and patients.

It is widely accepted that reducing healthcare cost growth requires genuine practice reform. Few institutions, however, are planning to reduce their own size. By focusing health information technology and interoperability on the physician-patient relationship we bypass the inertia of institutions, fertilize the environment for value-based payment, and optimize care options among hospitals, the community, and home, as appropriate.

Blockchain is widely recognized for its ability to empower innovators and individuals on a large scale in an environment that includes the necessity of institutions. The appropriate application of blockchain technology to health IT can shift the balance to the physician-patient relationship. It’s hard to imagine a more effective lubricant for innovation in our complex privatized healthcare system.

References:


corresponding evidences in mobile devices, we construct a consortium blockchain framework, which is composed of a detecting consortium chain shared by test members and a public chain shared by users. Specifically, in view of different malware families in Android-based system, we perform feature modeling by utilizing statistical analysis method, so as to extract malware family features, including software package feature, permission and application feature, and function call feature. Moreover, for reducing false-positive rate and improving the detecting ability of malware variants, we design a multi-feature detection method of Android-based system for detecting and classifying malware. In addition, we establish a fact-base of distributed Android malicious codes by blockchain technology. The experimental results show that, compared with the previously published algorithms, the new proposed method can achieve higher detection accuracy in limited time with lower false-positive and false-negative rates.


Reference Type: Journal Article

Abstract: Electronic Health Records (EHRs) are entirely controlled by hospitals instead of patients, which complicates seeking medical advices from different hospitals. Patients face a critical need to focus on the details of their own healthcare and restore management of their own medical data. The rapid development of blockchain technology promotes population healthcare, including medical records as well as patient-related data. This technology provides patients with comprehensive, immutable records, and access to EHRs free from service providers and treatment websites. In this paper, to guarantee the validity of EHRs encapsulated in blockchain, we present an attribute-based signature scheme with multiple authorities, in which a patient endorses a message according to the attribute while disclosing no information other than the evidence that he has attested to it. Furthermore, there are multiple authorities without a trusted single or central one to generate and distribute public/private keys of the patient, which avoids the escrow problem and conforms to the mode of distributed data storage in the blockchain. By sharing the secret pseudorandom function seeds among authorities, this protocol resists collusion attack out of N from N-1 corrupted authorities. Under the assumption of the computational bilinear Diffie-Hellman, we also formally demonstrate that, in terms of the unforgeability and perfect privacy of the attribute-signer, this attribute-based signature scheme is secure in the random oracle model. The comparison shows the efficiency and properties between the proposed method and methods proposed in other studies.


Reference Type: Electronic Book
Abstract: [FIRST FEW PARAGRAPHS] Welcome to Blockchain For Dummies, 2nd IBM Limited Edition, your guide to all things blockchain for business. It’s been said that blockchain will do for transactions what the Internet did for information. What that means is that blockchain allows increased trust and efficiency in the exchange of almost anything.

Blockchain can profoundly change how the world works. If you’ve ever bought a house, you’ve probably had to sign a huge stack of papers from a variety of different stakeholders to make that transaction happen. If you’ve ever registered a vehicle, you likely understand how painful that process can be. I won’t even get started on how challenging it can be to track your medical records.

Blockchain—most simply defined as a shared, immutable ledger—has the potential to be the technology that redefines those processes and many others. To be clear, when I talk about blockchain, I’m not talking about Bitcoin. I’m talking about the underlying digital foundation that supports applications such as Bitcoin. But the reaches of blockchain extend far beyond Bitcoin.


Reference Type: Electronic Article
Abstract: How many startups have you discovered that promise to solve every outstanding computer science and informatics challenge with blockchain? As a Harvard Medical School Professor of Innovation, Beth Israel Deaconess Chief Information Officer, and mentor to several accelerators /incubators, I listen to startup pitches virtually every day. An increasing number of them sound like this: “We’ve got a cloud-hosted, big-data, machine learning, API-driven (application program interface) mobile app, with blockchain!”

Reference Type: Electronic Article
Abstract: To review blockchain lessons learned in 2018 and near-future predictions for blockchain in healthcare, Blockchain in Healthcare Today (BHTY) asked the world's blockchain in healthcare experts to share their insights. Here, our internationally-renowned BHTY peer-review board discusses their major predictions. Based on their responses, ten major themes for the future of blockchain in healthcare will emerge over the 12 months.


Reference Type: Electronic Article
Abstract: A vexing problem facing health care systems throughout the world is how to share more medical data with more stakeholders for more purposes, all while ensuring data integrity and protecting patient privacy.

Traditionally, the interoperability of medical data among institutions has followed three models: push, pull, and view (discussed below), each of which has its strengths and weaknesses. Blockchain offers a fourth model, which has the potential to enable secure lifetime medical record sharing across providers.


Reference Type: Report
Available from: https://www.weforum.org/whitepapers/inclusive-deployment-of-blockchain-for-supply-chains-part-3-public-or-private-blockchains-which-one-is-right-for-you

Abstract: For supply chain organizations launching new blockchain projects, one of the most fraught considerations typically is whether to use a public or private ledger and what permission models. This decision affects functionality, security, compatibility with other stakeholders’ systems and, perhaps most important, competitive positioning for companies. It is important that supply chain decisionmakers can sort through the marketing hype to pick the best solution for their particular requirements. This paper explores important considerations in making the public-versus-private decision and demystify elements of the public-versus-private debate. The findings in this paper were gleaned from research as well as detailed interviews with blockchain users across diverse industries, geographies and applications. This paper is the third in a series covering the cocreation of new tools for the responsible deployment of distributed ledger technology (DLT) in supply chains.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/10/2228

Abstract: With the rapid development of communication technologies, the Internet of Things (IoT) is getting out of its infancy, into full maturity, and tends to be developed in an explosively rapid way, with more and more data transmitted and processed. As a result, the ability to manage devices deployed worldwide has been given more and advanced requirements in practical application performances. Most existing IoT platforms are highly centralized architectures, which suffer from various technical limitations, such as a cyber-attack and single point of failure. A new solution direction is essential to enhance data accessing, while regulating it with government mandates in privacy and security. In this paper, we propose an integrated IoT platform using blockchain technology to guarantee sensing data integrity. The aim of this platform is to afford the device owner a practical application that provides a comprehensive, immutable log and allows easy access to their devices deployed in different domains. It also provides characteristics of general IoT systems, allows for real-time monitoring, and control between the end user and device. The business logic of the application is defined by the smart contract, which contains rules and conditions. The proposed approach is backed by a proof of concept implementation in realistic IoT scenarios, utilizing Raspberry Pi devices and a permissioned network called Hyperledger Fabric. Lastly,
a benchmark study using various performance metrics is made to highlight the significance of the proposed work. The analysis results indicate that the designed platform is suitable for the resource-constrained IoT architecture and is scalable to be extended in various IoT scenarios.


Reference Type: Electronic Article

Abstract: We present a mechanism that puts users in the center of control and empowers them to dictate the access to their collections of data. Revisiting the fundamental mechanisms in security for providing protection, our solution uses capabilities, access lists, and access rights following well-understood formal notions for reasoning about access. This contribution presents a practical, correct, auditable, transparent, distributed, and decentralized mechanism that is well-matched to the current emerging environments including Internet of Things, smart city, precision medicine, and autonomous cars. It is based on well-tested principles and practices used in distributed authorization, cryptocurrencies, and scalable computing.


Reference Type: Journal Article

Available from: https://www.jmir.org/2019/6/e13665/

Abstract: BACKGROUND: Distributed ledger technology (DLT) holds great potential to improve health information exchange. However, the immutable and transparent character of this technology may conflict with data privacy regulations and data processing best practices. OBJECTIVE: The aim of this paper is to develop a proof-of-concept system for immutable, interoperable, and General Data Protection Regulation (GDPR)-compliant exchange of blood glucose data. METHODS: Given that there is no ideal design for a DLT-based patient-provider data exchange solution, we proposed two different variations for our proof-of-concept system. One design was based purely on the public IOTA distributed ledger (a directed acyclic graph-based DLT) and the second used the same public IOTA ledger in combination with a private InterPlanetary File System (IPFS) cluster. Both designs were assessed according to (1) data reversal risk, (2) data linkability risks, (3) processing time, (4) file size compatibility, and (5) overall system complexity. RESULTS: The public IOTA design slightly increased the risk of personal data linkability, had an overall low processing time (requiring mean 6.1, SD 1.9 seconds to upload one blood glucose data sample into the DLT), and was relatively simple to implement. The combination of the public IOTA with a private IPFS cluster minimized both reversal and linkability risks, allowed for the exchange of large files (3 months of blood glucose data were uploaded into the DLT in mean 38.1, SD 13.4 seconds), but involved a relatively higher setup complexity. CONCLUSIONS: For the specific use case of blood glucose explored in this study, both designs presented a suitable performance in enabling the interoperable exchange of data between patients and providers. Additionally, both systems were designed considering the latest guidelines on personal data processing, thereby maximizing the alignment with recent GDPR requirements. For future works, these results suggest that the conflict between DLT and data privacy regulations can be addressed if careful considerations are made regarding the use case and the design of the data exchange system.


Reference Type: Journal Article


Abstract: Blockchain systems are a fast emerging and a currently widely discussed novel strategy for a decentralized cryptographically enhanced digital ledger recording transactions among stakeholders. This perspective paper looks at its potential uses in the context of high value and mostly low volume botanical material traded globally and used as medicines, health foods, in cosmetics and other applications. We offer a perspective on key areas in the supply of such products globally and how blockchain systems may help in sustainable sourcing, quality assurance, and in tackling supply problems in cases of complex multiherbal preparations. Both open and closed blockchain systems are feasible, and it seems likely that, at least in the initial development, closed ones are the main ones to be utilized. While blockchain’s potential is not yet clear, the examples presented here highlight the opportunities of this new technology.

Reference Type: Journal Article

Available from: http://oro.open.ac.uk/56264/

Abstract: Radicalism is to be found in the apparent attempt within the blockchain ecosystem to forge a linkage between a metaphysic of "the good" and the instrumental performativity inherent to contractual status.

* that this connection should be made by machines and software automatically and autonomously rather than as a precondition of human needs, rights and desires, thus skewing and intertwining the logic of "the good" and contract.

* regulating blockchain as it is defined here asks whether blockchain is a necessary technology in a given context versus alternative technologies or even, perhaps, whether the option of no technology at all is or might be the most appropriate response. "The goal of GDPR is to 'give citizens back the control of their personal data, whilst imposing strict rules on those hosting and 'processing' this data, anywhere in the world," says Van Humbeeck, and "one of the things GDPR states is that data 'should be erasable. Since throwing away your encryption keys is not the same as 'erasure of data', GDPR prohibits us from storing personal data on a blockchain level. Overcoming the Hype 43-51 (Inte Gloerich et al. eds., Institute of Network Cultures, 2018).

* as Lana Swartz has argued, the "incorporative blockchain" of back-office functions is no longer pursuing the libertarian dream of holistically remaking society, but is in fact quite "boring" (Swartz, Lana, Blockchain Dreams: Imagining Techno-economic Alternatives after Bitcoin, in Another Economy Is Possible, 96 (Manuel Castells, ed., Polity Press, 2017), in the sense that it has very quickly fallen into step with the needs and desires of big business.


Reference Type: Journal Article


Abstract: In the present techno-political moment it is clear that ignoring or dismissing the hype surrounding blockchain is unwise, and certainly for regulatory authorities and governments who must keep a grip on the technology and those promoting it, in order to ensure democratic accountability and regulatory legitimacy within the blockchain ecosystem and beyond. Blockchain is telling (and showing) us something very important about the evolution of capital and neoliberal economic reason, and the likely impact in the near future on forms and patterns of work, social organization, and, crucially, on communities and individuals who lack influence over the technologies and data that increasingly shape and control their lives. In this short essay I introduce some of the problems in the regulation of blockchain and offer counter-narratives aimed at cutting through the hype fueling the ascendency of this most contemporary of technologies.


Reference Type: Journal Article


Abstract: Healthcare complexity and costs can be decreased through the application of blockchain technology to medical records and insurance companies. Estonia has taken a leadership role in blockchain based services both in the commercial sector and in government. The Estonian government's innovation strategy was to create GovTech partnerships to implement blockchain based technologies throughout the country, and become a global leader in the technology. Starting in 2011, just 3 years after Satoshi Nakamoto published the first description of distributed ledgers and blockchain technology, the Estonian Government started partnering with the private technology startup company Guardtime to use blockchains to secure public and internal records. Then in 2016, Estonia once again reinforced its global leadership in blockchain technology when it announced it would use blockchain technology to secure the health records of over a million citizens. Estonia’s systematic method of applying blockchain technologies through GovTech partnerships demonstrates how innovation is a process. Estonia also identified early the value of the blockchain as a disruptive platform innovation. The application of blockchain technology to healthcare is a radical innovation given that nearly all previous applications have been in the financial and legal sectors.


Reference Type: Report
Abstract: Distributed ledger and blockchain technology promise to have far-reaching implications for global trade and supply chains. However, the extent to which this new technology realizes its potential depends upon how well supply chain actors steward this development. To that end, the World Economic Forum has convened a multi-stakeholder community to design a framework to guide decision-making towards inclusivity, interoperability, and integrity. This highlights the most pressing concerns of a wide group of supply-chain decision-makers with blockchain deployment. It is the starting point for a series of white papers and the framework.
application introduced in this article is technology that is capable of indicating the authenticity of digital media. Put simply, using the trust mechanisms of blockchain technology, the tool can show, beyond doubt, the provenance of any source of digital media, including images used out of context in attempts to mislead. Although the application is an early prototype and its capability to find fake resources is somewhat limited, we outline future improvements that would overcome such limitations. Furthermore, we believe that our application (and its use of blockchain technology and standardized metadata) introduces a novel approach to overcoming falsities in news reporting and the provenance of media resources used therein. However, while our application has the potential to be able to verify the originality of media resources, we believe that technology is only capable of providing a partial solution to fake news. That is because it is incapable of proving the authenticity of a news story as a whole. We believe that takes human skills.

Reference Type: Journal Article

Abstract: Nursing informatics as defined by the American Nurses Association is “the specialty that integrates nursing science, computer science, and information science to manage and communicate data, information, and knowledge in nursing practice” (Lippincott Solutions, 2016). Today, nursing informatics play an integral role in health care delivery and influencing health care information system features and functions (Murphy, 2010). By the end of 2020, there will be over 50 billion connected devices, all of which set the stage for millions of data transactions. As we move forward in this connected, digital first world, data are becoming a new kind of currency, or more specifically, we are moving into a data economy. In this new data economy, privacy, which is a fundamental human right, becomes increasingly difficult to maintain. With the Internet of Things, defined as “a network of physical and virtual objects, devices, or things that are capable of collecting surrounding data and exchanging it between them or through the internet” and applications such as wearable personal health trackers, consumers are becoming the center of their own personal care management (Sembroiz, Ricciardi, & Careglio, 2018, p. 215).

Privacy and security are foundational to the safety of health care data, especially given the epidemic of data breaches, generally, and health care data breaches, specifically. The latter have been traced to actors who have access to health records—so called insiders.

What then does this mean for nurses? Are we sufficiently engaged in discussions to support our patients? What aspects of the impact of this technology do we need to understand?

Reference Type: Journal Article

Abstract: Abstract The central theme of this paper is that the development of a technology that is predicted to have a major impact on the way we transact with each other should be a matter where the needs of society at large are taken into account. Where the technology is one that emerges from the domain of the Internet, inclusivity becomes even more acute in order to avoid widening the already existing gap in reaping the ?digital dividend.? With blockchain, the obligation could even be seen as a moral one, as blockchain is said to have the potential to negate the scope for the abuse of trust by states and institutions. This could be a game changer in areas such as public procurement and the conduct of elections where abuse can lead to the denial of essential resources and a concomitant loss of life, or to conflict and mass killings. Blockchain presents an opportunity for the Internet development community to claim a degree of recognition in the human rights realm by aiding civil intervention in areas where military intervention has been deemed inappropriate.

Reference Type: Journal Article

Abstract: The blockchain has received significant attention from technology focused researchers, highlighting its perceived impact and emerging disruption potential, but has been slow to engender any
significant momentum within the Information Systems (IS) and Information Management (IM) literature. This study approaches the subject through an IS/IM lens developing the key themes from the blockchain based research via a comprehensive review. This analysis of the body of literature highlights that although few commercial grade blockchain applications currently exist, the technology demonstrates significant potential to benefit a number of industry wide use cases. This study expands on this point articulating through each of the key themes to develop a detailed narrative on the numerous potential blockchain applications and future direction of the technology, whilst discussing the many barriers to adoption. The study asserts that blockchain technology has the potential to contribute to a number of the UN Sustainability Development Goals and engender widespread change within a number of established industries and practices.


Reference Type: Journal Article
Open access; http://www.sciencedirect.com/science/article/pii/S1389041718301177 Subscription required to view.

Abstract: The privacy of patients is jeopardised when medical records and data are spread or shared beyond the protected cloud of institutions. This is because breaches force them to the brink that they start abstaining from full disclosure of their condition. This type of condition has a negative effect on scientific research, patients and all stakeholders. A blockchain-based data sharing system is proposed to tackle this issue, which employs immutability and autonomy properties of the blockchain to sufficiently resolve challenges associated with access control and handle sensitive data. Our proposed system is supported by a Discrete Wavelet Transform to enhance the overall security, and a Genetic Algorithm technique to optimise the queuing optimization technique as well. Introducing this cryptographic key generator enhances the immunity and system access control, which allows verifying users securely in a fast way. This design allows further accountability since all users involved are already known and the blockchain records a log of their actions. Only when the users’ cryptographic keys and identities are confirmed, the system allows requesting data from the shared queuing requests. The achieved execution time per node, confirmation time per node and robust index for block number of 0.19s, 0.17s and 20 respectively that based on system evaluation illustrates that our system is robust, efficient, immune and scalable.


Reference Type: Journal Article

Abstract: Blockchain and blockchain-related technologies are being rapidly invented to the point that it is difficult to define specifically which properties are necessary to constitute a blockchain. It may therefore seem far too early to meaningfully discuss the creation of international blockchain standards. This article will argue the opposite by summarizing some existing international standards work related to blockchains and propose directions for additional standards development that could meaningfully be explored in the near future without negatively impacting additional invention.


Reference Type: Journal Article
Available from: http://www.jmir.org/2019/8/e13592/

Abstract: Background: Blockchain has the potential to disrupt the current modes of patient data access, accumulation, contribution, exchange, and control. Using interoperability standards, smart contracts, and cryptographic identities, patients can securely exchange data with providers and regulate access. The resulting comprehensive, longitudinal medical records can significantly improve the cost and quality of patient care for individuals and populations alike. Objective: This work presents HealthChain, a novel patient-centered blockchain framework. The intent is to bolster patient engagement, data curation, and regulated dissemination of accumulated information in a secure, interoperable environment. A mixed-block blockchain is proposed to support immutable logging and redactable patient blocks. Patient data are generated and exchanged through Health Level-7 Fast Healthcare Interoperability Resources, allowing seamless transfer with compliant systems. In addition, patients receive cryptographic identities
in the form of public and private key pairs. Public keys are stored in the blockchain and are suitable for securing and verifying transactions. Furthermore, the envisaged system uses proxy re-encryption (PRE) to share information through revocable, smart contracts, ensuring the preservation of privacy and confidentiality. Finally, several PRE improvements are offered to enhance performance and security.

Methods: The framework was formulated to address key barriers to blockchain adoption in health care, namely: information security, interoperability, data integrity, identity validation, and scalability. It supports 16 configurations through the manipulation of 4 modes. An open-source, proof-of-concept tool was developed to evaluate the performance of the novel patient block components and system configurations. To demonstrate the utility of the proposed framework and evaluate resource consumption, extensive testing was performed on each of the 16 configurations over a variety of scenarios involving a variable number of existing and imported records. Results: The results indicate several clear high-performing, low-bandwidth configurations, although they are not the strongest cryptographically. Of the strongest models, one’s anticipated cumulative record size is shown to influence the selection. Although the most efficient algorithm is ultimately user specific, Advanced Encryption Standard–encrypted data with static keys, incremental server storage, and no additional server-side encryption are the fastest and least bandwidth intensive, whereas proxy re-encrypted data with dynamic keys, incremental server storage, and additional server-side encryption are the best performing of the strongest configurations. Conclusions: Blockchain is a potent and viable technology for patient-centered access to and exchange of health information. By integrating a structured, interoperable design with patient-accumulated and generated data shared through smart contracts into a universally accessible blockchain, HealthChain presents patients and providers with access to consistent and comprehensive medical records. Challenges addressed include data security, interoperability, block storage, and patient-administered data access, with several configurations emerging for further consideration regarding speed and security.


Abstract: Contracts, transactions, and the records of them are among the defining structures in our economic, legal, and political systems. They protect assets and set organizational boundaries. They establish and verify identities and chronicle events. They govern interactions among nations, organizations, communities, and individuals. They guide managerial and social action. And yet these critical tools and the bureaucracies formed to manage them have not kept up with the economy’s digital transformation. They’re like a rush-hour gridlock trapping a Formula 1 race car. In a digital world, the way we regulate and maintain administrative control has to change.

Blockchain promises to solve this problem. The technology at the heart of bitcoin and other virtual currencies, blockchain is an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way. The ledger itself can also be programmed to trigger transactions automatically.


Abstract: In pursuing the storage point of view for blockchain technology, the test team has come up against a recurrent theme. This recurrent theme is that no new storage is needed for off-chain data as most companies are already using the data to be utilized by the blockchain. Because the companies are already using the data, it already exists somewhere in their storage environment and only needs to be referenced by the blockchain application programming interface (API). This paper examines this to see if it is valid.


Abstract: Background: Digital health technologies, including telemedicine, mobile health (mHealth), and remote monitoring, are playing a greater role in medical practice. Safe and accurate management of medical information leads to the advancement of digital health, which in turn results in a number of beneficial effects. Furthermore, mHealth can help lower costs by facilitating the delivery of care and connecting people to their health care providers. Mobile apps help empower patients and health care providers to proactively address medical conditions through near real-time monitoring and treatment,
regardless of the location of the patient or the health care provider. Additionally, mHealth data are stored in servers, and consequently, data management that prevents all forms of manipulation is crucial for both medical practice and clinical trials.

**Objective:** The aim of this study was to develop and evaluate a tamper-resistant mHealth system using blockchain technology, which enables trusted and auditable computing using a decentralized network. Methods: We developed an mHealth system for cognitive behavioral therapy for insomnia using a smartphone app. The volunteer data collected with the app were stored in JavaScript Object Notation format and sent to the blockchain network. Thereafter, we evaluated the tamper resistance of the data against the inconsistencies caused by artificial faults.

**Results:** Electronic medical records collected using smartphones were successfully sent to a private Hyperledger Fabric blockchain network. We verified the data update process under conditions where all the validating peers were running normally. The mHealth data were successfully updated under network faults. We further ensured that any electronic health record registered to the blockchain network was resistant to tampering and revision. The mHealth data update was compatible withtamper resistance in the blockchain network.

**Conclusions:** Blockchain serves as a tamperproof system for mHealth. Combining mHealth with blockchain technology may provide a novel solution that enables both accessibility and data transparency without a third party such as a contract research organization.


Reference Type: Journal Article

Available from: [https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204937](https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204937)

Abstract: Big data trends in biomedical and health research enable large-scale and multi-dimensional aggregation and analysis of heterogeneous data sources, which could ultimately result in preventive, diagnostic and therapeutic benefit. The methodological novelty and computational complexity of big data health research raises novel challenges for ethics review. In this study, we conducted a scoping review of the literature using five databases to identify and map the major challenges of health-related big data for Ethics Review Committees (ERCs) or analogous institutional review boards. A total of 1093 publications were initially identified, 263 of which were included in the final synthesis after abstract and full-text screening performed independently by two researchers. Both a descriptive numerical summary and a thematic analysis were performed on the full-texts of all articles included in the synthesis. Our findings suggest that while big data trends in biomedicine hold the potential for advancing clinical research, improving prevention and optimizing healthcare delivery, yet several epistemic, scientific and normative challenges need careful consideration. These challenges have relevance for both the composition of ERCs and the evaluation criteria that should be employed by ERC members when assessing the methodological and ethical viability of health-related big data studies. Based on this analysis, we provide some preliminary recommendations on how ERCs could adaptively respond to those challenges. This exploration is designed to synthesize useful information for researchers, ERCs and relevant institutional bodies involved in the conduction and/or assessment of health-related big data research.


Reference Type: Book Section

Available from: [https://smile.amazon.com/Digital-Health-Entrepreneurship-Informatics/dp/3030127184/ref=sr_1_1](https://smile.amazon.com/Digital-Health-Entrepreneurship-Informatics/dp/3030127184/ref=sr_1_1)

Abstract: A blockchain is a decentralized, distributed and tamper-proof cryptographic database most suitable for storing transaction information. It is maintained by multiple parties in a distributed fashion. Each record is timestamped, encrypted and linked to previous records.

Records are immutable, can only be added, never removed. Once added, a record can't be changed. Adding a record can only be done through a mechanism called consensus, where most or all parties maintaining the blockchain have to agree to adding it.

Since all records are cryptographically linked to previous records, if a party tries to manipulate previous records or maliciously add a new record, that action will break the overall consistency of the database and is easily detectable.


Reference Type: Government Document

Abstract: SECTION 1. PURPOSE
This notice describes how existing general tax principles apply to transactions using virtual currency. The notice provides this guidance in the form of answers to frequently asked questions.

SECTION 2. BACKGROUND
The Internal Revenue Service (IRS) is aware that “virtual currency” may be used to pay for goods or services, or held for investment. Virtual currency is a digital representation of value that functions as a medium of exchange, a unit of account, and/or a store of value. In some environments, it operates like “real” currency — i.e., the coin and paper money of the United States or of any other country that is designated as legal tender, circulates, and is customarily used and accepted as a medium of exchange in the country of issuance — but it does not have legal tender status in any jurisdiction.

SECTION 3. SCOPE
In general, the sale or exchange of convertible virtual currency, or the use of convertible virtual currency to pay for goods or services in a real-world economy transaction, has tax consequences that may result in a tax liability. This notice addresses only the U.S. federal tax consequences of transactions in, or transactions that use, convertible virtual currency, and the term “virtual currency” as used in Section 4 refers only to convertible virtual currency. No inference should be drawn with respect to virtual currencies not described in this notice.

Abstract: Trust in scientific research is diminished by evidence that data are being manipulated. Outcome switching, data dredging and selective publication are some of the problems that undermine the integrity of published research. Methods for using blockchain to provide proof of pre-specified endpoints in clinical trial protocols were first reported by Carlisle. We wished to empirically test such an approach using a clinical trial protocol where outcome switching has previously been reported. Here we confirm the use of blockchain as a low cost, independently verifiable method to audit and confirm the reliability of scientific studies.

Editorial note:
Concerns have been raised about the overlap between Version 1 of this article and a previously published blog by Carlisle, who proposed the method 2 years earlier [Carlisle, Benjamin Gregory. “Proof of prespecified endpoints in medical research with the bitcoin blockchain”, 25 August 2014], and that the correction (Version 2) published soon after the original was not sufficient to rectify the overlap.

The case has since been discussed in a Committee of Publication Ethics (COPE) Forum, and COPE advised that the correction was sufficient to correct the scientific literature.

The case has been referred to the University of Cambridge for consideration.


Reference Type: Journal Article

Abstract: In modern e-Healthcare systems, human activity recognition (HAR) is one of the most challenging tasks in remote monitoring of patients suffering from mental illness or disabilities for necessary assistance. One of the major issues is to provide security to a number of different connected devices to the Internet, known as Internet of Things (IoT). A potential solution to this problem is the blockchain-based architecture. In addition, the complex nature of activities performed by humans in diverse healthcare environments reduces the qualitative measures for extracting distinct features representing various human actions. To answer this challenge, we propose an activity monitoring and
recognition framework, which is based on multi-class cooperative categorization procedure to improve the activity classification accuracy in videos supporting the fog or cloud computing-based blockchain architecture. In the proposed approach, frame-based salient features are extracted from videos consisting of different human activities, which are further processed into action vocabulary for efficiency and accuracy. Similarly, the classification of activities is performed using support vector machine (SVM) based on the error-correction-output-codes (ECOC) framework. It has been observed through experimental results that the proposed approach is more efficient and achieves higher accuracy regarding human activity recognition as compared to other state-of-the-art action recognition approaches.

---

Ivan D. Blockchain-based method for secure storage of patient records. ONC/NIST Use of Blockchain for Healthcare and Research Workshop; 2016 Sep 26-27; Gaithersburg, MD. National Institute of Standards Technology.

Reference Type: Conference Proceedings

Abstract: Today's methods of recording and sharing patient data have a number of limitations that restrict patients' access to their clinical records, reduce availability of essential data to care providers, and ultimately present a barrier to transforming U.S. healthcare into a learning health system. Storing patient healthcare data in a blockchain-based storage scheme can remediate these shortcomings. This paper discusses blockchain as a novel approach to secure health data storage, implementation obstacles, and a plan for transitioning incrementally from current technology to a blockchain solution.

---


Reference Type: Magazine Article
Available from: https://universitybusiness.com/college-transcripts-transformed

Abstract: Every week at the University of Washington in Seattle, the registrar’s office staff comes across at least three fraudulent diplomas. Every month, they uncover about two fraudulent transcripts. “And these are just the ones we see,” says Helen Garrett, registrar and chief officer for enrollment information services. “Our student database has not been hacked and is secure, but people pretend to have UW credentials who never attended or graduated from the university, and they try to pass doctored diplomas by employers, when applying for scholarships or grants, and even when applying to academic programs.”

U.S.-based colleges and universities rely on transcripts to prove a student attended or graduated, and international institutions rely on diplomas. Both types of documents, frequently requested by former students seeking a job or additional academic credentials, are not easily copied. They are also difficult to obtain, often requiring former students to remember an old ID number or portal access code, and typically take three to five days to process.

Growing numbers of institutions want to revamp this antiquated process to provide academic credentials more quickly and securely with blockchain. The technology, which underlies bitcoin virtual currency, is a bookkeeping method that “chains” together entries so they’re difficult to modify later. It allows large groups of unrelated organizations—including colleges and universities—to keep a secure, common record.

Steps to blockchain adoption involve understanding the work required to make the switch, how the technology will improve service for students seeking academic records, and how it could disrupt the register’s office status quo.

---


Reference Type: Report

Abstract: We are living in a world that is rapidly undergoing a fundamental change, it is becoming driven by data. This transformation is about all societal systems: traffic, health, government, logistics, and defense; being more quantified and efficient, but also more transparent and accountable. This changes not only the economics of systems, but their management as well. It also blurs the lines between customer, citizen, company, and government. Everyone gets to see what is happening, and so everyone gets to have a role in shaping these new systems. As a consequence, businesses and governments are struggling to understand what the changing landscape means and how they can participate. In this paper, I discusses the state of the art in Blockchain technology and its applications, focusing on
applications and solutions in identity management


Reference Type: Report

Abstract: Blockchain is currently being tested by industry, but at this time does not appear to be a complete replacement for existing systems. Although the adoption of blockchain is in its early stages, Congress may have a role to play in several areas, including the oversight of federal agencies seeking to use blockchain for government business, and exploration of whether regulations are necessary to govern blockchain’s use in the private sector.

Some federal agencies are seeking to better manage identities, assets, data, and contracts through the adoption of blockchain technology. In addition, some federal agencies are issuing guidance on industry use of blockchain, and whether or not the current legal framework governs blockchain use.


Reference Type: Report

Abstract: Blockchain is an emerging technology that has the potential to disrupt many industries and businesses. It provides transaction consensus, provenance, immutability, and finality in a so-called decentralized economy and society. It disrupts the traditional concepts of trust, ownership, and trade and, consequently, internet and business transactions.

Like cloud computing, blockchain can be public, private, or permissioned—a type of private blockchain where anonymous or named authorized participants verify transactions. This report focuses on permissioned distributed ledger technologies.

Technology Evaluation Centers Principal Analyst PJ Jakovljevic explains blockchain technology, identifies the players, discusses its use cases, and speculates about blockchain’s future.


Reference Type: Report

Abstract: Global supply chains involve numerous organizations and transactions and are becoming increasingly digital. At the core of each of these digital transactions are trust-based interactions with partners. As such, organizations need a comprehensive system for the verification and management of digital business identities that is both dynamic and trustworthy – but current digital identity management systems are costly, inefficient, and may not be sustainable. This white paper lays out foundations for such a system, exploring considerations, proposed principles and recommendations for supply-chain organizations and governments in managing the growing complexity of the digital identities involved in global trade. The paper also introduces and investigates the possibilities enabled by a digital Global Trade Identity (GTID) for legal entities participating in global supply chains – a necessary step in digitizing global trade.


Reference Type: Journal Article

Abstract: The sharing of patients’ locations is an important part in mobile medical services and modern
smart healthcare. Although location sharing based on blockchains has advantages on decentralization and openness, there is also a challenge to guarantee the security and the privacy of locations recorded in a blockchain. To this end, this paper investigates the location sharing based on blockchains for telecare medical information systems. Firstly, we define the basic requirements of blockchain-based location sharing including decentralization, unforgeability, confidentiality, multi-level privacy protection, retrievability and verifiability. Then, using order-preserving encryption and merkle tree, we propose a blockchain-based multi-level location sharing scheme, i.e. BMPLS. The analysis results show that our scheme satisfies the above requirements. Finally, the performance of our scheme is evaluated and the experiment results show that our scheme is efficient and feasible for both patients and medical workers. In a word, our scheme can be applied to realize privacy-preserving location sharing based on blockchains for telecare medical information systems.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/18/11/3894

Abstract: Crowd sensing is a perception mode that recruits mobile device users to complete tasks such as data collection and cloud computing. For the cloud computing platform, crowd sensing can not only enable users to collaborate to complete large-scale awareness tasks but also provide users for types, social attributes, and other information for the cloud platform. In order to improve the effectiveness of crowd sensing, many incentive mechanisms have been proposed. Common incentives are monetary reward, entertainment & gamification, social relation, and virtual credit. However, there are rare incentives based on privacy protection basically. In this paper, we proposed a mixed incentive mechanism which combined privacy protection and virtual credit called a blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Its network structure can be divided into three parts which are intelligence crowd sensing networks, confusion mechanism, and blockchain. We conducted the experiments in the campus environment and the results shows that the incentive mechanism proposed in this paper has the efficacious effect in stimulating user participation.


Reference Type: Journal Article

Abstract: Blockchain-based distributed storage enables users to share data without the help of a centralized service provider. Decentralization eliminates traditional data loss brought by compromising the provider, but incurs the possible privacy leakage in a way that the supplier directly links the retrieved data to its ciphertext. Oblivious keyword search (OKS) has been regarded as a solution to this issue. OKS allows a user to retrieve the data associated with a chosen keyword in an oblivious way. That is, the chosen keyword and the corresponding ciphertext are unknown to the data supplier. But if the retrieval privilege is with an authorized keyword set, OKS is unavailable due to one-keyword restriction and public key encryption with keyword search (PEKS) might lead to high bandwidth consumption. In this paper, we introduce Searchain, a blockchain-based keyword search system. It enables oblivious search over an authorized keyword set in the decentralized storage. Searchain is built on top of a novel primitive called oblivious keyword search with authorization (OKSA), which provides the guarantee of keyword authorization besides oblivious search. We instantiate a provably secure OKSA scheme, featured with one-round interaction and constant size communication cost in the transfer phase. We apply OKSA and ordered multisignatures (OMS) to present a Searchain protocol, which achieves oblivious peer-to-peer retrieval with order-preserving transaction. The analysis and evaluation show that Searchain maintains reasonable cost without loss of retrieval privacy, and hence guarantees its practicality.


Reference Type: Conference Paper
Abstract: Nowadays, a great number of healthcare data are generated every day from both medical institutions and individuals. Healthcare information exchange (HIE) has been proved to benefit the medical industry remarkably. To store and share such large amount of healthcare data is important while challenging. In this paper, we propose BlocHIE, a Blockchain-based platform for healthcare information exchange. First, we analyze the different requirements for sharing healthcare data from different sources. Based on the analysis, we employ two loosely-coupled Blockchains to handle different kinds of healthcare data. Second, we combine off-chain storage and on-chain verification to satisfy the requirements of both privacy and authenticability. Third, we propose two fairness-based packing algorithms to improve the system throughput and the fairness among users jointly. To demonstrate the practicability and effectiveness of BlocHIE, we implement BlocHIE in a minimal-viable-product way and evaluate the proposed packing algorithms extensively.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/9/2042

Abstract: With the rapid development of the internet of things (IoT), traditional industries are setting off a massive wave of digitization. In the era of the Internet of Everything, millions of devices and links in IoT pose more significant challenges to data management. Most existing solutions employ centralized systems to control IoT devices, which brings about the privacy and security issues in IoT data management. Recently, blockchain has attracted much attention in the field of IoT due to its decentralization, traceability, and non-tamperability. However, it is non-trivial to apply the current blockchain techniques to IoT due to the lack of scalability and high resource costs. Different blockchain platforms have their particular advantages in the scenario of IoT data management. In this paper, we propose a cross-chain framework to integrate multiple blockchains for efficient and secure IoT data management. Our solution builds an interactive decentralized access model which employs a consortium blockchain as the control station. Other blockchain platforms customized for specific IoT scenarios run as the backbone of all IoT devices. It is equivalent to opening the off-chain channels on the consortium blockchain. Our model merges transactions in these channels for confirmation based on the notary mechanism. Finally, we implement a prototype of the proposed model based on Hyperledger Fabric and IOTA Tangle. We evaluate the performance of our method through extensive experiments. The results demonstrate the effectiveness and efficiency of our framework.


Reference Type: Journal Article

Abstract: In the digital healthcare era, it is of the utmost importance to harness medical information scattered across healthcare institutions to support in-depth data analysis and achieve personalized healthcare. However, the cyberinfrastructure boundaries of healthcare organizations and privacy leakage threaten place obstacles on the sharing of medical records. Blockchain, as a public ledger characterized by its transparency, tamper-evidence, trustlessness, and decentralization, can help build a secure medical data exchange network. This paper surveys the state-of-the-art schemes on secure and privacy-preserving medical data sharing of the past decade with a focus on blockchain-based approaches. We classify them into permissionless blockchain-based approaches and permissioned blockchain-based approaches and analyze their advantages and disadvantages. We also discuss potential research topics on blockchain-based medical data sharing.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/18/12/4268

Abstract: The Internet-of-things (IoT) and blockchain are growing realities of modern society, and both are rapidly transforming civilization, either separately or in combination. However, the leverage of both technologies for structural health monitoring (SHM) to enable transparent information sharing among involved parties and autonomous decision making has not yet been achieved. Therefore, this study combines IoT with blockchain-based smart contracts for SHM of underground structures to define a novel, efficient, scalable, and secure distributed network for enhancing operational safety. In this blockchain-IoT network, the characteristics of locally centralized and globally decentralized distribution have been activated by dividing them into core and edge networks. This division enhances the efficiency and scalability of the system. The proposed system was effective in simulation for autonomous
monitoring and control of structures. After proper design, the decentralized blockchain networks may effectively be deployed for transparent and efficient information sharing, smart contracts-based autonomous decision making, and data security in SHM.


