Blockchain Article Citations

Description

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Some *Magazine Articles*, (Company) *Reports*, or *Unpublished Work* were also included in this listing if they contributed unique perspective—even if not peer reviewed.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

Bibliographic references follow the standards summarized in the National Library of Medicine's (NLM) International Committee of Medical Journal Editors (ICMJE) Recommendations for the Conduct, Reporting, Editing, and Publication of Scholarly Work in Medical Journals. Sample references can be found at https://www.nlm.nih.gov/bsd/uniform_requirements.html, and detailed guidance found in the NLM's Citing Medicine, 2nd edition (www.ncbi.nlm.nih.gov/books/NBK7256/.

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.
    - Nature of website location: I provided the web location of the publisher's page so the reader can easily find the citation information and the link to download. When access to the article was limited by subscription, I searched to see if *Open Access* versions were also available on the internet. When more than one access method was available, I provided both methods of access.
    - Website locations found in the citation: Because ICMJE convention allows optional additional permission access notes such as "*Subscription required to view"* to be added to the citation, I provided this information in the citation. When no "Subscription" notes are provided, the reader should assume that the link is "*Open Access*."
    - Website locations provided as a courtesy on a separate line: The nature of access is explicitly stated as "*Subscription required to view*" or "*Open Access*" because more than one type of access may be available.

Contact Information

For questions or corrections, please contact me: Wendy Charles: wendy.charles [@] msn.com.

Citations

Digital footprints in drug development: a perspective from within the FDA. Digit Biomark. 2017;1(2):101-105. Epub 2017 Oct 17.

Reference Type: Journal Article

Available from: https://www.karger.com/Article/FullText/481274 Open access.

Abstract:

[INTRODUCTION ONLY] Dr. Sean Khozin is a thoracic oncologist and Acting Associate Director in the Food and Drug Administration's (FDA) Oncology Center of Excellence. He received his Doctor of Medicine from the University of Maryland School of Medicine and his Master of Public Health from George Washington University. Dr. Khozin is the Founding Director of FDA's Information Exchange and Data Transformation (INFORMED) and a member of the Editorial Board of Digital Biomarkers.

Ahram, T, Sargolzaei, A, Sargolzaei, S, Daniels, J, Amaba, B. Blockchain technology innovations. In: IEEE Technology and Engineering Management Society, editor. 2017 IEEE Technology & Engineering Management Conference (TEMSCON); June 8-10; Santa Clara, CA. Piscataway, NJ: IEEE Technology and Engineering Management Society; 2017. p. 137-141.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/7998367 Subscription required to view.

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.

Alhadhrami, A, Alghfeli, S, Alghfeli, M, Abedlla, JA, Shuaib, K. Introducing blockchains for healthcare. In: Z. Al-Qudah, editor. 2017 International Conference on Electrical and Computing Technologies and Applications (ICECTA); Nov 21-23; Ras Al Khaimah, United Arab Emirates. Piscataway, NJ: IEEE; 2017.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8252043 Subscription required to view.

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 and 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

Available from: https://ieeexplore.ieee.org/abstract/document/8378961 Subscription required to view.

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?

Alonso, SG, Arambarri, J, López-Coronado, M, de la Torre Díez, I. Proposing new blockchain challenges in eHealth. J Med Syst. 2019;43(3):64. Epub 2019 Feb 7.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-019-1195-7 Subscription required to view.

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.

Angeletti, F, Chatzigiannakis, I, Vitaletti, A. Privacy preserving data management in recruiting participants for digital clinical trials. Proceedings of the First International Workshop on Human-centered Sensing, Networking, and Systems; 2017; Delft, Netherlands. New York, NY: ACM.

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 focus 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.

Angeletti, F, Chatzigiannakis, I, Vitaletti, A. The role of blockchain and IoT in recruiting participants for digital clinical trials. In: D. Begusic, International Conference on Software Telecommunications and Computer Networks and IEEE Communications Society, editors. 2017 25th International Conference on Software, Telecommunications and Computer Networks (SoftCOM); Sept 21-23; Split, Croatia. Piscataway, NJ: IEEE Communications Society; 2017.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8115590 Subscription required to view.

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.

Angeletti, F, Chatzigiannakis, I, Vitaletti, A. Towards an architecture to guarantee both data privacy and utility in the first phases of digital clinical trials. Sensors (Basel). 2018;18(12):4175. Epub 2018 Nov 28.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/PMC6308650/ Open access.

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.

Angraal, S, Krumholz, HM, Schulz, WL. Blockchain technology: applications in health care. Circ Cardiovasc Qual Outcomes. 2017;10(9):1-3. Epub 2017 Sep 16.

Reference Type: Journal Article

Available from: https://www.ahajournals.org/doi/full/10.1161/CIRCOUTCOMES.117.003800 Open access.

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.

Arenas, R, Fernandez, P. CredenceLedger: a permissioned blockchain for verifiable academic credentials. 2018 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC); 2018 Jun 17-20; Stuttgart, Germany. Piscataway, NJ: IEEE Technology Engineering and Management Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8436324 Subscription required to view.

Abstract:

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.

Aspnes, J, Jackson, C, Krishnamurthy, A. Exposing computationally-challenged byzantine imposters. 2005 Jul 26. Report No.: TR-1332.

Reference Type: Report

Available from: http://www.collinjackson.com/research/papers/iptps.pdf Open access.

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.

Augot, D, Chabanne, H, Clémot, O, George, W. Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST); Aug 28-30; Calgary, AB, Canada. IEEE; 2017. p. 25-34.

Reference Type: Conference Paper

Available from: https://arxiv.org/abs/1710.02951 Open access;
https://ieeexplore.ieee.org/abstract/document/8476875 Subscription required to view.

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.