Reference Type: Journal Article

Available from: https://www.karger.com/Article/FullText/501643

Abstract: BACKGROUND: Biomedical research has recently moved through three stages in digital healthcare: (1) data collection; (2) data sharing; and (3) data analytics. With the explosion of stored health data (HD), dental medicine is edging into its fourth stage of digitization using artificial intelligence (AI). This narrative literature review outlines the challenge of managing HD and anticipating the potential of AI in oral healthcare and dental research by summarizing the current literature. SUMMARY: The basis of successful management of HD is the establishment of a generally accepted data standard that will guide its implementation within electronic health records (EHR) and health information technology ecosystems (HIT Eco). Thereby continuously adapted (self-) learning health systems (LHS) can be created. The HIT Eco of the future will combine (i) the front-end utilization of HD in clinical decision-making by providers using supportive diagnostic tools for patient-centered treatment planning, and (ii) back-end algorithms analyzing the standardized collected data to inform population-based policy decisions about resource allocations and research directions. Cryptographic methods in blockchain enable a safe, more efficient, and effective dental care within a global perspective. Key Message: The interoperability of HD with accessible digital health technologies is the key to deliver value-based dental care and exploit the tremendous potential of AI.


Reference Type: Journal Article

Available from: https://www.jmir.org/2019/8/e13600/

Abstract: BACKGROUND: The protection of private data is a key responsibility for research studies that collect identifiable information from study participants. Limiting the scope of data collection and preventing secondary use of the data are effective strategies for managing these risks. An ideal framework for data collection would incorporate feature engineering, a process where secondary features are derived from sensitive raw data in a secure environment without a trusted third party. OBJECTIVE: This study aimed to compare current approaches based on how they maintain data privacy and the practicality of their implementations. These approaches include traditional approaches that rely on trusted third parties and cryptographic, secure hardware, and blockchain-based techniques. METHODS: A set of properties were defined for evaluating each approach. A qualitative comparison was presented based on these properties. The evaluation of each approach was framed with a use case of sharing geolocation data for biomedical research. RESULTS: We found that approaches that rely on a trusted third party for preserving participant privacy do not provide sufficiently strong guarantees that sensitive data will not be exposed in modern data ecosystems. Cryptographic techniques incorporate strong privacy-preserving paradigms but are appropriate only for select use cases or are currently limited because of computational complexity. Blockchain smart contracts alone are insufficient to provide data privacy because transactional data are public. Trusted execution environments (TEEs) may have hardware vulnerabilities and lack visibility into how data are processed. Hybrid approaches combining blockchain and cryptographic techniques or blockchain and TEEs provide promising frameworks for privacy preservation. For reference, we provide a software implementation where users can privately share features of their geolocation data using the hybrid approach combining blockchain with TEEs as a supplement. CONCLUSIONS: Blockchain technology and smart contracts enable the development of new privacy-preserving feature engineering methods by obviating dependence on trusted parties and providing immutable, auditable data processing workflows. The overlap between blockchain and cryptographic techniques or blockchain and secure hardware technologies are promising fields for addressing important data privacy needs. Hybrid blockchain and TEE frameworks currently provide practical tools for implementing experimental privacy-preserving applications.


Reference Type: Journal Article

Available from: https://www.mdpi.com/2410-387X/3/1/7

Abstract: An essential requirement of any information management system is to protect data and
resources against breach or improper modifications, while at the same time ensuring data access to legitimate users. Systems handling personal data are mandated to track its flow to comply with data protection regulations. We have built a novel framework that integrates semantically rich data privacy knowledge graph with Hyperledger Fabric blockchain technology, to develop an automated access-control and audit mechanism that enforces users' data privacy policies while sharing their data with third parties. Our blockchain-based data-sharing solution addresses two of the most critical challenges: transaction verification and permissioned data obfuscation. Our solution ensures accountability for data sharing in the cloud by incorporating a secure and efficient system for End-to-End provenance. In this paper, we describe this framework along with the comprehensive semantically rich knowledge graph that we have developed to capture rules embedded in data privacy policy documents. Our framework can be used by organizations to automate compliance of their Cloud datasets.


Reference Type: Journal Article
Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0207000

Abstract: Bitcoin is a digital currency and electronic payment system operating over a peer-to-peer network on the Internet. One of its most important properties is the high level of anonymity it provides for its users. The users are identified by their Bitcoin addresses, which are random strings in the public records of transactions, the blockchain. When a user initiates a Bitcoin transaction, his Bitcoin client program relays messages to other clients through the Bitcoin network. Monitoring the propagation of these messages and analyzing them carefully reveal hidden relations. In this paper, we develop a mathematical model using a probabilistic approach to link Bitcoin addresses and transactions to the originator IP address. To utilize our model, we carried out experiments by installing more than a hundred modified Bitcoin clients distributed in the network to observe as many messages as possible. During a two month observation period we were able to identify several thousand Bitcoin clients and bind their transactions to geographical locations.


Reference Type: Conference Paper

Abstract: Stacked Denoising Autoencoders (SDA) are deep networks which have gained popularity owing to their superior performance in image classification applications, but they haven't been used much in healthcare applications. SDA can be efficiently retrained to adapt to large streams of data, and this property is used in this work to develop a technique for classification of arrhythmias in a patient-specific manner. This approach is particularly useful in continuous remote systems because they gather large amounts of data for longer periods of time. Blockchain is a decentralized distributed ledger which secures transactions with cryptography. It is proposed as an access control manager to securely store and access data required by the classifier during retraining in real-time from an external data storage. This work uses MIT-BIH Arrhythmia database and the results show an increased accuracy for Ventricular Ectopic Beats (VEB) (99.15%) and Supraventricular Ectopic Beats (SVEB) (98.55%), which is higher than the published results of deep networks that are not retrained.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/10/2310

Abstract: The existing LTE mobile system uses the vertical model to handle the session-based security management. However, the goal of this paper is to propose a packet key-based security management scheme on the blockchain control plane to enhance the existing session key-based security scheme and overcome the limitation that the existing vertical model, as well as the Software-Defined Networking (SDN) based horizontal model, confronts within solving end-to-end security management. The proposed blockchain-based security management (BSM) scheme enables each peer to easily obtain the necessary parameters required to manage the packet key-based security system. The important features of the BSM scheme include the renewal process, which enables the different packet data streams to use completely different security parameters for the security management. In addition, because even blind values cannot be exposed to the possible attackers, our BSM scheme guarantees very secure end-to-
end data transfer against active attacks such as falsification of data and transactions. Finally, this paper compares the BSM scheme with the existing vertical model to prove the advantageous effects on latency.


Reference Type: Magazine Article

Available from: https://www.chronicle.com/article/Will-Blockchain-Revolutionize/245073

Abstract: Since the 1990s, some academic netizens have predicted that open access will upend scholarly journal publishing, yet an oligopoly still dominates the $25-billion industry.

Orvium, a European start-up, recently joined those taking on the giant players. It offers a publishing and business plan based on blockchain — a coding structure that embeds origins and changes within a file. The format will allow for open-access or other licensing models to be determined by each client journal’s editors. The company’s ultimate objective is "to be the leading publication platform for the research community while returning the benefits of science to society."

Manuel Martin, Orvium’s 38-year-old CEO and cofounder, said in a phone interview from Geneva that the company is in a period of beta testing and should be operational in 2019. A data scientist who has worked with CERN and NASA, Martin, who was born in Spain, said that he and his fellow cofounders, Antonio Romero and Roberto Rabasco, started the company to make journal publishing cheaper, faster, and more transparent.

Skeptics acknowledge blockchain’s potential for greater transparency but doubt that it will be faster or cheaper than other platforms that include article preprints. They question Orvium’s intent to lift anonymity from article reviewers. They are dubious, too, about elements of the business plan and point to a history of would-be publishing disruptors being bought up by the very companies they planned to compete with.


Reference Type: Journal Article


Abstract: Blockchain is on the verge of revolutionizing how we interact in the digital world. It has far reaching applications from the Financial industry to many other sectors of the economy. The question is what is Blockchain, what are the underlying concepts, what is the current state of technological implementation and the current state of its regulatory landscape. While the answers to these questions take multiple volumes of articles by a vast array of experts in numerous related fields, in this article we will address these questions and provide some basic answers. For those active in the general Blockchain and Digital currency space, from the academic, technology, industry, legal or other points of view, it is important to have a broad overview of the space in general.

We provide a general description of Distributed Ledger Technology, Blockchains, Blockchain Technology and Digital Currencies, discuss the associated basic concepts and definitions and the interplay between these concepts. We discuss Blockchain Technical Concepts and infrastructure Implementations, their tradeoffs, benefits, limitations and metrics by which the performance these implementations are measured. We also address the concept of Permissioned Blockchains. In addition we discuss a number of practical applications of Blockchains beyond the financial industry applications.


Reference Type: Journal Article


Abstract: Blockchain technology is often discussed and theorized in relation to cryptocurrencies such as Bitcoin. Its quality as a technology that produces advanced encryption keys between objects, however, also makes it interesting to those who seek to connect physical objects to digital elements. The reason for this is that the link between objects needs to be ‘secure’ from undesired external interference. In relation to such interests, blockchain has been identified as a highly attractive technology to support the general digitalization of society towards the Internet of Things, smart cities etc. In extension, the implementation of blockchain technology implies that it may work as a tool that has the capacity to direct which objects may/may not interact with each other. The ‘ledger of everything’ that blockchain may possibly produce as regards the ‘Internet of Everything’ is even suggested to make humans and other
intermediary technologies redundant. In this essay, I argue that in order to sustain legal critique when the world moves into the next era of digitalization, we need to understand - and question - how technological control operates through e.g. blockchain technology by locking physical and digital elements to each other.


Reference Type: Journal Article


Abstract: In response to food contamination scandals worldwide, retail giant Walmart is tackling food safety in the supply chain using blockchain technology. In 2016, it established the Walmart Food Safety Collaboration Center in Beijing and plans to invest $25 million over five years to research global food safety (Yiannas and Liu, 2017). Using IBM’s blockchain solution based on Hyperledger Fabric, Walmart has successfully completed two blockchain pilots: pork in China and mangoes in the Americas (IBM, 2017). With a farm-to-table approach, Walmart’s blockchain solution reduced time for tracking mango origins from seven days to 2.2 seconds and promoted greater transparency across Walmart’s food supply chain (Yiannas, 2017). IBM called it “complete end-to-end traceability” (McDermott, 2017). This case study highlights the challenges of implementing blockchain technology in the food supply chain and the opportunities for deploying blockchain solutions throughout the global food ecosystem to increase safety and reduce waste.


Reference Type: Conference Paper


Abstract: The burden of disease is higher by far in developing countries than in the developed world. Developing countries today are turning to technology as the silver bullet or remedy. Indeed, Information and Communication Technology has turned into a key-enabling tool in the enhanced healthcare management. The electronic health records or electronic medical records (EMR) a key component of medical informatics symbolize potential solutions for enhanced healthcare. However, interoperability and security of EMR systems has been the two main challenges of EMR in the healthcare industry. By analyzing existing literature using scoping review research approach this paper explored the potential use of blockchain technology in improving the interoperability and security of EMR systems for the benefit of different stakeholders in health sector in developing countries such as Kenya. To achieve our main objective, five databases were searched and 204 papers screened for inclusion. As a result of the search and screen process, we identified 25 relevant articles.


Reference Type: Journal Article


Abstract: The moulding together of artificial intelligence (AI) and the geographic/geographic information systems (GIS) dimension creates GeoAI. There is an emerging role for GeoAI in health and healthcare, as location is an integral part of both population and individual health. This article provides an overview of GeoAI technologies (methods, tools and software), and their current and potential applications in several disciplines within public health, precision medicine, and Internet of Things-powered smart healthy cities. The potential challenges currently facing GeoAI research and applications in health and healthcare are also briefly discussed.


Reference Type: Journal Article

Abstract: A PubMed query run in June 2018 using the keyword 'blockchain' retrieved 40 indexed papers, a reflection of the growing interest in blockchain among the medical and healthcare research and practice communities. Blockchain's foundations of decentralisation, cryptographic security and immutability make it a strong contender in reshaping the healthcare landscape worldwide. Blockchain solutions are currently being explored for: (1) securing patient and provider identities; (2) managing pharmaceutical and medical device supply chains; (3) clinical research and data monetisation; (4) medical fraud detection; (5) public health surveillance; (6) enabling truly public and open geo-tagged data; (7) powering many Internet of Things-connected autonomous devices, wearables, drones and vehicles, via the distributed peer-to-peer apps they run, to deliver the full vision of smart healthy cities and regions; and (8) blockchain-enabled augmented reality in crisis mapping and recovery scenarios, including mechanisms for validating, crediting and rewarding crowdsourced geo-tagged data, among other emerging use cases. Geospatially-enabled blockchain solutions exist today that use a crypto-spatial coordinate system to add an immutable spatial context that regular blockchains lack. These geospatial blockchains do not just record an entry's specific time, but also require and validate its associated proof of location, allowing accurate spatiotemporal mapping of physical world events. Blockchain and distributed ledger technology face similar challenges as any other technology threatening to disintermediate legacy processes and commercial interests, namely the challenges of blockchain interoperability, security and privacy, as well as the need to find suitable and sustainable business models of implementation. Nevertheless, we expect blockchain technologies to get increasingly powerful and robust, as they become coupled with artificial intelligence (AI) in various real-world healthcare solutions involving AI-mediated data exchange on blockchains.


Abstract: Synergistic integration of the Internet of Things (IoT), cloud computing, and big data technologies in healthcare have led to the notion of "smart health." Smart health is an emerging concept that refers to the provision of healthcare services for prevention, diagnosis, treatment, and follow-up management at any time or any place by connecting information technologies and healthcare. As a significant breakthrough in smart healthcare development, IoT-enabled smart devices allow medical centers to carry out preventive care, diagnosis, and treatment more competently. This review focuses on recently developed patient health monitoring platforms based on IoT-enabled smart devices that can collect real-time patient data and transfer information for assessment by healthcare providers, including doctors, hospitals, and clinics, or for self-management. We aimed to summarize the available information about recently approved devices and state-of-the-art developments through a comprehensive, systematic literature review. In this review, we also discuss possible future directions for the integration of cloud computing and blockchain, which may offer unprecedented breakthroughs in on-demand medical services. The combination of IoT with real-time, remote patient monitoring empowers patients to assert more control over their care, thereby allowing them to actively monitor their particular health conditions.


Abstract: The blockchain emerged as a novel distributed consensus scheme that allows transactions, and any other data, to be securely stored and verified without the need of any centralized authority. Distributed trust and therefore security and privacy are at the core of the blockchain technologies, and have the potential to either make them a success or cause them to fail. This special issue of IEEE Security & Privacy is an attempt to collect the most interesting ideas from the community of researchers and professionals working on blockchain security and privacy.


Abstract: The healthcare data is an important asset and rich source of healthcare intellect. Medical databases, if created properly, will be large, complex, heterogeneous and time varying. The main challenge nowadays is to store and process this data efficiently so that it can benefit humans.
Heterogeneity in the healthcare sector in the form of medical data is also considered to be one of the biggest challenges for researchers. Sometimes, this data is referred to as large-scale data or big data. Blockchain technology and the Cloud environment have proved their usability separately, though these two technologies can be combined to enhance the exciting applications in healthcare industry. Blockchain is a highly secure and decentralized networking platform of multiple computers called nodes. It is changing the way medical information is being stored and shared. It makes the work easier, keeps an eye on the security and accuracy of the data and also reduces the cost of maintenance. A Blockchain-based platform is proposed that can be used for storing and managing electronic medical records in a Cloud environment.


Reference Type: Journal Article


Abstract: In recent years, the Edge computing paradigm has gained considerable popularity in academic and industrial circles. It serves as a key enabler for many future technologies like 5G, Internet of Things (IoT), augmented reality and vehicle-to-vehicle communications by connecting cloud computing facilities and services to the end users. The Edge computing paradigm provides low latency, mobility, and location awareness support to delay-sensitive applications. Significant research has been carried out in the area of Edge computing, which is reviewed in terms of latest developments such as Mobile Edge Computing, Cloudlet, and Fog computing, resulting in providing researchers with more insight into the existing solutions and future applications. This article is meant to serve as a comprehensive survey of recent advancements in Edge computing highlighting the core applications. It also discusses the importance of Edge computing in real life scenarios where response time constitutes the fundamental requirement for many applications. The article concludes with identifying the requirements and discuss open research challenges in Edge computing.


Reference Type: Conference Proceedings


Abstract: Wireless body area network (WBAN) has shown great potential in improving healthcare quality not only for patients but also for medical staff. However, security and privacy are still an important issue in WBANs especially in multi-hop architectures. In this paper, we propose and present the design and the evaluation of a secure lightweight and energy efficient authentication scheme BANZKP based on an efficient cryptographic protocol, Zero Knowledge Proof (ZKP) and a commitment scheme. ZKP is used to confirm the identity of the sensor nodes, with small computational requirement, which is favorable for body sensors given their limited resources, while the commitment scheme is used to deal with replay attacks and hence the injection attacks by committing a message and revealing the key later. BANZKP reduces the memory requirement by 56.13% compared to TinyZKP [16], the comparable alternative so far for Body Area Networks. Also, the simulation results demonstrate that our proposed scheme is 17 and 5 times more efficient in term of execution time, and uses 94.11% and 80% less energy compared to TinyZKP and W-ECDSA [25], respectively.


Reference Type: Journal Article

Available from: https://www.mdpi.com/2076-3417/9/9/1736

Abstract: One of the most important discoveries and creative developments that is playing a vital role in the professional world today is blockchain technology. Blockchain technology moves in the direction of persistent revolution and change. It is a chain of blocks that covers information and maintains trust between individuals no matter how far they are. In the last couple of years, the upsurge in blockchain technology has obliged scholars and specialists to scrutinize new ways to apply blockchain technology with a wide range of domains. The dramatic increase in blockchain technology has provided many new application opportunities, including healthcare applications. This survey provides a comprehensive review of emerging blockchain-based healthcare technologies and related applications. In this inquiry, we call attention to the open research matters in this fast-growing field, explaining them in some details. We also show the potential of blockchain technology in revolutionizing healthcare industry.

Reference Type: Electronic Article

Abstract: One of the most important discoveries and creative developments that is playing a vital role in the professional world today is blockchain technology. Blockchain technology moves in the direction of persistent revolution and change. It is a chain of blocks that covers information and maintains trust between individuals no matter how far they are. In the last couple of years, the upsurge in blockchain technology has obliged scholars and specialists to scrutinize new ways to apply blockchain technology with a wide range of domains. The dramatic increase in blockchain technology has provided many new application opportunities, including healthcare applications. This survey provides a comprehensive review of emerging blockchain-based healthcare technologies and related applications. In this inquiry, we call attention to the open research matters in this fast-growing field, explaining them in some details. We also show the potential of blockchain technology in revolutionizing healthcare industry.


Reference Type: Journal Article

Available from: https://www.researchprotocols.org/2019/3/e10654/

Abstract: More than 500,000 people experience homelessness in America each day. Local and federal solutions to the problem have had limited success because of the fragmentation of services and lack of valid and timely information. Billions of dollars spent to provide reliable, timely, and actionable information in health care have exposed the difficulty of establishing such a system using the prevalent information technology solutions. However, relying on successful examples of the use of blockchain to help refugee populations and poor farmers internationally, we have partnered to propose an innovative solution to this problem using the case of people experiencing homelessness in Austin, Texas. This paper aims to describe one of the first applications of blockchain technology for addressing homelessness in the United States by creating a digital identity for people experiencing homelessness and engaging emergency medical services and clinical providers. The authors argue that a lack of documentation to prove personal identity and the inability to access own records are major hurdles for empowering persons experiencing homelessness to be resilient and overcome the life challenges they face. Furthermore, it is argued that this lack of information causes misdiagnosis, duplication, and fragmentation in service delivery, which can be potentially addressed by blockchain technology. Further planning for creating a program on the ground with additional funding will demonstrate the results of using blockchain technology to establish digital identity for persons experiencing homelessness.


Reference Type: Electronic Article

Abstract: * Blockchains radically shift the economics of providing transactional assurances. * Blockchain proof of title, custody, and transaction history reduces the need to rely on external assurances. * This opens economic potential wherever there was previously a lack of reliable legal infrastructure.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/13/3028

Abstract: Smart grids incorporating internet-of-things are emerging solutions to provide a reliable, sustainable and efficient electricity supply, and electric vehicle drivers can access efficient charging services in the smart grid. However, traditional electric vehicle charging systems are vulnerable to distributed denial of service and privileged insider attacks when the central charging server is attacked. The blockchain-based charging systems have been proposed to resolve these problems. In 2018, Huang et al. proposed the electric vehicle charging system using lightning network and smart contract. However, their system has an inefficient charging mechanism and does not guarantee security of key. We propose a secure charging system for electric vehicles based on blockchain to resolve these security flaws. Our
charging system ensures the security of key, secure mutual authentication, anonymity, and perfect forward secrecy, and also provides efficient charging. We demonstrate that our proposed system provides secure mutual authentication using Burrows-Abadi-Needham logic and prevents replay and man-in-the-middle attacks using automated validation of internet security protocols and applications simulation tool. Furthermore, we compare computation and communication costs with previous schemes. Therefore, the proposed charging system efficiently applies to practical charging systems for electric vehicles.


Reference Type: Conference Proceedings

Abstract: Hospitals provide a considerable amount of questionnaires to patients, and their result data can be one of the significant measures to check a patient's current health. In many cases, however, such data utilization in another kind of healthcare services is unsatisfactory because patients cannot manage the data by themselves. We propose a blockchain-based medical questionnaire management system for data sharing. This system guarantees the integrity of questionnaire result data using characteristics of the blockchain. Furthermore, data in this system can be interoperable with other systems because it is generated based on the international standard Health Level 7 Fast Healthcare Interoperability Resources. This paper explores how to use medical questionnaire result data for the lifelong healthcare of patient and better quality of health care services and enhance the security of personal medical records.


Reference Type: Report
Available from: https://www.bna.com/cryptocurrency-blockchain-technological-m73014481927/ Open access after free site registration.

Abstract: Crafted by Bloomberg Law® legal editor Robert Kim, the Bloomberg Law special report Cryptocurrency and Blockchain – The Technological and Regulatory Frontier of FinTech details how these issues present specific legal and regulatory challenges. The report provides:
* An in-depth review of blockchain and its role in finance, starting with its first application in bitcoin and further as a method to help with identity verification, supply chain tracking, company recordkeeping and distribution, self-executing “smart” contracts, automated real-time regulatory reporting, and more.
* Explanations of how blockchain works in bitcoin and other applications.
* How the dramatic rise of ICOs has caused U.S. federal and state regulators to scrutinize them under federal securities and commodities laws, state securities laws, and Anti-Money Laundering/Combating the Financing of Terrorism (AML/CFT) laws.
* A review of state requirements for cryptocurrency exchanges, including descriptions of which states currently require licenses to operate cryptocurrency exchanges.
* Discussion of forthcoming regulatory challenges at the federal, state, and global levels as policies toward the regulation of cryptocurrencies develop.


Reference Type: Journal Article

Abstract: This fall, PricewaterhouseCoopers issued a report on blockchain in health care and outlined six areas where it could have a profound impact: supply chain and inventory management; enrollment and provider data management; back office functions and payments; data management; managing risk and regulatory issues; and research and development.


Reference Type: Journal Article
Abstract: The smart grid integrates the use of information and Communication Technologies (ICTs) in order to ensure the interaction between its computational and physical elements. Moreover, it supports bidirectional information flows between the energy users and the utility grid that motivate energy users not simply to consume but also to generate energy and to share it with the utility grid and/or with other consumers. Many researches have addressed the problem of energy management in the smart grid context and have been done in order to offer maximum savings on energy bills as efficiently as possible. However, many algorithms presented in the literature do not exploit storage systems and/or present high energy losses. Taking into consideration energy losses, this research discusses the effects of these losses on consumers' bill. Hence, we propose an agent-based solution that takes into consideration users’ loss minimization in the smart grid context. The contribution of this paper is twofold. Firstly, it highlights the effects of power loss on the energy cost in an electrical system. Secondly, a novel approach aiming to help the storage system meet consumers' daily demands will be presented. Simulation results show that our proposal minimizes consumers' energy costs and losses.


Reference Type: Journal Article

Abstract: Biomedical research and clinical decision depend increasingly on scientific evidence realized by a number of authoritative databases, mostly public and continually enriched via peer scientific contributions. Given the dynamic nature of biomedical evidence data and their usage in the sensitive domain of biomedical science, it is important to ensure retrieved data integrity and non-repudiation. In this work, we present a blockchain-based notarization service that uses smart digital contracts to seal a biomedical database query and the respective results. The goal is to ensure that retrieved data cannot be modified after retrieval and that the database cannot validly deny that the particular data has been provided as a result of a specific query. Biomedical evidence data versioning is also supported. The feasibility of the proposed notarization approach is demonstrated using a real blockchain infrastructure and is tested on two different biomedical evidence databases: a publicly available medical risk factor reference repository and on the PubMed database of biomedical literature references and abstracts.


Reference Type: Conference Paper

Abstract: Blockchain as technology described to be used in closed systems to conduct registers of official data in public healthcare. Also this technology had found its use in different other ways, for example it is education of medical staff, control of the contracts for healthcare services. And the role of Blockchain in CALS / PLM-technologies suggested.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/4/856

Abstract: Nowadays, we are surrounded by a large number of IoT (Internet of Things) devices and sensors. These devices are designed to make life easier and more comfortable. Blockchain technology, especially its mass application, is becoming a term number one. Adoption of blockchain into enterprise networks still has a few challenges that need to be tackled. Utilizing blockchain can bring increased security and efficiency of network maintenance. The key feature of the blockchain, immutability, brings resistance to unauthorized modifications. The whole history of device configuration changes is stored in the blockchain, hence recovery after incidents is very straightforward. This paper extends our previous studies. We are introducing an improved architecture for management and monitoring of IoT devices using a private blockchain. The majority of the system is built on a chaincode, which handles CRUD (Create, Read, Update, Delete) operations as well as encryption and access control. Device configuration files are stored in the blockchain. When a modification occurs, the device downloads a new configuration in a simple manner. The chaincode receives notification whether setup was successful and
Abstract: A blockchain powered health information exchange could unlock the true value of interoperability. Blockchain-based systems have the potential to reduce or eliminate the friction and costs of current intermediaries. Particularly compelling use cases for blockchain technology include the Precision Medicine Initiative, Patient Care and Outcomes Research (PCOR), and the Nationwide Interoperability Roadmap. For these and other high-potential areas, determining the viability of the business case for blockchain is paramount to realize the benefits of improved data integrity, decentralization and disintermediation of trust, and reduced transaction costs. The exchange of Personal Health Records and Health Information Exchange (HIE) data via the Integrating the Health care Enterprise (IHE) protocol is an important part of addressing the challenges of system interoperability and accessibility of medical records. The strategy outlined to date provides the technical requirements and specific incentives for health systems to meet the Meaningful Use interoperability standards necessary to support the envisioned National Health Information Network, buttressed by a network of HIEs operating on a broad scale. That unrealized scale, driven in large part by insufficient incentives outside of compliance, threatens the viability of HIEs and merits exploration of new models. It may be possible that new value based models embedded in MACRA will be sufficient to make the market model work, but HIEs have been seeking alternative business models. Meanwhile the health systems that see true benefits from establishing a clinically integrated network in order to engage in risk-based contracts focus on private exchanges and are looking for low cost solutions that enable secure integration and support the assembly of virtual health systems that move beyond organizational boundaries. While blockchain technology is not a panacea for data standardization or system integration challenges, it does offer a promising new distributed framework to amplify and support integration of health care information across a range of uses and stakeholders. It addresses several existing pain points and enables a system that is
more efficient, disintermediated, and secure.

Reference Type: Journal Article
Abstract: Blockchain technology has a potential to address many of the food safety challenges facing the world today. Some of the most promising blockchain applications developed to date have been in the food supply chains.

Reference Type: Journal Article
Abstract: Arrival of blockchain is set to transform supply chain activities. Scholars have barely begun to systematically assess the effects of blockchain on various organizational activities. This paper examines how blockchain is likely to affect key supply chain management objectives such as cost, quality, speed, dependability, risk reduction, sustainability and flexibility. We present early evidence linking the use of blockchain in supply chain activities to increase transparency and accountability. Case studies of blockchain projects at various phases of development for diverse purposes are discussed. This study illustrates the various mechanisms by which blockchain help achieve the above supply chain objectives. Special emphasis has been placed on the roles of the incorporation of the IoT in blockchain-based solutions and the degree of deployment of blockchain to validate individuals’ and assets’ identities.

Reference Type: Journal Article
Abstract: This paper evaluates blockchain’s roles in strengthening cybersecurity and protecting privacy. Since most of the data is currently stored in cloud data centers, it also compares how blockchain performs vis-a-vis the cloud in various aspects of security and privacy. Key underlying mechanisms related to the blockchain’s impacts on the Internet of Things (IoT) security are also covered. From the security and privacy considerations, it highlights how blockchain-based solutions could possibly be, in many aspects, superior to the current IoT ecosystem, which mainly relies on centralized cloud servers through service providers. Using practical applications and real-world examples, the paper argues that blockchain's decentralized feature is likely to result in a low susceptibility to manipulation and forgery by malicious participants. Special consideration is also given to how blockchain-based identity and access management systems can address some of the key challenges associated with IoT security. The paper provides a detailed analysis and description of blockchain's roles in tracking the sources of insecurity in supply chains related to IoT devices. The paper also delves into how blockchain can make it possible to contain an IoT security breach in a targeted way after it is discovered. It discusses and evaluates initiatives of organizations, inter-organizational networks and industries on this front. A number of policy implications are discussed. First, in order to strengthen IoT, regulators can make it obligatory for firms to deploy blockchain in supply chain, especially in systems that are mission critical, and have substantial national security and economic benefits. Second, public policy efforts directed at protecting privacy using blockchain should focus on providing training to key stakeholders and increasing investment in this technology. Third, one way to enrich the blockchain ecosystem would be to turn attention to public-private partnerships. Finally, national governments should provide legal clarity and more information for parties to engage in smart contracts that are enforceable.

Reference Type: Journal Article

Abstract: This column evaluates blockchain’s roles in strengthening security in the Internet of Things (IoT). Key underlying mechanisms related to the blockchain-IoT security nexus are covered. From a security standpoint, the article highlights how blockchain-based solutions could be, in many aspects, superior to the current IoT ecosystem, which relies mainly on centralized cloud servers. Using practical applications and real-world examples, the article argues that blockchain’s decentralized nature is likely to result in a low susceptibility to manipulation and forgery by malicious participants. Special consideration is given to how blockchain-based identity and access management systems can address some of the key challenges associated with IoT security. The column provides a detailed analysis and description of blockchain’s roles in tracking the sources of insecurity in supply chains related to IoT devices. Using blockchain, it is also possible to contain an IoT security breach in a targeted way after it is discovered. The column also discusses and evaluates initiatives of organizations, interorganizational networks, and industries on the frontlines of blockchain.


Reference Type: Journal Article
Available from: http://jips-k.org/q.jips?cp=pp&pn=645

Abstract: An individual’s health data is very sensitive and private. Such data are usually stored on a private or community owned cloud, where access is not restricted to the owners of that cloud. Anyone within the cloud can access this data. This data may not be read only and multiple parties can make to it. Thus, any unauthorized modification of health-related data will lead to incorrect diagnosis and mistreatment. However, we cannot restrict semipublic access to this data. Existing security mechanisms in e-health systems are competent in dealing with the issues associated with these systems but only up to a certain extent. The indigenous technologies need to be complemented with current and future technologies. We have put forward a method to complement such technologies by incorporating the concept of blockchain to ensure the integrity of data as well as its provenance.


Reference Type: Journal Article

Abstract: The internet of things (IoT) enabled a common operating picture (COP) across the various applications of modern day living. The COP is achieved through the advancements seen in wireless sensor network devices that were able to communicate through the network thereby exchanging information and performing various analysis. In IoT, the exchange of information and data authentication is only done through the central server thereby leading to the security and privacy concerns. Chances of device spoofing, false authentication, less reliability in data sharing could happen. To address such security and privacy concerns, a central server concept is eliminated and blockchain (BC) technology is introduced as a part of IoT. This paper elaborates the possible security and privacy issues considering the component interaction in IoT and studies how the distributed ledger based blockchain (DL-BC) technology contribute to it. Applications of BC with respect to focused sectors and category were clearly studied here. Various challenges specific to IoT and IoT with BC were also discussed to understand blockchain technology contribution.


Reference Type: Journal Article

Abstract: OBJECTIVE: Decentralized privacy-preserving predictive modeling enables multiple institutions
to learn a more generalizable model on healthcare or genomic data by sharing the partially trained models instead of patient-level data, while avoiding risks such as single point of control. State-of-the-art blockchain-based methods remove the "server" role but can be less accurate than models that rely on a server. Therefore, we aim at developing a general model sharing framework to preserve predictive correctness, mitigate the risks of a centralized architecture, and compute the models in a fair way.

**MATERIALS AND METHODS:** We propose a framework that includes both server and "client" roles to preserve correctness. We adopt a blockchain network to obtain the benefits of decentralization, by alternating the roles for each site to ensure computational fairness. Also, we developed GloreChain (Grid Binary LOGistic REgression on Permissioned BlockChain) as a concrete example, and compared it to a centralized algorithm on 3 healthcare or genomic datasets to evaluate predictive correctness, number of learning iterations and execution time. 

**RESULTS:** GloreChain performs exactly the same as the centralized method in terms of correctness and number of iterations. It inherits the advantages of blockchain, at the cost of increased time to reach a consensus model.

**DISCUSSION:** Our framework is general or flexible and can also address intrinsic challenges of blockchain networks. Further investigations will focus on higher-dimensional datasets, additional use cases, privacy-preserving quality concerns, and ethical, legal, and social implications. 

**CONCLUSIONS:** Our framework provides a promising potential for institutions to learn a predictive model based on healthcare or genomic data in a privacy-preserving and decentralized way.

---


**Reference Type:** Journal Article

**Available from:** https://academic.oup.com/jamia/article/24/6/1211/4108087

**Abstract:** To introduce blockchain technologies, including their benefits, pitfalls, and the latest applications, to the biomedical and health care domains. Biomedical and health care informatics researchers who would like to learn about blockchain technologies and their applications in the biomedical/health care domains. The covered topics include: (1) introduction to the famous Bitcoin cryptocurrency and the underlying blockchain technology; (2) features of blockchain; (3) review of alternative blockchain technologies; (4) emerging nonfinancial distributed ledger technologies and applications; (5) benefits of blockchain for biomedical/health care applications when compared to traditional distributed databases; (6) overview of the latest biomedical/health care applications of blockchain technologies; and (7) discussion of the potential challenges and proposed solutions of adopting blockchain technologies in biomedical/health care domains.

---


**Reference Type:** Journal Article

**Available from:** https://academic.oup.com/jamia/article/26/5/462/5419321

**Abstract:** To introduce healthcare or biomedical blockchain applications and their underlying blockchain platforms, compare popular blockchain platforms using a systematic review method, and provide a reference for selection of a suitable blockchain platform given requirements and technical features that are common in healthcare and biomedical research applications. Healthcare or clinical informatics researchers and software engineers who would like to learn about the important technical features of different blockchain platforms to design and implement blockchain-based health informatics applications. 

Covered topics include (1) a brief introduction to healthcare or biomedical blockchain applications and the benefits to adopt blockchain; (2) a description of key features of underlying blockchain platforms in healthcare applications; (3) development of a method for systematic review of technology, based on the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) statement, to investigate blockchain platforms for healthcare and medicine applications; (4) a review of 21 healthcare-related technical features of 10 popular blockchain platforms; and (5) a discussion of findings and limitations of the review.

---


**Reference Type:** Journal Article

**Available from:** https://www.thelancet.com/journals/lancet/article/PIIS0140-6736(18)32163-9/fulltext

**Abstract:** In 2019, Cyprus is expected to introduce its new National Health Insurance System, 13 years after Myria Antoniadou's World Report, which identified the Mediterranean island's health-care challenges. With the new National Health Insurance System, Cyprus will become a primary-care-driven country, and it will be the latest European Union (EU) member state to have a universal health-care system.
Toomas Hendrik Ilves, chairman of the EU eHealth Task Force to “redesign health in Europe for 2020”, notes that successfully ensuring health-care access for all EU citizens depends on information-technology application and data use. In Cyprus, patient medical records are generally paper based and highly fragmented, which increases the risk of duplicate investigations and of patients being prescribed unsuitable medication. The new health-care system, combined with the changes in data management in compliance with the EU General Data Protection Regulations (GDPR), indicates promising positive changes.

Lacity MC. Addressing key challenges to making enterprise blockchain applications a reality. MIS Q Exec. 2018;17(3):201-22.

Abstract: Many enterprises have not progressed their blockchain solutions beyond proofs-of-concept. Daunting managerial challenges in the areas of standards, regulations, shared governance models and viable ecosystems impede progress. We describe the strategies that LO3 Energy, Moog, Inc. and the Center for Supply Chain Studies are pursuing to address these challenges.


Abstract: Enterprise blockchain applications can allow trading partners to transact directly without relying on trusted third parties and promise to: eliminate the need for reconciliations, instantly track and trace assets through a supply chain, provide unbeatable data provenance, settle transactions quickly and cheaply, and enable an information security model that is fault tolerant, resilient, and available. Many of these promised benefits seemingly address the challenges of non-blockchain based inter-organizational systems. However, this research indicates that blockchain based inter-organizational applications pose significant challenges of their own. Based on interview and participant observation data, we identified five challenges: (1) competing blockchain standards, (2) adjusting to different shared governance models, (3) intellectual property concerns (4) industrial espionage risks, and (5) regulatory uncertainty. We also identified emerging practices stakeholders are using to address those challenges when considering enterprise blockchain applications.


Abstract: Despite the demand and interest for the blockchain technology, there are still major challenges for blockchain application initiatives (projects and ventures) to be sustainable and reliable. While starting a non-blockchain initiative already comes with its own sets of challenges and has around 50% failure rate, starting a blockchain initiative raises the rate to 90% due to additional variables and confusion on top of this. Such a situation deters innovators and eventually dampens innovation, requiring priority for actions. This paper attempts to contribute by compiling and outlining the various key variables to be considered, as a set of parameters for blockchain initiators. Through secondary data collection: literature reviews, report studies and primary data collection: interventional and observational case study, interviews with blockchain researchers, businesses and entrepreneurs, this paper categorizes variables into blockchain-related and business-related categories, outlining consideration points for each of the variables. By summarizing and integrating the variables and referring to theories of innovation and adoption, it is concluded that concept validation entailing both initiative feasibility and user-demand, is of key importance for blockchain innovations.

Abstract: Reliable computer systems must handle malfunctioning components that give conflicting information to different parts of the system. This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement. It is shown that, using only oral messages, this problem is solvable if and only if more than two-thirds of the generals are loyal; so a single traitor can confound two loyal generals. With unforgeable written messages, the problem is solvable for any number of generals and possible traitors. Applications of the solutions to reliable computer systems are then discussed.


Abstract: Technology is becoming increasingly intertwined with our lives every year. As technology advances, it offers promising new methods to help detect, manage, and improve the care of major depressive disorder (MDD). Unlike other specialties in medicine, psychiatry has been slow to adopt new technologies. Other areas of medicine, primarily cardiology and oncology, have made use of technological methods to patients’ great benefits. In psychiatry, new technological methods can predict which antidepressants will be most effective, provide therapies to patients, and empower patients to manage their own medical records. We offer an overview to new technologies and their applications to psychiatry for novices. Our particular focus is big data, machine learning, mobile applications, and blockchain technology. We summarise the uses of technology as assisting physicians in decision making, facilitating patient-patient interaction, and securely storing and managing health-care data. We suggest possible advantages and challenges to adopting these methods. Continued research and technological innovation is needed to improve the psychiatrist’s toolbox and to monitor the adoption and consequences of new technologies.


Abstract: With the underlying technology of Bitcoin or other crypto-currencies and its rapid growth nowadays, many places have begun accepting Bitcoin payments in hot debate. It is hardly to deny the emerging success of the creation Blockchain platform behind of Bitcoin in the field of mathematics, finance, banking, and healthcare. The paper aims to create a diagrammatic conceptual model of medical app using Blockchain technology to manage all database of patients and doctors when they have a surgery. The model is built based on the gap of previous models which are mostly using Blockchain in banking and finance sector. Focusing on the development of mission space conceptual models, this paper will continue to propose simulation space conceptual models in current studies, especially in the context of very few models applied blockchain in healthcare. After creation of this model, an app on smartphone using Bitcoin in payment could be created to facilitate doctors’ management of all their patients directly and effectively as well as helping patients have a good comparison of cost, procedure or preparation of pre and post-surgery. Hopefully this paper will contribute to the given field the conceptual model for medical stakeholders including researcher, public health authorities, etc. to participate in the network as Blockchain "miners", to synthesize anonymous data as mining rewards, in return for sustaining and securing the network via Proof of Work.

Abstract: Clinical Trials are becoming ever more complex, distributed and dynamic. The demand for precision medicine is bringing an unprecedented challenge for containing the costs of biomedical research and maintaining appropriate regulatory oversight.

Contract Research Organisations (CROs) are playing an increasingly important role in clinical trials, and are experts in providing the necessary back-office infrastructure, site management, and human resource.) to undertake trial activities. CROs are now becoming involved in all aspects of clinical trials from design, conduct, reporting, and final submissions to regulatory authorities. Recent estimates project that up to 70% of all trials will be managed by CROs by 2020. But despite this expenditure and expertise, the vast majority of trials still fail for avoidable reasons.

Blockchain and other Distributed Ledger Technologies (DLT) present the opportunity to transform the management of clinical trials. The role of CROs could be substituted by a technological platform that is more transparent and accountable to all relevant parties including trial sponsors, regulatory agencies, trial sites (hospitals, clinics), and patients themselves. Such a platform could prove far more cost-effective at managing safe and effective clinical trials, improving data availability for review and meta-analysis, as well as preventing non-publication and a posteriori analysis.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/2/574

Abstract: In the complicated settings of WSN (Wireless Sensor Networks) and IoT (Internet of Things) environments, keeping a number of heterogeneous devices updated is a challenging job, especially with respect to effectively discovering target devices and rapidly delivering the software updates. In this paper, we convert the traditional software update process to a distributed service. We set an incentive system for faithfully transporting the patches to the recipient devices. The incentive system motivates independent, self-interested transporters for helping the devices to be updated. To ensure the system correctly operates, we employ the blockchain system that enforces the commitment in a decentralized manner. We also present a detailed specification for the proposed protocol and validate it by model checking and simulations for correctness.


Reference Type: Journal Article


Abstract: [FIRST PARAGRAPH] To the Editor, Blockchain has turned the conventional wisdom about data storage and management on its head. Instead of keeping transaction data in a centralized server, blockchain distributes all users in the network and jointly manages them via a peer-to-peer network, thereby ensuring the safety, reliability, integrity, and transparency of data. While all data is stored in a central server and only the central authority owns the data in a traditional centralized network, a decentralized network powered by blockchain distributes ledgers that contain all the data across all users’ personal computers.1 Blockchain is hack-proof: hackers may attempt to alter or manipulate information contained in a blockchain network, but their attempts are futile when information is scattered across multiple individuals at once. Therefore, information is highly reliable and easy to track because it cannot be deleted or lost, and all transactions are transparent to everyone. Blockchain streamlines transaction processes and reduces time, saves costs for contract arbitration, and creates a new ecosystem of opensource service. The technology is expected to have huge social and economic ripple effects. Use of blockchain technology was originally confined to the financial sector, but has now forayed into various non-financial industries such as logistics, distribution, energy, public service, and, in particular, healthcare, arousing much interest among healthcare professionals on its potential.2 Currently, medical data are stored in electronic medical record systems and are owned by hospitals, which hampers information-sharing between hospitals. Patients who visit other hospitals often have to retake the same medical tests and doctors often fail fully understand the patient’s condition. In contrast, medical data that is distributed across a blockchain network are owned by patients rather than medical institutions. Blockchain technology, once implemented in medical data management, will give control over medical data back to patients themselves, allowing them to easily submit their digitalized medical records directly to the clinic of their choice. This not only eliminates the need for repeated examinations but also enables medical institutions to identify their patients quickly and easily using the information provided by the patients themselves. Medical practitioners can just focus on planning further examinations and the course of treatment.

Reference Type: Journal Article

Abstract: The promise of digital health care continues to be enthusiastically promoted but has been difficult to realise. Evidence-based practice, along with patient safety assurances, information governance, and certification, does not fit easily with schemes to accelerate innovation. Trust in the efficacy and safety of new models of care, such as that potentially delivered by artificial intelligence (AI), remains uncertain. Blockchain technology might contribute to overcoming these problems by enabling greater openness, transparency, and trust.

Blockchain was first conceptualised in 2009 for the first digital crypto-currency, Bitcoin. Blockchain is a decentralised collection of technologies to allow for the storage of data that are permanent and immune to fraud, such as financial transactions, without the need for a central or trusted authority like a bank. The concept has grown beyond the exchange of payments to include smart contracts in which software algorithms manage the exchange of value through the use of tokens. With investment from large multinational technology companies and venture capital, the use of blockchain technology is growing in markets beyond finance such as the pharmaceutical and health-care industries.


Reference Type: Journal Article

Abstract: Personal Health Records (PHRs) have the potential to give patients fine-grained, personalised and secure access to their own medical data and to enable self-management of care. Emergent trends around the use of Blockchain, or Distributed Ledger Technology, seem to offer solutions to some of the problems faced in enabling these technologies, especially to support issues consent, data exchange and data access. We present an analysis of existing blockchain-based health record solutions and a reference architecture for a “Ledger of Me” system that extends PHR to create a new platform combining the collection and access of medical data and digital interventions with smart contracts. Our intention is to enable patient use of the data in order to support their care and to provide a strong consent mechanisms for sharing of data between different organisations and apps. Ledger of Me is based on around the principle that this combination of event-driven smart contracts, medical record data and patient control is important for the adoption of blockchain-based solutions for the PHR. The reference architecture we present can serve as the basis of a range of future blockchain-based medical application architectures.


Reference Type: Journal Article

Abstract: Medical care has become an indispensable part of people's lives, with a dramatic increase in the volume of medical data (e.g., diagnosis certificates and medical records). Medical data, however, is easily stolen, tampered with, or even completely deleted. If the above occurs, medical data cannot be recorded or retrieved in a reliable manner, resulting in delay treatment progress, even endanger the patient's life. In this paper, we propose a novel blockchain-based data preservation system (DPS) for medical data. To provide a reliable storage solution to ensure the primitiveness and verifiability of stored data while preserving privacy for users, we leverage the blockchain framework. With the proposed DPS, users can preserve important data in perpetuity, and the originality of the data can be verified if tampering is suspected. In addition, we use prudent data storage strategies and a variety of cryptographic algorithms to guarantee user privacy: e.g., an adversary is unable to read the plain text even if the data are stolen. We implement a prototype of the DPS based on the real world blockchain-based platform Ethereum. Performance evaluation results demonstrate the effectiveness and efficiency of the proposed system.


Reference Type: Journal Article

Abstract: Medical care has become an indispensable part of people's lives, with a dramatic increase in the volume of medical data (e.g., diagnosis certificates and medical records). Medical data, however, is easily stolen, tampered with, or even completely deleted. If the above occurs, medical data cannot be recorded or retrieved in a reliable manner, resulting in delay treatment progress, even endanger the patient's life. In this paper, we propose a novel blockchain-based data preservation system (DPS) for medical data. To provide a reliable storage solution to ensure the primitiveness and verifiability of stored data while preserving privacy for users, we leverage the blockchain framework. With the proposed DPS, users can preserve important data in perpetuity, and the originality of the data can be verified if tampering is suspected. In addition, we use prudent data storage strategies and a variety of cryptographic algorithms to guarantee user privacy: e.g., an adversary is unable to read the plain text even if the data are stolen. We implement a prototype of the DPS based on the real world blockchain-based platform Ethereum. Performance evaluation results demonstrate the effectiveness and efficiency of the proposed system.
Abstract: With the development of Internet technology, the volume of data is increasing tremendously. To tackle with large-scale data, more and more applications choose to enlarge the storage capacity of users’ terminals with the help of cloud platforms. Before storing data to an untrusted cloud server, some measures should be adopted to guarantee the data security. However, the communication overhead will increase dramatically when users transmit files encrypted by a traditional encryption scheme. In this paper, we address the above problems by proposing a blockchain-based security architecture for distributed cloud storage, where users can divide their own files into encrypted data chunks, and upload those data chunks randomly into the P2P network nodes that provide free storage capacity. We customize a genetic algorithm to solve the file block replica placement problem between multiple users and multiple data centers in the distributed cloud storage environment. Numerical results show that the proposed architecture outperforms the traditional cloud storage architectures in terms of file security and network transmission delay. On average, the file loss rate based on the simulation assumptions utilized in this paper is close to 0% on our architecture while it’s nearly 100% and 71.66% on the architecture with single data center and the distributed architecture using genetic algorithm. Besides, with proposed scheme, the transmission delay on the proposed architecture is reduced by 39.28% and 76.47% on average on the user’s number and the number of file block replicas, respectively, in comparison to the architecture with single data center. Meanwhile, the transmission delay of file block replicas is also reduced by 41.36% on average than that on the distributed architecture using genetic algorithm.


Reference Type: Electronic Article

Abstract: Background: Access to accurate and complete medication histories across healthcare institutions enables effective patient care. Histories across healthcare institutions currently rely on centralized systems for sharing medication data. However, there is a lack of efficient mechanisms to ensure that medication histories transferred from one institution to another are accurate, secure, and trustworthy.

Methods: In this article, we introduce a decentralized medication management system (DMMS) that leverages the advantages of blockchain to manage medication histories. DMMS is realized as a decentralized network under the hyperledger fabric framework. Based on the network, we designed an architecture, within which each prescriber can create prescriptions for each patient and perform queries about historical prescriptions accordingly. Finally, we analyzed the advantages of DMMS over centralized systems in terms of accuracy, security, trustworthiness, and privacy.

Results: We developed a proof of concept to showcase DMMS. In this system, a prescriber prescribes medications for a patient and then encrypts the prescriptions via the patient’s public keys. Patients can query their own prescriptions from different histories across healthcare institutions and then decrypt the prescriptions via their private keys. At the same time, a prescriber can query a patient’s prescription records across healthcare institutions after approval from the patient. Analytic results show that DMMS can improve security, trustworthiness, and privacy in medication history sharing and exchanging across healthcare institutions. In addition, we discuss the potential for DMMS in e-prescribing markets.

Conclusions: This study shows that a distributed secure ledger can enable reliable, interoperable, and accurate medication history sharing.


Reference Type: Electronic Article

Abstract: Since its inception, the blockchain technology has shown promising application prospects. From the initial cryptocurrency to the current smart contract, blockchain has been applied to many fields. Although there are some studies on the security and privacy issues of blockchain, there lacks a systematic examination on the security of blockchain systems. In this paper, we conduct a systematic study on the security threats to blockchain and survey the corresponding real attacks by examining popular blockchain systems. We also review the security enhancement solutions for blockchain, which could be used in the development of various blockchain systems, and suggest some future directions to stir research efforts into this area.


Reference Type: Journal Article
Cryptocurrency is a well-developed blockchain technology application that is currently a heated topic throughout the world. The public availability of transaction histories offers an opportunity to analyze and compare different cryptocurrencies. In this paper, we present a dynamic network analysis of three representative blockchain-based cryptocurrencies: Bitcoin, Ethereum, and Namecoin. By analyzing the accumulated network growth, we find that, unlike most other networks, these cryptocurrency networks do not always densify over time, and they are changing all the time with relatively low node and edge repetition ratios. Therefore, we then construct separate networks on a monthly basis, trace the changes of typical network characteristics (including degree distribution, degree assortativity, clustering coefficient, and the largest connected component) over time, and compare the three. We find that the degree distribution of these monthly transaction networks cannot be well fitted by the famous power-law distribution, at the same time, different currency still has different network properties, e.g., both Bitcoin and Ethereum networks are heavy-tailed with disassortative mixing, however, only the former can be treated as a small world. These network properties reflect the evolutionary characteristics and competitive power of these three cryptocurrencies and provide a foundation for future research.


Abstract: Enabled by mobile and wearable technology, personal health data delivers immense and increasing value for healthcare, benefiting both care providers and medical research. The secure and convenient sharing of personal health data is crucial to the improvement of the interaction and collaboration of the healthcare industry. Faced with the potential privacy issues and vulnerabilities existing in current personal health data storage and sharing systems, as well as the concept of self-sovereign data ownership, we propose an innovative user-centric health data sharing solution by utilizing a decentralized and permissioned blockchain to protect privacy using channel formation scheme and enhance the identity management using the membership service supported by the blockchain. A mobile application is deployed to collect health data from personal wearable devices, manual input, and medical devices, and synchronize data to the cloud for data sharing with healthcare providers and health insurance companies. To preserve the integrity of health data, within each record, a proof of integrity and validation is permanently retrievable from cloud database and is anchored to the blockchain network. Moreover, for scalable and performance considerations, we adopt a tree-based data processing and batching method to handle large data sets of personal health data collected and uploaded by the mobile platform.


Abstract: Blockchain technologies is one of the most popular issue in recent years, it has already changed people's lifestyle in some area due to its great influence on many business or industry, and what it can do will still continue cause impact in many places. Although the feature of blockchain technologies may bring us more reliable and convenient services, the security issues and challenges behind this innovative technique is also an important topic that we need to concern.


Abstract: Identity-based cryptosystems mean that public keys can be directly derived from user identifiers, such as telephone numbers, email addresses, and social insurance number, and so on. So they can simplify key management procedures of certificate-based public key infrastructures and can be used to realize authentication in blockchain. Linearly homomorphic signature schemes allow to perform linear computations on authenticated data. And the correctness of the computation can be publicly verified. Although a series of homomorphic signature schemes have been designed recently, there are few homomorphic signature schemes designed in identity-based cryptography. In this paper, we
construct a new ID-based linear homomorphic signature scheme, which avoids the shortcomings of the use of public-key certificates. The scheme is proved secure against existential forgery on adaptively chosen message and ID attack under the random oracle model. The ID-based linearly homomorphic signature schemes can be applied in e-business and cloud computing. Finally, we show how to apply it to realize authentication in blockchain.


Reference Type: Conference Paper


Abstract: Blockchain technologies offer new open source-based opportunities for developing new types of digital platforms and services. While research on the topic is emerging, it has this far been predominantly focused on technical and legal issues. To broaden our understanding of blockchain technology-based services and platforms, we build on earlier literature on payments and payment platforms and propose a research agenda divided into three focal areas of 1) organizational issues; 2) issues related to the competitive environment; and 3) technology design issues. We discuss several salient themes within each of these areas, and derive a set of research questions for each theme, highlighting the need to address both risks and opportunities for users, as well as different types of stakeholder organizations.

With this research agenda, we contribute to the discussion on future avenues for Information Systems research on blockchain technology-based platforms and services.

Linn LA, Koo MB. Blockchain for health data and its potential use in health IT and health care related research. ONC/NIST Use of Blockchain for Healthcare and Research Workshop; 2016 Sep 26-27; Gaithersburg, MD. National Institute of Standards Technology; 2016.

Reference Type: Conference Proceedings


Abstract: The American Recovery and Reinvestment Act required all public and private health care providers to adopt electronic medical records (EMR) by January 1, 2014, in order to maintain their existing Medicaid and Medicare reimbursement levels. This EMR mandate spurred significant growth in the availability and utilization of EMRs. However, the vast majority of these systems do not have the capacity to share their health data.

Blockchain technology has the potential to address the interoperability challenges currently present in health IT systems and to be the technical standard that enables individuals, health care providers, health care entities and medical researchers to securely share electronic health data.

In this paper we describe a blockchain-based access-control manager to health records that would advance the industry interoperability challenges expressed in the Office of the National Coordinator for Health Information Technology’s (ONC) Shared Nationwide Interoperability Roadmap. Interoperability is also a critical component any infrastructure supporting Patient Centered Outcomes Research (PCOR) and the Precision Medicine Initiative (PMI). A national health IT infrastructure based on blockchain has far-reaching potential to promote the development of precision medicine, advance medical research and invite patients to be more accountable for their health.


Reference Type: Journal Article


Abstract: We study the evolution of ideas related to creation of asset-backed currencies over the last 200 years and argue that recent developments related to distributed ledger technologies and blockchains give asset-backed currencies a new lease of life. We propose a practical mechanism combining novel technological breakthroughs with well-established hedging techniques for building an asset-backed transactional oriented cryptocurrency, which we call the digital trade coin (DTC). We show that in its mature state, the DTC can serve as a much-needed counterpoint to fiat reserve currencies of today.

Litke A, Anagnostopoulos D, Varvarigou T. Blockchains for supply chain management: architectural

Reference Type: Journal Article
Available from: https://www.mdpi.com/2305-6290/3/1/5

Abstract: Blockchains are attracting the attention of stakeholders in many industrial domains, including the logistics and supply chain industries. Blockchain technology can effectively contribute in recording every single asset throughout its flow on the supply chain, contribute in tracking orders, receipts, and payments, while track digital assets such as warranties and licenses in a unified and transparent way. The paper provides, through its methodology, a detailed analysis of the blockchain fit in the supply chain industry. It defines the specific elements of blockchain that affect supply chain such as scalability, performance, consensus mechanism, privacy considerations, location proof and cost, and details on the impact that blockchains will have in disrupting the supply chain industry. Discussing the tradeoff between consensus cost, throughput and validation time it proceeds with a suggested high-level architectural approach, and concludes as a result with a discussion on changes needed and challenges faced for an in-vivo deployment of blockchains in the supply chain industry. While the technological features of modern blockchains can effectively facilitate supply chain uses cases, the various challenges that still remain, bring in front of us a wide set of needed changes and further research efforts for achieving a global, production level blockchain for the supply chain industry.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/7/1513

Abstract: The implementation of IP technology in wireless sensor networks has promoted the development of many smart scenarios. To enhance secure access in IP-enabled wireless sensor networks, access control to sensor nodes is a necessary process. However, access control currently faces two challenges, feasibility and preservation of user access privacy. In this paper, we propose eHAPAC, a novel privacy-preserving access control model for IP-enabled wireless sensor networks. The contributions of our paper include three parts. First, this paper integrates the Hidra access control protocol and APAC privacy-preserving model, addressing the issue of privacy-preserving access control in resource-constrained devices. Second, this paper proposes an enhanced Hidra protocol to implement the unlinkability of protocol message exchanges. Third, to solve the problem of third party credibility, this paper improves the group signature-based APAC model and utilizes blockchain technology to manage the storage and publication of public group signature keys. Security analysis and performance evaluation prove that our protocol is secure and effective.


Reference Type: Conference Paper

Abstract: Information security is the key to the development of modern Internet technology. The distributed mechanism, decentralized mechanism, password mechanism and scripted mechanism of the Blockchain present a completely new perspective for the development of Internet information security technology. The Blockchain technology redefines the storage and dissemination methods of the information in the network. Neither participant needs to know each other, and nor does it require third-party certification bodies to participate. It records, transmits and stores transferring activities of the information value by distributed technology, ensures that data is not tampered and forged based on an asymmetric cryptographic algorithm, enables all participants reached a consensus on the status of blockchain data information. And from the current industry research on blockchain technology, it expounds the application of blockchain technology in identity authentication, data protection and network security. The Blockchain technology will be a great driving force in the process of information security technology change, and will have a far-reaching impact on the expansion of information security.


Reference Type: Conference Paper
Abstract: This paper describes our blockchain architecture as a new system solution to supply a reliable mechanism for secure and efficient medical record exchanges. The Advanced Block-Chain (ABC) approach was designed to meet the demands in healthcare growth as well as in the new form of social interactive norms. It is going to revolutionize the e-Health industry with greater efficiency by eliminating many of the intermediates as we know them today.


Reference Type: Journal Article

Abstract: Neural networks are widely used in the field of cognitive diagnosis. Cognitive diagnosis can diagnose the subjects’ knowledge of cognitive attributes according to their responses, so as to obtain the specific cognitive status of the subjects and provide remedial measures. The studies on the convergence of cultural industry and tourism industry are emerging, but the theoretical system needs to be improved. The research on the convergence mechanism between cultural industry and tourism industry can complement each other on the basis of independent theoretical system, which establishes relationship between the two theoretical systems. Based on the adaptive neural network algorithm and from the perspective of blockchain, this study takes cultural industry and rural tourism industry as examples to diagnose the industry convergence of rural cultural industry and rural tourism industry development, which will further consolidate the theoretical basis for the convergence and development of tourism industry and cultural industry, as well as contribute to promoting development of industry convergence.


Reference Type: Conference Paper

Abstract: In this paper, we propose a decentralized identity management system based on Blockchain. The function of the system mainly includes identity authentication and reputation management. The technical advantages of the Blockchain makes the data in the system safe and credible. In addition, we use smart contracts to write system rules to ensure the reliability of user information. We bind the user's entity information with the public key address and determine the true identity of a virtual user on the Blockchain. We use the token to represent the reputation which is shown to be an effective reputation model, making the participants in the system prefer to maintain and manage their personal reputation. Our system makes it possible for users to securely manage their identity and reputation on the Internet.


Reference Type: Journal Article

Abstract: Advancements in Information Technology landscape over the past two decades have made the collection, preservation, and analysis of digital evidence an extremely important tool for solving cybercrimes and preparing court cases. Digital evidence plays an important role in cybercrime investigation, as it is used to link individuals with criminal activities. Thus it is of utmost importance to guarantee integrity, authenticity, and auditability of digital evidence as it moves along different levels of hierarchy in the chain of custody during cybercrime investigation. Modern day technology is more advanced in terms of portability and power. A huge amount of information is generated by billions of devices connected to the internet that needs to be stored and accessed, thus posing great challenges in maintaining the integrity and authenticity of digital evidence for its admissibility in the court of law. Handling digital evidences poses unique challenges because of the fact they are latent, volatile, fragile, can cross jurisdictional borders quickly and easily and in many cases can be time/machine dependent too. Thus guaranteeing the authenticity and legality of processes and procedures used to gather and transfer the evidence in a digital society is a real challenge. Blockchain technology’s capability of enabling comprehensive view of transactions (events/actions) back to origination provides enormous promise for the forensic community. In this research we proposed Forensic-Chain: A Blockchain based Digital Forensics Chain of Custody, bringing integrity and tamper resistance to digital forensics chain of custody. We also provided Proof of Concept in Hyperledger Composer and evaluated its performance.

Reference Type: Journal Article

Abstract: Departing from established research on entrepreneurship, design-based entrepreneurship places an explicit emphasis on the entrepreneurial process as evolutionary and emergent in which knowledge and understanding of an opportunity are acquired incrementally by means of design and evaluation of alternative solutions. This paper develops a use case of BioBeats Ltd., a UK-based university spin-off which has successfully managed to turn an opportunity in digital health into a commercially viable enterprise. Adopting a design-based paradigm, the company under study started by building a technical solution informed by a set of design principles which subsequently allowed the company to convert the socio-technical nature of the opportunity into technological artefacts that were further refined and tested by means of real-world experiments with third parties and citizens.

______________________________________________________


Reference Type: Journal Article

Abstract: The old mantra of decentralizing the Internet is coming again with fanfare, this time around the blockchain technology hype. We have already seen a technology supposed to change the nature of the Internet: peer-to-peer. The reality is that peer-to-peer naming systems failed, peer-to-peer social networks failed, and yes, peer-to-peer storage failed as well. In this paper, we will review the research on distributed systems in the last few years to identify the limits of open peer-to-peer networks. We will address issues like system complexity, security and frailty, instability and performance. We will show how many of the aforementioned problems also apply to the recent breed of permissionless blockchain networks. The applicability of such systems to mature industrial applications is undermined by the same properties that make them so interesting for a libertarian audience: namely, their openness, their pseudo-anonymity and their unregulated cryptocurrencies. As such, we argue that permissionless blockchain networks are unsuitable to be the substrate for a decentralized Internet. Yet, there is still hope for more decentralization, albeit in a form somewhat limited with respect to the libertarian view of decentralized Internet: in cooperation rather than in competition with the superpowerful datacenters that dominate the world today. This is derived from the recent surge in interest in byzantine fault tolerance and permissioned blockchains, which opens the door to a world where use of trusted third parties is not the only way to arbitrate an ensemble of entities. The ability of establish trust through permissioned blockchains enables to move the control from the datacenters to the edge, truly realizing the promises of edge-centric computing.

______________________________________________________


Reference Type: Journal Article

Abstract: We adjust the Proof of Work (PoW) consensus mechanism used in Bitcoin and Ethereum so that we can build on its strength while also addressing, in part, some of its perceived weaknesses. Notably, our work is motivated by the high energy consumption for mining PoW, and we want to restrict the use of PoW to a configurable, expected size of nodes, as a function of the local blockchain state. The approach we develop for this rests on three pillars: (i) Proof of Kernel Work (PoKW), a means of dynamically reducing the set of nodes that can participate in the solving of PoW puzzles such that an adversary cannot increase his attack surface because of such a reduction; (ii) Practical Adaptation of Existing Technology, a realization of this PoW reduction through an adaptation of existing blockchain and enterprise technology stacks; and (iii) Machine Learning for Adaptive System Resiliency, the use of techniques from artificial intelligence to make our approach adaptive to system, network and attack dynamics. We develop here, in detail, the first pillar and illustrate the second pillar through a real use case, a pilot project done with Porsche on controlling permissions to vehicle and data log accesses. We also discuss pertinent attack vectors for PoKW consensus and their mitigation. Moreover, we sketch how our approach may lead to more democratic PoKW-based blockchain systems for public networks that may inherit the resilience of blockchains based on PoW.

______________________________________________________

Ma C, Kong X, Lan Q, Zhou Z. The privacy protection mechanism of Hyperledger Fabric and its
Abstract: Blockchain technology ensures that data is tamper-proof, traceable, and trustworthy. This article introduces a well-known blockchain technology implementation—Hyperledger Fabric. The basic framework and privacy protection mechanisms of Hyperledger Fabric such as certificate authority, channel, Private Data Collection, etc. are described. As an example, a specific business scenario of supply chain finance is figured out. And accordingly, some design details about how to apply these privacy protection mechanisms are described.


Abstract: Blockchain is a shared distributed digital ledger technology that can better facilitate data management, provenance and security, and has the potential to transform healthcare. Importantly, blockchain represents a data architecture, whose application goes far beyond Bitcoin – the cryptocurrency that relies on blockchain and has popularized the technology. In the health sector, blockchain is being aggressively explored by various stakeholders to optimize business processes, lower costs, improve patient outcomes, enhance compliance, and enable better use of healthcare-related data. However, critical in assessing whether blockchain can fulfill the hype of a technology characterized as ‘revolutionary’ and ‘disruptive’, is the need to ensure that blockchain design elements consider actual healthcare needs from the diverse perspectives of consumers, patients, providers, and regulators. In addition, answering the real needs of healthcare stakeholders, blockchain approaches must also be responsive to the unique challenges faced in healthcare compared to other sectors of the economy. In this sense, ensuring that a health blockchain is ‘fit-for-purpose’ is pivotal. This concept forms the basis for this article, where we share views from a multidisciplinary group of practitioners at the forefront of blockchain conceptualization, development, and deployment.


Abstract: INTRODUCTION: The globalization of the pharmaceutical supply chain has introduced new challenges, chief among them, fighting the international criminal trade in fake medicines. As the manufacture, supply, and distribution of drugs becomes more complex, so does the need for innovative technology-based solutions to protect patients globally. Areas covered: We conducted a multidisciplinary review of the science/health, information technology, computer science, and general academic literature with the aim of identifying cutting-edge existing and emerging ‘digital’ solutions to combat fake medicines. Our review identified five distinct categories of technology including mobile, radio frequency identification, advanced computational methods, online verification, and blockchain technology. Expert opinion: Digital fake medicine solutions are unifying platforms that integrate different types of anti-counterfeiting technologies as complementary solutions, improve information sharing and data collection, and are designed to overcome existing barriers of adoption and implementation. Investment in this next generation technology is essential to ensure the future security and integrity of the global drug supply chain.
the growing data hunger of the research and policy maker institutions. On one side the general availability of the data is vital in emergency situations and supports heavily the different research, population health management and development activities, on the other side using the same data can lead to serious social and ethical problems caused by malicious actors. Currently, the regulation of the privacy data varies all over the world, however underlying principles are always defensive and protective towards patient privacy against general availability. The protective principles cause a defensive, data hiding attitude of the health system developers to avoid breaching the overall law regulations. It makes the policy makers and different - primarily drug - developers to find ways to treat data such a way that lead to ethical and political debates. In our paper we introduce how the blockchain technology can help solving the problem of secure data storing and ensuring data availability at the same time. We use the basic principles of the American HIPAA regulation, which defines the public availability criteria of health data, however the different local regulations may differ significantly. Blockchain's decentralized, intermediary-free, cryptographically secured attributes offer a new way of storing patient data securely and at the same time publicly available in a regulated way, where a well-designed distributed peer-to-peer network incentivize the smooth operation of a fullFeatured EHR system.


Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5814166/

Abstract: The increased availability of data and recent advancements in artificial intelligence present the unprecedented opportunities in healthcare and major challenges for the patients, developers, providers and regulators. The novel deep learning and transfer learning techniques are turning any data about the person into medical data transforming simple facial pictures and videos into powerful sources of data for predictive analytics. Presently, the patients do not have control over the access privileges to their medical records and remain unaware of the true value of the data they have. In this paper, we provide an overview of the next-generation artificial intelligence and blockchain technologies and present innovative solutions that may be used to accelerate the biomedical research and enable patients with new tools to control and profit from their personal data as well with the incentives to undergo constant health monitoring. We introduce new concepts to appraise and evaluate personal records, including the combination--time- and relationship-value of the data. We also present a roadmap for a blockchain-enabled decentralized personal health data ecosystem to enable novel approaches for drug discovery, biomarker development, and preventative healthcare. A secure and transparent distributed personal data marketplace utilizing blockchain and deep learning technologies may be able to resolve the challenges faced by the regulators and return the control over personal data including medical records back to the individuals.


Reference Type: Conference Paper

Available from: http://ebooks.iospress.nl/publication/49424 Subscription required to view.

Abstract: INTRODUCTION: Interoperability of health information systems is one of the key challenges of modern healthcare systems. A weak spot in this technology stack of interoperability protocols as defined by HL7 and IHE is cross affinity domain exchange of access control information and policies. In several industries the Blockchain technology had a major breakthrough. The goal of this paper is to elaborate how to exchange cross affinity domain access information enhancing well established IHE networks with block chain technology. METHODS: Using literature analysis and research on current interoperability standards the state of the art of securely exchanging medical information was elaborated. We enhanced this system with the capabilities of the peer2peer based Blockchain network elaborating the workflows of exchanging the access control specific information. RESULTS: We extended an IHE based affinity domain by adding a block chain ledger to the deployment. This ledger is fed with XACML based policies which are propagated through the peer2peer based system. Using the Blockchain protocol other affinity domains are informed of the change and can retrieve the information. Acting as an additional source of policies and consents the policy decision point is capable of querying this network and building a decision based on the retrieved information.


Reference Type: Journal Article
Abstract: The use of teledermatology in primary care has been shown to be reliable, offering the possibility of improving access to dermatological care by using telecommunication technologies to connect several medical centers and enable the exchange of information about skin conditions over long distances. This paper describes the main points of a teledermatology project that we have implemented to promote and facilitate the diagnosis of skin diseases and improve the quality of care for rural and remote areas. Moreover, we present a blockchain-based approach which aims to add new functionalities to an innovative teledermatology platform which we developed and tested in the Sardinian Region (Italy). These functionalities include giving the patient complete access to his/her medical records while maintaining security. Finally, the advantages that this new decentralized system can provide for patients and specialists are presented.


Reference Type: Journal Article


Abstract: The building of the blockchain is predicted to harken the end of the contemporary sovereign order. Some go further to claim that as a powerful decentering technology, blockchain contests the continued functioning of world capitalism. Are such claims merited? In this paper we consider sovereignty and blockchain technology theoretically, posing possible futures for sovereignty in a blockchain world. These possibilities include various forms of individual, popular, technological, corporate, and techno-totalitarian state sovereignty. We identify seven structural tendencies of blockchain technology and give examples as to how these have manifested in the construction of new forms of sovereignty. We conclude that the future of sovereignty in a blockchain world will be articulated in the conjuncture of social struggle and technological agency and we call for a stronger alliance between technologists and democrats.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1660-4601/15/8/1627

Abstract: The food supply chain is a complex system that involves a multitude of "stakeholders" such as farmers, production factories, distributors, retailers and consumers. "Information asymmetry" between stakeholders is one of the major factors that lead to food fraud. Some current researches have shown that applying blockchain can help ensure food safety. However, they tend to study the traceability of food but not its supervision. This paper provides a blockchain-based credit evaluation system to strengthen the effectiveness of supervision and management in the food supply chain. The system gathers credit evaluation text from traders by smart contracts on the blockchain. Then the gathered text is analyzed directly by a deep learning network named Long Short Term Memory (LSTM). Finally traders' credit results are used as a reference for the supervision and management of regulators. By applying blockchain, traders can be held accountable for their actions in the process of transaction and credit evaluation. Regulators can gather more reliable, authentic and sufficient information about traders. The results of experiments show that adopting LSTM results in better performance than traditional machine learning methods such as Support Vector Machine (SVM) and Navie Bayes (NB) to analyze the credit evaluation text. The system provides a friendly interface for the convenience of users.


Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4586338/

Abstract: BACKGROUND: Mobile health Applications (mHealth Apps) are opening the way to patients'
The team joins a growing number of academic scientists and start-ups who are using blockchain to make medical data with researchers easily and securely — and retain control over it. Their method, which is based on the blockchain technology that underlies the cryptocurrency Bitcoin, will soon be put to the test. By May, Hadley and his colleagues will launch a study to train their AI algorithm to detect cancer using mammograms that they hope to obtain from between three million and five million US women.

So Hadley, a physician and computational biologist at the University of California, San Francisco, is trying a radical solution. He and his colleagues are building a system that allows people to share their medical data with researchers easily and securely — and retain control over it. Their method, which is based on the blockchain technology that underlies the cryptocurrency Bitcoin, will soon be put to the test. By May, Hadley and his colleagues will launch a study to train their AI algorithm to detect cancer using mammograms that they hope to obtain from between three million and five million US women.

The team joins a growing number of academic scientists and start-ups who are using blockchain to make sharing medical scans, hospital records and genetic data more attractive — and more efficient. Some projects will even pay people to use their information. The ultimate goal of many teams is to train AI algorithms on the data they solicit using the blockchain systems.

Abstract: BACKGROUND: Blockchain technology is emerging as an innovative tool in data and software security. OBJECTIVE: This study aims to explore the role of blockchain in supporting clinical trials data management and develop a proof-of-concept implementation of a patient-facing and researcher-facing system. METHODS: Blockchain-based Smart Contracts were built using the Ethereum platform. RESULTS: We described BlockTrial, a system that uses a Web-based interface to allow users to run trials-related Smart Contracts on an Ethereum network. Functions allow patients to grant researchers access to their data and allow researchers to submit queries for data that are stored off chain. As a type of distributed ledger, the system generates a durable and transparent log of these and other transactions. BlockTrial could be used to increase the trustworthiness of data collected during clinical research with benefits to researchers, regulators, and drug companies alike. In addition, the system could empower patients to become more active and fully informed partners in research. CONCLUSIONS: Blockchain technology presents an opportunity to address some of the common threats to the integrity of data collected in clinical trials and ensure that the analysis of these data comply with prespecified plans. Further technical work is needed to add additional functions. Policies must be developed to determine the optimal models for participation in the system by its various stakeholders.

Abstract: [FIRST FEW PARAGRAPHS] Dexter Hadley thinks that artificial intelligence (AI) could do a far better job at detecting breast cancer than doctors do — if screening algorithms could be trained on millions of mammograms. The problem is getting access to such massive quantities of data. Because of privacy laws in many countries, sensitive medical information remains largely off-limits to researchers and technology companies.

So Hadley, a physician and computational biologist at the University of California, San Francisco, is trying a radical solution. He and his colleagues are building a system that allows people to share their medical data with researchers easily and securely — and retain control over it. Their method, which is based on the blockchain technology that underlies the cryptocurrency Bitcoin, will soon be put to the test. By May, Hadley and his colleagues will launch a study to train their AI algorithm to detect cancer using mammograms that they hope to obtain from between three million and five million US women.

The team joins a growing number of academic scientists and start-ups who are using blockchain to make sharing medical scans, hospital records and genetic data more attractive — and more efficient. Some projects will even pay people to use their information. The ultimate goal of many teams is to train AI algorithms on the data they solicit using the blockchain systems.
Abstract: Blockchain has a range of built-in features, such as distributed ledger, decentralized storage, authentication, security, and immutability, and has moved beyond hype to practical applications in industry sectors such as Healthcare. Blockchain applications in the healthcare sector generally require more stringent authentication, interoperability, and record sharing requirements, due to exacting legal requirements, such as Health Insurance Portability and Accountability Act of 1996 (HIPAA). Building on existing blockchain technologies, researchers in both academia and industry have started to explore applications that are geared toward healthcare use. These applications include smart contracts, fraud detection, and identity verification. Even with these improvements, there are still concerns as blockchain technology has its own specific vulnerabilities and issues that need to be addressed, such as mining incentives, mining attacks, and key management. Additionally, many of the healthcare applications have unique requirements that are not addressed by many of the blockchain experiments being explored, as highlighted in this survey paper. A number of potential research opportunities are also discussed in this paper.
Abstract: Smart contracts are an emerging technology that could revolutionize commercial transactions by eliminating inefficiencies and uncertainty created by the current transactional ecosystem of lawyers, courts, regulators, banks, and other parties with divergent interests. However, a lack of consensus around how smart contracts are implemented, uncertainty regarding enforceability, and scarcity of on point statutes and case law means that a stable legal, commercial and technical smart contract landscape has yet to emerge. The implementation of universal legal, technical and commercial standards and best practices will reduce uncertainty and promote widespread adoption and use of smart contracts.