Azaria, A, Ekblaw, A, Vieira, T, Lippman, A. MedRec: using blockchain for medical data access and permission management. In: I. Awan, M. Younas and IEEE Computer Society Technical Committee on the Internet, editors. 2016 2nd International Conference on Open and Big Data (OBD); Aug 22-24; Vienna, Austria. Piscataway, NJ: IEEE Computer Society; 2016. p. 25-30.

Reference Type: Conference Paper

Available from: http://dpnm.postech.ac.kr/cs490u/MedRec.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/7573685 Subscription required to view.

Abstract:

Years of heavy regulation and bureaucratic inefficiency have slowed innovation for electronic medical records (EMRs). 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 EMRs, 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 short paper is to expose, prior to field tests, a working prototype through which we analyze and discuss our approach.

Back, A, Corallo, M, Dashjr, L, Friedenbach, M, Maxwell, G, Miller, A, et al. Enabling blockchain innovations with pegged sidechains. Blockstream, 2014 Oct 22. Report No.: 5650e43.

Reference Type: Report

Available from: https://blockstream.com/sidechains.pdf Open access.

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 decentralised 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.

Balakrishnan, YV. Redefining regulatory information management with blockchain. Tata Consultancy Services, 2018 Mar 23. Report No.: M I 03 I 18.

Reference Type: Report

Available from: https://www.tcs.com/content/dam/tcs/pdf/Industries/life-sciences-and-healthcare/solution-brochure/Redefining-RIM.pdf Open access.

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 care givers. 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.

Banga, R, Juneja, M. Clinical trials on blockchain. PhUSE EU Connect; 2018 Nov 4-7; Frankfurt, Germany. Kent, United Kingdom: PhUSE.

Reference Type: Conference Proceedings

Available from: https://www.lexjansen.com/phuse/2018/tt/TT11.pdf Open access.

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.

Bass, J. The truth about blockchain and its application to health care. HFM Magazine. 2019 Feb 1.

Reference Type: Magazine Article

Available from: https://www.hfma.org/Content.aspx?id=63125 Subscription required to view.

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.

Bell, L, Buchanan, WJ, Cameron, J, Lo, O. Applications of blockchain within healthcare. BHTY [Internet]. 2018 May 29; 1(8):[7 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/8

Reference Type: Electronic Article

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.

Bellini, V, Petroni, A, Palumbo, G, Bignami, E. Data quality and blockchain technology. Anaesth Crit Care Pain Med. 2019 (in press). Epub 2019 Jan 8.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S2352556818305368 Subscription required to view.

Abstract:

[FIRST PARAGRAPH] 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.

Benchoufi, M, Porcher, R, Ravaud, P. Blockchain protocols in clinical trials: transparency and traceability of consent. F1000Res. 2017;6:66. Epub 2018 Feb 1.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5676196/ Open access.

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, unfalsifiable 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 unfalsifiable 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.

Benchoufi, M, Ravaud, P. Blockchain technology for improving clinical research quality. Trials. 2017;18:335.

Reference Type: Journal Article

Available from: http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5517794/ Open access.

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.

Bennett, B. Blockchain HIE overview: a framework for healthcare interoperability. TMT. 2017;2(3).

Reference Type: Journal Article

Available from: https://telehealthandmedicinetoday.com/index.php/journal/article/view/14 Open access.

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.

Bennett, B. Using telehealth as a model for blockchain HIT adoption. TMT. 2017;2(4):1-4.

Reference Type: Journal Article

Available from: https://telehealthandmedicinetoday.com/index.php/journal/article/view/25 Open access.

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.

Blackford, WJ. Hashing it out: blockchain as a solution for Medicare improper payments. Belmont L Rev. 2018;5(10):219-252. Epub 2019 Feb 22.

Reference Type: Journal Article

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

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.

Blemus, S. Law and blockchain: a legal perspective on current regulatory trends worldwide. RTDF [Internet]. 2017 Dec 11 [cited 2019 Feb 28]; (4-2017):[15 p.]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080639

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.

Boucher, P, Nascimento, S, Kritikos, M. How blockchain technology could change our lives [Internet]. Brussels, Belgium: European Parliamentary Research Service. 2017 [updated 2017 Feb; cited 2018 Oct 23]. 24 p. Available from: http://www.europarl.europa.eu/RegData/etudes/IDAN/2017/581948/EPRS_IDA(2017)581948_EN.pdf

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, to 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 themselves obsolete, but to enhance their services. There are also some wider issues to consider. For example, blockchain's transparency is fine for matters of public record such as land registries, but what about bank balances and other sensitive data? It is possible (albeit only sometimes and with substantial effort), to identify the individuals associated with transactions. This could compromise their privacy and anonymity. While some blockchains do offer full anonymity, some sensitive information simply should not be distributed in this way. Nevertheless, although blockchains are not the solution for every problem and even if they will not revolutionise every aspect of our lives, they could have a substantial impact in many areas and it is necessary to be prepared for the challenges and opportunities they present.

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.

Brogan, J, Baskaran, I, Ramachandran, N. Authenticating health activity data using distributed ledger technologies. Comput Struct Biotechnol J. 2018;16:257-266. Epub 2018 Jul 17.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S2001037018300345 Open access.

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 distributed ledger 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.

Cai, Y, Zhu, D. Fraud detections for online businesses: a perspective from blockchain technology. Financ Innov. 2016;2(20):1-10. Epub 2016 Dec 6.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1186/s40854-016-0039-4 Open access.

Abstract:

Background: 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.

Casado-Vara, R, Prieto, J, De la Prieta, F, Corchado, JM. How blockchain improves the supply chain: case study alimentary supply chain. In: E. Shakshuki and A. Yasar, editors. 15th International Conference on Mobile Systems and Pervasive Computing (MobiSPC 2018) / The 13th International Conference on Future Networks and Communications (FNC-2018) / Affiliated Workshops; Aug 13-15; Gran Canaria, Spain. Oxford, UK: Elsevier; 2018. p. 393-398.

Reference Type: Conference Paper

Available from: http://www.sciencedirect.com/science/article/pii/S187705091831158X Open access.

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.

Casino, F, Dasaklis, TK, Patsakis, C. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat Inform. 2019;36:55-81.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0736585318306324 Open access.

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.

Chen, L, Lee, WK, Chang, CC, Choo, KWR, Zhang, N. Blockchain based searchable encryption for electronic health record sharing. Future Gener Comp Sy. 2019;95:420-429. Epub 2019 Jan 19.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0167739X18314134 Subscription required to view.

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.

Chen, Y, Ding, S, Xu, Z, Zheng, H, Yang, S. Blockchain-based medical records secure storage and medical service framework. J Med Syst. 2018;43(1):5. Epub 2018 Nov 22.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007%2Fs10916-018-1121-4 Subscription required to view.

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.

Chia, V, Hartel, P, Hum, Q, Ma, S, Piliouras, G, Reijsbergen, D, et al. Rethinking blockchain security: position paper. arXiv [Internet]. 2018 Jun 12 [cited 2019 Feb 1]; 1806.04358:[8 p.]. Available from: https://arxiv.org/abs/1806.04358

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.

Choudhury, O, Sarker, H, Rudolph, N, Foreman, M, Fay, N, Dhuliawala, M, et al. Enforcing human subject regulations using blockchain and smart contracts. BHTY [Internet]. 2018 Mar 23 [cited 2018 Mar 23]; 1(10):[14 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/10

Reference Type: Electronic 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.

Cichosz, SL, Stausholm, MN, Kronborg, T, Vestergaard, P, Hejlesen, O. How to use blockchain for diabetes health care data and access management: an operational concept. J Diabetes Sci Technol. 2019;13(2):248-253. Epub 2018 Jul 26.

Reference Type: Journal Article

Available from: https://journals.sagepub.com/doi/abs/10.1177/1932296818790281 Subscription required to view.

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.

Cisneros, JLB. Public health surveillance using decentralized technologies. BHTY [Internet]. 2018 Mar 23 [cited 2018 Oct 23]; 1(17):[14 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/17

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.

Clauson, KA, Breeden, EA, Davidson, C, Mackey, TK. Leveraging blockchain technology to enhance supply chain management in healthcare. BHTY [Internet]. 2018 Mar 23 [cited 2018 Oct 23]; 1(20):[12 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/20

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.

Coelho, FC. Optimizing disease surveillance by reporting on the blockchain. bioRxiv [Internet]. 2018 Nov 25 [cited 2018 Feb 19]. Available from: https://www.biorxiv.org/content/10.1101/278473v2

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.

Colón, KA. Creating a patient-centered, global, decentralized health system. BHTY [Internet]. 2018 Sep 14 [cited 2018 Nov 2]; 1(30):[18 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/30

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.

Conte de Leon, D, Stalick, AQ, Jillepalli, AA, Haney, MA, Sheldon, FT. Blockchain: properties and misconceptions. APJIE. 2017;11(3):286-300. Epub 2017 Dec 4.

Reference Type: Journal Article

Available from: https://www.emeraldinsight.com/doi/full/10.1108/APJIE-12-2017-034 Open access.

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.

Crosby, M, Nachiappan, Pattanayak, P, Verma, S, Kalyanaraman, V. Blockchain technology: beyond bitcoin. Appl Innov Rev. 2016;2(June):6-10.

Reference Type: Journal Article

Available from: https://j2-capital.com/wp-content/uploads/2017/11/AIR-2016-Blockchain.pdf Open access.

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 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.

Cyran, MA. Blockchain as a foundation for sharing healthcare data. BHTY [Internet]. 2018 Mar 23 [cited 2018 Oct 23]; 1(13):[6 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/13

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.

---

da Conceição, AF, da Silva, FSC, Rocha, V, Locoro, A, Barguil, JM. Electronic health records using blockchain technology. arXiv [Internet]. 2018 Apr 26 [cited 2018 Oct 23]; 1804.10078:[15 p.]. Available from: https://arxiv.org/abs/1804.10078

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.

Dagher, GG, Mohler, J, Milojkovic, M, Marella, PB. Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. SCS. 2018;39:283-297. Epub 2018 Feb 17.

Reference Type: Journal Article

Available from: http://kddlab.zjgsu.edu.cn:7200/research/blockchain/huyiyang-reference/Ancile%20Privacy-preserving%20framework%20for%20access%20control%20and%20interoperability.pdf Open access; http://www.sciencedirect.com/science/article/pii/S2210670717310685 Subscription required to view.

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.

Dai, H, Young, HP, Durant, TJS, Gong, G, Kang, M, Krumholz, HM, et al. TrialChain: a blockchain-based platform to validate data integrity in large, biomedical research studies. arXiv [Internet]. 2018 Jul 10 [cited 2019 Feb 22]; 1807.03662:[7 p.]. Available from: https://arxiv.org/abs/1807.03662

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.

Dasaklis, TK, Casino, F, Patsakis, C. Blockchain meets smart health: towards next generation healthcare services. 2018 9th International Conference on Information, Intelligence, Systems and Applications (IISA); 2018 Jul 23-25; Zankynthos, Greece. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8633601 Subscription required to view.

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.

Dasgupta, D, Shrein, JM, Gupta, KD. A survey of blockchain from security perspective. J Bank Financ Technol. 2019:1-17. Epub 2019 Jan 3.

Reference Type: Journal Article

Available from:
https://www.researchgate.net/profile/Kishor_Datta_Gupta/publication/330125746_A_survey_of_blockchain_from_security_perspective/links/5c341d00a6fdccd6b59af4a5/A-survey-of-blockchain-from-security-perspective.pdf
Open access; https://link.springer.com/article/10.1007/s42786-018-00002-6 Subscription required to view.

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.

De Filippi, P, Hassan, S. Blockchain technology as a regulatory technology: from code is law to law is code. arXiv

[Internet]. 2018 Jan 8 [cited 2018 Oct 23]; 1801.02507:[23 p.]. Available from: https://arxiv.org/abs/1801.02507

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).