Reference Type: Report

Abstract: Policymakers can and should do more to support blockchain innovation and adoption, such as ensuring regulations are targeted and flexible, so as to encourage blockchain experimentation.

* Blockchain is a powerful new technology that creates a distributed digital ledger that allows multiple parties to engage in secure, trusted transactions with one another without an intermediary.
* Blockchain is best suited for certain types of applications, including cryptocurrencies, shared data services, smart contracts applications, decentralized marketplaces, authenticity tracking, and digital identity.
* Governments can and should do more to support blockchain innovation and adoption, including by supporting public sector adoption, creating a flexible regulatory environment to allow experimentation, and using targeted regulatory enforcement.


Reference Type: Magazine Article

Abstract: The concept of Identification as a Service (IDaaS) is radically changing the way biometric matching and identity services are provided. So why is this transformation important? Mainly because it is a market disruption that will propel new growth in the industry. It’s also likely to change the way we interact with applications requiring strong authentication or identification services, moving from captive, closely held applications into efficient and indispensable, widely available utilities.


Reference Type: Journal Article
Available from: http://www.researchprotocols.org/2019/2/e10994/

Abstract: Background: A blockchain is a digitized, decentralized, distributed public ledger that acts as a shared and synchronized database that records cryptocurrency transactions. Despite the shift toward digital platforms enabled by electronic medical records, demonstrating a will to reform the health care sector, health systems face issues including security, interoperability, data fragmentation, timely access to patient data, and silos. The application of health care blockchains could enable data interoperability, enhancement of precision medicine, and reduction in prescription frauds through implementing novel methods in access and patient consent.

Objective: To summarize the evidence on the strategies and frameworks utilized to implement blockchains for patient data in health care to ensure privacy and improve interoperability and scalability. It is anticipated this review will assist in the development of recommendations that will assist key stakeholders in health care blockchain implementation, and we predict that the evidence generated will challenge the health care status quo, moving away from more traditional approaches and facilitating decision making of patients, health care providers, and researchers.

Methods: A systematic search of MEDLINE/PubMed, Embase, Scopus, ProQuest Technology Collection and Engineering Index will be conducted. Two experienced independent reviewers will conduct titles and abstract screening followed by full-text reading to determine study eligibility. Data will then be extracted onto data extraction forms before using the Cochrane Collaboration Risk of Bias Tool to appraise the quality of included randomized studies and the Risk of Bias in nonrandomized studies of Interventions to assess the quality of nonrandomized studies. Data will then be analyzed and synthesized.

Results: Database searches will be initiated in September 2018. We expect to complete the review in January 2019.
Conclusions: This review will summarize the strategies and frameworks used to implement blockchains in health care to increase data privacy, interoperability, and scalability. This review will also help clarify if the strategies and frameworks required for the operationalization of blockchains in health care ensure the privacy of patient data while enabling efficiency, interoperability, and scalability.


Reference Type: Conference Paper
Available from: https://link.springer.com/chapter/10.1007/978-3-030-00066-0_45 Subscription required to view.

Abstract: We introduce our solution developed for data privacy, and specifically for cognitive security that can be enforced and guaranteed using blockchain technology in SAAL (Smart Ambient Assisted Living) environments. Using our proposal the access to a patient’s clinical process resists tampering and ransomware attacks that have recently plagued the HIS (Hospital Information Systems) in various countries. One important side effect of this data infrastructure is that it can be accessed in open form, for research purposes for instance, since no individual re-identification or group profiling is possible by any means.


Reference Type: Journal Article
Available from: http://ebooks.iospress.nl/publication/50496

Abstract: We introduce our solution developed for data privacy, and specifically for cognitive security that can be enforced and guaranteed using blockchain technology in SAAL (Smart Ambient Assisted Living) environments. Personal clinical and demographic information segments to various levels that assures that it can only be rebuilt at the interested and authorized parties and no profiling can be extracted from the blockchain itself. Using our proposal the access to a patient’s clinical process resists tampering and ransomware attacks that have recently plagued the HIS (Hospital Information Systems) in various countries. The core of the blockchain model assures non-repudiation possible by any of the involved information producers thus maintaining ledger fidelity of the enclosed historical process information. One important side effect of this data infrastructure is that it can be accessed in open form, for research purposes for instance, since no individual re-identification or group profiling is possible by any means.


Reference Type: Conference Paper
Available from: http://ebooks.iospress.nl/publication/49419 Subscription required to view.

Abstract: The characteristics of the "blockchain" technology and especially its decentralized nature lead to the notion of neutrality, censorship resistance, and absolute truths, which makes the concept interesting for many different domains, such as finance, supply chain management, or the energy sector - of course also for the healthcare area (eHealth). Blockchains also offer the possibility for well-known access points for a distributed system with easy to use and simple to integrate programming interfaces, which makes it interesting as a central point for electronic healthcare data exchange in a distributed environment. This paper presents a concept for integrating and sharing distributed personal healthcare records based on smart contracts implemented on an Ethereum blockchain.


Reference Type: Journal Article
Abstract: Electronic health records may have digitized patient data, but getting that data from one clinician to another remains a huge challenge, especially since patients often have multiple doctors ordering tests, prescribing drugs, and providing treatment. Many experts now believe that blockchain technology might be just the thing to get a patient's pertinent medical information from where it is stored to where it is needed, as well as to allow patients to easily view their own medical histories. In addition, blockchain technology might also be able to help with other aspects of health care, such as improving the insurance claim or other administrative processes within healthcare networks and making health-related population data available to biomedical researchers.


Reference Type: Journal Article

Abstract: Work is already underway to bring blockchain technology to the healthcare industry, and hospital administrators are trying to figure out what it can do for them, their clinicians, and their patients. That includes administrators at Beth Israel Deaconess Medical Center, a leading academic medical center located in Boston.

Mettler M. Blockchain technology in healthcare: the revolution starts here. 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom); 2016 Sep 14-16; Munich, Germany. Piscataway, NJ: IEEE Healthcom.

Reference Type: Conference Proceedings

Abstract: Blockchain technology has shown its considerable adaptability in recent years as a variety of market sectors sought ways of incorporating its abilities into their operations. While so far most of the focus has been on the financial services industry, several projects in other service related areas such as healthcare show this is beginning to change. Numerous starting points for Blockchain technology in the healthcare industry are the focus of this report. With examples for public healthcare management, user-oriented medical research and drug counterfeiting in the pharmaceutical sector, this report aims to illustrate possible influences, goals and potentials connected to this disruptive technology.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/15/3267

Abstract: Real-time data about various traffic events and conditions—offences, accidents, dangerous driving, or dangerous road conditions—is crucial for safe and efficient transportation. Unlike roadside infrastructure data which are often limited in scope and quantity, crowdsensing approaches promise much broader and comprehensive coverage of traffic events. However, to ensure safe and efficient traffic operation, assessing trustworthiness of crowdsourced data is of crucial importance; this also includes detection of intentional or unintentional manipulation, deception, and spamming. In this paper, we design and demonstrate a road traffic event detection and source reputation assessment system for unreliable data sources. Special care is taken to adapt the system for operation in decentralized mode, using smart contracts on a Turing-complete blockchain platform, eliminating single authority over such systems and increasing resilience to institutional data manipulation. The proposed solution was evaluated using both a synthetic traffic event dataset and a dataset gathered from real users, using a traffic event reporting mobile application in a professional driving simulator used for driver training. The results show the proposed system can accurately detect a range of manipulative and misreporting behaviors, and quickly converges to the final trust score even in a resource-constrained environment of a blockchain platform virtual machine.


Reference Type: Conference Paper
Abstract: Blockchain has proved itself to be tamper resistant and secure. It is increasingly getting attention from companies changing from centralized to decentralized systems. This paper proposes a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system. A prototype demonstrates the application of blockchain in identity and access management using the Hyperledger Fabric framework. It provides a proof of concept based on a use case concerning Electronic Health Records from the healthcare domain where an immutable and auditable history is desired for data concerning patients. Basic authentication and authorization operations are able to execute in 2-3 seconds with an initial size of blockchain of about 3.8 MB covering physicians in Denmark.

Reference Type: Journal Article
Abstract: Blockchain has recently joined a long line of technological innovations that have been characterised as disruptive to, and possibly even subversive of, fundamental legal principles. This article looks behind the hype to examine how blockchain might – or might not – be compatible with established legal and regulatory models. Data protection is discussed as an example of an area of law that some have claimed cannot be reconciled with blockchain. Various other conflicts are also identified and concerns about blockchain are placed in the context of wider historical debates about new technologies vs law.

Reference Type: Journal Article
Abstract: With the soaring value of bitcoin and frenzy over cryptocurrency, the blockchain technology that sparked the bitcoin revolution has received heightened attention from both practitioners and academics. Blockchain technology often causes controversies surrounding its application potential and business ramifications. The blockchain is a peer-to-peer network of information technology that keeps records of digital asset transactions using distributed ledgers that are free from control by intermediaries such as banks and governments. Thus, it can mitigate risks associated with intermediaries’ interventions, including hacking, compromised privacy, vulnerability to political turmoil, costly compliance with government rules and regulation, instability of financial institutions, and contractual disputes. This article unlocks the mystique of blockchain technology and discusses ways to leverage blockchain technology to enhance supply chain resilience in times of increased risks and uncertainty.

Reference Type: Conference Proceedings
Abstract: The Internet Of Things (IoT) is poised to make substantial inroads in all aspects of modern life before the end of this decade, including applications in smart grids, smart cities, transportation, crowdsensing, e-health, ambient assisted living, and home automation, to list just a few. Although it is recognized that IoTSec mechanisms and principles are needed across the entire IoT ecosystem, many of the intrinsic features of IoT systems make the IoT vulnerable to cybersecurity breaches. Firms wonder if the mechanisms required to protect the users and the data are ready for “prime time”, especially in the e-health arena. The field of big data as related to security event processing, is relatively new, especially in the context of IoT. Challenges include but are not limited to capture, transmission, analysis and curation of the data. This article provides a novel IoT protocol architecture and examines security tools and techniques that can be leveraged as part of the deployment of IoT, these mechanisms are particularly important in e-health and assisted living applications.

Reference Type: Conference Proceedings
Available from: https://www.researchgate.net/publication/334591932_Towards_a_Blockchain-Based_Healthcare_Information_System

Abstract: Healthcare information systems are the next big application area for Blockchain technology. However, straightforward extensions of existing digital cryptocurrency systems such as Bitcoin and Ethereum results in systems that are unsuitable for the challenges posed by healthcare systems. In this paper, we propose an architecture for a blockchain-based healthcare information system in which block validation is performed through collective signatures initiated by a designated leader and executed by a pool of witnesses. Furthermore, we describe a smart-contract based approach that allows data owners to explicitly grant or revoke authorizations for other actors to access healthcare data. All accesses, successful or not, are recorded on the blockchain as separate transactions, thus ensuring transparency and privacy protection.


Reference Type: Journal Article

Abstract: Current incentives for publishing in academic journals result in a “winner-take-all” contest-like situation, with significant benefits for publishing research in quality journals. At the same time, empirically, we observe a greater incidence of research misconduct. The purpose of this paper is to summarize the nature and extent of the misconduct problem, to show why it may persist in the absence of conscious remedial action, and to discuss solutions that help lower the likelihood of spurious research escaping undetected. A simple model is constructed to emphasize that there exists the potential for a Prisoners’ Dilemma in academia, where scholars engage in misconduct at equilibrium (the Academic Dilemma). The paper then examines why conventional “centralized” regulatory solutions under the current system are not likely to succeed in resolving the problem, analyzes the properties of a decentralized solution utilizing blockchains, and argues that once incentive structures in academia are factored in, a permissioned blockchain may emerge as an effective middle-ground solution for mitigating scientific misconduct. In doing so, the paper highlights the importance of new technologies and recent advancements in Open Science for battling misconduct, and takes stock of the evolving nature of academic publishing.


Reference Type: Journal Article

Abstract: In medical systems for patient’s authentication, keeping biometric data secure is a general problem. Many studies have presented various ways of protecting biometric data especially finger vein biometric data. Thus, It is needs to find better ways of securing this data by applying the three principles of information security aforementioned, and creating a robust verification system with high levels of reliability, privacy and security. Moreover, it is very difficult to replace biometric information and any leakage of biometrics information leads to earnest risks for example replay attacks using the robbed biometric data. In this paper presented criticism and analysis to all attempts as revealed in the literature review and discussion the proposes a novel verification secure framework based confidentiality, integrity and availability (CIA) standard in triplex blockchain-particle swarm optimization (PSO)-advanced encryption standard (AES) techniques for medical systems patient’s authentication. Three stages are performed on discussion. Firstly, proposes a new hybrid model pattern in order to increase the randomization based on radio frequency identification (RFID) and finger vein biometrics. To achieve this, proposed a new merge algorithm to combine the RFID features and finger vein features in one hybrid and random pattern. Secondly, how the propose verification secure framework are followed the CIA standard for teledemecine authentication by combination of AES encryption technique, blockchain and PSO in steganography technique based on proposed pattern model. Finally, discussed the validation and evaluation of the proposed verification secure framework.
corporate models, society and global institutions. Blockchain infiltration will be met with resistance, trust layer. Blockchains are enormous catalysts for change that hit at governance, ways of life, traditional as the Web was that first layer back in 1990. That new layer is mostly about trust, so we could call it the way by the force of its progression. Plainly, it is the second significant overlay on top of the Internet, just marching phenomenon, slowly advancing like a tsunami, and gradually enveloping everything along its path. Our article offers a primer on blockchain technology aimed at general managers and executives. The key contributions of this article lie in providing an explanation of blockchain, including how a blockchain transaction works and a clarification of terms, and outlining different types of blockchain technologies. We also discuss how different types of blockchain impact business models. Building on the well-established business model framework by Osterwalder and Pigneur, we outline the effect that blockchain technologies can have on each element of the business model, along with illustrations from firms developing blockchain technology.


Reference Type: Journal Article
Available from: https://www.jmir.org/2019/5/e13385/

Abstract: BACKGROUND: Blockchain is emerging as an innovative technology for secure data management in many areas, including medical practice. A distributed blockchain network is tolerant against network fault, and the registered data are resistant to tampering and revision. The technology has a high affinity with digital medicine like mobile health (mHealth) and provides reliability to the medical data without labor-intensive third-party contributions. On the other hand, the reliability of the medical data is not insured before registration to the blockchain network. Furthermore, there are issues with regard to how the clients’ mobile devices should be dealt with and authenticated in the blockchain network in order to avoid impersonation. OBJECTIVE: The aim of the study was to design and validate an mHealth system that enables the compatibility of the security and scalability of the medical data using blockchain technology. METHODS: We designed an mHealth system that sends medical data to the blockchain network via relay servers. The architecture provides scalability and convenience of operation of the system. In order to ensure the reliability of the data from clients’ mobile devices, hash values with chain structure (client hashchain) were calculated in the clients’ devices and the results were registered on the blockchain network. RESULTS: The system was applied and deployed in mHealth for insomnia treatment. Clinical trials for mHealth were conducted with insomnia patients. Medical data of the recruited patients were successfully registered with the blockchain network via relay servers along with the hashchain calculated on the clients’ mobile devices. The correctness of the data was validated by identifying illegal data, which were made by simulating fraudulent access. CONCLUSIONS: Our proposed mHealth system, blockchain combined with client hashchain, ensures compatibility of security and scalability in the data management of mHealth medical practice. TRIAL REGISTRATION: UMIN Clinical Trials Registry UMIN000032951; https://upload.umin.ac.jp/cgi-open-bin/ctr_e/ctr_view.cgi?recptno=R000037564 (Archived by WebCite at http://www.webcitation.org/78HP5iFIw).

Purchase required.

Reference Type: Electronic Book

Abstract: [FIRST PARAGRAPH] If the blockchain has not shocked you yet, I guarantee it will shake you soon. I have not seen anything like this since the start of the Internet, in terms of capturing the imagination of people, a small number first, but then spreading rapidly. Welcome to the new world of the blockchain and blockchains. At its core, the blockchain is a technology that permanently records transactions in a way that cannot be later erased but can only be sequentially updated, in essence keeping a never-ending historical trail. This seemingly simple functional description has gargantuan implications. It is making us rethink the old ways of creating transactions, storing data, and moving assets, and that's only the beginning. The blockchain cannot be described just as a revolution. It is a marching phenomenon, slowly advancing like a tsunami, and gradually enveloping everything along its path by the force of its progress. Plainly, it is the second significant overlay on top of the Internet, just as the Web was that first layer back in 1990. That new layer is mostly about trust, so we could call it the trust layer. Blockchains are enormous catalysts for change that hit at governance, ways of life, traditional corporate models, society and global institutions. Blockchain infiltration will be met with resistance,
because it is an extreme change.


Reference Type: Conference Proceedings

Abstract: A blockchain system is different from the hitherto used featuring robustness and disintermediation. A blockchain consists of records (blocks) recorded in a digital ledger, thoroughly decentralized where transactions are recorded in contrast to the tables in the relational database. A transaction once recorded in the system is resistant to alteration. The paper proposed several applications of blockchain system integrating it with the national identity of an individual. The national identification records of an individual must contain the fundamental details regarding the individual along with the biometrics. The available attributes of the national identification records can be used efficaciously in applications such as banking, digitizing healthcare, digital voting, etc. An example for such a national identity is the Aadhar in India which is currently utilized in centralized applications. Integrating Aadhar with blockchain yields illimitable applications in a decentralized, secure and transparent manner.


Reference Type: Report
Available from: https://www.weforum.org/whitepapers/blockchain-beyond-the-hype

Abstract: This common sense and practical framework is designed to assist executives in understanding whether blockchain is an appropriate and helpful tool for their business needs. It starts from the premise that blockchain is merely a technology – much like many others that are already used in society – and like other technologies it is as much about change management and careful attention to the economics and business models of industries and companies involved as it is about technology evangelism. For any organization, blockchain technology should not be a goal in itself but a tool deployed to achieve specific purposes.

This toolkit is based on real-world experience of blockchain in a variety of projects across a variety of industries that have been analysed by Imperial College London to develop an initial framework. The framework has been reviewed and further developed by members of the 2017 World Economic Forum’s Global Future Council on Blockchain and has been trialled through a variety of means, including with global chief executive officers (CEOs) at the World Economic Forum Annual Meeting 2018 in Davos-Klosters. Over the coming months, the World Economic Forum’s Center for the Fourth Industrial Revolution, in partnership with various institutions, will be releasing customized versions of this toolkit focused on specific sectors and use cases.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5911506/

Abstract: Modeling and simulation in computational neuroscience is currently a research enterprise to better understand neural systems. It is not yet directly applicable to the problems of patients with brain disease. To be used for clinical applications, there must not only be considerable progress in the field but also a concerted effort to use best practices in order to demonstrate model credibility to regulatory bodies, to clinics and hospitals, to doctors, and to patients. In doing this for neuroscience, we can learn lessons from long-standing practices in other areas of simulation (aircraft, computer chips), from software engineering, and from other biomedical disciplines. In this manuscript, we introduce some basic concepts that will be important in the development of credible clinical neuroscience models: reproducibility and replicability; verification and validation; model configuration; and procedures and processes for credible mechanistic multiscale modeling. We also discuss how garnering strong community involvement can promote model credibility. Finally, in addition to direct usage with patients, we note the potential for simulation usage in the area of Simulation-Based Medical Education, an area which to date has been primarily reliant on physical models (mannequins) and scenario-based simulations rather than on numerical simulations.
Myers W. Blockchain is coming — ready or not, expert warns clinical research site executives. CenterWatch Weekly. 2018 May 29:1, 4.

Reference Type: Magazine Article


Abstract: Blockchain technology offers a lot of promise to sites but it can also destabilize those companies that don’t properly prepare for it, a site executive warned her fellow professionals Tuesday.

When Wendy Charles, the operations manager and researcher at Rocky Mountain Poison & Drug Center at Denver Health asked an audience at the MAGI Clinical Research Conference 2018 East in Arlington, VA, how many had heard of blockchain, very few hands went up. When she asked them how many of their companies were already using blockchain in their business, no hands went up.

“This is coming,” Charles said, “and blockchain will be a part of your everyday life in the near future so it’s important to be aware of what people face.”


Reference Type: Conference Proceedings

Available from: https://www.academia.edu/38066792/Information_sharing_for_supply_chain_management_based_on_BC?email_work_card=view-paper

Open access: https://ieeexplore.ieee.org/idm.oclc.org/document/8010716 Subscription required to view.

Abstract: Supply Chain Management systems provide information sharing and analysis to companies and support their planning activities. They are not based on the real data because there is asymmetric information between companies, then leading to disturbance of the planning algorithms. On the other hand, sharing data between manufacturers, suppliers and customers becomes very important to ensure reactivity towards markets variability. Especially, double marginalization is a widespread and serious problem in supply chain management. Decentralized systems under wholesale price contracts are investigated, with double marginalization effects shown to lead to supply insufficiencies, in the cases of both deterministic and random demands. This paper proposes a blockchain based solution to address the problems of supply chain such as Double Marginalization and Information Asymmetry etc.


Reference Type: Journal Article


Abstract: Health data exchange is a major challenge due to the sensitive information and the privacy issues entailed. Considering the European context, in which health data must be exchanged between different European Union (EU) Member States, each having a different national regulatory framework as well as different national healthcare system structures/organizations, the challenge is even greater.

Europe has tried to address this challenge by launching in 2008, the epSOS (“Smart Open Services for European Patients”) project, which was a European large-scale pilot on cross-border sharing of specific health data and services. The adoption of the framework for cross-border health data exchange proposed in epSOS, with most Member States planning the implementation of this framework by 2020. Yet, this framework is quite generic and leaves a wide space to each Member State regarding the definition of roles, processes, workflows and especially the specific integration with the National Infrastructure for eHealth. The aim of this paper is to present the current landscape of the evolving eHealth infrastructure for cross-border health data exchange in Europe as a result of past and ongoing initiatives, and illustrate challenges, open issues and limitations through a specific case study describing how Italy is approaching its adoption and accommodates the identified barriers. The paper discusses ethical, regulatory and organizational issues, while it focuses technical aspects such as interoperability and cybersecurity, as applicable in this context. Regarding cybersecurity aspects per se, we present the approach of the KONFIDO EU-funded project, which aims to reinforce trust and security in European cross-border health data exchange by leveraging novel approaches and cutting-edge technologies, such as homomorphic encryption, photonic Physical Unclonable Functions (p-PUF), a Security Information and Event Management (SIEM) system, and blockchain-based auditing. In particular, we explain how KONFIDO will test its outcomes through a dedicated pilot based on a realistic scenario, in which Italy is involved in health data exchange with other European countries.
Abstract: The traditional medical education ecosystems are largely centralised and confined to the boundaries of academic institutions [1]. Rather than promoting efficiency and global forward thinking, a number of medical institutions have become inwardly focused, confining themselves to their own institutional rules and frameworks [2,3]. In the past two years, the utility of blockchain in the higher education setting has been extensively studied [4]. A blockchain is essentially a distributed, immutable, trustworthy, decentralised database that keeps an irreversible, time-stamped record of transfer of value between users for every operation that has ever been carried out on its network [5]. This has traditionally been used in cryptocurrency transactions, however, with the rise of blockchain based Decentralised Applications (DApps), the potential benefits of this ground-breaking technology in higher education are now being explored [6]. Although still in the early developmental stages, blockchain holds promising potential for use in medical education. Some of these are budding hypothesis while in other areas, we have witnessed real, tangible progress [7].

This article analyses the potential use cases for blockchain deployment in medical education ecosystems, to improve the efficiency, security, functionality and effectiveness of existing infrastructures [8]. We conclude the essay by proposing how blockchain can eliminate the growing problem of fraudulent academic accreditations.
Abstract: In the Summer of 2016, a hacker by the name of “thedarkoverlord” stole over 650,000 medical records from the databases of three separate healthcare institutions. The hacker was not only selling the records for hundreds of thousands of dollars online, but may also have been extorting the institutions by demanding money to prevent further attacks and distribution of records. The value of these medical records is ten to sixty times greater than a credit card number on the black market, as the information on the records may be used to perpetrate other types of fraud, such as filing fraudulent tax returns, making these records a prime target for malicious hackers.

Unfortunately, this is not an isolated or uncommon incident. In 2015, nearly 100 million healthcare records were compromised. The attacks affect everyone, from everyday people to celebrities such as Kanye West. The combination of the value of medical records and the relatively low cybersecurity of healthcare facilities make healthcare records one of the most lucrative targets for cybercriminals. According to the Department of Health and Human Services, more than 113 million records were compromised in 2015, and during the first quarter of 2016, the healthcare industry averaged 4 attacks per week. In fact, the 2016 IBM Cyber Security Intelligence Index named the healthcare industry the single most attacked industry. Efforts to modernize healthcare facilities to match the rapidly advancing technological landscape has created and exposed a host of vulnerabilities that are actively targeted by malicious parties.


Abstract: Smart contracts—stateful executable objects hosted on blockchains like Ethereum—carry billions of dollars worth of coins and cannot be updated once deployed. We present a new systematic characterization of a class of trace vulnerabilities, which result from analyzing multiple invocations of a contract over its lifetime. We focus attention on three example properties of such trace vulnerabilities: finding contracts that either lock funds indefinitely, leak them carelessly to arbitrary users, or can be killed by anyone. We implemented MAIAN1, the first tool for precisely specifying and reasoning about trace properties, which employs inter-procedural symbolic analysis and concrete validator for exhibiting real exploits. Our analysis of nearly one million contracts flags 34,200 (2,365 distinct) contracts vulnerable, in 10 seconds per contract. On a subset of 3,759 contracts which we sampled for concrete validation and manual analysis, we reproduce real exploits at a true positive rate of 89%, yielding exploits for 3,686 contracts. Our tool finds exploits for the infamous Parity bug that indirectly locked 200 million dollars worth in Ether, which previous analyses failed to capture.


Abstract: The future health care system will contain an ever expanding number of digital elements. The data stored both at a centralized health care level and at a local, patient level (e.g. on a smartphone) will be core elements when deciding treatment strategies in a health care scenario with Internet of Things (IoT) based elements. The current way of manufacturing pharmaceutical products and related existing logistic solutions are not ready for such a revolution. One of the key challenges is cybersecurity and related robust public key infrastructure (PKI) solution. This work introduces one element of a potential solution at a prototype level: the concept of cryptopharmaceuticals, where pharmaceutical products are connected in a patient-specific blockchain of individual dosage units. This technology is based on the concept where each produced dosage unit has a unique information-rich pattern (IRP). A proof of concept smartphone app was applied to demonstrate the visualization of this blockchain at different levels. This includes the manufacturing of the individualized dosage unit, the patient view for his/her personal blockchain, and integration of these products into a health IoT system. This unbreakable blockchain of personal medication history will provide means to avoid counterfeit products and to enable innovative logistic solutions.

Nortey RN, Yue L, Agdedanu PR, Adjeisah M. Privacy module for distributed electronic health records (EHRs) using the blockchain. 2019 IEEE 4th International Conference on Big Data Analytics (ICBDA);
Abstract: Currently, storing patient's sensitive data by medical healthcare into Electronic Healthcare Records (EHR) has evolved immensely. Specifically, distributed healthcare records have brought ease to how hospitals and other different third parties access the sensitive medical health information of patients for various uses leading to generation of big data. Big data in healthcare is important as it can be used in the prediction of outcome of diseases, prevention of co-morbidities fatality and saving the cost of medical treatment. However, this has also made it easy for security breaches and privacy violations during the data collection process. In this paper, we propose a platform which uses the blockchain technology for privacy preservation during collection, management and distribution of EHR data. The aim of this paper is to ensure the total privacy, integrity and access control of distributed electronic health records to the data owners during its distribution on the blockchain. Simulated results demonstrate our proposed system establishes total transparency and ensures perfect privacy within the distributed network of sharing EHRs in the medical setting using the blockchain.


architecture, who are referred to as “participating professionals.” Business entities, such as corporations, partnerships and limited liability companies, can also participate as “enterprise users,” with linkage through the network to both standard users and participating professionals. The network enables standard users, participating professionals and enterprise users to communicate, share information, conduct studies, and negotiate and/or create documents relating to the professional disciplines.


Reference Type: Journal Article

Abstract: It is a common practice to issue a summary of a learner’s learning achievements in form of a transcript or certificate. However, detailed information on the depth of learning and how learning or teachings were conducted is not present in the transcript of scores. This work presents the first practical implementation of a new platform for keeping track of learning achievements beyond transcripts and certificates. This is achieved by maintaining digital hashes of learning activities and managing access rights through the use of smart contracts on the blockchain. The blockchain of learning logs (BOLL) is a platform that enable learners to move their learning records from one institution to another in a secure and verifiable format. This primarily solves the cold-start problem faced by learning data analytic platforms when trying to offer personalized experience to new learners. BOLL enables existing learning data analytic platforms to access the learning logs from other institutions with the permission of the learners and/or institution who originally have ownership of the logs. The main contribution of this paper is to investigate how learning records could be connected across institutions using BOLL. We present an overview of how the implementation has been carried out, discuss resource requirements, and compare the advantages BOLL has over other similar tools.


Reference Type: Journal Article
Available from: https://www.jmir.org/2019/5/e12426/

Abstract: Background: A blockchain is a list of records that uses cryptography to make stored data immutable; their use has recently been proposed for electronic medical record (EMR) systems. This paper details a systematic review of trade-offs in blockchain technologies that are relevant to EMRs. Trade-offs are defined as “a compromise between two desirable but incompatible features.” Objective: This review’s primary research question was: “What are the trade-offs involved in different blockchain designs that are relevant to the creation of blockchain-based electronic medical records systems?” Methods: Seven databases were systematically searched for relevant articles using the Preferred Reporting Items for Systematic Reviews and Meta-Analyses (PRISMA). Papers published from January 1, 2017 to June 15, 2018 were selected. Quality assessments of papers were performed using the Risk Of Bias In Non-randomized Studies—of Interventions (ROBINS-I) tool and the Critical Assessment Skills Programme (CASP) tool. Database searches identified 2885 articles, of which 15 were ultimately included for analysis. Results: A total of 17 trade-offs were identified impacting the design, development, and implementation of blockchain systems; these trade-offs are organized into themes, including business, application, data, and technology architecture. Conclusions: The key findings concluded the following: (1) multiple trade-offs can be managed adaptively to improve EMR utility; (2) multiple trade-offs involve improving the security of blockchain systems at the cost of other features, meaning EMR efficacy highly depends on data protection standards; and (3) multiple trade-offs result in improved blockchain scalability. Consideration of these trade-offs will be important to the specific environment in which electronic medical records are being developed. This review also uses its findings to suggest useful design choices for a hypothetical National Health Service blockchain. International Registered Report Identifier (IRR-ID): RR2-10.2196/10994


Reference Type: Report
Available from: https://www.hhs.gov/sites/default/files/combined-onc.pdf

Abstract: A successful health system relies on interoperable health IT to collect, share, and use information to transform healthcare from volume-based fiscal incentives towards more outcomes-based care. The goal is a system that promotes high-quality care, increases accessibility, lowers costs, and encourages free market innovation to empower individual patients and consumers. Through the passage
of the HITECH Act, HHS has increased adoption of EHRs and stimulated demand for a growing range of health IT and health information exchange (HIE) products and services. Achieving interoperability requires a technical, policy and stakeholder engagement driven approach. ONC is working towards meeting this demand through high level coordination between government and the private sector, advancing federally recognized standards, enhancing our certification program, and delivering key policy directives. ONC is continuing to leverage its existing authorities and responsibilities, which include technical standards coordination and harmonization work and a regulatory certification program. These are in addition to ONC’s core function of coordinating federal health IT policy through multiple mechanisms, including the Federal Health IT Coordinating Council which manages the development of the Health IT Strategic Plan, and the facilitation of our federal advisory committee.

Reference Type: Conference Paper

Abstract: Distributed Ledger technology and its most notable implementation, the Blockchain, is disrupting today’s industry in extremely fast pace with a potential to change the world. The security posture of Blockchain remains one of key topics in today’s industry and distributed services. On and on, we can embrace the attempts to implement the Blockchain technology in sensitive areas of our daily life like finance [1], insurance services [2], health care [3] etc. It is therefore crucial raise awareness of its limitations, possible improvements, as well as embedded compensations. In this paper, we provide a holistic view on the security aspects of the Blockchain technology. We identify the most notable security threats applicable in the above context and reveal technology-specific challenges that need to be taken into account. Our analysis lists the security features already embedded in the Blockchain and sample uses in nowadays industry. Our results lead to several observations, recommendations, and open points that could be considered in ongoing development of the technology.

Reference Type: Journal Article

Abstract: Blockchain refers to a range of general purpose technologies to exchange information and transact digital assets in distributed networks. The core question addressed in this paper is whether blockchain technology will lead to innovation and transformation of governmental processes. To address this question we present a critical assessment of the often exaggerated benefits of blockchain technology found in the literature and discuss their implications for governmental organizations and processes. We plea for a shift from a technology-driven to need-driven approach in which blockchain applications are customized to ensure a fit with requirements of administrative processes and in which the administrative processes are changed to benefit from the technology. Having sound governance models are found to be a condition for realizing benefits. Based on a critical assessment we offer directions for further research into the potential benefits of BC applications in e-government and the role of governance of BC architectures and applications to comply with societal needs and public values.

Reference Type: Conference Paper
Available from: http://ebooks.iospress.nl/publication/50493

Abstract: The GDPR fixes general rules applying to any kind of personal data processing as well as specific rules applying to the processing of special categories of personal data such as health data taking place in the context of scientific research or clinical software development. A short overview of new rules about how to consider where scientific and professional projects include the processing of personal health data, genetic data or biometric data and other kinds of sensitive information whose use is strictly regulated by the GDPR is provided. Some key facts to researchers and developers to adapt their practices and ensure compliance to the EU laws are included.
Abstract: Three-dimensional electron microscopy techniques like electron tomography provide valuable insights into cellular structures, and present significant challenges for data storage and dissemination. Here we explored a novel method to publicly release more than 11,000 such datasets, more than 30 TB in total, collected by our group. Our method, based on a peer-to-peer file sharing network built around a blockchain ledger, offers a distributed solution to data storage. In addition, we offer a user-friendly browser-based interface, https://etdb.caltech.edu, for anyone interested to explore and download our data. We discuss the relative advantages and disadvantages of this system and provide tools for other groups to mine our data and/or use the same approach to share their own imaging datasets.
technology, blockchain, may help ameliorate some of these problems. In broad terms, the blockchain technology enables decentralized, immutable, incorruptible public ledgers. In this Perspective, we aim to introduce current developments toward using blockchain to address several problems in omics, and to provide an outlook of possible future implications of the blockchain technology to life sciences.


Reference Type: Conference Paper
Available from: http://ebooks.iospress.nl/publication/52455

Abstract: This contribution outlines a conceptual model of a novel approach to chronic disease prevention and management: Preventative Health Account Supported by Electronic Medical Records (PHASE). The PHASE model combines predictive computation of risk scores for chronic disease and use of alternative currencies on blockchain technology to build a preventative health account to help individuals invest in a healthier lifestyle, reduce their risk scores and, in turn, reduce the related potential cost to the healthcare system.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/18/8/2575

Abstract: The Internet of Things (IoT) refers to the interconnection of smart devices to collect data and make intelligent decisions. However, a lack of intrinsic security measures makes IoT vulnerable to privacy and security threats. With its "security by design," Blockchain (BC) can help in addressing major security requirements in IoT. BC capabilities like immutability, transparency, auditability, data encryption and operational resilience can help solve most architectural shortcomings of IoT. This article presents a comprehensive survey on BC and IoT integration. The objective of this paper is to analyze the current research trends on the usage of BC-related approaches and technologies in an IoT context. This paper presents the following novelties, with respect to related work: (i) it covers different application domains, organizing the available literature according to this categorization, (ii) it introduces two usage patterns, i.e., device manipulation and data management (open marketplace solution), and (iii) it reports on the development level of some of the presented solutions. We also analyze the main challenges faced by the research community in the smooth integration of BC and IoT, and point out the main open issues and future research directions. Last but not least, we also present a survey about novel uses of BC in the machine economy.


Reference Type: Conference Paper

Abstract: The Blockchain paradigm provides a popular mechanism for establishing trust and consensus in distributed environments. While Blockchain technology is currently primarily deployed in cryptocurrency systems like Bitcoin, the concept is also expected to emerge as a key component of the Internet-of-Things (IoT), enabling novel applications in digital health, smart energy, asset tracking and smart transportation. As Blockchain networks evolve to industrial deployments with large numbers of geographically distributed nodes, the block transfer and processing delays arise as a critical issue which may create greater potential for forks and vulnerability to adversarial attacks. Motivated by these issues, we develop stochastic network models to capture the Blockchain evolution and dynamics and analyze the impact of the block dissemination delay and hashing power of the member nodes on Blockchain performance in terms of the overall block generation rate and required computational power for launching a successful attack. The results provide useful insight in crucial design issues, e.g., how to adjust the 'difficulty-of-work' in the presence of delay so as to achieve a target block generation rate or appropriate level of immunity from adversarial attacks. We employ a combination of analytical calculations and simulation experiments to investigate both stationary and transient performance features, and demonstrate close agreement with measurements on a wide-area network testbed running the Ethereum protocol.
Abstract: **Objective:** This article aims to provide a primer on blockchain technology and implementation considerations for blockchain at healthcare institutions.

**Results:** After research and interviews, we developed a primer and a high-level implementation guide for healthcare systems exploring the use of blockchain technology.

**Conclusions:** The use of blockchain technology in healthcare is at a promising stage in development but blockchain-based applications are yet to be demonstrated as a viable platform for exchanging and reviewing information. Healthcare systems should be cautiously optimistic regarding the potential of blockchain and do a thorough business and technical diligence that is driven by targeted use cases to be successful.

---


Reference Type: Journal Article


Abstract: Blockchain has drawn attention as the next-generation financial technology due to its security that suits the informatization era. In particular, it provides security through the authentication of peers that share virtual cash, encryption, and the generation of hash value. According to the global financial industry, the market for security-based blockchain technology is expected to grow to about USD 20 billion by 2020. In addition, blockchain can be applied beyond the Internet of Things (IoT) environment; its applications are expected to expand. Cloud computing has been dramatically adopted in all IT environments for its efficiency and availability. In this paper, we discuss the concept of blockchain technology and its hot research trends. In addition, we will study how to adapt blockchain security to cloud computing and its secure solutions in detail.

---


Reference Type: Journal Article

Available from: [https://www.mdpi.com/1424-8220/18/10/3577](https://www.mdpi.com/1424-8220/18/10/3577)

Abstract: Internet of Things (IoT)-based devices, especially those used for home automation, consist of their own sensors and generate many logs during a process. Enterprises producing IoT devices convert these log data into more useful data through secondary processing; thus, they require data from the device users. Recently, a platform for data sharing has been developed because the demand for IoT data increases. Several IoT data marketplaces are based on peer-to-peer (P2P) networks, and in this type of marketplace, it is difficult for an enterprise to trust a data owner or the data they want to trade. Therefore, in this study, we propose a review system that can confirm the reputation of a data owner or the data traded in the P2P data marketplace. The traditional server-client review systems have many drawbacks, such as security vulnerability or server administrator's malicious behavior. However, the review system developed in this study is based on Ethereum smart contracts; thus, this system is running on the P2P network and is more flexible for the network problem. Moreover, the integrity and immutability of the registered reviews are assured because of the blockchain public ledger. In addition, a certain amount of gas is essential for all functions to be processed by Ethereum transactions. Accordingly, we tested and analyzed the performance of our proposed model in terms of gas required.

---


Reference Type: Journal Article

Available from: [https://www.jmir.org/2019/2/e12533/](https://www.jmir.org/2019/2/e12533/)

Abstract: **BACKGROUND:** There are many perspectives on the advantages of introducing blockchain in the medical field, but there are no published feasibility studies regarding the storage, propagation, and management of personal health records (PHRs) using blockchain technology. **OBJECTIVE:** The purpose of this study was to investigate the usefulness of blockchains in the medical field in relation to transactions with and propagation of PHRs in a private blockchain. **METHODS:** We constructed a private
blockchain network using Ethereum version 1.8.4 and conducted verification using the de-identified PHRs of 300 patients. The private blockchain network consisted of one hospital node and 300 patient nodes. In order to verify the effectiveness of blockchain-based PHR management, PHRs at a time were loaded in a transaction between the hospital and patient nodes and propagated to the whole network. We obtained and analyzed the time and gas required for data transaction and propagation on the blockchain network. For reproducibility, these processes were repeated 100 times. RESULTS: Of 300 patient records, 74 (24.7%) were not loaded in the private blockchain due to the data block size of the transaction block. The remaining 226 individual health records were classified into groups A (80 patients with outpatient data from between 1 and 3 years before data collection), and C (62 patients with outpatient data 3 to 5 years old). With respect to mean transaction time in the blockchain, C (128.9 seconds) had the shortest time, followed by A (132.2 seconds) and then B (159.0 seconds). The mean propagation times for groups A, B, and C were 2138.9 seconds, and 4111.4 seconds, respectively; mean file sizes were 5.6 KB, 18.6 KB, and 45.38 KB, respectively. The mean gas consumption values were 1,900,767; 4,224,341; and 4,112,784 for groups A, B, and C, respectively. CONCLUSIONS: This study confirms that it is possible to exchange PHR data in a private blockchain network. However, to develop a blockchain-based PHR platform that can be used in practice, many improvements are required, including reductions in data size, improved personal information protection, and reduced operating costs.


Reference Type: Conference Paper

Available from: http://ebooks.iospress.nl/publication/52393

Abstract: Information sharing in healthcare remains an unsolved problem despite a plethora of standards and architectures. Effective information sharing is difficult because of the heterogeneity of health information users and data sources, organisational, ethical and legislative constraints and the very demanding requirements of clinical practice. This paper argues that the key requirement of a viable sharing architecture is to support trust in the system and between stakeholders. It uses the concept of a “democratic” approach where citizens can control and verify the use and sharing of data about them and identify ways that some of the value extracted from the data could be assigned to the patient themselves. The reasons for the survival of obsolescent methods are used to inform the design of a proposed citizen-centric architecture using blockchain technology.


Reference Type: Journal Article

Available from: https://doi.org/10.1016/j.jval.2018.10.009

Abstract: Editor’s note (January 4, 2144): The following commentary was accepted for publication in December 2143. Although it is not particularly well written, little has been published in scholarly journals discussing the demise of stand-alone human clinical experiments. The title alludes to the enormously popular 1868 science fiction novel Looking Backward: 2000-1887 by Edward Bellamy.

In the fall of 1943, British scientist healer Philip D’Arcy Hart was asked to investigate whether the fungus Penicillium patulum, administered by nasal spray, could “cure” a low-morbidity respiratory disease known as “coryza,” which was a viral syndrome largely caused by enterovirii and subsequently eradicated after the introduction of the late 21st-century nano-atmospheric cleansing procedures and modern-day global approaches to atmospheric regulation. This now eradicated and largely forgotten ailment, also called “the common cold,” afflicted human populations living in densely populated conditions, such as urban dwellers and soldiers in close quarters, as recently as the mid-21st century. Although not fatal, coryza inflicted maddening discomforts to large numbers of individuals; anecdotal evidence before that experiment led some to believe that the patulin formula would end the host’s symptoms and alleviate suffering. To investigate whether this was true, Hart conducted the first blinded randomized controlled trial (RCT) of the 20th century—an approach through which subjects and matched controls could be studied and results analyzed without previous knowledge of treatment assignment by either the subjects or the researchers.


Reference Type: Journal Article

Abstract: The electronic sharing of medical imaging data is an important element of modern healthcare systems, but current infrastructure for cross-site image transfer depends on trust in third-party intermediaries. In this work, we examine the blockchain concept, which enables parties to establish consensus without relying on a central authority. We develop a framework for cross-domain image sharing that uses a blockchain as a distributed data store to establish a ledger of radiological studies and patient-defined access permissions. The blockchain framework is shown to eliminate third-party access to protected health information, satisfy many criteria of an interoperable health system, and readily generalize to domains beyond medical imaging. Relative drawbacks of the framework include the complexity of the privacy and security models and an unclear regulatory environment. Ultimately, the large-scale feasibility of such an approach remains to be demonstrated and will depend on a number of factors which we discuss in detail.


Reference Type: Report

Abstract: A blockchain system for electronic health records (EHRs), framed as a protocol through which to access and maintain health data, guarantees security and privacy through empowering the user with control of their own data. While using a blockchain architecture approaches interoperability through centralization of data, the use of Ethereum’s smart contracts enables an unprecedented ease of data sharing which transcends in simplicity of use and security. Despite this potential, these advancements depend on patients’ ability to own their health data and the establishment of a structure for identity verification. Furthermore, the establishment of these systems is contingent on the ability of patients to navigate these systems with competence. Separate even from patient use, the viability of a blockchain solution is determined by the security and standardization of the existing EHR systems. And aside from the security of a blockchain solution, there are few incentives for individual hospitals to work to make their EHRs accessible through a blockchain, and thus the government must lead this endeavor.

Peck ME. Blockchain world - do you need a blockchain? This chart will tell you if the technology can solve your problem. IEEE Spectr. 2017;54(10):38-60. Epub 2017 Sep 28.

Reference Type: Journal Article

Abstract: According to a study released this July by Juniper Research, more than half the world's largest companies are now researching blockchain technologies with the goal of integrating them into their products. Projects are already under way that will disrupt the management of health care records, property titles, supply chains, and even our online identities. But before we remount the entire digital ecosystem on blockchain technology, it would be wise to take stock of what makes the approach unique and what costs are associated with it. Blockchain technology is, in essence, a novel way to manage data. As such, it competes with the data-management systems we already have. Relational databases, which orient information in updatable tables of columns and rows, are the technical foundation of many services we use today. Decades of market exposure and well-funded research by companies like Oracle Corp. have expanded the functionality and hardened the security of relational databases. However, they suffer from one major constraint: They put the task of storing and updating entries in the hands of one or a few entities, whom you have to trust won't mess with the data or get hacked.


Reference Type: Journal Article

Abstract: Bitcoin was hatched as an act of defiance. Unleashed in the wake of the Great Recession, the cryptocurrency was touted by its early champions as an antidote to the inequities and corruption of the traditional financial system. They cherished the belief that as this parallel currency took off, it would compete with and ultimately dismantle the institutions that had brought about the crisis. Bitcoin’s unofficial catchphrase, “In cryptography we trust,” left no doubt about who was to blame: It was the middlemen, the bankers, the “trusted” third parties who actually couldn’t be trusted. These humans simply got in the way of other humans, skimming profits and complicating transactions.

Reference Type: Journal Article


Abstract: When bitcoin was unleashed on the world eight years ago, it filled a specific need, for a digital currency that wasn't under anybody's control. But it wasn't long before people realized the technology behind Bitcoin—the blockchain—could do much more than record monetary transactions. That realization has lately blossomed into a dazzling and often bewildering array of startup companies, initiatives, corporate alliances, and research projects. Collectively, they're facing a question that will have an enormous impact: What can the blockchain do better than conventional databases? Billions of dollars will hinge on the answer in the next several years. Can the technology link neighborhood buyers and sellers of rooftop-generated solar electricity? Can it keep track of property titles, academic transcripts, energy market credits, and state licenses for health care providers? Can it check the status of airline flights—and make reparations to weary travelers if their flights are delayed? We'll soon see: All of those proposals have been embodied in blockchain-based agreements called smart contracts, which are being tested right now.


Reference Type: Electronic Article

Abstract: This exploratory study examines how distributed ledger technologies could be used within the plasma derivatives supply chain. The plasma derivatives are used increasingly in the pharmaceutical market and the supply chain is global. However, there are significant risks relating to the governance of the supply. The risks include unclear origin of plasma and the propagation of contaminated or poor-quality blood to the pharmaceutical production process. From an ethical perspective, the risk is that vulnerable individuals are exploited in the donation process. Finally, the plasma supply chain currently depends on only a few exporters of plasma, which presents a supply chain risk.

Design: The blockchain technology is piloted in other areas of pharmaceutical supply chains and in this study we examine those solutions and conceptualize how a similar solution can be applied to the plasma supply chain. We identify risks within the plasma supply chain and discuss how blockchain-based solutions can mitigate those risks.

Results: Drawing on existing literature within the pharmaceutical blockchain arena, we introduce a solution to verify the origin of plasma. We also model how the blockchain technology can be used to tackle ethical and supply chain risks.

Conclusions: Blockchain can have a role in mitigating plasma supply chain risks. The area is, however, novel and requires more research.


Reference Type: Journal Article


Abstract: Unspent Transaction Outputs (UTXOs) are the internal mechanism used in many cryptocurrencies to represent coins. Such representation has some clear benefits, but also entails some complexities that, if not properly handled, may leave the system in an inefficient state. Specifically, inefficiencies arise when wallets (the software responsible for transferring coins between parties) do not manage UTXOs properly when performing payments. In this paper, we study three cryptocurrencies: Bitcoin, Bitcoin Cash and Litecoin, by analysing the state of their UTXO sets, that is, the status of their sets of spendable coins. These three cryptocurrencies are the top-3 UTXO-based cryptocurrencies by market capitalization. Our analysis shows that the usage of each cryptocurrency presents some differences, and led to different results. Furthermore, it also points out that the management of the transactions has not always been performed efficiently and therefore, the current state of the UTXO sets is far from ideal.


Reference Type: Journal Article
New network technologies are framed as eliminating ‘transaction costs’, a notion first developed in economic theory that now drives the design of market systems. However, the actual promise of the elimination of transaction costs seems unfeasible, because of a cyclical pattern in which network technologies that make that promise create processes of institutionalization that create new forms of transaction costs. Nonetheless, the promises legitimize the exemption of innovations of network technologies from critical scrutiny.


Reference Type: Journal Article

Abstract: Blockchain technology—the platform underpinning Bitcoin, a global digital payment system—has attracted more than $1.2 billion of investment from some of the world’s leading corporations for its security and immutability. More than 130 million secure Bitcoin transactions have occurred since the digital currency launched in 2009. Today, Bitcoin can be used to make purchases from Microsoft, buy food in neighborhood cafes, book flights and hotel rooms, and even pay for medical care.

For the health care industry, blockchain technology stands to revolutionize the interoperability, security, and accountability of electronic health records (EHR) and health information technology (HIT), medical supply chains, payment methodologies, research capabilities, and data ownership. In fact, in the 2015 report “Connecting Health and Care for the Nation, a Shared Nationwide Interoperability Roadmap,” the Office of the National Coordinator for Health Information Technology set a goal of establishing full EHR interoperability by 2024.

As blockchain technology continues to develop, it is important that surgeons and other stakeholders understand both its capabilities and its limitations. This article describes blockchain technology’s implications for health care, research, and the practice of surgery, and introduces the term “electronic health chain” (EHC).


Reference Type: Electronic Book Section

Abstract: This paper expounds the main principles behind blockchain technology and some of its cutting-edge applications. Firstly, we present the core concepts at the heart of the blockchain, and we discuss the potential risks and drawbacks of public distributed ledgers, and the shift toward hybrid solutions. Secondly, we expose the main features of decentralized public ledger platforms. Thirdly, we show why the blockchain is a disruptive and foundational technology, and fourthly, we sketch out a list of important applications, bearing in mind the most recent evolutions.


Reference Type: Journal Article

Abstract: We set out to examine the relevance of blockchain technology for healthcare management in general, and for consumer medical electronics and the portable devices connected in particular. After considering the shortcomings of private and centralized organizations for access to patient data in a fist part, we analyze the transformative role of blockchain for the management of electronic health records (EHRs). We evoke the role of public private partnerships for the design of healthcare blockchain strategies, and we address the fast-growing segment of consumer medical electronics and the Internet of Medical Things.

Abstract: At this point last year, most of us had little idea what “Blockchain”, “Bitcoin”, “Cryptocurrency”, or a “Hyperledger” were. However, thanks to the recent rise of cryptocurrencies in media outlets and social media, most of the public, including medical professionals, are able to catch a glimpse of a technology that could potentially improve some portions of the medical data conundrum.

What is blockchain and why would we use it in the healthcare system? “Blockchain is a shared, immutable record of peer-to-peer transactions built from linked transaction blocks and stored in a digital ledger” [1]. To put more simply, blockchain offers a record of peer-to-peer transactions kept out in the open so that everyone can see each of the transactions.

REFERENCE


Economy has created many new opportunities for investing, purchasing goods and services, compensating employees, and streamlining business processes. However, like many technological developments that have occurred over the past several decades, the legal system has struggled to keep pace. This unsettled landscape has created unique challenges for attorneys tasked with advising clients on the many potential legal implications posed by the increased proliferation of virtual currencies and the repurposing of blockchain technology for other economic uses. This article explains this new technology, examines its legal and economic implications, and provides a roadmap for researching these issues.


Reference Type: Journal Article

Abstract: Humanity’s notion of trust is shaped by new platforms operating in the emerging sharing economy, acting as intermediate matchmaker for ride sharing, housing facilities or freelance labour, effectively creating an environment where strangers trust each other. While millions of people worldwide rely on online sharing activities, such services are often facilitated by a few predatory companies, managing trust relations. This centralization of responsibility raises questions about ethical and political issues like regulatory compliance, data portability and monopolistic behaviour. Recently, blockchain technology has gathered a significant amount of support and adoption, due to its inherent decentralized and tamper-proof structure. We present a blockchain-powered blueprint for a shared and public programmable economy. The focus of our architecture is on four essential primitives: digital identities, blockchain-based trust, programmable money and marketplaces. Trust is established using only historical interactions between strangers to estimate trustworthiness. Every component of our proposed technology stack is designed according to the defining principles of the Internet itself: self-governance, autonomy and shared ownership. Real-world viability of each component is demonstrated with a functional prototype or running code. Our vision is that the highlighted technology stack devies trust, new acts, principles and rules beyond the possibilities in current economic, legal and political systems.


Reference Type: Journal Article

Abstract: Information sharing, analysis of various company and customer demands, planning activities etc can be coordinated and monitored with the help of supply chain management system. The planning algorithms are disturbed with the asymmetric information between companies. One of the major problem in supply chain management is double marginalization. This paper proposes a block chain based solution and homomorphism encryption to address the problems of supply chain such as double marginalization and information asymmetry etc.


Reference Type: Journal Article
Available from: https://search.proquest.com/openview/bc1594ace75fe74f55660832a0e3e1c0/1 Subscription required to view.

Abstract: The article focuses on a revelation by a World Economic Forum (WEF) that financial infrastructure could be reformed by blockchain. It is mentioned that by lowering operating costs, increasing security and revolutionizing payment networks, blockchain could change financial intermediation. It is noted that existing regulatory requirements would not be abolished by blockchain although it could render some market infrastructure redundant.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/PMC5741780/
Abstract: The Republic of Estonia leads Europe in the provision of public digital services. The national communications and transactions platform allows for twenty-first century governance by allowing for transparency, e-safety (inter alia privacy), e-security, entrepreneurship and, among other things, rising levels of prosperity, and well-being for all its Citizens. However, a series of Information Infrastructure attacks against the Estonian e-society infrastructure in 2007 became one of the best known incidents and experiences that fundamentally changed both Estonian and international discussions about Cyber Security and Privacy. Estonian experience shows that an open and transparent attitude provides a good foundation for trust between the citizen and the State, and gives more control to the real owner of the data - the Citizen. Another important lesson is that the Citizen needs to be confident in the government's ability to keep their data safe – in terms of confidentiality, integrity and availability - establishing a strong link between privacy and information security. This paper discusses certain critical choices, context, and events connected to the birth and growth of the Estonian e-society in terms of Privacy.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/10/2337

Abstract: In this paper, we present Low-Bandwidth Distributed Applications Framework (LDAF)-an application-aware gateway for communication-constrained Internet of things (IoT) devices. A modular approach facilitates connecting to existing cloud backend servers and managing message formats and APIs’ native application logic to meet the communication constraints of resource-limited end devices. We investigated options for positioning the LDAF server in fog computing architectures. We demonstrated the approach in three use cases: (i) a simple domain name system (DNS) query from the device to a DNS server, (ii) a complex interaction of a blockchain-based IoT device with a blockchain network, and (iii) difference based patching of binary (system) files at the IoT end devices. In a blockchain smart meter use case we effectively enabled decentralized applications (DApps) for devices that without our solution could not participate in a blockchain network. Employing the more efficient binary content encoding, we reduced the periodic traffic from 16 kB/s to ~1.1 kB/s, i.e., 7% of the initial traffic. With additional optimization of the application protocol in the gateway and message filtering, the periodic traffic was reduced to ~1% of the initial traffic, without any tradeoffs in the application's functionality or security. Using a function of binary difference we managed to reduce the size of the communication traffic to the end device, at least when the binary patch was smaller than the patching file.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/11/2647

Abstract: Those working on Blockchain technologies have described several new innovative directions and novel services in the Internet of things (IoT), including decentralized trust, trusted and verifiable execution of smart contracts, and machine-to-machine communications and automation that reach beyond the mere exchange of data. However, applying blockchain principles in the IoT is a challenge due to the constraints of the end devices. Because of fierce cost pressure, the hardware resources in these devices are usually reduced to the minimum necessary for operation. To achieve the high coverage needed, low bitrate mobile or wireless technologies are frequently applied, so the communication is often constrained, too. These constraints make the implementation of blockchain nodes for IoT as standalone end-devices impractical or even impossible. We therefore investigated possible design approaches to decentralized applications based on the Ethereum blockchain for the IoT. We proposed and evaluated three application architectures differing in communication, computation, storage, and security requirements. In a pilot setup we measured and analyzed the data traffic needed to run the blockchain clients and their applications. We found out that with the appropriate designs and the remote server architecture we can strongly reduce the storage and communication requirements imposed on devices, with predictable security implications. Periodic device traffic is reduced to 2400 B/s (HTTP) and 170 B/s (Websocket) from about 18 kB/s in the standalone-device full client architecture. A notification about a captured blockchain event and the corresponding verification resulted in about 2000 B of data. A transaction sent from the application to the client resulted in an about 500 B (HTTP) and 300 B message (Websocket). The key store location, which affects the serialization of a transaction, only had a small influence on the transaction-related data. Raw transaction messages were 45 B larger than when passing the JSON transaction objects. These findings provide directions for fog/cloud IoT application designers to avoid unrealistic expectations imposed upon their IoT devices and blockchain technologies, and enable them to select the appropriate system design according to the intended use case and system constraints. However, for very low bit-rate communication networks, new communication protocols for device to blockchain-client need to be considered.

Puthal D, Malik N, Mohanty SP, Kougianos E, Das G. Everything you wanted to know About the

Reference Type: Journal Article


Abstract: In 2008, the emergence of the blockchain as the foundation of the first-ever decentralized cryptocurrency not only revolutionized the financial industry but proved a boon for peer-to-peer (P2P) information exchange in the most secure, efficient, and transparent manner. The blockchain is a public ledger that works like a log by keeping a record of all transactions in chronological order, secured by an appropriate consensus mechanism and providing an immutable record. Its exceptional characteristics include immutability, irreversibility, decentralization, persistence, and anonymity.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/8/2449

Abstract: The adaptive coordination of trust services can provide highly dependable and personalized solutions for industrial requirements in the service-oriented industrial internet of things (IIoT) architecture to achieve efficient utilization of service resources. Although great progress has been made, trust service coordination still faces challenging problems such as trustless industry service, poor coordination, and quality of service (QoS) personalized demand. In this paper, we propose a QoS-driven and adaptive trust service coordination method to implement Pareto-efficient allocation of limited industrial service resources in the background of the IIoT. First, we established a Pareto-effective and adaptive industrial IoT trust service coordination model and introduced a blockchain-based adaptive trust evaluation mechanism to achieve trust evaluation of industrial services. Then, taking advantage of a large and complex search space for solution efficiency, we introduced and compared multi-objective gray-wolf algorithms with the particle swarm optimization (PSO) and dragonfly algorithms. The experimental results showed that by judging and blacklisting malicious raters quickly and accurately, our model can efficiently realize self-adaptive, personalized, and intelligent trust service coordination under the given constraints, improving not only the response time, but also the success rate in coordination.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/9/2784

Abstract: With the fast development and expansion of the Internet of Things (IoT), billions of smart devices are being continuously connected, and smart homes, as a typical IoT application, are providing people with various convenient applications, but face security and privacy issues. The idea of Blockchain (BC) theory has brought about a potential solution to the IoT security problem. The emergence of blockchain technology has brought about a change of decentralized management, providing an effective solution for the protection of network security and privacy. On the other hand, the smart devices in IoT are always lightweight and have less energy and memory. This makes the application of blockchain difficult. Against this background, this paper proposes a blockchain model based on hypergraphs. The aims of this model are to reduce the storage consumption and to solve the additional security issues. In the model, we use the hyperedge as the organization of storage nodes and convert the entire networked data storage into part network storage. We discuss the design of the model and security strategy in detail, introducing some use cases in a smart home network and evaluating the storage performance of the model through simulation experiments and an evaluation of the network.


Reference Type: Journal Article


Abstract: The digitalization phenomenon is leveraging new relationship models through the entire supply
chain network. In this outlook, blockchain is a cutting-edge technology that is already transforming and remodeling the relationships between all members of logistics and supply chain systems. Yet, while studies on blockchain have gained a relative pace over the recent years, the literature on this topic does not report sufficient research cases on blockchain adoption behavior at the individual level. The present study, therefore, aims to bridge this gap, notably by helping understand the individual blockchain adoption behavior in the logistics and supply chain field in India and the USA. Drawing on the emerging literature on blockchain, supply chain and network theory, as well as on technology acceptance models (TAMs), we have developed a model based on a slightly-altered version of the classical unified theory of acceptance and use of technology (UTAUT). The model being developed was then estimated using the Partial least squares structural equation modeling (PLS-SEM). As the model was eventually supported, the results obtained revealed the existence of distinct adoption behaviors between India-based and USA-based professionals. In parallel, the findings appear as a useful contribution to and a sign of progress for the literature on IT adoption, SCM, and blockchain.


Reference Type: Electronic Article

Abstract: Purpose: This paper aims to identify, analyse and organise the literature about blockchains in supply chain management (SCM) context (blockchain-SCM integration) and proposes an agenda for future research. This study aims to shed light on what the main current blockchain applications in SCM are, what the main disruptions and challenges are in SCM because of blockchain adoption and what the future of blockchains holds in SCM. Design/methodology/approach: This study followed the systematic review approach to analyse and synthesise the extant literature on blockchain-SCM integration. The review analysed 27 papers between 2008 and 2018 in peer-reviewed journals. Findings: Blockchain-SCM integration is still in its infancy. Scholars and practitioners are not fully aware of the potential of blockchain technology to disrupt traditional business models. However, the electric power industry seems to have a relatively mature understanding of blockchain-SCM integration, demonstrated by the use of smart contracts. Additionally, the disintermediation provided by blockchain applications has the potential to disrupt traditional industries (e.g. health care, transportation and retail). Research limitations/implications: The limitations of this study are represented mainly by the scarcity of studies on blockchain-SCM integration in leading journals and databases. Practical implications: This study highlights examples of blockchain-SCM integration, emphasising the need to rethink business models to incorporate blockchain technology. Originality/value: This study is the first attempt to synthesise existing publications about the blockchain-SCM integration, shedding light on the disruption caused by, and the necessity of, the SCM reconfigurations.


Reference Type: Journal Article

Available from: http://medicine.mrjournals.org/index.php/medicine/article/view/6

Abstract: Blockchain, the technology that began with Bitcoin in 2009, today promises to provide the safe, interoperable sharing of real-time data between providers, payers and patients in the healthcare industry. Majorly, blockchain’s automated data verification capabilities, in particular, are able to resolve many of the trust issues regarding pulling data from disparate sources. Applications of the technology in healthcare shows promise for solving issues such as its used in EHR distribution of data and nationwide interoperability. The use of blockchain in healthcare is expected to reinvent the ecosystem in limitless ways to benefit the patient and advancements in treatments, outcomes, security and costs. In effect, blockchain technology has the potential to transform healthcare delivery, placing patient at the center of the healthcare ecosystems and the capability to increase the security, privacy, and interoperability of healthcare data. It’s envisaged that this technology is expected to provide a new model for health information exchanges (HIE) by making electronic medical records more efficient, disintermediated, and secure. One of blockchain technology’s core offerings that make it a no-brainer for supply chains across industries is its immutable, time-stamped, tamper-proof ledger, accessible by its all or pre-approved participants. In this review paper we’re to step through how blockchain aid in the providing efficiency, security and privacy to management of patient care.


Reference Type: Journal Article

Abstract: Blockchain technology is a decentralized database that stores a registry of assets and transactions across a peer-to-peer computer network, which is secured through cryptography, and over time, its history gets locked in blocks of data that are cryptographically linked together and secured. So far, there have been use cases of this technology for cryptocurrencies, digital contracts, financial and public records, and property ownership. It is expected that future uses will expand into medicine, science, education, intellectual property, and supply chain management. Likely applications in the field of medicine could include electronic health records, health insurance, biomedical research, drug supply and procurement processes, and medical education. Utilization of blockchain is not without its weaknesses and currently, this technology is extremely immature and lacks public or even expert knowledge, making it hard to have a clear strategic vision of its true future potential. Presently, there are issues with scalability, security of smart contracts, and user adoption. Nevertheless, with capital investments into blockchain technology projected to reach US$400 million in 2019, health professionals and decision makers should be aware of the transformative potential that blockchain technology offers for healthcare organizations and medical practice.


Reference Type: Journal Article

Available from: https://academic.oup.com/ijebm/article/10/5/1847979018790589/1847979018790589

Abstract: OBJECTIVE: To introduce the basic concepts of blockchain technologies in tackling the opioid epidemic. DESIGN: A narrative review. SETTING/BACKGROUND: The opioid epidemic is taking a big toll in terms of lives and livelihood in America. Various public and private sector agencies are actively implementing different strategies to contain the epidemic. Development of robust real-time databases that are secure and easily accessible to the stakeholders in the opioid/paincare ecosystem is essential. Blockchain technologies, with their inherent features of decentralization, immutability, and easy access are well suited to achieving these goals. Some practical applications of blockchain technologies include data collection/aggregation/analysis, patient/provider identification, traceability/monitoring of opioids, supply chain provenance, prescription monitoring, licensure and credentialing, interoperability, seamless integration/communication, development of opioid alternatives, and research incentivization. CONCLUSIONS: Blockchain technologies may help support the efforts of different agencies in curtailing the opioid epidemic.

Rahimzadeh V. Ethics governance outside the box: reimagining blockchain as a policy tool to facilitate single ethics review and data sharing for the 'omics' sciences. Blockchain Healthc Today [Internet]. 2018 Mar 27 [cited 2018 Jul 18]; 1(18):[10 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/18

Reference Type: Electronic Article

Abstract: Clinical research and health information data sharing are but ripples in a growing wave of reimagined applications of distributed ledger technologies beyond the digital marketplace for which they were originally created. This paper explores the use of distributed ledger technologies to facilitate single institutional ethics review of multi-site, collaborative studies in the data-intensive sciences such as genetics and genomics. Immutable record-keeping, automatable protocol amendments and direct connectivity between stakeholders in the research enterprise (e.g., researchers, research ethics committees, institutions, funders and regulators) comprise several of the conceptual and technological advantages of distributed ledger technologies to research ethics review. This novel-use proposal dovetails recent policy reforms to research ethics review across North America that mandate a single ethics review for any study that takes place across more than one research site. Such reforms in the United States, Canada and Australia replace prior institution-by-institution approval mechanisms that contributed to significant research delays and duplicative procedures for collaborative research worldwide. While this paper centers on the Common Rule revision in the United States, the single ethics review mandate is a noteworthy example of regulation evolving in parallel with advances in the data-intensive sciences it governs. The informational exchange capacities of distributed ledger technologies align well with the procedural goals of streamlining the ethics review system under the new Common Rule ahead of its official implementation on January 19, 2020. The ethical, legal and social implications of applying such technologies to ethics review will be explored in this concept paper. Namely, the paper proposes how administrative data from research ethics committees (REC) could be protected and shared responsibly, as well as interinstitutional cooperation negotiated within a centralized network of research ethics committees using the blockchain.


Reference Type: Journal Article


CONCLUSIONS: Blockchain technologies may help support the efforts of different agencies in curtailing the opioid epidemic.


Reference Type: Journal Article
Abstract: The personal health information (PHI) is an activity among the health-care providers and the patients in terms of managing the data which is sensitive to the parties. The PHI data have been maintained by multiple health-care providers, thus resulting in separated data. Moreover, the PHI data are stored in the provider’s database, hence the patients have no authority to manage their own information. Therefore, in this article, we propose a conceptual model for managing the PHI data which is derived from several health-care providers by relying on the blockchain technology in the peer-to-peer overlay network. In addition, we elaborate the security analysis that might be occurring in the proposed model. By leveraging on our model, it allows the patients and the providers to collect effectively the PHI data onto a single view as well guarantee of data integrity. The blockchain offers an immutable of the data record without having to trust a third party. The experimental results show that the proposed approach is promising to be developed due to the high success rate in terms of data dissemination.


Reference Type: Journal Article


Abstract: In this manuscript, we present a novel method, process and system for calculating dyslexic symptoms, generating metric data for an individual user, community or group in general. We present a mobile multimedia Internet of Things (IoT) based environment, which can capture multimodal smartphone or tab-based user interaction data during dyslexia testing and share it via a mobile edge network, which employs auto-grading algorithms to find dyslexia symptoms. In addition to algorithm-based auto-grading, the captured mobile multimedia payload is stored in a decentralized repository, which can be shared with a medical practitioner for replay and further manual analysis purposes. Since the framework is language-independent and based on Blockchain and a decentralized big data repository, dyslexic patterns and a massive amount of captured multimedia IoT test data can be shared for further clinical research, statistical analysis, and quality assurance. Notwithstanding, our proposed Blockchain and off-chain based decentralized and secure dyslexia data storage, management and sharing framework will allow security, anonymity, and multimodal visualization of the captured test data for mobile users. This paper presents the detailed design, implementation and test results, which demonstrate the strong potential for wider adoption of the dyslexia mobile health management globally.


Reference Type: Electronic Article

Abstract: Blockchain technology and the associated cryptocurrencies have the ability to transform industries including healthcare. We suggest the decentralized and programmable nature of blockchain applications can be used to change health information technology to gain greater efficiency in public and private healthcare systems. Current public health information technology systems such as eligibility, enrollment and electronic health records have documented issues with interoperability and are slow to adapt to changing program and technology demands. We suggest that blockchain can potentially solve these issues. We argue that a public program such as the U.S. Medicaid program with $553 Billion in total program costs and over $25 Billion spent on health information technology and administration last fiscal year could benefit from the use of blockchain based distributed ledger and smart contracts. We finally argue that a decentralized benefits administration system can provide greater efficiency to enrollment, eligibility, claims payment and adjudication processes thus driving efficiency and reducing systemic fraud.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/14/3165

Abstract: Recently, connected vehicles (CV) are becoming a promising research area leading to the concept of CV as a Service (CVaaS). With the increase of connected vehicles and an exponential growth in the field of online cab booking services, new requirements such as secure, seamless and robust information exchange among vehicles of vehicular networks are emerging. In this context, the original concept of vehicular networks is being transformed into a new concept known as connected and autonomous vehicles. Autonomous vehicular use yields a better experience and helps in reducing congestion by allowing current information to be obtained by the vehicles instantly. However, malicious
users in the internet of vehicles may mislead the whole communication where intruders may compromise smart devices with the purpose of executing a malicious ploy. In order to prevent these issues, a blockchain technique is considered the best technique that provides secrecy and protection to the control system in real time conditions. In this paper, the issue of security in smart sensors of connected vehicles that can be compromised by expert intruders is addressed by proposing a blockchain framework. This study has further identified and validated the proposed mechanism based on various security criteria, such as fake requests of the user, compromise of smart devices, probabilistic authentication scenarios and alteration in stored user’s ratings. The results have been analyzed against some existing approach and validated with improved simulated results that offer 79% success rate over the above-mentioned issues.


Reference Type: Report

Abstract: Terms such as cryptocurrency, blockchain, and distributed ledger technology (DLT) have gradually entered our daily lexicon, featured prominently in news and media, and fuelled discussion and debate among communities, industry practitioners and policymakers. Nevertheless, there is no rigorously defined set of terminologies or commonly acceptable taxonomy available. As a result, people are often talking past each other, and these terms are often misconstrued, misused, and misinterpreted.

Without undertaking a systematic and holistic approach, attention and analysis can be narrowly devoted to fractions, parts, and the surface of the phenomenon, rather than the whole. Consequently, people ‘can’t see the forest for the trees’ and they are more susceptible to bias, misunderstanding, inflated claims, or conflicted views.


Reference Type: Report
Available from: https://w3c-ccg.github.io/did-spec/

Abstract: Decentralized Identifiers (DIDs) are a new type of identifier for verifiable, "self-sovereign" digital identity. DIDs are fully under the control of the DID subject, independent from any centralized registry, identity provider, or certificate authority. DIDs are URLs that relate a DID subject to means for trustable interactions with that subject. DIDs resolve to DID Documents — simple documents that describe how to use that specific DID. Each DID Document may contain at least three things: proof purposes, verification methods, and service endpoints. Proof purposes are combined with verification methods to provide mechanisms for proving things. For example, a DID Document can specify that a particular verification method, such as a cryptographic public key or pseudonymous biometric protocol, can be used to verify a proof that was created for the purpose of authentication. Service endpoints enable trusted interactions with the DID controller.

This document specifies a common data model, format, and operations that all DIDs support.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/10/2395

Abstract: Wireless body area networks (WBANs) are expected to play a vital role in the field of patient-health monitoring shortly. They provide a convenient way to collect patient data, but they also bring serious problems which are mainly reflected in the safe storage of the collected data. The privacy and security of data storage in WBAN devices cannot meet the needs of WBAN users. Therefore, this paper adopts blockchain technology to store data, which improves the security of the collected data. Moreover, a storage model based on blockchain in WBAN is proposed in our solution. However, blockchain storage brings new problems, for example, that the storage space of blockchain is small, and the stored content is open to unauthorized attackers. To solve the problems above, this paper proposed a sequential aggregate signature scheme with a designated verifier (DVSSA) to ensure that the user's data can only be viewed by the designated person and to protect the privacy of the users of WBAN. In addition, the
new signature scheme can also compress the size of the blockchain storage space.


Abstract: Edge computing is an important tool for smart computing, which brings convenience to data processing as well as security problems. In particular, the security of data storage under edge computing has become an obstacle to its widespread use. To solve the problem, the mechanism combing blockchain with regeneration coding is proposed to improve the security and reliability of stored data under edge computing. Our contribution is as follows. 1) According to the three-tier edge computing architecture and data security storage requirements, we proposed hybrid storage architecture and model specifically adapted to edge computing. 2) Making full use of the data storage advantages of edge network devices and cloud storage servers, we build a global blockchain in the cloud service layer and local blockchain is built on the terminals of the Internet of things. Moreover, the regeneration coding is utilized to further improve the reliability of data storage in blockchains. 3) Our scheme provides a mechanism for periodically validating hash values of data to ensure the integrity of data stored in global blockchain.


Abstract: Nowadays, the society is witnessing a keen urge to enhance the quality of healthcare services with the intervention of technology in the health sector. The main focus in transforming traditional healthcare to smart healthcare is on facilitating the patients as well as medical professionals. However, this changeover is not easy due to various issues of security and integrity associated with it. Security of patient’s personal health record and privacy can be handled well by permitting only authorized access to the confidential health-data via suitably designed authentication scheme. In pursuit to contribute in this direction, we acrossed the role of Universal Serial Bus (USB), the most widely accepted interface, in enabling communication between peripheral devices and a host controller like laptop, personal computer, smart phone, tablet etc. In the process, we analysed a recently proposed a three-factor authentication scheme for consumer USB Mass Storage Devices (MSD) by He et al. In this paper, we demonstrate that He et al.’s scheme is vulnerable to leakage of temporary but session specific information attacks, late detection of message replay, forward secrecy attacks, and backward secrecy attacks. Then motivated with the benefits of USB, we propose a secure three-factor authentication scheme for smart healthcare.

Research 2 Guidance. mHealth app developer economics 2017: current status and trends of the mHealth app market. Berlin, Germany; 2017 Nov.

Abstract: The mHealth Economics program has been exploring the developments of digital health for 7 years now, and counting. Since the first report on the mobile health app market, a total of 6.7 million data points have been revealed, which illustrate mHealth and digital health market developments dating back as far as 2010. The mHealth Economics program is the largest digital health research program globally, with more than 15,000 participants since its beginnings. The aim of the program is to reveal current market conditions, and future trends in the digital health arena. It examines how successful mHealth app publishers are operating, how the market is changing, and where it is heading. In doing so, the report helps stakeholders to understand current and future market developments. Each year the program emphasizes several trending topics relevant to digital health. For 2017, trending topics include; digital health business models, typical project budgets and digital health accelerator programs. Also new to this year’s program is the release of not only one, but several free-to-download reports. This year more than 2,400 decision makers and experts in mobile and digital health have partaken in the market survey and have contributed to this year’s report.

Abstract: Blockchain and distributed ledger technology is a disruptive force in healthcare. This article provides a globally relevant, interdisciplinary perspective intended to aid disparate group of actors, participants, and users that represent the diverse stakeholders of an increasingly complex and technologically reliant healthcare system. Domain expertise reinforced by literature published via industry, technical, and academic venues was used to inform these perspectives. Results: Key characteristics of blockchain and distributed ledger technology are highlighted and framed for a readership ranging from healthcare executive to policy makers to researchers. Antecedent application of blockchain in the financial sector is explored followed by the technical, security, and interoperability considerations specific to healthcare. Conclusion: Blockchain remains an emerging technology both fraught with unanticipated challenges and the promise of unrealized potential in healthcare.