Deshpande, A, Stewart, K, Lepetit, L, Gunashekar, S. Distributed ledger technologies/blockchain: challenges, opportunities, and prospects for standards. British Standards Institution, 2017 May. Report No.: 201706.

Reference Type: Report

Available from: https://www.bsigroup.com/LocalFiles/zh-tw/InfoSec-newsletter/No201706/download/BSI_Blockchain_DLT_Web.pdf Open access.

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.

Destefanis, G, Marchesi, M, Ortu, M, Tonelli, R, Bracciali, A, Hierons, R. Smart contracts vulnerabilities: a call for blockchain software engineering? In: R. Tonelli, S. Ducasse, G. Fenu and A. Bracciali, editors. 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE); Mar 20; Campobasso, Italy. IEEE Computer Society; 2018. p. 19-25.

Reference Type: Conference Paper

Available from: https://dspace.stir.ac.uk/bitstream/1893/27135/1/smart-contracts-vulnerabilities-3.pdf Open access; https://ieeexplore.ieee.org/abstract/document/8327567 Subscription required to view.

Abstract:

Smart Contracts have gained tremendous popularity in the past few years, to the point that billions of US Dollars are currently exchanged every day through such technology. However, since the release of the Frontier network of Ethereum in 2015, there have been many cases in which the execution of Smart Contracts managing Ether coins has led to problems or conflicts. Compared to traditional Software Engineering, a discipline of Smart Contract and Blockchain programming, with standardized best practices that can help solve the mentioned problems and conflicts, is not yet sufficiently developed. Furthermore, Smart Contracts rely on a non-standard software life-cycle, according to which, for instance, delivered applications can hardly be updated or bugs resolved by releasing a new version of the software. In this paper we advocate the need for a discipline of Blockchain Software Engineering, addressing the issues posed by smart contract programming and other applications running on blockchains. We analyse a case of study where a bug discovered in a Smart Contract library, and perhaps "unsafe" programming, allowed an attack on Parity, a wallet application, causing the freezing of about 500K Ethers (about 150M USD, in November 2017). In this study we analyze the source code of Parity and the library, and discuss how recognised best practices could mitigate, if adopted and adapted, such detrimental software misbehavior. We also reflect on the specificity of Smart Contract software development, which makes some of the existing approaches insufficient, and call for the definition of a specific Blockchain Software Engineering.

Dhillon, V. Designing decentralized ledger technology for electronic health records. TMT. 2018;1(2):1-13. Epub 2018 May 3.

Reference Type: Journal Article

Available from: https://telehealthandmedicinetoday.com/index.php/journal/article/view/77 Open access.

Abstract:

A proposal to implement distributed ledger technology for electronic health records is outlined here. The rationale for integration of distributed ledgers in the healthcare domain is introduced, followed by a discussion of the features enabled by the use of a blockchain. An open source implementation of a distributed ledger is then presented. The article concludes with an examination of opportunities and challenges ahead in deploying blockchains for digital health.

Dimitrov, DV. Blockchain applications for healthcare data management. Healthc Inform Res. 2019;25(1):51-56. Epub 2019 Jan 31.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6372466/ Open access.

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.

Disparte, D. Blockchain could make the insurance industry much more transparent. Harvard Bus Rev [Internet]. 2017 Jul 12 [cited 2017 Jul 27]:[about 7 p.]. Available from: https://hbr.org/2017/07/blockchain-could-make-the-insurance-industry-much-more-transparent

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.

Dorri, A, Kanhere, SS, Jurdak, R. Blockchain in internet of things: challenges and solutions. arXiv [Internet]. 2016 Aug 18 [cited 2018 Oct 23]; 1608.05187:[13 p.]. Available from: https://arxiv.org/abs/1608.05187

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.

Drosatos, G, Kaldoudi, E. Blockchain applications in the biomedical domain: a scoping review. Comput Struct Biotechnol J. 2019;17:229-240. Epub 2019 Feb 8.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S200103701830285X Open access.

Abstract:

Blockchain is a distributed, immutable ledger technology introduced as the enabling mechanism to support cryptocurrencies. Blockchain solutions are currently being proposed to address diverse 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.

Du, Y, Liu, J, Guan, Z, Feng, H. A medical information service platform based on distributed cloud and blockchain. 2018 3rd IEEE International Conference on Smart Cloud (SmartCloud); 2018 Sep 21-23; New York, NY. Los Alamitos, CA: IEEE Computer Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8513712 Subscription required to view.

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.

Dubovitskaya, A, Xu, Z, Ryu, S, Schumacher, M, Wang, F. Secure and trustable electronic medical records sharing using blockchain. In: AMIA Annu Symp Proc; Nov 4-8; Washington, DC. American Medical Informatics Association; 2017. p. 650-659.

Reference Type: Conference Paper

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5977675/ Open access.

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.

Dunphy, P, Garratt, L, Petitcolas, F. Decentralizing digital identity: open challenges for distributed ledgers. In: F. Piessens and S. Fahl, editors. 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW); Apr 23-27; London, United Kingdom. Piscataway, NJ: IEEE; 2018. p. 75-78.

Reference Type: Conference Paper

Available from: https://www.dunph.com/SB2018.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8406563 Subscription required to view.

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.

Dunphy, P, Petitcolas, FAP. A first look at identity management schemes on the blockchain. IEEE Security Privacy. 2018;16(4):20-29. Epub 2018 Aug 6.

Reference Type: Journal Article

Available from: https://arxiv.org/abs/1801.03294 Open access;
https://ieeexplore.ieee.org/abstract/document/8425607/ Subscription required to view.

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.

Dwivedi, DA, Srivastava, G, Dhar, S, Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors (Basel). 2019;19(2):326. Epub 2019 Jan 15.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/2/326 Open access.

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.