Rifi N, Rachkidi E, Agoulmine N, Taher NC. Towards using blockchain technology for eHealth data access management. 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME); 2017 Oct 19-21; Beirut, Lebanon. Piscataway, NJ: IEEE.

Abstract: eHealth is a technology that is growing in importance over time, varying from remote access to Medical Records, such as Electronic Health Records (EHR), or Electronic Medical Records (EMR), to real-time data exchange from different on-body sensors coming from different patients. With this huge amount of critical data being exchanged, problems and challenges arise. Privacy and confidentiality of this critical medical data are of high concern to the patients and authorized persons to use this data. On the other hand, scalability and interoperability are also important problems that should be considered in the final solution. This paper illustrates the specific problems and highlights the benefits of the blockchain technology for the deployment of a secure and a scalable solution for medical data exchange in order to have the best performance possible.


Abstract: While blockchain technology is commonly considered potentially disruptive in various regards, there is a lack of understanding where and how blockchain technology is effectively applicable and where it has mentionable practical effects. This issue has given rise to critical voices that judge the technology as over-hyped. Against this backdrop, this study adapts an established research framework to structure the insights of the current body of research on blockchain technology, outline the present research scope as well as disregarded topics, and sketch out multidisciplinary research approaches. The framework differentiates three groups of activities (design and features, measurement and value, management and organization) at four levels of analysis (users and society, intermediaries, platforms, firms and industry). The review shows that research has predominantly focused on technological questions of design and features, while neglecting application, value creation, and governance. In order to foster substantial blockchain research that addresses meaningful questions, this study identifies several avenues for future studies. Given the breadth of open questions, it shows where research can benefit from multidisciplinary collaborations and presents data sources as starting points for empirical investigations.


Abstract: Nowadays, in this digital world, one of the biggest concerns for business and many other public entities, is to know precisely the “identity” of the users that are behind of their systems. Since the data can define a person, there have been many tries to develop technology to determine accurately who the users are and certify their basics attributes like name, address, credit record, as well as other personal
Abstract: The advances in the Information and Communications Technology (ICT) brought many benefits to the healthcare area, especially to digital storage of patients’ health records. However, it is still a challenge to have a unified viewpoint of patients’ health history, because typically health data is scattered among different health organizations. Furthermore, there are several standards for these records, some of them open and others proprietary. Usually health records are stored in databases within health organizations and rarely have external access. This situation applies mainly to cases where patients’ data are maintained by healthcare providers, known as EHRs (Electronic Health Records). In case of PHRs (Personal Health Records), in which patients by definition can manage their health records, they usually have no control over their data stored in healthcare providers’ databases. Thereby, we envision two main challenges regarding PHR context: first, how patients could have a unified view of their scattered health records, and second, how healthcare providers can access up-to-date data regarding their patients, even though changes occurred elsewhere. For addressing these issues, this work proposes a model named OmniPHR, a distributed model to integrate PHRs, for patients and healthcare providers use. The scientific contribution is to propose an architecture model to support a distributed PHR, where patients can maintain their health history in a unified viewpoint, from any device anywhere. Likewise, for healthcare providers, the possibility of having their patients data interconnected among health organizations. The evaluation demonstrates the feasibility of the model in maintaining health records distributed in an architecture model that promotes a unified view of PHR with elasticity and scalability of the solution.


Reference Type: Journal Article


Abstract: Background The Personal Health Record (PHR) and Electronic Health Record (EHR) play a key role in more efficient access to health records by health professionals and patients. It is hard, however, to obtain a unified view of health data that is distributed across different health providers. In particular, health records are commonly scattered in multiple places and are not integrated. Objective This article presents the implementation and evaluation of a PHR model that integrates distributed health records using blockchain technology and the openEHR interoperability standard. We thus follow OmniPHR architecture model, which describes an infrastructure that supports the implementation of a distributed and interoperable PHR. Methods Our method involves implementing a prototype and then evaluating the integration and performance of medical records from different production databases. In addition to evaluating the unified view of records, our evaluation criteria also focused on non-functional performance requirements, such as response time, CPU usage, memory occupation, disk, and network usage. Results We evaluated our model implementation using the data set of more than 40 thousand adult patients anonymized from two hospital databases. We tested the distribution and reintegration of the data to compose a single view of health records. Moreover, we profiled the model by evaluating a scenario with 10 superpeers and thousands of competing sessions transacting operations on health records simultaneously, resulting in an average response time below 500ms. The blockchain implemented in our prototype achieved 98% availability. Conclusion Our performance results indicated that data distributed via a blockchain could be recovered with low average response time and high availability in the scenarios we tested. Our study also demonstrated how OmniPHR model implementation can integrate distributed data into a unified view of health records.


Reference Type: Journal Article
Abstract: Although the best-known use of blockchain technology (BCT) is in the field of economics and cryptocurrencies in general, its usefulness is extending to other fields, including the biomedical field. The purpose of this article is to clarify the role that BCT can play in the field of medicine. We have performed a narrative review of the literature on BCT in general and on medicine in particular. The great advantage of BCT in the health arena is that it allows development of a stable and secure data set with which users can interact through transactions of various types. This environment allows the entry and operation of clinical data without compromising other sensitive data. Another important advantage of BCT is that the entire network is decentralized and is maintained by the users themselves; thus, there is no need to rely on organizations for storage. The Blockchain code is open source and can be used, modified and revised by its users. BCT literature is scarce so far. This article describes the basics of this technology and summarizes the various aspects in which BCT could change the paradigm of current medicine. The great potential of BCT, as well as its many applications in the field of health sciences, encompasses the fields of legal medicine, research, electronic medical records, medical data analysis (big data), teaching and the regulation of payment for medical services. If technological advances continue along these lines, it could bring about a revolution in medicine as we know it.


Reference Type: Journal Article


Abstract: Abstract Introduction Population health involves integration of health, education, and social services to keep a defined population healthy, to address health challenges holistically, and to assist with the realities of being mortal. The fragmentation of the US population health delivery system is addressed. The impacts of this fragmentation on the treatment of substance abuse in the United States are considered. Innovations needed to overcome this fragmentation are proposed. Approach Treatment capacity issues, including scheduling practices, are discussed. Costs of treatment and lack of treatment are considered. Models of integrated care delivery are reviewed. Potential innovations from systems science, behavioral economics, and social networks are considered. The implications of these innovations are discussed in terms of information technology (IT) systems and governance. Conclusions Enormous savings are possible with more integrated treatment. Based on a range of empirical findings, it is argued that investments of these resources in integrated delivery of care have the potential to dramatically improve health outcomes, thereby significantly reducing the costs of population health.


Reference Type: Conference Paper

Available from: http://ebooks.iospress.nl/publication/51508

Abstract: The penetration of digital platforms and ecosystem based business-model together with the use algorithm and machine learning are changing the environment where pHealth takes place. Traditional pHealth is changing to Digital pHealth. This development brings new ethical, privacy and trust problems which have to solve to make Digital pHealth successful. In this paper ethical, privacy and trust problems in Digital pHealth are studied at conceptual level. Concerns caused by the use novel ICT-technology and regulatory environment are also discussed. The starting point is that the Digital pHealth as a system and its applications and algorithms should be ethically acceptable, trustworthy and enable the service user to set own context-aware privacy policies. Mutual trust is needed between application and all stakeholders. Solution proposed for trustworthy Digital pHealth include ethical design, policy based privacy management and on-line calculation of privacy and trust levels using proven mathematical methods. In the future, novel solutions such as algorithm based access control and data sharing, and algorithm based privacy prediction together with cryptography based blockchain seems to have potential to change the way privacy is managed in Digital pHealth. Technology alone cannot solve current privacy and trust problems. New regulations which not only give users of the Digital pHealth right to set personal privacy polies but also force pHealth service providers and platform owners to prove regulatory compliance of their services are needed.


Reference Type: Journal Article

Available from: https://opus.lib.uts.edu.au/handle/10453/127958
Abstract: Much of the discussion around blockchain-based smart contracts has focused on whether or not they operate in the same way as legal contracts. However, it is argued that most contracts are social rather than legal in nature and are entered into because the parties trust each other to perform the agreed exchange. Little has been written to address how the blockchain’s trust protocol can enable the kind of social contracting that characterized the way exchanges were conducted before the Internet. This article aims to fill that gap by exploring blockchain-based smart contracts primarily as non-contractual social exchanges.

Sadu I. Auditing blockchain: internal auditors need to focus on new risks and opportunities posed by blockchain technologies. Intern Audit. 2018 Dec:17-8.
Reference Type: Magazine Article

Abstract: Businesses and government agencies alike are pursuing blockchain’s promise of greater accuracy, transparency, and efficiency. Accounting firms are investing more than $3 billion a year on blockchain technology, while IBM predicts that two-thirds of all banks will have blockchain products by 2020. These organizations are attracted to blockchain’s ability to record relevant details of every transaction in a distributed network.

Like other new technologies, blockchain presents challenges and opportunities for internal auditors. Blockchain carries the typical IT risks such as unauthorized access and threats to confidentiality, but it also could impact traditional audit procedures. Yet, blockchain may enable auditors to be more innovative and efficient.

Reference Type: Conference Paper
Available from: https://dl.acm.org/citation.cfm?id=3324083

Abstract: Recently, blockchain has been a disruptive technology for many systems, such as finance, e-health, supply-chain, and etc. Secure access to blockchain is the grand challenge for many systems. Key management is one of challenges to ensure secure access to blockchain. In this paper, we propose a framework for secure accessing to blockchain via multi-factor authentication. We combine both biometric and password authentications to secure private keys of users. The framework contains a secure device which has a biometric sensor to ensure secure access to private keys that extends the usability for secure accessing to blockchain.

Reference Type: Journal Article

Abstract: We propose an agile softwarized infrastructure for flexible, cost effective, secure and privacy preserving deployment of Internet of Things (IoT) for smart healthcare applications and services. It integrates state-of-the-art networking and virtualization techniques across IoT, fog and cloud domains, employing Blockchain, Tor and message brokers to provide security and privacy for patients and healthcare providers. We propose a novel platform using Machine-to-Machine (M2M) messaging and rule-based beacons for seamless data management and discuss the role of data and decision fusion in the cloud and the fog, respectively, for smart healthcare applications and services.

Reference Type: Journal Article
Abstract: OBJECTIVE: The Veterans Health Administration (VHA) has deployed a large number of tablet computers in the last several years. However, little is known about how clinicians may use these devices with a newly planned Web-based electronic health record (EHR), as well as other clinical tools. The objective of this study was to understand the types of use that can be expected of tablet computers versus desktops. METHODS: Semi-structured interviews were conducted with 24 clinicians at a Veterans Health Administration (VHA) Medical Center. RESULTS: An inductive qualitative analysis resulted in findings organized around recurrent themes of: (1) Barriers, (2) Facilitators, (3) Current Use, (4) Anticipated Use, (5) Patient Interaction, and (6) Connection. CONCLUSIONS: Our study generated several recommendations for the use of tablet computers with new health information technology tools being developed. Continuous connectivity for the mobile device is essential to avoid interruptions and clinician frustration. Also, making a physical keyboard available as an option for the tablet was a clear desire from the clinicians. Larger tablets (e.g., regular size iPad as compared to an iPad mini) were preferred. Being able to use secure messaging tools with the tablet computer was another consistent finding. Finally, more simplicity is needed for accessing patient data on mobile devices, while balancing the important need for adequate security.


Reference Type: Electronic Article

Abstract: This paper deals with the Electronic Health Records for storing information of the patient which consist of the medical reports. Electronic Health Records (EHRs) are entirely controlled by Hospitals instead of patients, which complicates seeking medical advices from different hospitals. In the existing system of storing details of the patients are very dependent on the servers of the organization. In the proposed all the information of the patient are stored in the blockchain by using the Metamask and these details are stored in the block chain as a blocks of data. Each block consists of the data which is encrypted data. Electronic Health Record (EHR) systems record health-related information on an individual so that it can be consulted by clinicians or staff for patient care. The data is encrypted by the algorithm known as SHA-256 which is used to encrypt all the data of the patients into a single line 256 bit encrypted text which will be stored in the block at etherscan. These records for not only useful for the consultation but also for creation of historic family health information tree that keeps track of genetic health issues and diseases it can also be used for any health service with the authorization from both the patient and medical organization.

Sanyal V. Blockchain technology and mental health care in India. Yourstoryin. 2018 Sep 3.

Reference Type: Newspaper Article


Abstract: There are a lot of mixed feelings about the possible introduction of blockchain in the Indian market. A lot of research and development is currently being conducted and countless man hours being invested in making blockchain technology accessible and user-friendly. The aim of this article is to understand the basic principles of the technology, the role it can play in the mental health arena, and some of the perceived advantages and disadvantages of using the technology. It is important to mention that it is difficult to fully ascertain the benefits of blockchain at this point in time.

Until and unless the technology is widely accepted and used, we will not be able to come to a realistic conclusion of its effectiveness.


Reference Type: Conference Proceedings


Abstract: In recent years, cryptocurrencies gained popularity with Bitcoin. The main promising technology behind Bitcoin was ‘Blockchain’. Blockchain provided unique features like transactional privacy, system transparency, immutability of data, security with cryptography, etc. These features paved way for Blockchain in advancing many technologies like voting systems, IOT applications, supply chain management, banking, healthcare, insurance, etc. Blockchain development was boosted with the increasing demand of the technological update. Many blockchain platforms are available like Hyperledger fabric, Ethereum, corda, etc. We always end up with perplexity while choosing a platform for blockchain development. Through our survey, we provide a comparative analysis of all the Hyperledger platforms,

Reference Type: Conference Proceedings


Abstract: Wearable health devices, mobile apps and diagnostic tools revolutionize the medical field by introducing new assisting devices for patients in a way to create comfort, communication and augmented intelligence. Internet of Things involved in this transformation to provide an environment where a patient’s vital parameters get transmitted by sensor devices via a gateway onto secure cloud-based platforms where it is stored, aggregated and analyzed. It also helps to store data for millions of patients and performs analysis in real time, ultimately promoting an evidence-based medicine system. Privacy and security are concerns in this environment. Based on the latest trends, this paper introduces a new healthcare paradigm named as SMEAD by developing an end-to-end secured system for assisting diabetic patients. It includes wearables to monitor different parameters thus observe and predict the diabetes status of the patient. The proposed system employs a MEDIBOX which is used to configure the dosage required and provides an alert to the users reminding them to take medication on time. In this case, the insulin dosage is maintained at suitable cooling conditions and is continuously monitored using the mentioned system. To keep all the data secure and to enable access to this data by the doctor and other trusted parties, a Blockchain-based disruptive technology is implemented which facilitates cryptographic security and formalized data access through smart contracts for medical communities. In case of an emergency like missing a dosage, abnormal blood sugar levels or any security lapse, an alert is sent to the caretakers via social networks like Twitter, Facebook or WhatsApp using mobile as a gateway which can continuously communicate the data over the internet that could save patients from fatal effects of the disease.


Reference Type: Conference Proceedings


Abstract: Enterprises have paid attention to blockchain (BC), recently permissioned BC characterized with smart-contract, where business transactions among inter-authorized companies (forming consortium) can automatically be executed based on distributed consensus protocol over user-defined business logics pre-built with program codes. A single BC system will be built across multiple management domains having different operational policies, e.g., datacenter of each organization; this will trigger a problem that its system operations (e.g., backup) will become time-consuming and costly due to the difficulty in unifying and/or adjusting operational policy, schedule, etc. Toward solving the problem, we propose an operations execution method for BC systems; a primary idea is to define operations as smart-contract so that unified and synchronized cross-organizational operations can be executed effectively by using BC-native features. We de-sign the proposed method as hybrid architecture including in-BC consensus establishment and out-BC event-based instruction execution, in order to be adaptable to the recent heterogeneous BC architecture. Performance evaluation using a prototype with Hyperledger Fabric v1.0 shows that the proposed method can start executing operations within 5 seconds. Furthermore, cost evaluation using model-based estimation shows that the total yearly cost of monthly operations on a 5-organizational BC system could be reduced by 61 percent compared to a conventional manual method.


Reference Type: Journal Article


Abstract: The paper focuses on various legal-related aspects of the application of blockchain technologies in the copyright sphere. Specifically, it outlines the existing challenges for distribution of copyrighted works in the digital environment, how they can be solved with blockchain, and what associated issues need to be addressed in this regard. It is argued that blockchain can introduce long-awaited transparency in matters of copyright ownership chain; substantially mitigate risks of online piracy by enabling control over digital copy and creating a civilized market for “used” digital content. It also
allows to combine the simplicity of application of creative commons/open source type of licenses with revenue streams, and thus facilitate fair compensation of authors by means of cryptocurrency payments and Smart contracts. However, these benefits do not come without a price: many new issues will need to be resolved to enable the potential of blockchain technologies. Among them are: where to store copyrighted content (on blockchain or “off-chain”) and the associated need to adjust the legal status of online intermediaries; how to find a right balance between immutable nature of blockchain records and the necessity to adjust them due to the very nature of copyright law, which assigns ownership based on a set of informal facts, not visible to the public. Blockchain as a kind of time stamping service cannot itself ensure the trustworthiness of facts, which originate “off-chain”. More work needs to be done on the legal side: special provisions aimed at facilitating user's trust in blockchain records and their good faith usage of copyrighted works based on them need to be introduced and transactions with cryptocurrencies have to be legalized as well as the status of Smart contracts and their legal consequences. Finally, the economics of blockchain copyright management systems need to be carefully considered in order to ensure that they will have necessary network effects. If those issues are resolved in a satisfactory way, blockchain has the potential to rewrite how the copyright industry functions and digital content is distributed.

Reference Type: Electronic Article
Abstract: In this paper we present reclaimID: An architecture that allows users to reclaim their digital identities by securely sharing identity attributes without the need for a centralised service provider. We propose a design where user attributes are stored in and shared over a name system under user-owned namespaces. Attributes are encrypted using attribute-based encryption (ABE), allowing the user to selectively authorize and revoke access of requesting parties to subsets of his attributes. We present an implementation based on the decentralised GNU Name System (GNS) in combination with ciphertext-policy ABE using type-1 pairings. To show the practicality of our implementation, we carried out experimental evaluations of selected implementation aspects including attribute resolution performance. Finally, we show that our design can be used as a standard OpenID Connect Identity Provider allowing our implementation to be integrated into standard-compliant services.

Reference Type: Report
Abstract: Blockchain technology can potentially make a great many things more secure and accountable: financial transactions, micropayments, IoT applications, health records, corporate audits, and more. If you’re not up to speed on blockchain, you need to be.

Reference Type: Report
Abstract: The Health Information Traceability (HIT) Foundation offers a distributed online marketplace for personal health data that allows users and patients to trace data usage and participate in its monetization. The user/patient is the one granting access to his data under a smart contract that determines the conditions of the data usage by information seekers such as market researchers, academic institutions or hospitals. HIT Foundation is the first ecosystem that allows everybody to get rewarded for sharing health information digitally instead of paying others to process or store it. The HIT token is used as an incentive and aligns the motivation of all network participants. At the same time, blockchain technology allows to maintain the privacy of the user/patient. The distributed system supports the global execution of new or existing business cases for information seekers on top of the HIT platform without the need for intermediaries.

Reference Type: Journal Article
Abstract: Decentralization is a term widely used in a variety of contexts, particularly in political science and discourses surrounding the Internet. It is popular today among advocates of blockchain technology. While frequently employed as if it were a technical term, decentralization more reliably appears to operate as a rhetorical strategy that directs attention toward some aspects of a proposed social order and away from others. It is called for far more than it is theorized or consistently defined. This non-specificity has served to draw diverse participants into common political and technological projects. Yet even the most apparently decentralized systems have shown the capacity to produce economically and structurally centralized outcomes. The rhetoric of decentralization thus obscures other aspects of the re-ordering it claims to describe. It steers attention from where concentrations of power are operating, deferring worthwhile debate about how such power should operate. For decentralization to be a reliable concept in formulating future social arrangements and related technologies, it should come with high standards of specificity. It also cannot substitute for anticipating centralization with appropriate mechanisms of accountability.

Schöner MM, Kourouklis D, Sandner P, Gonzalez E, Förster J. Blockchain technology in the pharmaceutical industry. Frankfurt am Main, Germany: Frankfurt School Blockchain Center, 2017.

Reference Type: Report

Abstract: With this paper, we present a blockchain-based solution to increase supply chain security for the pharmaceutical industry. Supply chain security is one aspect that has recently won attention, when the Drug Supply Chain Security Act (DSCSA) has been implemented in the U.S to, amongst others, fight the counterfeit drug problem. During the second "Life Science meets IT" hackathon in Heidelberg a team of enthusiastic young professionals and students developed a prototype solution that is able to guard people’s life with a patient-empowering blockchain solution and won the first price with their prototype LifeCrypter.


Reference Type: Journal Article

Abstract: The present work deals with the interrelationships of blockchain technology and the new European General Data Protection Regulation, that will be intact after May 28th, 2018. The regulation harmonizes personal data protection across the European Union and aims to return the ownership of personal data to the individual. This thesis, therefore, addresses the question how this new technology that is characterized by decentralization, immutability and truly digitized values will be affected by the strict privacy regulation and vice versa. The aim of this work is to clarify whether blockchains can comply with the new regulation on the one hand and to identify how blockchain could support its compliance, on the other hand. The questions are validated through an extensive literature review and are further investigated by using a Delphi study that asks a panel of 25 renowned experts to find opportunities, limitations and general suggestions about both topics. In addition, a framework is proposed to support the assessment of privacy and related risks of blockchains. As a result, it becomes apparent that blockchains can become more privacy friendly and comply with the regulation if an active dialogue between blockchain developers and regulatory authorities helps to strengthen their mutual understanding and work. With the support of this work and the blockchain Privacy Impact Assessment canvas a foundation for the necessary next steps is laid to overcome the challenges of defining a data controller or deleting personal data within a blockchain.


Reference Type: Journal Article

Abstract: Researchers analyzed 23 blockchain implementation projects, each tracked for design decisions and architectural alignment showing benefits, detriments, or no effects from blockchain use. The results provide the basis for a framework that lets engineers, architects, investors, and project leaders evaluate blockchain technology’s suitability for a given application. This analysis also led to an understanding of why some domains are inherently problematic for blockchains. Blockchains can be used to solve some trust-based problems but aren’t always the best or optimal technology. Some
problems that can be solved using them can also be solved using simpler methods that don’t necessitate as big an investment.


Abstract: Smart healthcare technologies are widely in use for the prevention and early diagnosis of diseases and are instrumental in transforming conventional medical care to patient-centric care. However, the traditional hospitals cannot entirely be replaced by home health systems, rather forcing them to become smart. The future smart hospitals are expected to have artificial intelligence (AI) tools for performing the patient diagnosis and robots for performing surgeries. The physicians will have the managing role, which could be performed through a touchscreen. This paper explores the challenges and opportunities associated with smart hospitals, and how they contribute to the objective of quality healthcare for everyone. The methodology used for the research is literature review. Machines do not have the common sense and blindly do what human beings instruct them to do. Thus, in spite of the digitalization and technology transformation of the healthcare processes, we cannot have hospitals without the human element.


Abstract: Blockchain-based platforms are emerging to provide solutions for technical and governance challenges associated with genomic data sharing. Providing capabilities for distributed data stewardship and participatory access control along with effective ways for enforcement of the data access agreements and data ownership are among the major promises of these platforms.


Abstract: This paper provides a vision and proposes mechanisms to transform the blockchain duplicated computing into distributed parallel computing architecture by transforming smart contract which features data driven from the ground up to support moving computing to native data strategy. This new distributed parallel computing architecture can be employed to build a large size of data set from various distributed hosted medical data sets which might consist of personal electronic medical record (EMR) and various medical data. This large medical data set will enable researchers to jump start the deep learning research for medical domain. Distributed data management, distributed data sharing, and distributed learning are the core mechanisms in the new architecture. The required new researches and developments to employ Google federated learning and transfer learning algorithms in this new architecture are discussed. The approach and mechanism enabled by the new architecture is illustrated to build a real world evidence of clinical trial toward personal and precision medicine. Research issues and technical challenges are provided.


Abstract: This paper proposes a blockchain platform architecture for clinical trial and precision medicine
and discusses various design aspects and provides some insights in the technology requirements and challenges. We identify 4 new system architecture components that are required to be built on top of traditional blockchain and discuss their technology challenges in our blockchain platform: (a) a new blockchain based general distributed and parallel computing paradigm component to devise and study parallel computing methodology for big data analytics, (b) blockchain application data management component for data integrity, big data integration, and integrating disparity of medical related data, (c) verifiable anonymous identity management component for identity privacy for both person and Internet of Things (IoT) devices and secure data access to make possible of the patient centric medicine, and (d) trust data sharing management component to enable a trust medical data ecosystem for collaborative research.


Reference Type: Journal Article

Abstract: Advancement of consensus protocols in recent years has enabled distributed ledger technologies (DLTs) to find its application and value in sectors beyond cryptocurrencies. Here we reviewed 66 known consensus protocols and classified them into philosophical and architectural categories, also providing a visual representation. As a case study, we focus on the public sector and highlighted potential protocols. We have also listed these protocols against basic features and sector preference in a tabular format to facilitate selection. We argue that no protocol is a silver bullet, therefore should be selected carefully, considering the sector requirements and environment.


Reference Type: Conference Proceedings

Abstract: Conducting experiments to evaluate blockchain applications is a challenging task for developers, because there is a range of configuration parameters that control blockchain environment. Many public testnets (e.g. Rinkeby Ethereum) can be used for testing, however, we cannot adjust their parameters (e.g. Gas limit, Mining difficulty) to further the understanding of the application in question and of the employed blockchain. This paper proposes an easy to use orchestration framework over the Grid’5000 platform. Grid’5000 is a highly reconfigurable and controllable large-scale testbed. We developed a tool that facilitates nodes reservation, deployment and blockchain configuration over the Grid’5000 platform. In addition, our tool can fine-tune blockchain and network parameters before and between experiments. The proposed framework offers insights for private and consortium blockchain developers to identify performance bottlenecks and to assess the behavior of their applications in different circumstances.


Reference Type: Journal Article
Available from: https://www.mdpi.com/2076-3417/9/6/1207

Abstract: Healthcare information exchange is an important research topic, which can benefit both healthcare providers and patients. In healthcare data sharing, many cloud-based solutions have been proposed, but the trustworthiness of a third-party cloud service is questionable. Recently, blockchain has been introduced in healthcare record sharing, which does not rely on trusting a third party. However, existing approaches only focus on the records collected from medical examination. They are not efficient in sharing data streams continuously generated from sensors and other monitoring devices. Today, IoT devices have been widely deployed and sensors and mobile applications can monitor patients & body conditions. The collected data are shared to laboratories and institutions for diagnosis and further study. Moreover, existing approaches are too rigid to efficiently support metadata change. In this paper, an efficient data-sharing scheme is proposed, called MedChain, which combines blockchain, digest chain, and structured P2P network techniques to overcome the above efficiency issues in the existing approaches for sharing both types of healthcare data. Based on MedChain, a session-based healthcare data-sharing scheme is devised, which brings flexibility in data sharing. The evaluation results show that MedChain can achieve higher efficiency and satisfy the security requirements in data sharing.

Reference Type: Journal Article

Abstract: BACKGROUND: Entropy has become increasingly popular in computer science and information theory because it can be used to measure the predictability and redundancy of knowledge bases, especially ontologies. However, current entropy applications that evaluate ontologies consider only single-point connectivity rather than path connectivity, and they assign equal weights to each entity and path. RESULTS: We propose an Entropy-Aware Path-Based (EAPB) metric for ontology quality by considering the path information between different vertices and textual information included in the path to calculate the connectivity path of the whole network and dynamic weights between different nodes. The information obtained from structure-based embedding and text-based embedding is multiplied by the connectivity matrix of the entropy computation. EAPB is analytically evaluated against the state-of-the-art criteria. We have performed empirical analysis on real-world medical ontologies and a synthetic ontology based on the following three aspects: ontology statistical information (data quantity), entropy evaluation (data quality), and a case study (ontology structure and text visualization). These aspects mutually demonstrate the reliability of the proposed metric. The experimental results show that the proposed EAPB can effectively evaluate ontologies, especially those in the medical informatics field.
CONCLUSIONS: We leverage path information and textual information to enrich the network representational learning and aid in entropy computation. The analytics and assessments of semantic web can benefit from the structure information but also the text information. We believe that EAPB is helpful for managing ontology development and evaluation projects. Our results are reproducible and we will release the source code and ontology of this work after publication. (Source code and ontology: https://github.com/AnonymousResearcher1/ontologyEvaluate).


Reference Type: Journal Article

Abstract: Efficient representations of drugs provide important support for healthcare analytics, such as drug-drug interaction (DDI) prediction and drug-drug similarity (DDS) computation. However, incomplete annotated data and drug feature sparseness create substantial barriers for drug representation learning, making it difficult to accurately identify new drug properties prior to public release. To alleviate these deficiencies, we propose KMR, a knowledge-oriented feature-driven method which can learn drug related knowledge with an accurate representation. We conduct series of experiments on real-world medical datasets to demonstrate that KMR is capable of drug representation learning. KMR can support to discover meaningful DDI with an accuracy rate of 92.19%, demonstrating that techniques developed in KMR significantly improve the prediction quality for new drugs not seen at training. Experimental results also indicate that KMR can identify DDS with an accuracy rate of 88.7% by facilitating drug knowledge, outperforming existing state-of-the-art drug similarity measures.


Reference Type: Journal Article
Available from: http://ebooks.iospress.nl/publication/51707 Subscription required to view.

Abstract: The blockchain is one of the most popular information technologies and, at the same time, it was discredited by stories about crashes of multiple cryptocurrency projects. Even though this technology has recently found application in many areas not related to cryptocurrencies, mainly for security purposes, the attitude towards it remains wary. Herein we shall try to demonstrate that blockchain is something going far beyond cryptocurrency and security issues, and may become one of the fundamental information technologies in future healthcare.


Reference Type: Journal Article
Abstract: Blockchain as an emerging technology has been gaining in popularity, with more possible applications to utilize the technology in the near future. With the offer of a decentralized, distributed environment by merging the need for a third trusted party (TTP), blockchains are being used to solve issues in systems that are susceptible to cyberattacks. One possible field that could benefit from blockchains that researchers have been focusing on is healthcare. Current healthcare information systems face several challenges, such as fragmented patient data, centralized systems which are viewed as single points of attacks, and the lack of patient-oriented services. In this paper, we investigate and analyze recent literature related to the use of blockchains to tackle issues found in modern healthcare information systems. This is done to understand issues that researchers commonly focus on, to discover remaining areas of concern in any proposed solution, and to understand the possible directions of the integration of blockchains in healthcare and personalized medicine. Background information regarding blockchains and existing healthcare information systems is reviewed, followed by the methodology used in the preparation of this review, where the research questions to consider are stated. Afterwards, an analysis of the results is provided, concluding with a discussion of the remaining issues that need to be focused on, and how blockchains could benefit the healthcare sector and empower personalized medicine.


Reference Type: Thesis
Available from: https://etd.ohiolink.edu/!etd.send_file?accession=kent149364959335823&disposition=attachment

Abstract: Malignant tumors are a worldwide concern. Breast cancer is the most common cause of death among women and is ranked as the second most serious malignant tumor in women, after lung cancer. Consequently, different techniques and technologies have been studied, researched, and developed to detect breast cancer at an early stage. Early diagnosis contributes to the preservation of lives in both developed and developing countries. The survival rate increases dramatically when the cancer tumors are discovered via a screening process before the appearance of cancer symptoms. Therefore, monitoring the responses of breast cancer patients and detecting the presence of new lesions are the main intended outcomes of this research. In this research, we use a breast ultrasound imaging technique to monitor the response of breast cancer patients who receive neoadjuvant chemotherapy (the systemic therapy of breast cancer before surgical therapy), as well as detecting new tumors which may arise during treatment. In this technique, the Support Vector Machine (SVM) algorithm is used for image classification, and the regionprops tool in Matlab is used for calculating the tumor size. SVM is a supervised learning method that is used for classification and regression predictive problems. In this work, SVM is considered as a binary classifier by which the abnormalities in the breast tissues can be distinguished, and then it can be determined whether these abnormalities are cancerous or not. To establish remote healthcare to monitor cancerous tumors treatments, telecommunication infrastructure through primarily Teleradiology and blockchain technology along with smart contract will be used. Blockchain technology is deemed as one of the main components of Bitcoin cryptocurrency. The smart contract concept is a collection of code that is governing something important or valuable in the blockchain. This remote healthcare will be achieved through specialized medical centers as well as technologies in patient homes. Based on prior research in the area of medical imaging techniques, the Support Vector Machines algorithm has the capability to achieve precise approximations with fast convergence. Additionally, the SVM algorithm has other features (e.g., it is computationally less expensive and yields good results based on strong mathematical foundations) which satisfy the best requirements of breast imaging technology.


Reference Type: Journal Article
Available from: https://www.mdpi.com/2410-387X/3/1/3

Abstract: Blockchain technology has gained considerable attention, with an escalating interest in a plethora of numerous applications, ranging from data management, financial services, cyber security, IoT, and food science to healthcare industry and brain research. There has been a remarkable interest witnessed in utilizing applications of blockchain for the delivery of safe and secure healthcare data management. Also, blockchain is reforming the traditional healthcare practices to a more reliable means, in terms of effective diagnosis and treatment through safe and secure data sharing. In the future, blockchain could be a technology that may potentially help in personalized, authentic, and secure healthcare by merging the entire real-time clinical data of a patient’s health and presenting it in an up-to-date secure healthcare setup. In this paper, we review both the existing and latest developments in the field of healthcare by implementing blockchain as a model. We also discuss the applications of blockchain, along with the challenges faced and future perspectives.
In our nursing program, we require a transcript for every course taken at any university or college, and it is always frustrating when we have to wait for copies to arrive before making our decisions. To be honest, if a candidate took Religion 101 at a community college and later transferred to the BSN program, I would be willing to pass on the community college transcript, but the admissions office is less flexible. And, although we used to be able to ask the student to have another copy sent if we did not have a transcript in the file, we now must wait for the student to have the college upload the transcript into an admissions system and wait for verification. I can assure you, most nurses, like other students today, take a lot of courses across many colleges without getting a degree. I sometimes have as many as 10 transcripts to review.

When I saw an article titled “Blockchain: Letting Students Own Their Credentials” (Schaffnauser, 2017), I was therefore intrigued. I had already heard of blockchain as a tool to take the middleman out of the loop when doing financial transactions with Bitcoin. Now the thought of students owning their own credentials got me thinking about the movement toward new forms of credentialing from professional organizations (e.g., badges, certification documents). Hence, my decision to explore blockchain and its potential.

Blockchain implementation in Health Informatics is a significant challenge in a rapidly evolving era of privacy and security concerns. Dealing with such concerns, healthcare institutions are presented with a serious problem in how to manage new technology and allocate finite resources to maximize value. It is important to understand how organizations address these concerns by exploring blockchain implementation management in the context of cybersecurity. The problem question is twofold: First, how can objectives that are important based on the strategic values of an organization with regard to the implementation of blockchain technology be used to ensure privacy and security of vulnerable patient data? Second, how can these objectives then be used to evaluate proposed solutions for blockchain implementation in electronic medical record systems? In this paper we utilize Keeney’s (1992) value focused thinking to demonstrate how the process can occur to maximize value-add within healthcare organizations.

Inherent to the widespread adoption of ever more efficient electronic devices was the systemic capacity to create a distributed database of records, a “public ledger” or sorts, where all transactions or “digital events” that have occurred are shared among participating parties. A blockchain is such a functionality, where information – once entered – can never be erased, where each transaction in this “public ledger” is verified by consensus of a system-wide majority of participants. It has been postulated that the blockchain technology is one of the most innovative and disruptive developments in history, effectively creating “…a public ledger of value transfer…” readily applicable to “…information, copyright, deeds, wills, almost anything you think of….”
As academic physicians, it is only natural for us to ask, “How could this technology be of benefit to the academic medical community?” In this Editorial, we will present a brief overview of the blockchain technology, its current and future applications in medicine and academia, as well as the potential to revolutionize how medical care, insurance and payment systems, academic recognition, and scientific merit can all be objectivized globally through implementing existing blockchain-based solutions.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6496988/

Abstract: Technological progress is reshaping multiple domains of human activity, from financial transactions to medical care. This paradigm shift represents a global movement that will transform our lives for generations to come. The democratization of decision-making capacity, including consensus-based mechanisms for transaction verification, will enable global implementation of projects that were previously not feasible because of the requirement for centralized control. Blockchain represents a decentralized ledger technology that operates by consensus and serves to democratize decision-making processes and to disintermediate traditionally understood intermediaries. According to Deutsche Bank forecasts, by mid-2020's, approximately 10% of the worldwide gross domestic product could be regulated by blockchain-based solutions. It is estimated that more than $400 billion will be invested in this technology in 2019 to advance its capabilities. Within this broader context, it is important to understand that cryptocurrencies and financial transactions constitute only one small aspect of the blockchain concept, which also incorporates areas like verification, transparency, encryption, and maintenance of data integrity.


Reference Type: Journal Article
Available from: http://journal.pda.org/content/early/2019/02/05/pdajpst.2018.009407.abstract
Subscription required to view.

Abstract: In the pharmaceutical industry, process validation tasks are based on the generated process raw and derived analytical results. Risks to fail in process validation, affect both, the patient's safety as well as the economic success of the manufacturing company. Hence, data integrity is highly critical in this area. Regulatory agencies, such as the FDA, reacted to past data integrity breaches, by publishing new guidelines on data integrity for the correct handling of data in the pharmaceutical context. In this contribution, we want to show how data integrity can be improved on a technological level, removing the need for trusted third parties and centralised systems for this task. Therefore, we implemented an approach that uses existing tools, today mostly used by software developers, and combined them with a new smart contract built on top of the Ethereum blockchain. In a case study, we test how data manipulation or back-dating of results can be easily detected and how regulatory agencies can audit the complete data flow, from the regulatory report back to the original raw data. The results of this contribution outline a possible roadmap for the development of production-ready tools, like versioned database systems that natively interoperate with distributed ledgers. This will improve the trustworthiness of pharmaceutical manufacturing data by doing both, protecting the intellectual property of the industrial company and improving the safety of the patients.


Reference Type: Journal Article

Abstract: Quantum computers are expected to have a dramatic impact on numerous fields due to their anticipated ability to solve classes of mathematical problems much more efficiently than their classical counterparts. This particularly applies to domains involving integer factorization and discrete logarithms, such as public key cryptography. In this paper, we consider the threats a quantum-capable adversary could impose on Bitcoin, which currently uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to sign transactions. We then propose a simple but slow commit-delay-reveal protocol, which allows users to securely move their funds from old (non-quantum-resistant) outputs to those adhering to a quantum-resistant digital signature scheme. The transition protocol functions even if ECDSA has already been compromised. While our scheme requires modifications to the Bitcoin protocol, these can be implemented as a soft fork.