Efanov, D, Roschin, P. The all-pervasiveness of the blockchain technology. In: A. V. Samsonovich and V. V. Klimov, editors. 8th Annual International Conference on Biologically Inspired Cognitive Architectures; Aug 1-6; Moscow, Russia. Procedia Computer Science; 2018. p. 116-121.

Reference Type: Conference Paper

Available from: http://www.sciencedirect.com/science/article/pii/S1877050918300206 Open access.

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.

Ekblaw, A, Azaria, A, Halamka, JD, Lippman, A. A case study for blockchain in healthcare: “MedRec” prototype for electronic health records and medical research data. OBD 2016 2nd International Conference on Open and Big Data; 2016 Aug 22-24; Vienna, Austria. Future Generation Computer Systems, Elsevier.

Reference Type: Conference Proceedings

Available from: https://pdfs.semanticscholar.org/56e6/5b469cad2f3ebd560b3a10e7346780f4ab0a.pdf Open access.

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.

Ekİn, A, Ünay, D. [Blockchain applications in healthcare] Sağlıkta Blok Zinciri Uygulamaları. 2018 26th Signal Processing and Communications Applications Conference (SIU); 2018 May 2-5; Izmir, Turkey. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8404275 Subscription required to view.

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.

Engelhardt, MA. Hitching healthcare to the chain: an introduction to blockchain technology in the healthcare sector. Technol Innov Manag Rev. 2017;7(10):22-34.

Reference Type: Journal Article

Available from: https://timreview.ca/article/1111 Open access.

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.

Esposito, C, De Santis, A, Tortora, G, Chang, H, Choo, KR. Blockchain: a panacea for healthcare cloud-based data security and privacy? IEEE Trans Cloud Comput. 2018;5(1):31-37. Epub 2018 Mar 28.

Reference Type: Journal Article

Available from: https://pdfs.semanticscholar.org/7f8f/4ff1377ebf0a084c44dbf6926af03dd2cdd8.pdf Free; https://ieeexplore.ieee.org/abstract/document/8327543/ Subscription required to view.

Abstract:

One particular trend observed in healthcare is the progressive shift of data and services to the cloud, partly due to convenience (e.g. availability of complete patient medical history in real-time) and savings (e.g. economics of healthcare data management). There are, however, limitations to using conventional cryptographic primitives and access control models to address security and privacy concerns in an increasingly cloud-based environment. In this paper, we study the potential to use the Blockchain technology to protect healthcare data hosted within the cloud. We also describe the practical challenges of such a proposition and further research that is required.

Fabiano, N. Internet of things and blockchain: legal issues and privacy. The challenge for a privacy standard. In: Y. Wu, G. Min, N. Georgalas and 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. 727-734.

Reference Type: Conference Paper

Available from: https://fardapaper.ir/mohavaha/uploads/2018/08/Fardapaper-Internet-of-Things-and-Blockchain-legal-issues-and-privacy.-The-challenge-for-a-privacy-standard.pdf Open access; https://ieeexplore.ieee.org/abstract/document/8276831 Subscription required to view.

Abstract:

The IoT is innovative and important phenomenon prone to several services and applications, but it should consider the legal issues related to the 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, adopting 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 use 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, a- cording 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.

Fan, K, Wang, S, Ren, Y, Li, H, Yang, Y. MedBlock: efficient and secure medical data sharing via blockchain. J Med

Syst. 2018;42(8):136. Epub 2018 Jun 21.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0993-7 Subscription required to view.

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.

Fawcett, JP. Bitcoin regulations and investigations: a proposal for U.S. policies [Master's Thesis]: Utica College; 2016.

Reference Type: Thesis

Available from: https://infoskirmish.com/wp-content/uploads/2017/11/BITCOIN-REGULATIONS-AND-INVESTIGATIONS.pdf Open access.

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, FinCENs 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).

Fedorov, AK, Kiktenko, EO, Lvovsky, AI. Quantum computers put blockchain security at risk. Nature. 2018;563(7732):465. Epub 2018 Nov 19.

Reference Type: Journal Article

Available from: https://www.nature.com/articles/d41586-018-07449-z/ Open access.

Abstract:

[FIRST FEW PARAGRAPHS] By 2025, up to 10% of global gross domestic product is likely to be stored on blockchains1. A blockchain is a digital tool that uses cryptography techniques to protect information from unauthorized changes. It lies at the root of the Bitcoin cryptocurrency2. 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.

Feng, Q, He, D, Zeadally, S, Khan, MK, Kumar, N. A survey on privacy protection in blockchain system. J Netw Comput Appl. 2019;126:45-58. Epub 2018 Nov 13.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S1084804518303485 Subscription required to view.

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.

Fernández-Caramés, TM, Fraga-Lamas, P. A review on the use of blockchain for the internet of things. IEEE Access. 2018;6:32979-33001. Epub 2018 May 31.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8370027 Open access.

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.

Firdaus, A, Anuar, NB, Razak, MFA, Hashem, IAT, Bachok, S, Sangaiah, AK. Root exploit detection and features optimization: mobile device and blockchain based medical data management. J Med Syst. 2018;42(6):112. Epub 2018 May 4.

Reference Type: Journal Article

Available from: https://umexpert.um.edu.my/file/publication/00006193_161638_73389.pdf Open access; https://link.springer.com/article/10.1007/s10916-018-0966-x Subscription required to view.

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).

Florea, BC. Blockchain and internet of things data provider for smart applications. In: R. Stojanović, L. Jóźwiak, D. Jurišić and B. Lutovac, editors. 2018 7th Mediterranean Conference on Embedded Computing (MECO); Jun 10-14; Budva, Montenegro. Piscataway, NJ: IEEE; 2018.

Reference Type: Conference Paper

Available from: https://fardapaper.ir/mohavaha/uploads/2018/08/Fardapaper-Blockchain-and-Internet-of-Things-Data-Provider-for-Smart-Applications.pdf Open access; https://ieeexplore.ieee.org/abstract/document/8406041 Subscription required to view.

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 3rd 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.

Friebe, S, Sobik, I, Zitterbart, M. DecentID: decentralized and privacy-preserving identity storage system using smart contracts. In: IEEE Computer Society, editor. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications ; the 12th IEEE International Conference on Big Data Science and Engineering; Jul 31-Aug 3; New York, NY. Los Alamitos, CA: IEEE Computer Society; 2018. p. 37-42.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8455884 Subscription required to view.

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.

Funk, E, Riddell, J, Ankel, F, Cabrera, D. Blockchain technology: a data framework to improve validity, trust, and accountability of information exchange in health professions education. Acad Med. 2018;93(12):1791-1794. Epub 2018 Dec 1.

Reference Type: Journal Article

Available from:
https://journals.lww.com/academicmedicine/Fulltext/2018/12000/Blockchain_Technology___A_Data_Framework_to.21.aspx Subscription required to view.

Abstract:
Health professions educators face multiple challenges, among them the need to adapt educational methods to new technologies. In the last decades, multiple new digital platforms have appeared in the learning arena, including massive open online courses and social-media-based education. The major critique of these novel methods is the lack of the ability to ascertain the origin, validity, and accountability of the knowledge that is created, shared, and acquired. Recently, a novel technology based on secured data storage and transmission, called blockchain, has emerged as a way to generate networks where validity, trust, and accountability can be created. Conceptually, blockchain is 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 health care 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.

Furlanello, C, De Domenico, M, Jurman, G, Bussola, N. Towards a scientific blockchain framework for reproducible data analysis. arXiv [Internet]. 2017 Jul 20 [cited 2018 Nov 2]; 1707.06552:[8 p.]. Available from: https://arxiv.org/abs/1707.06552

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–including 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.

Gagnon, ML, Stephen, G. A pragmatic solution to a major interoperability problem: using blockchain for the nationwide patient index. BHTY [Internet]. 2018 Aug 16 [cited 2019 Mar 12]; 1(18):[9 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/28

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 Open access.

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 technology. 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.

Gatteschi, V, Lamberti, F, Demartini, C, Pranteda, C, Santamaría, 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

Available from: https://ieeexplore.ieee.org/abstract/document/8338007 Subscription required to view.

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.

Giancaspro, M. Is a ‘smart contract’ really a smart idea? Insights from a legal perspective. CLSR. 2017;33(6):825-

835. Epub 2017 Jun 5.

Reference Type: Journal Article

Available from:
https://www.researchgate.net/profile/Mark_Giancaspro/publication/317354410_Is_a_%27smart_contract%27_really_a_smart_idea_Insights_from_a_legal_perspective/links/5c2d5891a6fdccfc707902d8/Is-a-smart-contract-really-a-smart-idea-Insights-from-a-legal-perspective.pdf Open access;
http://www.sciencedirect.com/science/article/pii/S026736491730167X Subscription required to view.

Abstract:
Swift developments in the emerging field of blockchain technology have facilitated the birth of 'smart contracts': computerised transaction protocols which autonomously execute the terms of a contract. Smart contracts are disintermediated and generally transparent in nature, offering the promise of increased commercial efficiency, lower transaction and legal costs, and anonymous transacting. The business world is actively investigating the use of blockchain technology for various commercial purposes. Whilst questions surround the security and reliability of this technology, and the negative impact it may have upon traditional intermediaries, there are equally significant concerns that smart contracts will encounter considerable difficulty adapting to current legal frameworks regulating contracts across jurisdictions. This article considers the potential issues with legal and practical enforceability that arise from the use of smart contracts within both civil and common law jurisdictions.

Glover, DG, Hermans, J. Improving the traceability of the clinical trial supply chain. Appl Clin Trials. 2017;26(12):36-38. Epub 2017 Dec 1.

Reference Type: Journal Article

Available from: http://www.appliedclinicaltrialsonline.com/print/347703?page=full Open access.

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 view that data. The data is auditable, immutable, and can help create a longitudinal record of a patient's health status.

Gordon, WJ, Catalini, C. Blockchain technology for healthcare: facilitating the transition to patient-driven interoperability. Comput Struct Biotechnol J. 2018;16:224-230. Epub 2018 Aug 03.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S200103701830028X Open access.

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 patient-driven 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.

Griggs, KN, Ossipova, O, Kohlios, CP, Baccarini, AN, Howson, EA, Hayajneh, T. Healthcare blockchain system using smart contracts for secure automated remote patient monitoring. J Med Syst. 2018;42(7):130. Epub 2018 Jun 6.

Reference Type: Journal Article

Available from:
https://www.researchgate.net/profile/Alessandro_Baccarini/publication/325605811_Healthcare_Blockchain_System_Using_Smart_Contracts_for_Secure_Automated_Remote_Patient_Monitoring/links/5b22803baca272277fab615b/Healthcare-Blockchain-System-Using-Smart-Contracts-for-Secure-Automated-Remote-Patient-Monitoring.pdf Open access; https://link.springer.com/article/10.1007/s10916-018-0982-x Subscription required to view.

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.

Grishin, D, Obbad, K, Estep, P, Quinn, K, Wait Zaranek, S, Wait Zeranek, A, et al. Accelerating genomic data generation and facilitating genomic data access using decentralization, privacy-preserving technologies and equitable compensation. BHTY [Internet]. 2018 Dec 17 [cited 2019 Mar 12]; 1(34):[23 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/34

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, sharing genomic data with researchers promises identification of the causes of many diseases and the development of new therapies. However, 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.

Gu, J, Sun, B, Du, X, Wang, J, Zhuang, Y, Wang, Z. Consortium blockchain-based malware detection in mobile devices. IEEE Access. 2018;6:12118-12128. Epub 2018 Feb 13.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8290934 Open access.

Abstract:
To address the problem of detecting malicious codes in malware and extracting the 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.

Guo, R, Shi, R, Zhao, Q, Zheng, D. Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems. IEEE Access. 2018;6:11676-11686. Epub 2018 Feb 2.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8279429/ Open access.