Reference Type: Electronic Article

Abstract: Blockchain technology has been hailed as the next disruptive leap forward in data sciences. Most legal scholarship related to the topic has focused on its relevance to finance, but it could revolutionize business supply chains. Specifically, blockchain-enabled solutions are expected to improve the reliability of data related to supply chains and to help businesses eliminate fraud, inefficiencies, waste, and harms to people and the environment. Despite the surrounding hype, this paper will explain why the promise of distributed electronic ledgers will only be realized in the context of effective governance and legal frameworks. This paper draws upon scholarly articles and the opinions of entrepreneurs actively engaged in bringing blockchain-enabled technologies to market to arrive at two sets of related conclusions. First, that the benefits of the technology — including its potential to help businesses prosper while eliminating societal and environmental harms — will only be realized in the context of enabling frameworks of law. Second, the author articulates how the role of the legal profession vis-à-vis business clients will evolve in the era of blockchain-enabled business supply chain optimization.


Reference Type: Journal Article


Abstract: In December 2014, Estonia became the first nation to open its digital borders to enable anyone, anywhere in the world to apply to become an e-Resident. Estonian e-Residency is essentially a commercial initiative. The e-ID issued to Estonian e-Residents enables commercial activities with the public and private sectors. It does not provide citizenship in its traditional sense, and the e-ID provided to e-Residents is not a travel document. However, in many ways it is an international ‘passport’ to the virtual world. E-Residency is a profound change and the recent announcement that the Estonian government is now partnering with Bitnation to offer a public notary service to Estonian e-Residents based on blockchain technology is of significance. The application of blockchain to e-Residency has the potential to fundamentally change the way identity information is controlled and authenticated. This paper examines the legal, policy, and technical implications of this development.


Reference Type: Conference Proceedings


Abstract: Blockchain is one of the technology innovations for sharing data across organizations through a peer to peer overlay network. Many blockchain-based data sharing applications, such as sharing Electronic Health Records (EHRs) among different Care Delivery Organizations (CDOs), require privacy preserving verification services with dual capabilities. On one hand, the users want to verify the authenticity of EHR data as well as the identity of the signer. On the other hand, the signer wants to keep his real identity private such that others cannot trace and infer his identity information. However, typical blockchain systems that use pseudonyms as public keys, such as Bitcoin’s blockchain, cannot support such privacy-preserving verification. In such systems, it is hard to verify the authenticity of signer’s identity, and adversaries or curious parties can guess the real identity from the series of statements and actions taken with a specific pseudonym through inference attacks, such as by transaction graph analysis. In this paper, we propose a decentralized attribute-based signature scheme for healthcare blockchain, which provides efficient privacy-preserving verification of authenticity of EHR data and signer’s identity. We also describe a holistic on-chain and off-chain collaborative storage system for efficient storage and verification EHR data. The analysis and experiments show that our scheme is effective and deployable.

Abstract: We present the results of our eighth annual horizon scan of emerging issues likely to affect global biological diversity, the environment, and conservation efforts in the future. The potential effects of these novel issues might not yet be fully recognized or understood by the global conservation community, and the issues can be regarded as both opportunities and risks. A diverse international team with collective expertise in horizon scanning, science communication, and conservation research, practice, and policy reviewed 100 potential issues and identified 15 that qualified as emerging, with potential substantial global effects. These issues include new developments in energy storage and fuel production, sand extraction, potential solutions to combat coral bleaching and invasive marine species, and blockchain technology.
be developed: one for Ethereum and another for Hyperledger Fabric. The proof-of-work (PoW) consensus algorithm of Ethereum will be modified into a delegated proof-of-stake (DPoS) or practical Byzantine fault tolerance (PBFT) consensus algorithm as it is scalable and fits the drug supply chain environment. The system will adopt the GS1 pedigree standard and will satisfy the data points in the data standardization guidelines from the US FDA. Simulations will use the following 5 nodes: for FDA, manufacturer, wholesaler, retailer, and the consumer portal. RESULTS: Development is underway. The design of the system will place FDA in a supervisory data verification role, with each pedigree type-specific data source serving a primary data verification role. The supply chain process will be initiated by the manufacturer, with recursive verification for every transaction. It will allow consumers to scan a code printed on the receipt of their purchases to review the drug distribution history. CONCLUSIONS: Development and testing will be conducted in a simulated network, and thus, results may differ from actual practice. The project being proposed is disruptive; once tested, the team intends to engage the Philippine FDA to discuss implementation plans and formulate policies to facilitate adoption and sustainability. REGISTERED REPORT IDENTIFIER: RR1-10.2196/10163.


Reference Type: Conference Paper


Abstract: Digital identity is the cornerstone of a digital economy. However, proving identity remotely is difficult to do. To complicate things further, identity is usually not a global, absolute construct, but the information shared with different parties differs, based on the relationship to the user. Therefore, a viable solution for digital identity should enable users to have full control over their personal information and share only the information that they wish to share with each service. Blockchain technology can help to realize a self-sovereign identity that puts the user in control of her information, by enabling a decentralized way to handle public key infrastructure. In the current contribution, we present the Sora identity system, which is a mobile app that utilizes blockchain technology to create a secure protocol for storing encrypted personal information, as well as sharing verifiable claims about personal information.


Reference Type: Journal Article


Abstract: In proof-of-work (PoW)-based blockchain networks, the miners contribute their distributed computation in solving a crypto-puzzle competition to win the reward. To secure stable profits, some miners organize mining pools and share the rewards from the pool in proportion to each miner’s contribution. However, some miners may exhibit malicious behaviors which cause a waste of distributed computation resource, even posing a threat on the efficiency of blockchain networks. In this paper, we propose a new game-theoretic framework to incentivize miners mining honestly and help to bring about a higher total welfare of blockchain networks. We first formulate the mining process as a noncooperative iterated game. We then propose a mechanism in terms of zero-determinant strategies (ZD strategies) to encourage the cooperative mining and improve the efficiency of mining in PoW-based blockchain networks. In addition, we theoretically analyze the maximum system welfare of the target pool through the method of optimization. Numerical illustrations are also presented to support our theoretical results.


Reference Type: Journal Article


Abstract: In traditional electronic health records (EHRs), medical-related information is generally separately controlled by different hospitals and thus it leads to the inconvenience of information sharing. Cloud-based EHRs solve the problem of information sharing in the traditional EHRs. However, cloud-based EHRs suffer the centralized problem, i.e., cloud service center and key-generation center. This paper works on creating a new EHRs paradigm which can help in dealing with the centralized problem of cloud-based EHRs. Our solution is to make use of the emerging technology of blockchain to EHRs (denoted as blockchain-based EHRs for convenience). First, we formally define the system model of blockchain-based EHRs in the setting of consortium blockchain. In addition, the authentication issue is very important for EHRs. However, existing authentication schemes for blockchain-based EHRs have their own weak points. Therefore, in this paper, we also propose an authentication scheme for blockchain-based EHRs. Our proposal is an identity-based signature scheme with multiple authorities which can
Abstract: The technology that has had the most impact on our lifestyles in the last decade is Blockchain. A word that often arises when talking about Blockchain is Bitcoin. Many people still confuse Blockchain with Bitcoin; however, they are not the same. Bitcoin is just one of many applications that use Blockchain technology. In this paper, the authors conduct a survey of Blockchain applications using Blockchain technology and the challenges these face.

Tasatanatkool P, Techapanupreeda C. Blockchain: challenges and applications. 2018 International Conference on Information Networking (ICOIN); 2018 Jan 10-12; Chiang Mai, Thailand. IEEE.

Reference Type: Conference Proceedings


Abstract: At present, medical images account for nearly 70% of medical diagnostic data, which is an important basis for disease diagnosis. However, medical data leakage incidents have occurred in more than 90% medical institutions, the protection of patients' medical data is of great urgency. At present, all types of medical institutions involved in the medical imaging business use the PACS to archive, manage, and use the collected medical images, but only sharing the managed video resources within the organization. This method applies only the traditional data protection strategy and cannot guarantee a stronger protection for patients' private information. And patients have no control over medical information at the time of treatment. For this reason, this paper proposes a method of secure sharing of medical images based on smart contracts of block chain and credit scores. Through a blockchain based on distributed, reliable database of recording image sharing process, we realize a cross-organizational, cross-regional, trustworthy, and supervisory medical image sharing system. And the establishment of smart contracts based on credit scores of patients and medical institutions guarantee intelligent sharing by rules and conditions. Compared with traditional PACS, the method proposed in this paper extends its scope of application on the basis of PACS, increases its robustness, and provides new ideas for more extensive, multi-level, safe and reliable medical images sharing.

Tang H, Tong N, Ouyang J. Medical images sharing system based on blockchain and smart contract of credit scores. 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN); 2018 Aug 15-17; Shenzhen, China. IEEE.

Reference Type: Conference Proceedings


Abstract: The proliferation of inter-connected devices in critical industries, such as healthcare and power grid, is changing the perception of what constitutes critical infrastructure. The rising interconnectedness of new critical industries is driven by the growing demand for seamless access to information as the world becomes more mobile and connected and as the Internet of Things (IoT) grows. Critical industries are essential to the foundation of today's society, and interruption of service in any of these sectors can reverberate through other sectors and even around the globe. In today's hyper-connected world, the critical infrastructure is more vulnerable than ever to cyber threats, whether state sponsored, criminal groups or individuals. As the number of interconnected devices increases, the number of potential access points for hackers to disrupt critical infrastructure grows. This new attack surface emerges from fundamental changes in the critical infrastructure of organizations technology systems. This paper aims to improve understanding the challenges to secure future digital infrastructure while it is still evolving. After introducing the infrastructure generating big data, the functionality-based fog architecture is defined. In addition, a comprehensive review of security requirements in fog-enabled IoT systems is presented. Then, an in-depth analysis of the fog computing security challenges and big data privacy and trust concerns in relation to fog-enabled IoT are given. We also discuss blockchain as a key enabler to address many security related issues in IoT and consider closely the complementary interrelationships between blockchain and fog computing. In this context, this work formalizes the task of securing big data and its scope, provides a taxonomy to categories threats to fog-based IoT systems, presents a comprehensive comparison of state-of-the-art contributions in the field according to their security service and recommends promising research directions for future investigations.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/8/1788

Abstract: The technology that has had the most impact on our lifestyles in the last decade is Blockchain. Furthermore, our scheme is provably secure in the random oracle model and has more efficient signing and verification algorithms than existing authentication schemes of blockchain-based EHRs.

Reference Type: Conference Proceedings

Abstract: Digital technologies is one of the priorities in the development of the healthcare sector worldwide, this market is increasing by a quarter every year. The process can provide a breakthrough in the availability and quality of services without increasing health care costs. Therefore the development of digital medicine is carried out with the active participation of the state. Russia is not an exception. In Russia, several information-analytical projects of noticeable global scale are already being introduced. In the near future, fundamentally new ways of development may emerge in the healthcare sector: digitalization of medical data, use of mobile devices to monitor and transmit medical indicators online, developing cloud services providing their storage and processing, introducing artificial intelligence to help doctors quickly take the right decisions. The article considers digital technologies in healthcare as a complex of financial, economic, technical, social, organizational, production business processes that can affect the quality of medical services, the performance of the state guarantees program of medical care, and ultimately, the quality of life of citizens and the implementation of the state strategic plans as a whole. The authors provide analysis of the implementation of digital technologies in health care and assert that digital health technologies are successfully implemented in the Russian Federation, and make appropriate generalizations and conclusions.


Reference Type: Conference Paper

Abstract: Blockchain technology though originally designed for keeping financial ledgers, recently has found applications in many different fields including healthcare. Sharing healthcare data for research purposes will boost research innovation in this area. That being said, healthcare data sharing raises many privacy and security issues for the Patients who share their data. In this work, we present the potential of Blockchain technology to facilitate (i) private and auditable healthcare data sharing and (ii) healthcare data access permission handling by proposing a blockchain-based system architecture design.


Reference Type: Journal Article

Abstract: [FIRST PARAGRAPH] The world is changing exponentially—never before in the history of human kind have we experienced such change. There is an unprecedented opportunity to connect creatively disruptive innovations to transform the world for the better. One such creative disruption is blockchain technology. Blockchain is a decentralized distributed ledger, which is immutable and un hackable. In August 2016, the World Economic Forum released a report calling blockchain technology a "mega-trend" that will shape society in the next decade, predicting that blockchains could store as much as 10% of global GDP by 2027.


Reference Type: Journal Article
Abstract: Medical data are important in diagnosis, treatment, recovery, and medical accident investigation. The integrity and availability of medical data are the basic guarantee for the smooth operation of these activities. The privacy of medical data is a natural demand from the sensitivity of medical data. At present, there are mainly two ways to protect the privacy of medical data. One way is to store medical data in a local database and set up an access control strategy of the database. The other way is to encrypt medical data with the patient’s key and to share the key when needed. The problem with the first method is that the data in the local database may be modified or deleted. The problem with the second method is that the key cannot be shared when the patient dies during the diagnosis and treatment. These two problems will damage the availability of data. This paper proposes to establish a shared key that could be reconstructed by the legitimate parties before the process of diagnosis and treatment begins. The data in the diagnosis and treatment process is encrypted and stored in a blockchain using the shared key. The proposal meets the integrity, availability and privacy requirements of medical data. It uses the sibling intractable function families (SIFF) to establish a shared key, and uses the Hyperledger Fabric to store encrypted data. The simulation shows that the system has good efficiency. Additionally, it is the first time to introduce SIFF to a blockchain application.


Reference Type: Journal Article
Available from: https://gh.bmj.com/content/2/4/e000570.abstract
Abstract: Blockchain technology and cryptocurrencies could remake global health financing and usher in an era global health equity and universal health coverage. We outline and provide examples for at least four important ways in which this potential disruption of traditional global health funding mechanisms could occur: universal access to financing through direct transactions without third parties; novel new multilateral financing mechanisms; increased security and reduced fraud and corruption; and the opportunity for open markets for healthcare data that drive discovery and innovation. We see these issues as a paramount to the delivery of healthcare worldwide and relevant for payers and providers of healthcare at state, national and global levels; for government and non-governmental organisations; and for global aid organisations, including the WHO, International Monetary Fund and World Bank Group.

Reference Type: Conference Paper
Abstract: Blockchain has recently attracted tremendous interest due to its ability to enhance security and privacy through an immutable shared distributed ledger. Blockchain's ability to detect integrity violations are particularly key in providing assured data provenance in cloud platform. The practical adoption of blockchain will largely hinge on consensus protocols meeting performance and security guarantees. In this paper, we present the design issues for consensus protocols for blockchain based cloud provenance. We present the blockchain based data provenance framework for cloud. We find that there are performance and security challenges in adopting proof-of-work consensus protocol within this framework. We present unique design challenges and opportunities in developing proof-of-stake for data provenance in cloud platform.

Reference Type: Journal Article
Available from: https://www.mdpi.com/2305-6290/3/1/10
Abstract: Integrating triple bottom line (TBL) goals into supply chains (SCs) is a challenging task which necessitates the careful coordination of numerous stakeholders; individual interests. Recent technological advancements can impact TBL sustainability by changing the design, structure, and management of modern SCs. Blockchain technology enables immutable data records and facilitates a
shared data view along the supply chain. The Physical Internet (PI) is an overarching framework that can be applied to create a layered and comprehensive view of the SC. In this conceptual paper, I define and combine these technologies and derive several high-level research areas and research questions (RQ) to investigate adoption and management as well as structural SC issues. I suggest a theory-based research agenda for the years to come that exploits the strengths of rigorous academic research, while remaining relevant for industry. Furthermore, I suggest various well-established theories to tackle the respective research questions and provide specific directions for future research.


Reference Type: Journal Article


Abstract: Purpose: This paper aims to strive to close the current research gap pertaining to potential implications of the blockchain for supply chain management (SCM) by presenting a framework built on four established economic theories, namely, principal agent theory (PAT), transaction cost analysis (TCA), resource-based view (RBV) and network theory (NT). These theories can be used to derive research questions that are theory-based as well as relevant for the industry. This paper is intended to initiate and stimulate an academic discussion on the potential impact of the blockchain and introduces a framework for middle-range theorizing together with several research questions.

Design/methodology/approach: This paper builds on previous theories that are frequently used in SCM research and shows how they can be adapted to blockchain-related questions.

Findings: This paper introduces a framework for middle-range theorizing together with several research questions.

Research limitations/implications: The paper presents blockchain-related research questions derived from four frequently used theories, namely, PAT, TCA, RBV and (NT). These questions will guide future research pertaining to structural (PAT, TCA) and managerial issues (RBV, NT) and will foster middle-range theory development in SCM research.

Practical implications: Blockchain technology has the potential to significantly change SCM. Given the huge investments by industry, academic research is needed which investigates potential implications and supports companies. In this paper, various research questions are introduced that illustrate how the implications of blockchain on SCM can be investigated from different perspectives.

Originality/value: To the best of the author’s knowledge, no academic papers are published in leading academic journals that investigate the relationship between SCM and blockchain from a theory-based perspective.


Reference Type: Journal Article


Abstract: About a decade ago the fundamental operating principle of the Blockchain was introduced. It took several years before the technology gained widespread recognition in industry and academic communities outside of the computer science sphere. Since then many academic communities have taken up the topic, but so far no well-defined research agenda has emerged: research topics are scattered and rigorous approaches are scarce. More often than not, use cases implemented by industry apply a trial and error approach and there exists a dearth of theory-based academic papers on the topic following robust methodologies. Being a nascent research topic, case studies on Blockchain applications are a suitable approach to systematically transfer industry experience into research agendas which benefit both theory development and testing as well as design science research. In this paper I offer guidelines and suggestions on how to design and structure Blockchain case studies to create value for academia and the industry. More specifically, I describe Blockchain characteristics and challenges, present existing Blockchain case studies, and discuss various types of case study research and how they can be useful for industry and academic research. I conclude with a framework and a checklist for Blockchain case study research.


Reference Type: Conference Paper

Abstract: With the increasingly serious problem of food safety in China, it directly or indirectly endangers people's health, quality of life and safety of life. The global economy, politics and society as a whole have a greater impact. As an effective means of product quality and safety management and control, many countries and regions have been researched, developed and operated of the traceability system. On the one hand, these technologies have not been able to achieve more accurate traceability, these results cannot be directly used in Chinese market. Therefore, the article introduces the concept of Blockchain technology, putting forward the application of Blockchain technology in information security of the food supply chain and comparing it with the traditional supply chain system.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1660-4601/15/6/1055

Abstract: As a trust machine, blockchain was recently introduced to the public to provide an immutable, consensus based and transparent system in the Fintech field. However, there are ongoing efforts to apply blockchain to other fields where trust and value are essential. In this paper, we suggest Gcoin blockchain as the base of the data flow of drugs to create transparent drug transaction data. Additionally, the regulation model of the drug supply chain could be altered from the inspection and examination only model to the surveillance net model, and every unit that is involved in the drug supply chain would be able to participate simultaneously to prevent counterfeit drugs and to protect public health, including patients.


Reference Type: Journal Article

Abstract: Since its initial popularization in 2008 as the underpinnings of the digital currency Bitcoin, blockchain has seen its implications spread beyond the financial industry. The field of dermatology presents promising potential applications for this burgeoning technology. Blockchain facilitates communication on a peer-to-peer platform with users sharing data directly with each other. Computational algorithms ensure that the database is permanent, chronologically ordered and universally available on a network while remaining cryptographically secure. These attributes allow blockchain to remove intermediary costs, reduce manual errors and decrease risks of single points of failure.


Reference Type: Conference Paper
Available from: http://ebooks.iospress.nl/publication/49193 Subscription required to view.

Abstract: Healthcare directories are vital for interoperability among healthcare providers, researchers and patients. Past efforts at directory services have not provided the tools to allow integration of the diverse data sources. Many are overly strict, incompatible with legacy databases, and do not provide Data Provenance. A more architecture-independent system is needed to enable secure, GDPR-compatible service discovery across organizational boundaries. We review our development of a portable Data Provenance Toolkit supporting provenance within Health Information Exchange (HIE) systems. The Toolkit has been integrated with client software and successfully leveraged in clinical data integration. The Toolkit validates provenance stored in a Blockchain or Directory record and creates provenance signatures, providing standardized provenance that moves with the data. This healthcare directory suite implements discovery of healthcare data by HIE and EHR systems via FHIR. Shortcomings of past directory efforts include the ability to map complex datasets and enabling interoperability via exchange endpoint discovery. By delivering data without dictating how it is stored we improve exchange and facilitate discovery on a multi-national level through open source, fully interoperable tools. With the development of Data Provenance resources we enhance exchange and improve security and usability throughout the health data continuum.

U. S. Government Accountability Office. Urgent actions are needed to address cybersecurity challenges

Abstract: Federal agencies and the nation’s critical infrastructures—such as energy, transportation systems, communications, and financial services—are dependent on information technology systems to carry out operations. The security of these systems and the data they use is vital to public confidence and national security, prosperity, and well-being.

The risks to these systems are increasing as security threats evolve and become more sophisticated. GAO first designated information security as a government-wide high-risk area in 1997. This was expanded to include protecting cyber critical infrastructure in 2003 and protecting the privacy of personally identifiable information in 2015.

This report provides an update to the information security high-risk area. To do so, GAO identified the actions the federal government and other entities need to take to address cybersecurity challenges. GAO primarily reviewed prior work issued since the start of fiscal year 2016 related to privacy, critical federal functions, and cybersecurity incidents, among other areas. GAO also reviewed recent cybersecurity policy and strategy documents, as well as information security industry reports of recent cyberattacks and security breaches.


Abstract: The Internet of Things (IoT) has facilitated services without human intervention for a wide range of applications, including continuous remote patient monitoring (RPM). However, the complexity of RPM architectures, the size of data sets generated and limited power capacity of devices make RPM challenging. In this paper, we propose a tier-based End to End architecture for continuous patient monitoring that has a patient centric agent (PCA) as its center piece. The PCA manages a blockchain component to preserve privacy when data streaming from body area sensors needs to be stored securely. The PCA based architecture includes a lightweight communication protocol to enforce security of data through different segments of a continuous, real time patient monitoring architecture. The architecture includes the insertion of data into a personal blockchain to facilitate data sharing amongst healthcare professionals and integration into electronic health records while ensuring privacy is maintained. The blockchain is customized for RPM with modifications that include having the PCA select a Miner to reduce computational effort, enabling the PCA to manage multiple blockchains for the same patient, and the modification of each block with a prefix tree to minimize energy consumption and incorporate secure transaction payments. Simulation results demonstrate that security and privacy can be enhanced in RPM with the PCA based End to End architecture.


Abstract: Continuous monitoring of patient’s physiological signs has the potential to augment traditional medical practice, particularly in developing countries that have a shortage of healthcare professionals. However, continuously streamed data presents additional security, storage and retrieval challenges and further inhibits initiatives to integrate data to form electronic health record systems. Blockchain technologies enable data to be stored securely and inexpensively without recourse to a trusted authority. Blockchain technologies also promise to provide architectures for electronic health records that do not require huge government expenditure that challenge developing nations. However, Blockchain deployment, particularly with streamed data challenges existing Blockchain algorithms that take too long to place data in a block, and have no mechanism to determine whether every data point in every stream should be stored in such a secure way. This article presents an architecture that involves a Patient Agent, coordinating the insertion of continuous data streams into Blockchains to form an electronic health record.

Reference Type: Book Section

Abstract: Emily Vaughn was one of the early leaders in the blockchain space. In this chapter she reflects on the origins of blockchain and how it arrived in healthcare. This perspective serves to inform her transition in to the healthcare blockchain space first at Gem, then at Change Healthcare. In the latter parts of this chapter, she provides insights in to the earliest proofs of concept by companies like Philips and Tieto. And she goes on to describe how, in her current role at Change Healthcare, she views the various stages of incorporating blockchain in to Change's enterprise strategy.


Reference Type: Journal Article
Available from: https://www.jmir.org/2019/2/e12439/

Abstract: BACKGROUND: The decentralized nature of sensitive health information can bring about situations where timely information is unavailable, worsening health outcomes. Furthermore, as patient involvement in health care increases, there is a growing need for patients to access and control their data. Blockchain is a secure, decentralized online ledger that could be used to manage electronic health records (EHRs) efficiently, therefore with the potential to improve health outcomes by creating a conduit for interoperability. OBJECTIVE: This study aimed to perform a systematic review to assess the feasibility of blockchain as a method of managing health care records efficiently. METHODS: Reviewers identified studies via systematic searches of databases including PubMed, MEDLINE, Scopus, EMBASE, ProQuest, and Cochrane Library. Suitability for inclusion of each was assessed independently. RESULTS: Of the 71 included studies, the majority discuss potential benefits and limitations without evaluation of their effectiveness, although some systems were tested on live data. CONCLUSIONS: Blockchain could create a mechanism to manage access to EHRs stored on the cloud. Using a blockchain can increase interoperability while maintaining privacy and security of data. It contains inherent integrity and conforms to strict legal regulations. Increased interoperability would be beneficial for health outcomes. Although this technology is currently unfamiliar to most, investments into creating a sufficiently user-friendly interface and educating users on how best to take advantage of it would lead to improved health outcomes.


Reference Type: Journal Article

Abstract: Blockchain can be considered as a digital database of cryptographically validated transactions stored as blocks of data. Copies of the database are distributed on a peer-to-peer network adhering to a consensus protocol for authentication of new blocks into the chain. While confined to financial applications in the past, this technology is quickly becoming a hot topic in healthcare and scientific research. Potential applications in radiology range from upgraded monitoring of training milestones achievement for residents to improved control of clinical imaging data and easier creation of secure shared databases.


Reference Type: Journal Article

Abstract: In the context of logistics, blockchain can help to increase end-to-end visibility along global supply chains. Thus, it can lead to improved tracking of goods and offer tamper-proof data to build trust among parties. Although a variety of blockchain use cases already exists, not all of them seem to rely on blockchain-specific features, but could rather be solved with traditional technologies. The purpose of this
paper is, therefore, to identify characteristic use cases described for blockchain in the field of LSCM and to analyze them regarding their mindful technology use based on five mindful technology adoption principles: engagement with the technology; Technological novelty seeking; awareness of local context; cognizance of alternative technologies; and anticipation of technology alteration. The authors identified five blockchain case clusters and chose one case for each category to be analyzed in detail. Most cases demonstrate high engagement with the technology, but there are significant differences when it comes to the other mindful use principles. This paper highlights the need to understand the problem and to apply the right technology in order to solve it. When solving a problem, care should be taken to address a technology's unique features to ensure effectiveness and cost-efficiency.


Reference Type: Newspaper Article
Available from: https://www.wsj.com/articles/the-bots-manipulating-bitcoins-price-1538481600
Subscription required to view.

Abstract: Investors know bitcoin’s violent mood swings well. What they often don’t know is that unscrupulous traders, wielding purpose-built software, can be behind them.

Manipulation in cryptocurrencies is a growing concern for regulators—and even for some proponents of the digital coins. The Securities and Exchange Commission cited that risk in August when rejecting several bitcoin-based exchange-traded funds. The office of New York Attorney General Barbara D. Underwood highlighted the issue last month in a report warning that crypto exchanges were vulnerable to manipulation.

“When any venue tolerates manipulative or abusive conduct, the integrity of the entire market is at risk,” the report said, citing automated trading programs, or “bots,” as a source of price manipulation. Trading programs exist in other markets, like stocks, and they can be used for both legitimate and manipulative strategies. Crypto traders can create bots themselves or buy them online.


Reference Type: Journal Article
Subscription required to view.

Abstract: [FIRST PARAGRAPH] Drug manufacturing is expensive, and it takes approximately two billion dollars to manufacture a single type of drug. Replacement of these drugs with counterfeit drugs is a prevailing problem and causes about 150 billion dollar [1] loss to the pharmaceutical industry annually. In addition to loss of money, counterfeit drugs also pose a threat to lives, and sabotages reputed brand names. The counterfeit drug problem is encouraged because of lack of coordination and traceability of the drug itself within the pharmaceutical supply chain. The pharmaceutical supply chain is a highly complex and branched chain where many players are involved in moving the drug from one point to the other. Since there is no system in place to accurately trace the drug movement, counterfeiters enter the supply chain, and replace the authentic drugs with fake ones.


Reference Type: Journal Article
Subscription required to view.

Abstract: To achieve confidentiality, authentication, integrity of medical data, and support fine-grained access control, we propose a secure electronic health record (EHR) system based on attribute-based cryptosystem and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data, and use identity-based signature (IBS) to implement digital signatures. To achieve different functions of ABE, IBE and IBS in one cryptosystem, we introduce a new cryptographic primitive, called combined attribute-based/identity-based encryption and signature (C-AB/IB-ES). This greatly facilitates the management of the system, and does not need to introduce different cryptographic systems for different security requirements. In addition, we use blockchain techniques to ensure the integrity and traceability of medical data. Finally, we give a demonstrating application for medical insurance scene.

Reference Type: Conference Paper

Abstract: With the continuous development and application of blockchain technology, the academic and commercial circles are constantly exploring the research directions and practical applications of blockchains. Today, in the financial, sales, medical and other fields, the blockchain has already played its advantages. In this paper, we focus on the related research and applications of blockchain technology in the field of intellectual property, analyze the academic research and commercial application in this direction, and try to provide a new feasible direction for the research and development of the blockchain in the next stage.


Reference Type: Journal Article

Abstract: To improve the accuracy of diagnosis and the effectiveness of treatment, a framework of parallel healthcare systems (PHSs) based on the artificial systems + computational experiments + parallel execution (ACP) approach is proposed in this paper. PHS uses artificial healthcare systems to model and represent patients’ conditions, diagnosis, and treatment process, then applies computational experiments to analyze and evaluate various therapeutic regimens, and implements parallel execution for decision-making support and real-time optimization in both actual and artificial healthcare processes. In addition, we combine the emerging blockchain technology with PHS, via constructing a consortium blockchain linking patients, hospitals, health bureaus, and healthcare communities for comprehensive healthcare data sharing, medical records review, and care audiability. Finally, a prototype named parallel gout diagnosis and treatment system is built and deployed to verify and demonstrate the effectiveness and efficiency of the blockchain-powered PHS framework.


Reference Type: Journal Article

Abstract: Purpose: This paper aims to investigate the way in which blockchain technology is likely to influence future supply chain practices and policies. Design/methodology/approach: A systematic review of both academic and practitioner literature was conducted. Multiple accounts of blockchain adoption within industry were also consulted to gain further insight. Findings: While blockchain technologies remain in their infancy, they are gaining momentum within supply chains, trust being the predominant factor driving their adoption. The value of such technologies for supply chain management lies in four areas: extended visibility and traceability, supply chain digitalisation and disintermediation, improved data security and smart contracts. Several challenges and gaps in understanding and opportunities for further research are identified by this research. How a blockchain-enabled supply chain should be configured has also been explored from a design perspective. Research limitations/implications: This systematic review focuses on the diffusion of blockchain technology within supply chains, and great care was taken in selecting search terms. However, the authors acknowledge that their choice of terms may have excluded certain blockchain articles from this review. Practical implications: This paper offers valuable insight for supply chain practitioners into how blockchain technology has the potential to disrupt existing supply chain provisions as well as a number of challenges to its successful diffusion. Social implications: The paper debates the potential social and economic impact brought by blockchain. Originality/value: This paper is one of the first studies to examine the current state of blockchain diffusion within supply chains. It lays a firm foundation for future research.
Abstract: Blockchain has recently gained momentum. Startups, enterprises, banks, and government agencies around the world are exploring the use of blockchain for broad applications including public registries, supply chains, health records, and voting. Dependability properties, like availability, are critical for many of these applications, but the guarantees offered by the blockchain technology remain unclear, especially from an application perspective. In this paper, we identify the availability limitations of two mainstream blockchains, Ethereum and Bitcoin. We demonstrate that while read availability of blockchains is typically high, write availability - for transaction management - is actually low. For Ethereum, we collected 6 million transactions over a period of 97 days. First, we measured the time for transactions to commit as required by the applications. Second, we observed that some transactions never commit, due to the inherent blockchain design. Third and perhaps even more dramatically, we identify the consequences of the lack of built-in options for explicit abort or retry that can maintain the application in an uncertain state, where transactions remain pending (neither aborted nor committed) for

Reference Type: Journal Article


Abstract: This research uses sensemaking theory to explore how emerging blockchain technology may transform supply chains. We investigate three research questions (RQs): What are blockchain technology's perceived benefits to supply chains, where are disruptions mostly likely to occur and what are the potential challenges to further blockchain diffusion? We conducted in-depth interviews with 14 supply chain experts. Cognitive mapping and narrative analysis were deployed as the two main data analysis techniques to aid our understanding and evaluation of people's cognitive complexity in making sense of blockchain technology. We found that individual experts developed different cognitive structures within their own sensemaking processes. After merging individual cognitive maps into a strategic map, we identified several themes and central concepts that then allowed us to explore potential answers to the three RQs. Our study is among the very few to date to explicitly explore how blockchains may transform supply chain practices. Using the sensemaking approach afforded a deeper understanding of how senior executives diagnose the symptoms evident from blockchains and develop assumptions, expectations and knowledge of the technology, which will then shape their future actions regarding its utilisation. We demonstrate the usefulness of sensemaking theory as an alternative lens in investigating contemporary supply chain phenomena such as blockchains. Bringing sensemaking theory to this discipline in particular enriches emerging behavioural operations research. Our contributions also lie in extending the theories of prospective sensemaking and adding further insights to the stream of technology adoption studies.

Reference Type: Report


Abstract: This research uses sensemaking theory to explore how emerging blockchain technology may transform supply chains. We investigate three research questions (RQs): What are blockchain technology's perceived benefits to supply chains, where are disruptions mostly likely to occur and what are the potential challenges to further blockchain diffusion? We conducted in-depth interviews with 14 supply chain experts. Cognitive mapping and narrative analysis were deployed as the two main data analysis techniques to aid our understanding and evaluation of people's cognitive complexity in making sense of blockchain technology. We found that individual experts developed different cognitive structures within their own sensemaking processes. After merging individual cognitive maps into a strategic map, we identified several themes and central concepts that then allowed us to explore potential answers to the three RQs. Our study is among the very few to date to explicitly explore how blockchains may transform supply chain practices. Using the sensemaking approach afforded a deeper understanding of how senior executives diagnose the symptoms evident from blockchains and develop assumptions, expectations and knowledge of the technology, which will then shape their future actions regarding its utilisation. We demonstrate the usefulness of sensemaking theory as an alternative lens in investigating contemporary supply chain phenomena such as blockchains. Bringing sensemaking theory to this discipline in particular enriches emerging behavioural operations research. Our contributions also lie in extending the theories of prospective sensemaking and adding further insights to the stream of technology adoption studies.


Reference Type: Conference Paper


Abstract: Blockchain has recently gained momentum. Startups, enterprises, banks, and government agencies around the world are exploring the use of blockchain for broad applications including public registries, supply chains, health records, and voting. Dependability properties, like availability, are critical for many of these applications, but the guarantees offered by the blockchain technology remain unclear, especially from an application perspective. In this paper, we identify the availability limitations of two mainstream blockchains, Ethereum and Bitcoin. We demonstrate that while read availability of blockchains is typically high, write availability - for transaction management - is actually low. For Ethereum, we collected 6 million transactions over a period of 97 days. First, we measured the time for transactions to commit as required by the applications. Second, we observed that some transactions never commit, due to the inherent blockchain design. Third and perhaps even more dramatically, we identify the consequences of the lack of built-in options for explicit abort or retry that can maintain the application in an uncertain state, where transactions remain pending (neither aborted nor committed) for

Reference Type: Conference Paper

an unknown duration. Finally we propose techniques to mitigate the availability limitations of existing blockchains, and experimentally test the efficacy of these techniques.


Reference Type: Journal Article


Abstract: (NOTE: This article doesn't seem to address blockchain but was found in the PubMed blockchain search results. In my effort to include all PubMed results, this article was then included in this listing.)

BACKGROUND: We aimed to assess the feasibility of a video-augmented fluoroscopy (VAF) technique using a camera-augmented mobile C-arm (CamC) for distal interlocking of intramedullary nails.

METHODS: Three surgeons performed distal interlocking on seven pairs of cadaveric bovine carpal bones using the VAF system and conventional fluoroscopy. We compared radiation exposure, procedure time and drilling quality between the VAF system and conventional fluoroscopic guidance. RESULTS: Distal interlocking using VAF significantly reduced the number of fluoroscopic images compared to conventional fluoroscopy (P<0.05). No significant difference in overall procedure time (P=0.96) or drilling quality (P=0.12) was detected. VAF demonstrated improvement in radiation exposure when used by a less experienced surgeon (P<0.05). CONCLUSION: VAF is a feasible technique for distal interlocking. Overlaid visualization of the osseous anatomy in relation to the surgical field of view appears to improve surgeons' perception of relevant structures and their spatial orientation for the use of surgical instruments.


Reference Type: Journal Article

Available from: https://www.nature.com/articles/s41467-019-08874-y

Abstract: Monitoring and ensuring the integrity of data within the clinical trial process is currently not always feasible with the current research system. We propose a blockchain-based system to make data collected in the clinical trial process immutable, traceable, and potentially more trustworthy. We use raw data from a real completed clinical trial, simulate the trial onto a proof of concept web portal service, and test its resilience to data tampering. We also assess its prospects to provide a traceable and useful audit trail of trial data for regulators, and a flexible service for all members within the clinical trials network. We also improve the way adverse events are currently reported. In conclusion, we advocate that this service could offer an improvement in clinical trial data management, and could bolster trust in the clinical research process and the ease at which regulators can oversee trials.


Reference Type: Journal Article

Available from: https://eprints.utas.edu.au/27633/

Abstract: Blockchain technology is often considered as the fourth industrial revolution that will change the world. The enthusiasm of the transformative nature of blockchain technology has infiltrated healthcare. Blockchain is often seen as the much needed and perfect technology for healthcare, addressing the difficult and complex issues of security and inter-operability. More importantly, the “value” and trust-based system can deliver automated action and response via its smart contract mechanism. Healthcare, however, is a complex system. Health information technology (HIT) so far, has not delivered its promise of transforming healthcare due to its complex socio-technical and context sensitive interaction. The introduction of blockchain technology will need to consider a whole range of socio-technical issues in order to improve the quality and safety of patient care. This paper presents a discussion on these socio-technical issues. More importantly, this paper argues that in order to achieve the best outcome from blockchain technology, there is a need to consider a clinical transformation from “information” to “value” and trust. This paper argues that urgent research is needed to address these socio-technical issues in order to facilitate best outcomes for blockchain in healthcare. These socio-technical issues must then be further evaluated by means of working prototypes in the medical domain in coming years.

Abstract: There are many potential benefits to the application of Artificial Intelligence (AI) technologies, including the reduction of economic inefficiencies and increase in high-skilled jobs. There are also significant risks that must be managed — through both technical design and policy-making instruments — to maximize these benefits for any given society while protecting its important ethical values.

Technical solutions alone are insufficient to ensure ethics permeate AI systems design, absent legal mandate and economic incentives. While legislation can incentivize competition, it is also limited by territorial and time-based constraints. This raises the importance of using alternative policy-making instruments that demonstrate “agile governance.”

Human-centric AI governance is a complex enterprise that requires leveraging mixed policy tools to address the multi-layered ethical concerns at play.


Abstract: The Forum’s Global Future Council on Neurotechnologies highlights the role technology is now playing in helping to address mental health concerns, mapping the areas for special focus and highlighting the ethical considerations for governments, policy makers and health leaders. The Council urges governments, policy-makers, business leaders and practitioners to address the barriers keeping effective treatments from those who need them, which include ethical considerations and a lack of evidence-based research. The report outlines eight actions that will enable technology to ethically address mental ill-health at scale.


Abstract: Fourth Industrial Revolution trends are disrupting long-established business models. Growing demand for customized products. Shifts and skill mismatches in production value chains. Digitization across every dimension of manufacturing. A volatile socioeconomic climate marked by protectionism and populism. These trends are transforming the production landscape, and leadership is no exception.

The scale, complexity and urgency of today’s challenges are significant. How do leaders balance delivering short-term results while being stewards to their people? What takes primacy: shareholder and market priorities or long-term impacts on people, families and communities? How do leaders navigate their own personal transformations while simultaneously guiding their people in uncharted territory? The common denominator across all these questions: How do we put people at the centre? This question guided our project work in 2018. Taking a field-based approach, we explored the authentic experiences of production constituents who are managing this complexity on the ground, along with the advice of external leadership experts, to examine a new leadership paradigm. Starting with the six dimensions of the World Economic Forum’s Leadership Transformation Map, a refreshed set of supporting behaviours emerged that help leaders navigate today’s disruption to influence tomorrow’s success – by putting people at the centre.


Abstract: Just as decentralization communication systems lead to the creation of the Internet, today a new technology — the blockchain — has the potential to decentralize the way we store data and manage
information, potentially leading to a reduced role for one of the most important regulatory actors in our society: the middleman.

Blockchain technology enables the creation of decentralized currencies, self-executing digital contracts (smart contracts) and intelligent assets that can be controlled over the Internet (smart property). The blockchain also enables the development of new governance systems with more democratic or participatory decision-making, and decentralized (autonomous) organizations that can operate over a network of computers without any human intervention. These applications have led many to compare the blockchain to the Internet, with accompanying predictions that this technology will shift the balance of power away from centralized authorities in the field of communications, business, and even politics or law.

In this Article, we explore the benefits and drawbacks of this emerging decentralized technology and argue that its widespread deployment will lead to expansion of a new subset of law, which we term Lex Cryptographia: rules administered through self-executing smart contracts and decentralized (autonomous) organizations. As blockchain technology becomes widely adopted, centralized authorities, such as governmental agencies and large multinational corporations, could lose the ability to control and shape the activities of disparate people through existing means. As a result, there will be an increasing need to focus on how to regulate blockchain technology and how to shape the creation and deployment of these emerging decentralized organizations in ways that have yet to be explored under current legal theory.


Reference Type: Magazine Article


Abstract: A health-care system gathers comprehensive physiological information and medical records, making its data more important than ever. For example, for years now, the National Health Insurance Administration (https://www.nhi.gov.tw/English) of Taiwan has requested every doctor, whether in a medical center or private clinic, to upload the diagnosis result, treatment, and prescription. These anamneses have also been stored in the National Health Insurance Research Database (http://nhird.nhi.org.tw/en/index.html) since 1 March 1995, and 99.9% of the Taiwanese population have been enrolled since 2014. With this comprehensive database, analytics tools can be run to uncover useful information to further understand the etiological factors for rare disorders. This database is successful primarily because Taiwan is a small but densely populated island, making it relatively easy for the government to collect most, if not all, the anamneses.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/10/3472

Abstract: Blockchain has emerged as a decentralized and trustable ledger for recording and storing digital transactions. The mining process of Blockchain, however, incurs a heavy computational workload for miners to solve the proof-of-work puzzle (i.e., a series of the hashing computation), which is prohibitive from the perspective of the mobile terminals (MTs). The advanced multi-access mobile edge computing (MEC), which enables the MTs to offload part of the computational workloads (for solving the proof-of-work) to the nearby edge-servers (ESs), provides a promising approach to address this issue. By offloading the computational workloads via multi-access MEC, the MTs can effectively increase their successful probabilities when participating in the mining game and gain the consequent reward (i.e., winning the bitcoin). However, as a compensation to the ESs which provide the computational resources to the MTs, the MTs need to pay the ESs for the corresponding resource-acquisition costs. Thus, to investigate the trade-off between obtaining the computational resources from the ESs (for solving the proof-of-work) and paying for the consequent cost, we formulate an optimization problem in which the MTs determine their acquired computational resources from different ESs, with the objective of maximizing the MTs’ social net-reward in the mining process while keeping the fairness among the MTs. In spite of the non-convexity of the formulated problem, we exploit its layered structure and propose efficient distributed algorithms for the MTs to individually determine their optimal computational resources acquired from different ESs. Numerical results are provided to validate the effectiveness of our proposed algorithms and the performance of our proposed multi-access MEC for Blockchain.


Reference Type: Journal Article
Abstract: The dissemination of patients' medical records results in diverse risks to patients' privacy as malicious activities on these records cause severe damage to the reputation, finances, and so on of all parties related directly or indirectly to the data. Current methods to effectively manage and protect medical records have been proven to be insufficient. In this paper, we propose MeDShare, a system that addresses the issue of medical data sharing among medical big data custodians in a trust-less environment. The system is blockchain-based and provides data provenance, auditing, and control for shared medical data in cloud repositories among big data entities. MeDShare monitors entities that access data for malicious use from a data custodian system. In MeDShare, data transitions and sharing from one entity to the other, along with all actions performed on the MeDShare system, are recorded in a tamper-proof manner. The design employs smart contracts and an access control mechanism to effectively track the behavior of the data and revoke access to offending entities on detection of violation of permissions on data. The performance of MeDShare is comparable to current cutting edge solutions to data sharing among cloud service providers. By implementing MeDShare, cloud service providers and other data guardians will be able to achieve data provenance and auditing while sharing medical data with entities such as research and medical institutions with minimal risk to data privacy.

Reference Type: Journal Article
Abstract: In recent years, blockchain technology has attracted considerable attention. It records cryptographic transactions in a public ledger that is difficult to alter and compromise because of the distributed consensus. As a result, blockchain is believed to resist fraud and hacking.

Reference Type: Conference Paper
Abstract: Imaging studies are one of the leading drivers of modern medical decision making, and thus, their accessibility to healthcare providers and patients is of critical importance. However, current techniques for storage and transferring medical imaging data are inconvenient and sometimes wholly inadequate. In this paper, we propose a decentralized autonomous medical image processing approach using blockchain technology. Blockchain will enable the sharing of key relevant data using a distributed, decentralized, shared ledger that is available to participants. We outline a framework that utilizes blockchain to enable users to access imaging data in a secure and autonomous manner. A user case is experimentally investigated to validate our proposed approach.

Reference Type: Journal Article
Available from: https://www.mdpi.com/2072-666X/10/8/541
Abstract: Blockchain technology is increasingly being used in Internet of things (IoT) devices for information security and data integrity. However, it is challenging to implement complex hash algorithms with limited resources in IoT devices owing to large energy consumption and a long processing time. This paper proposes an RISC-V processor with memristor-based in-memory computing (IMC) for blockchain technology in IoT applications. The IMC-adapted instructions were designed for the Keccak hash algorithm by virtue of the extendibility of the RISC-V instruction set architecture (ISA). Then, an RISC-V processor with area-efficient memristor-based IMC was developed based on an open-source core for IoT applications, Hummingbird E200. The general compiling policy with the data allocation method is also disclosed for the IMC implementation of the Keccak hash algorithm. An evaluation shows that >70% improvements in both performance and energy saving were achieved with limited area overhead after introducing IMC in the RISC-V processor.

Reference Type: Electronic Article

Abstract: With a growing trend in medicine towards individualized, patient-centric care, traditional health information technology limits progress. With high administrative costs and the lack of universal data access, contemporary electronic medical records serve more the institution rather than the patient. Blockchain technology, as presently described, was initially developed for use in financial markets, serving as a decentralized, distributed ledger of transactions. However, certain inherent characteristics of this technology suit it for use in the healthcare sector. Potential applications of the blockchain in medicine include interoperable health data access, data storage and security, value-based payment mechanisms, medical supply chain efficiency, amongst others. While the technology remains in nascent stages, it is essential that members of the healthcare community understand the fundamental concepts behind blockchain, and recognize its potential impact on the future of medical care.


Reference Type: Report


Abstract: Blockchains are tamper evident and tamper resistant digital ledgers implemented in a distributed fashion (i.e., without a central repository) and usually without a central authority (i.e., a bank, company, or government). At their basic level, they enable a community of users to record transactions in a shared ledger within that community, such that under normal operation of the blockchain network no transaction can be changed once published. This document provides a high-level technical overview of blockchain technology. The purpose is to help readers understand how blockchain technology works.


Reference Type: Journal Article


Abstract: With the rapid development of cloud storage, more and more data owners store their data on the remote cloud, that can reduce data owners' overhead because the cloud server maintaining the data for them, e.g., storing, updating and deletion. However, that leads to data deletion becomes a security challenge because the cloud server may not delete the data honestly for financial incentives. Recently, plenty of research works have been done on secure data deletion. However, most of the existing methods can be summarized with the same protocol essentially, which called "one-bit-return" protocol: the storage server deletes the data and returns a one-bit result. The data owner has to believe the returned result because he cannot verify it. In this paper, we propose a novel blockchain-based data deletion scheme, which can make the deletion operation more transparent. In our scheme, the data owner can verify the deletion result no matter how malevolently the cloud server behaves. Besides, with the application of blockchain, the proposed scheme can achieve public verification without any trusted third party.


Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/4/970

Abstract: A trusted routing scheme is very important to ensure the routing security and efficiency of wireless sensor networks (WSNs). There are a lot of studies on improving the trustworthiness between routing nodes, using cryptographic systems, trust management, or centralized routing decisions, etc. However, most of the routing schemes are difficult to achieve in actual situations as it is difficult to dynamically identify the untrusted behaviors of routing nodes. Meanwhile, there is still no effective way to prevent malicious node attacks. In view of these problems, this paper proposes a trusted routing scheme using blockchain and reinforcement learning to improve the routing security and efficiency for WSNs. The feasible routing scheme is given for obtaining routing information of routing nodes on the blockchain, which makes the routing information traceable and impossible to tamper with. The reinforcement learning
model is used to help routing nodes dynamically select more trusted and efficient routing links. From the experimental results, we can find that even in the routing environment with 50% malicious nodes, our routing scheme still has a good delay performance compared with other routing algorithms. The performance indicators such as energy consumption and throughput also show that our scheme is feasible and effective.


Reference Type: Journal Article

Abstract: Blockchain is an emerging field which works on the concept of a digitally distributed ledger and consensus algorithm removing all the threats of intermediaries. Its early applications were related to the finance sector but now this concept has been extended to almost all the major areas of research including education, IoT, banking, supply chain, defense, governance, healthcare, etc. In the field of healthcare, stakeholders (provider, patient, payer, research organizations, and supply chain bearers) demand interoperability, security, authenticity, transparency, and streamlined transactions. Blockchain technology, built over the internet, has the potential to use the current healthcare data into peer to peer and interoperable manner by using a patient-centric approach eliminating the third party. Using this technology, applications can be built to manage and share secure, transparent and immutable audit trails with reduced systematic fraud. This study reviews existing literature in order to identify the major issues of various healthcare stakeholders and to explore the features of blockchain technology that could resolve identified issues. However, there are some challenges and limitations of this technology which are needed to be focused on future research.


Reference Type: Journal Article

Abstract: A discussion on the smart regulatory hands-off approach adopted in the European Union and the USA shows that this approach bodes well for future innovative contributions of blockchains in the financial services and related sectors and toward enhanced financial inclusiveness.


Reference Type: Journal Article
Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477

Abstract: Blockchain is a decentralized transaction and data management technology developed first for Bitcoin cryptocurrency. The interest in Blockchain technology has been increasing since the idea was coined in 2008. The reason for the interest in Blockchain is its central attributes that provide security, anonymity and data integrity without any third party organization in control of the transactions, and therefore it creates interesting research areas, especially from the perspective of technical challenges and limitations. In this research, we have conducted a systematic mapping study with the goal of collecting all relevant research on Blockchain technology. Our objective is to understand the current research topics, challenges and future directions regarding Blockchain technology from the technical perspective. We have extracted 41 primary papers from scientific databases. The results show that focus in over 80% of the papers is on Bitcoin system and less than 20% deals with other Blockchain applications including e.g. smart contracts and licensing. The majority of research is focusing on revealing and improving limitations of Blockchain from privacy and security perspectives, but many of the proposed solutions lack concrete evaluation on their effectiveness. Many other Blockchain scalability related challenges including throughput and latency have been left unstudied. On the basis of this study, recommendations on future research directions are provided for researchers.


Reference Type: Journal Article
Abstract: A blockchain is a distributed, public ledger, recording transaction and tracking assets, and of which immutability is guaranteed by a peer-to-peer network of computers, not by any centralized authority. Assets can be tangible, such as homes or cash, or they can be intangible, such as patents or copyrights. A blockchain consists of ordered records arranged in a block structure. Each data block contains a hash (digital fingerprint or unique identifier), timestamped batches of recent transactions, and a hash of the previous block. With this design, each block is connected in chronological order and the connected blocks are called a blockchain. It is practically impossible to modify one of the blocks in the middle of the chain because all of the blocks after the modified block must be modified at the same time. With this mechanism, the data on the blockchain network are immutable.


Reference Type: Journal Article


Abstract: The Internet of Things (IoT) has already reshaped and transformed our lives in many ways, ranging from how we communicate with people or manage our health to how we drive our cars and manage our homes. With the rapid development of the IoT ecosystem in a wide range of applications, IoT devices and data are going to be traded as commodities in the marketplace in the near future, similar to cloud services or physical objects. Developing such a trading platform has previously been identified as one of the key grand challenges in the integration of IoT and data science. Deployment of such a platform raises concerns about the security and privacy of data and devices since their ownership is hard to trace and manage without a central trusted authority. A central trusted authority is not a viable solution for a fully decentralized and distributed IoT ecosystem with a large number of distributed device vendors and consumers. Blockchain, as a decentralized system, removes the requirement for a trusted third party by allowing participants to verify data correctness and ensure its immutability. IoT devices can use blockchain to register themselves and organize, store, and share streams of data effectively and reliably. We demonstrate the applicability of blockchain to IoT devices and data management with an aim of providing end-to-end trust for trading. We also give a brief introduction to the topics and challenges for future research toward developing a trustworthy trading platform for IoT ecosystems.


Reference Type: Journal Article


Abstract: Healthcare data are a valuable source of healthcare intelligence. Sharing of healthcare data is one essential step to make healthcare system smarter and improve the quality of healthcare service. Healthcare data, one personal asset of patient, should be owned and controlled by patient, instead of being scattered in different healthcare systems, which prevents data sharing and puts patient privacy at risks. Blockchain is demonstrated in the financial field that trusted, auditable computing is possible using a decentralized network of peers accompanied by a public ledger. In this paper, we proposed an App (called Healthcare Data Gateway (HGD)) architecture based on blockchain to enable patient to own, control and share their own data easily and securely without violating privacy, which provides a new potential way to improve the intelligence of healthcare systems while keeping patient data private. Our proposed purpose-centric access model ensures patient own and control their healthcare data; simple unified Indicator-Centric Schema (ICS) makes it possible to organize all kinds of personal healthcare data practically and easily. We also point out that MPC (Secure Multi-Party Computing) is one promising solution to enable untrusted third-party to conduct computation over patient data without violating privacy.


Reference Type: Journal Article


Abstract: The adoption of blockchain technology is taking place at a fast pace. Security features inherent in blockchain make it resistant to attack, but they do not make it immune, and blockchain security risks do exist. This paper details the associated risks and concerns of the blockchain. We explore relevant standards and regulations related to blockchain and survey and analyze 38 blockchain incidents to
determine the root cause to provide a view of the most frequent vulnerabilities exploited. The paper reviews six of these 38 incidents in greater detail. The selection is made by choosing incidents with the most frequent root cause. In the review of the incidents, the paper details what happened and why and aims to address what could have been done to mitigate the attack. The paper concludes with a recommendation on a framework to reduce cyber security risks when using blockchain technologies.


Reference Type: Journal Article

Abstract: Electronic health record sharing can help to improve the accuracy of diagnosis, where security and privacy preservation are critical issues in the systems. In recent years, blockchain has been proposed to be a promising solution to achieve personal health information (PHI) sharing with security and privacy preservation due to its advantages of immutability. This work proposes a blockchain-based secure and privacy-preserving PHI sharing (BSPP) scheme for diagnosis improvements in e-Health systems. Firstly, two kinds of blockchains, private blockchain and consortium blockchain, are constructed by devising their data structures, and consensus mechanisms. The private blockchain is responsible for storing the PHI while the consortium blockchain keeps records of the secure indexes of the PHI. In order to achieve data security, access control, privacy preservation and secure search, all the data including the PHI, keywords and the patients' identity are public key encrypted with keyword search. Furthermore, the block generators are required to provide proof of conformance for adding new blocks to the blockchains, which guarantees the system availability. Security analysis demonstrates that the proposed protocol can meet with the security goals. Furthermore, we implement the proposed scheme on JUICE to evaluate the performance.


Reference Type: Journal Article

Abstract: Modern technologies of mobile computing and wireless sensing prompt the concept of pervasive social network (PSN)-based healthcare. To realize the concept, the core problem is how a PSN node can securely share health data with other nodes in the network. In this paper, we propose a secure system for PSN-based healthcare. Two protocols are designed for the system. The first one is an improved version of the IEEE 802.15.6 display authenticated association. It establishes secure links with unbalanced computational requirements for mobile devices and resource-limited sensor nodes. The second protocol uses blockchain technique to share health data among PSN nodes. We realize a protocol suite to study protocol runtime and other factors. In addition, human body channels are proposed for PSN nodes in some use cases. The proposed system illustrates a potential method of using blockchain for PSN-based applications.


Reference Type: Journal Article
Available from: https://peerj.com/preprints/26942/

Abstract: A problem facing healthcare record systems throughout the world is how to share the medical data with more stakeholders for various purposes without sacrificing data privacy and integrity. Blockchain, operating in a state of consensus, is the underpinning technology that maintains the Bitcoin transaction ledger. Blockchain as a promising technology to manage the transactions has been gaining popularity in the domain of healthcare. Blockchain technology has the potential of securely, privately, and comprehensively manage patient health records. In this work, we discuss the latest status of blockchain technology and how it could solve the current issues in healthcare systems. We evaluate the blockchain technology from the multiple perspectives around healthcare data, including privacy, security, control, and storage. We review the current projects and researches of blockchain in the domain of healthcare records and provide the insight into the design and construction of next generations of blockchain-based healthcare systems.

Abstract: Blockchain is a decentralized, trustless protocol that combines transparency, immutability, and consensus properties to enable secure, pseudo-anonymous transactions. Smart contracts are built atop a blockchain to support on-chain storage and enable Decentralized Apps (DApps) to interact with the blockchain programatically. Programmable blockchains have generated interest in the healthcare domain as a potential solution to resolve key challenges, such as gapped communications, inefficient clinical report delivery, and fragmented health records. This paper provides evaluation metrics to assess blockchain-based DApps in terms of their feasibility, intended capability, and compliance in the healthcare domain.


Abstract: Secure and scalable data sharing is essential for collaborative clinical decision making. Conventional clinical data efforts are often siloed, however, which creates barriers to efficient information exchange and impedes effective treatment decision made for patients. This paper provides four contributions to the study of applying blockchain technology to clinical data sharing in the context of technical requirements defined in the "Shared Nationwide Interoperability Roadmap" from the Office of the National Coordinator for Health Information Technology (ONC). First, we analyze the ONC requirements and their implications for blockchain-based systems. Second, we present FHIRChain, which is a blockchain-based architecture designed to meet ONC requirements by encapsulating the HL7 Fast Healthcare Interoperability Resources (FHIR) standard for shared clinical data. Third, we demonstrate a FHIRChain-based decentralized app using digital health identities to authenticate participants in a case study of collaborative decision making for remote cancer care. Fourth, we highlight key lessons learned from our case study.


Abstract: Blockchain offers an innovative approach to storing information, executing transactions, performing functions, and establishing trust in an open environment. Many consider blockchain as a technology breakthrough for cryptography and cybersecurity, with use cases ranging from globally deployed cryptocurrency systems like Bitcoin, to smart contracts, smart grids over the Internet of Things, and so forth. Although blockchain has received growing interests in both academia and industry in the recent years, the security and privacy of blockchains continue to be at the center of the debate when deploying blockchain in different applications. This paper presents a comprehensive overview of the security and privacy of blockchain. To facilitate the discussion, we first introduce the notion of blockchains and its utility in the context of Bitcoin like online transactions. Then we describe the basic security properties that are supported as the essential requirements and building blocks for Bitcoin like cryptocurrency systems, followed by presenting the additional security and privacy properties that are desired in many blockchain applications. Finally, we review the security and privacy techniques for achieving these security properties in blockchain-based systems, including representative consensus algorithms, hash chained storage, mixing protocols, anonymous signatures, non-interactive zero-knowledge proof, and so forth. We conjecture that this survey can help readers to gain an in-depth understanding of the security and privacy of blockchain with respect to concept, attributes, techniques and systems.

Zhang X, Poslad S. Blockchain support for flexible queries with granular access control to electronic medical records (EMR). 2018 IEEE International Conference on Communications (ICC); 2018 May 20-24; Kansas City, MO. Piscataway, NJ: IEEE.

Abstract: In this paper, we propose an architecture for Blockchain-based Electronic Medical Records (EMRs) called GAA-FQ (Granular Access Authorisation supporting Flexible Queries) that comprises an
access model and an access authorisation scheme. Unlike existing Blockchain schemes, our access model can authorise different levels of granularity of authorisation, whilst maintaining compatibility with the underlying Blockchain data structure. Furthermore, the authorisation, encryption, and decryption algorithms proposed in the GAA-FQ scheme dispense with the need to use a public key infrastructure (PKI) and hence improve the computation performance needed to support more granular and distributed, yet authorised, EMR data queries. We validated the computation performance and transmission efficiency for GAA-FQ using a simulation of GAA-FQ against an access control scheme for EMRs called ESPAC as our baseline that was not designed using a Blockchain. To the best of our knowledge, GAA-FQ is the first Blockchain-oriented access authorisation scheme with granular access control, supporting flexible data queries, that has been proposed for secure EMR information management.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/19/14/3091

Abstract: With the development of information technology, films, music, and other publications are inclined to be distributed in digitalized form. However, the low cost of data replication and dissemination leads to digital rights problems and brings huge economic losses. Up to now, existing digital rights management (DRM) schemes have been powerless to deter attempts of infringing digital rights and recover losses of copyright holders. This paper presents a YODA-based digital watermark management system (Y-DWMS), adopting non-repudiation of smart contract and blockchain, to implement a DRM mechanism to infinitely amplify the cost of infringement and recover losses copyright holders suffered once the infringement is reported. We adopt game analysis to prove that in Y-DWMS, the decision of non-infringement always dominates rational users, so as to fundamentally eradicate the infringement of digital rights, which current mainstream DRM schemes cannot reach.


Reference Type: Journal Article

Abstract: Healthcare is a big application scenario of blockchain, and blockchains used in healthcare are called health blockchain. In general, blockchain blocks are open and the transactions in them are public. If some privacy data are involved in these transactions, they will be leaked. Owing to healthcare system involving a great deal of privacy data, certain security mechanisms must be built to protect these privacy data in health blockchain. Furthermore, because the core of security mechanisms is the key management schemes, the appropriate key management schemes should be designed before blockchains can be used in healthcare system. Here, according to the features of health blockchain, the authors use a body sensor network to design a lightweight backup and efficient recovery scheme for keys of health blockchain. The authors‘ analyses show that the scheme has high security and performance, and it can be used to protect privacy messages on health blockchain effectively and to promote the application of health blockchain.


Reference Type: Conference Paper

Abstract: Blockchain is a technology of recording ledgers in a distributed manner. It uses a consensus mechanism, digital signature and hash chains to realize the reliable storage of ledgers, and provide services such as traceability, integrity and non-repudiation for transactions in ledgers in a decentralized way. These services make blockchain have great application potentiality in the fields of healthcare, FinTech, computational law and so on. Before wide spreading its applications, blockchain must solve problems such as efficiency and privacy. Among these problems the privacy is an important one. Because blocks on blockchain are open, when transactions in blocks involve privacy data, these data can be leaked. Thus, certain security mechanisms must be built to protect privacy data. The core of these mechanisms is the appropriate key management schemes. However, blockchain is a developing technology, and few studies have been done on key management schemes for it. Because healthcare is a big application scenario of blockchain, in this paper, according to the features of health blockchain, we use body sensor network to design a lightweight backup and efficient recovery scheme for keys of health
Analyses show that the scheme has high security and performance, and it can be used to protect privacy messages on health blockchain effectively and to promote the application of health blockchain.


Reference Type: Journal Article

Abstract: The recent bust of the Blockchain bubble was detrimental to many projects intended to return control and ownership of human life data to the hands of individuals. As the industry struggles to recover and rebrand, new applications of digital ledger technologies in traditional healthcare applications have started to emerge.


Reference Type: Journal Article
Available from: https://www.jmir.org/2019/6/e13583/

Abstract: Background: Huge amounts of health-related data are generated every moment with the rapid development of Internet of Things (IoT) and wearable technologies. These big health data contain great value and can bring benefit to all stakeholders in the health care ecosystem. Currently, most of these data are siloed and fragmented in different health care systems or public and private databases. It prevents the fulfillment of intelligent health care inspired by these big data. Security and privacy concerns and the lack of ensured authenticity trails of data bring even more obstacles to health data sharing. With a decentralized and consensus-driven nature, distributed ledger technologies (DLTs) provide reliable solutions such as blockchain, Ethereum, and IOTA Tangle to facilitate the health care data sharing. Objective: This study aimed to develop a health-related data sharing system by integrating IoT and DLT to enable secure, fee-less, tamper-resistant, highly-scalable, and granularly-controllable health data exchange, as well as build a prototype and conduct experiments to verify the feasibility of the proposed solution. Methods: The health-related data are generated by 2 types of IoT devices: wearable devices and stationary air quality sensors. The data sharing mechanism is enabled by IOTA’s distributed ledger, the Tangle, which is a directed acyclic graph. Masked Authenticated Messaging (MAM) is adopted to facilitate data communications among different parties. Merkle Hash Tree is used for data encryption and verification. Results: A prototype system was built according to the proposed solution. It uses a smartwatch and multiple air sensors as the sensing layer; a smartphone and a single-board computer (Raspberry Pi) as the gateway; and a local server for data publishing. The prototype was applied to the remote diagnosis of tremor disease. The results proved that the solution could enable costless data integrity and flexible access management during data sharing. Conclusions: DLT integrated with IoT technologies could greatly improve the health-related data sharing. The proposed solution based on IOTA Tangle and MAM could overcome many challenges faced by other traditional blockchain-based solutions in terms of cost, efficiency, scalability, and flexibility in data access management. This study also showed the possibility of fully decentralized health data sharing by replacing the local server with edge computing devices.


Reference Type: Journal Article
Available from: https://www.prd-journal.com/article/S1353-8020(18)30331-6/fulltext

Abstract: BACKGROUND: Essential tremor (ET), one of the most common neurological disorders is typically evaluated with validated rating scales which only provide a subjective assessment during a clinical visit, underestimating the fluctuations tremor during different daily activities. Motion sensors have shown favorable performances in both quantifying tremor and voluntary human activity recognition (HAR). OBJECTIVE: To create an automated system of a reference scale using motion sensors supported by deep learning algorithms to accurately rate ET severity during voluntary activities, and to propose an IOTA based blockchain application to share anonymously tremor data. METHOD: A smartwatch-based tremor monitoring system was used to collect motion data from 20 subjects while they were doing standard tasks. Two neurologists rated ET by Fahn-Tolosa Marin Tremor Rating Scale (FTMTRS). Supported by deep learning techniques, activity classification models (ACMs) and tremor evaluation models (TEMs) were created and algorithms were implemented, to distinguish voluntary human activities and evaluate tremor severity respectively. RESULT: A practical application example
showed that the proposed ACMs can classify six typical activities with high accuracy (89.73%-98.84%) and the results produced by the TEMs are significantly correlated with the FTMTLS ratings of two neurologists ($r_1=0.92$, $p_1=0.008$; $r_2=0.93$, $p_2=0.007$). CONCLUSION: This study demonstrated that motion sensor data, supported by deep learning algorithms, can be used to classify human activities and evaluate essential tremor severity during different activities.


Reference Type: Journal Article
Available from: https://www.mdpi.com/1424-8220/18/11/3785

Abstract: Blockchain-enabled Internet of Things (IoT) systems have received extensive attention from academia and industry. Most previous constructions face the risk of leaking sensitive information since the servers can obtain plaintext data from the devices. To address this issue, in this paper, we propose a decentralized outsourcing computation (DOC) scheme, where the servers can perform fully homomorphic computations on encrypted data from the data owner according to the request of the data owner. In this process, the servers cannot obtain any plaintext data, and dishonest servers can be detected by the data owner. Then, we apply the DOC scheme in the IoT scenario to achieve a confidential blockchain-enabled IoT system, called BeeKeeper 2.0. To the best of our knowledge, this is the first work in which servers of a blockchain-enabled IoT system can perform any-degree homomorphic multiplications and any number of additions on encrypted data from devices according to the requests of the devices without obtaining any plaintext data of the devices. Finally, we provide a detailed performance evaluation for the BeeKeeper 2.0 system by deploying it on Hyperledger Fabric and using Hyperledger Caliper for performance testing. According to our tests, the time consumed between the request stage and recover stage is no more than 3.3 s, which theoretically satisfies the production needs.


Reference Type: Journal Article

Abstract: Currently, blockchain technology, which is decentralized and may provide tamper-resistance to recorded data, is experiencing exponential growth in industry and research. In this paper, we propose the MIStore, a blockchain-based medical insurance storage system. Due to blockchain’s the property of tamper-resistance, MIStore may provide a high-credibility to users. In a basic instance of the system, there are a hospital, patient, insurance company and n servers. Specifically, the hospital performs a (t, n)-threshold MIStore protocol among the n servers. For the protocol, any node of the blockchain may join the protocol to be a server if the node and the hospital wish. Patient’s spending data is stored by the hospital in the blockchain and is protected by the n servers. Any t servers may help the insurance company to obtain a sum of a part of the patient’s spending data, which servers can perform homomorphic computations on. However, the n servers cannot learn anything from the patient’s spending data, which recorded in the blockchain, forever as long as more than n - t servers are honest. Besides, because most of verifications are performed by record-nodes and all related data is stored at the blockchain, thus the insurance company, servers and the hospital only need small memory and CPU. Finally, we deploy the MIStore on the Ethereum blockchain and give the corresponding performance evaluation.


Reference Type: Journal Article

Abstract: The dissemination of electronic medical data among professional personnel has been perceived to be an important breakthrough for the discovery of new technologies and therapies for curing diseases. However, in the current medical data management, it is difficult to share medical data due to the fragmentation of medical data and the lack of effective sharing methods. On the other hand, the security of medical data is difficult to protect because the centralized data storage is vulnerable to attack and tampering. Therefore, we propose a model called Med-PPPHIS, which consists of a permission-less blockchain and a permissioned blockchain, named Med-DLattice, to serve the management of user’s personal health information and form a chained protection mechanism for medical data. Med-DLattice features Directed Acyclic Graph (DAG) structure, where each account updates its Account-DAG asynchronously to other unrelated accounts. The Med-DLattice nodes can reach an efficient consensus
with proposed DPoS-Quorum algorithm. Based on this model, by converting the medical data into on-chain tokens, a safe and efficient channel for data circulation is established, while the privacy of data is secured. We implement a prototype of Med-PPPHIS and introduce a blockchain-based closed-loop method for chronic disease management, which initially applies the model to national physique monitoring in Anhui Province, China. The performance of the model is evaluated by simulating 500 nodes on 25 AliCloud ECS virtual machines. Experimental result shows that Med-PPPHIS has low latency and high throughput, and the security analysis shows that the model is able to prevent Sybil attacks, DDoS attacks, etc.


Reference Type: Electronic Article

Abstract: With the more and more extensive application of blockchain, blockchain security has been widely concerned by the society and deeply studied by scholars. Moreover, the security of blockchain data directly affects the security of various applications of blockchain. In this survey, we perform a comprehensive classification and summary of the security of blockchain data. First, we present classification of blockchain data attacks. Subsequently, we present the attacks and defenses of blockchain data in terms of privacy, availability, integrity and controllability. Data privacy attacks present data leakage or data obtained by attackers through analysis. Data availability attacks present abnormal or incorrect access to blockchain data. Data integrity attacks present blockchain data being tampered. Data controllability attacks present blockchain data accidentally manipulated by smart contract vulnerability. Finally, we present several important open research directions to identify follow-up studies in this area.


Reference Type: Conference Paper


Abstract: The Internet of Things (IoT) will connect not only computers and mobile devices, but it will also interconnect smart buildings, houses, and cities, as well as electrical grids, gas plants, and water networks, automobiles, airplanes, etc. IoT will lead to the development of a wide range of advanced information services that are pervasive, cost-effective, and can be accessed from anywhere and at any time. However, due to the exponential number of interconnected devices, cyber-security in the IoT is a major challenge. It heavily relies on the digital identity concept to build security mechanisms such as authentication and authorization. Current centralized identity management systems are built around third party identity providers, which raise privacy concerns and present a single point of failure. In addition, IoT unconventional characteristics such as scalability, heterogeneity and mobility require new identity management systems to operate in distributed and trustless environments, and uniquely identify a particular device based on its intrinsic digital properties and its relation to its human owner. In order to deal with these challenges, we present a Blockchain-based Identity Framework for IoT (BIFIT). We show how to apply our BIFIT to IoT smart homes to achieve identity self-management by end users. In the context of smart home, the framework autonomously extracts appliances signatures and creates blockchain-based identifies for their appliance owners. It also correlates appliances signatures (low level...
identities) and owners identifies in order to use them in authentication credentials and to make sure that any IoT entity is behaving normally.


Reference Type: Journal Article
Available from: https://www.jmir.org/2019/7/e13767/

Abstract: BACKGROUND: In recent years, researchers have made significant efforts in advancing blockchain technology. This technology, with distinct features of decentralization and security, can be applied to many fields. In areas of health data and resource sharing, applications of blockchain technology are also emerging. OBJECTIVE: In this study, we propose a cloud health resource-sharing model based on consensus-oriented blockchain technology and have developed a simulation study on breast tumor diagnosis. METHODS: The proposed platform is built on a consortium or federated blockchain that possesses features of both centralization and decentralization. The consensus mechanisms generate operating standards for the proposed model. Open source Ethereum code is employed to provide the blockchain environment. Proof of Authority is selected as the consensus algorithm of block generation. RESULTS: Based on the proposed model, a simulation case study for breast tumor classification is constructed. The simulation includes 9893 service requests from 100 users; 22 service providers are equipped with 22 different classification methods. Each request is fulfilled by a service provider recommended by the weighted k-nearest neighbors (KNN) algorithm. The majority of service requests are handled by 9 providers, and provider service evaluation scores tend to stabilize. Also, user priority on KNN weights significantly affects the system operation outcome. CONCLUSIONS: The proposed model is feasible based on the simulation case study for the cloud service of breast tumor diagnosis and has the potential to be applied to other applications.


Reference Type: Journal Article
Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6371378/

Abstract: "Blockchain" is a distributed ledger technology originally applied in the financial sector. This technology ensures the integrity of transactions without third-party validation. Its functions of decentralized transaction validation, data provenance, data sharing, and data integration are a good fit for the needs of health information exchange and clinical trials. We investigated the current workflow of Health Information Exchange and clinical trials; conducted design thinking processes with clinicians, trial managers, informaticians, and blockchain professionals; and implemented a private blockchain model to tackle known issues. We used coded Smart Contract regulations to simulate several scenarios in healthcare processes. This proof-of-concept work provides a feasible simulation for potential solutions to monitor clinical trials across different census regions persistently. Various levels of data access privileges have been designed to utilize a suite of customized Smart Contract settings. These settings emulate the workflow protocols for the monitoring entities, trial sponsors, clinical sponsors and participating subjects. Keywords: Blockchain, Smart Contract, Health Information Exchange, Clinical Trial, Persistent Monitoring.


Reference Type: Journal Article
Available from: https://www.mdpi.com/2079-9292/8/6/679

Abstract: Recently, there have been increasing calls for healthcare providers to provide controls for patients over their personal health records. Nevertheless, security issues concerning how different healthcare providers exchange healthcare information have caused a flop in the deployment of such systems. The ability to exchange data securely is important so that new borderless integrated healthcare services can be provided to patients. Due to its decentralized nature, blockchain technology is a suitable driver for the much-needed shift towards integrated healthcare, providing new insights and addressing some of the main challenges of many healthcare areas. Blockchain allows healthcare providers to record and manage peer-to-peer transactions through a network without central authority. In this paper, we discuss the concept of blockchain technology and hurdles in their adoption in the healthcare domain. Furthermore, a review is conducted on the latest implementations of blockchain technology in healthcare. Finally, a new case study of a blockchain-based healthcare platform is presented addressing the drawbacks of current designs, followed by recommendations for future blockchain researchers and developers.

Reference Type: Journal Article
Available from: https://www.nature.com/articles/s41587-019-0187-y Subscription required to view.

Abstract: Nebula Genomics announced in June its first partnership with pharma to use its blockchain-based platform. EMD Serono will use Nebula’s network of anonymized genomic data in a lung cancer project. Founded in 2016 by George Church and two Harvard students, Kamal Obbad and Dennis Grishin, Nebula is one of a small cadre of companies that have set up blockchain-based platforms to enable people to maintain control of their genome and manage access to it in a secure, yet transparent, environment. For Serono, a subsidiary of Merck KGaA of Darmstadt, Germany, the collaboration has the potential to provide scientific insights that will help researchers understand the causes of disease and accelerate discovery and drug development.

This healthcare technology is off the blockchain. J AHIMA. 2017;88(1):64. Epub 2017 Jan 1.

Reference Type: Journal Article

Abstract: Predicting the future--particularly when it comes to technology--can be a fool's errand. But it's a pretty safe bet that one innovation those in the health IT world can expect to hear more about is "blockchain." If you've heard of blockchain before, it's likely because it is most frequently associated with Bitcoin, a form of currency used on the internet--and a method of payment favored by ransomware developers. Last summer, the Office of the National Coordinator for Health IT (ONC) announced its Blockchain Challenge, which encouraged competitors to submit white papers detailing the best ways to use blockchain in healthcare--for the good of the industry.