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.

Gupta, M. Blockchain for dummies [Internet]. Hoboken, NJ: John Wiley & Sons, Inc. 2018 [updated 2018 Aug 3; cited 2018 Nov 2]. 44 p. Available from: https://www.ibm.com/downloads/cas/36KBMBOG

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.

Halamka, JD. Separating signal from noise: advice for blockchain startups. BHTY [Internet]. 2018 Jun 4 [cited 2019 Feb 17]; 1(29):[2 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/29

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!”

Halamka, JD, Alterovitz, G, Buchanan, WJ, Cenaj, T, Clauson, KA, Dhillon, V, et al. Top 10 blockchain predictions for the (near) future of healthcare. BHTY [Internet]. 2019 Feb 7 [cited 2019 Mar 12]; 2(106):[9 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/106

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.

Halamka, JD, Lippman, A, Ekblaw, A. The potential for blockchain to transform electronic health records. Harvard Bus Rev [Internet]. 2017 Mar 3 [cited 2018 May 22]:[about 6 p.]. Available from: https://hbr.org/2017/03/the-potential-for-blockchain-to-transform-electronic-health-records

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.

Hashemi, SH, Faghri, F, Campbell, RH. Decentralized user-centric access control using pubsub over blockchain. arXiv [Internet]. 2017 Sep 29 [cited 2018 Oct 23]; 00110:[15 p.]. Available from: https://arxiv.org/abs/1710.00110 Free

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.

Herian, R. Regulating disruption: blockchain, GDPR, and questions of data sovereignty. J Int Law. 2018;22(2):1-16. Epub 2018 Dec 7.

Reference Type: Journal Article

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

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 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.

Herian, R. Taking blockchain seriously. Law Critique. 2018;29(2):163-171. Epub 2018 May 12.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10978-018-9226-y Open access.

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.

Heston, T. A case study in blockchain healthcare innovation. Int J Curr Res. 2017;9(11):60587-60588. Epub 2017 Nov 30.

Reference Type: Journal Article

Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3077455 Open access.

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.

Hoy, MB. An introduction to the blockchain and its implications for libraries and medicine. Med Ref Serv Q. 2017;36(3):273-279. Epub 2017 Jul 17.

Reference Type: Journal Article

Available from: https://www.tandfonline.com/doi/abs/10.1080/02763869.2017.1332261 Subscription required to view.

Abstract:
The blockchain is a relatively new technology used to verify and store transaction records for online cryptocurrencies like Bitcoin. The system is redundant and distributed, making it difficult for transactions to be rescinded, duplicated, or faked. Beyond online currencies, the blockchain has potential uses in health care, education, and many other fields. This column will briefly describe what the blockchain is and how it is being used, potential future uses that may be of interest to librarians and medical practitioners, and some of the problems with the system.

Hussein, AF, ArunKumar, N, Ramirez-Gonzalez, G, Abdulhay, E, Tavares, JMRS, de Albuquerque, VHC. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. Cogn Syst Res. 2018;52:1-11. Epub 2018 May 30.

Reference Type: Journal Article

Available from: https://web.fe.up.pt/~tavares/downloads/publications/artigos/COGSYS_2018_105.pdf 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 0.19 s, 0.17 s and 20 respectively that based on system evaluation illustrates that our system is robust, efficient, immune and scalable.

Iansiti, M, Lakhani, KR. The truth about blockchain. Harvard Bus Rev. 2017 Jan-Feb:118-127.

Reference Type: Magazine Article

Available from: https://hbr.org/2017/01/the-truth-about-blockchain Open access.

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.

Ichikawa, D, Kashiyama, M, Ueno, T. Tamper-resistant mobile health using blockchain technology. JMIR Mhealth

Uhealth. 2017;5(7):e111. Epub 2017 Jul 28.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5550736/ Open access.

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 with tamper 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.

Ienca, M, Ferretti, A, Hurst, S, Puhan, M, Lovis, C, Vayena, E. Considerations for ethics review of big data health research: a scoping review. PLoS ONE. 2018;13(10):e0204937. Epub 2018 Oct 11.

Reference Type: Journal Article

Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0204937 Open access.

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.

Jackson, NM. Transcripts transformed: incorporating blockchain to verify academic credentials. Univ Bus. 2018 Nov:27-30.

Reference Type: Magazine Article

Available from: https://universitybusiness.com/college-transcripts-transformed Open access.

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.

Jakovljevic, PJ. Demystifying blockchain: the technology and its providers. Longueuil, QC, Canada: Technology Evaluation Centers, Inc., 2018 Jan 2. Report No.: BLO20180102.

Reference Type: Report

Available from: https://www3.technologyevaluation.com/research/tec-report/demystifying-blockchain-the-technology-and-its-providers.html Open access.

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.

Ji, Y, Zhang, J, Ma, J, Yang, C, Yao, X. BMPLS: blockchain-based multi-level privacy-preserving location sharing scheme for telecare medical information systems. J Med Syst. 2018;42(8):147. Epub 2018 Jun 30.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0998-2 Subscription required to view.

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.

Jia, B, Zhou, T, Li, W, Liu, Z, Zhang, J. A blockchain-based location privacy protection incentive mechanism in crowd sensing networks. Sensors (Basel). 2018;18(11):3894. Epub 2018 Nov 12.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/11/3894 Open access.

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.

Jiang, P, Guo, F, Liang, K, Lai, J, Wen, Q. Searchain: blockchain-based private keyword search in decentralized storage. Future Gener Comp Sy. 2017;http://dx.doi.org/10.1016/j.future.2017.08.036. Epub 2017 Sep 12.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S0167739X17318630 Subscription required to view.

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.

Jiang, S, Cao, J, Wu, H, Yang, Y, Ma, M, He, J. BlocHIE: a BLOCkchain-based platform for healthcare information exchange. In: IEEE Computer Society, editor. 2018 IEEE International Conference on Smart Computing (SMARTCOMP); Jun 18-20; Taormina, Italy. Piscataway, NJ: IEEE Computer Society; 2018. p. 49-56.

Reference Type: Conference Paper

Available from:
https://www.researchgate.net/profile/Shan_Jiang70/publication/324728250_BlockHIE_a_BLOCkchain-based_platform_for_Healthcare_Information_Exchange/links/5adf463ba6fdcc29358e0fde/BlockHIE-a-BLOCkchain-based-platform-for-Healthcare-Information-Exchange.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8421331 Subscription required to view.

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.

Jo, BW, Khan, MR, Lee, Y-S. Hybrid blockchain and internet-of-things network for underground structure health monitoring. Sensors (Basel). 2018;18(12):4268. Epub 2018 Dec 4.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/12/4268 Open access.

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.

Joshi, KP, Banerjee, A. Automating privacy compliance using policy integrated blockchain. Cryptogr. 2019;3(7):1-21. Epub 2019 Feb 5.

Reference Type: Journal Article

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

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.

Juneja, A, Marefat, M. Leveraging blockchain for retraining deep learning architecture in patient-specific arrhythmia classification. In: D. I. Fotiadis, J. Penders, M. D. Wang, O. Amft and IEEE Engineering in Medicine and Biology Society, editors. 2018 IEEE EMBS International Conference on Biomedical & Health Informatics (BHI); Mar 4-7; Las Vegas, NV. Piscataway, NJ: IEEE Engineering in Medicine and Biology Society; 2018. p. 393-397.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8333451 Subscription required to view.

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.

Kafka, AC. Will blockchain revolutionize scholarly journal publishing? Chron High Educ. 2018 Nov 30:A22-A23.

Reference Type: Magazine Article

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

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.

Kakavand, H, Kost De Sevres, N, Chilton, B. The blockchain revolution: an analysis of regulation and technology related to distributed ledger technologies. SSRN. 2017;https://dx.doi.org/10.2139/ssrn.2849251. Epub 2017 Jan 5.

Reference Type: Journal Article

Available from:
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2849251_code2599390.pdf?abstractid=2849251&mirid=1
Open access.

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.

Käll, J. Blockchain control. Law Critique. 2018;29(2):133-140. Epub 2018 May 30.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10978-018-9227-x Open access.

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.

Kamau, G, Boore, C, Maina, E, Njenga, S. Blockchain technology: is this the solution to EMR interoperability and security issues in developing countries? In: P. Cunningham and M. Cunningham, editors. 2018 IST-Africa Week Conference (IST-Africa); May 9-11; Gaborone, Botswana. Piscataway, NJ: IEEE; 2018. p. 1-8.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8417357 Subscription required to view.

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.

Kamel Boulos, MN, Wilson, JT, Clauson, KA. Geospatial blockchain: promises, challenges, and scenarios in health and healthcare. Int J Health Geogr. 2018;17(1):25. Epub 2018 Jul 5.

Reference Type: Journal Article

Available from: https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-018-0144-x Open access.

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-word healthcare solutions involving AI-mediated data exchange on blockchains.

Karame, G, Capkun, S. Blockchain security and privacy. IEEE Security Privacy. 2018;16(4):11-12. Epub 2018 Aug 6.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8425621 Open access.

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.

Kaur, H, Alam, MA, Jameel, R, Mourya, AK, Chang, V. A proposed solution and future direction for blockchain-based heterogeneous Medicare data in cloud environment. J Med Syst. 2018;42(8):156. Epub 2018 Jul 10.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-1007-5 Subscription required to view.

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.

Kilbride, N. Custody, control, and assurances: improving legal operations with blockchain. Bus Law Today [Internet]. 2018 2018 Dec 18 [cited 2019 Feb 11]:[about 3 p.]. Available from: https://businesslawtoday.org/2018/12/custody-control-assurances-improving-legal-operations-blockchain/

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.

Kim, MG, Lee, AR, Kwon, HJ, Kim, JW, Kim, IK. Sharing medical questionnaires based on blockchain. 2018 IEEE International Conference on Bioinformatics and Biomedicine (BIBM); 2018 Dec 3-6; Madrid, Spain. Piscataway, NJ: IEEE Computer Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8621154 Subscription required to view.

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 in 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.

Kim, R. Cryptocurrency and blockchain: the technological and regulatory frontier of FinTech. Bloomberg Law, Bureau of National Affairs Inc.; 2018 2018 Aug 15. Report No.: MKT-13253.

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.

Kirkner, RM. Why blockchain for health care may be finally turning the corner. Manag Care. 2018;27(12):22-23. Epub

2018 Nov 25.

Reference Type: Journal Article

Available from: https://www.managedcaremag.com/linkout/2018/12/22 Open access.

Abstract:

> [FIRST PARAGRAPH] 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.

Klaimi, J, Rahim-Amoud, R, Merghem-Boulahia, L, Jrad, A. A novel loss-based energy management approach for smart grids using multi-agent systems and intelligent storage systems. SCS. 2018;39:344-357. Epub 2018 Mar 7.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S2210670717307552 Subscription required to view.

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.

Kleinaki, AS, Mytis-Gkometh, P, Drosatos, G, Efraimidis, PS, Kaldoudi, E. A blockchain-based notarization service for biomedical knowledge retrieval. Comput Struct Biotechnol J. 2018;16:288-297. Epub 2018 Aug 17.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S2001037018300400 Open access.

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.

Koshechkin, KA, Klimenko, GS, Ryabkov, IV, Kozhin, PB. Scope for the application of blockchain in the public healthcare of the Russian Federation. In: International Conference on Knowledge Based and Intelligent Information and Engineering Systems, KES 2018; Sep 3-5; Belgrade, Serbia. Procedia Comput Sci; 2018. p. 1323-1328.

Reference Type: Conference Paper

Available from: http://www.sciencedirect.com/science/article/pii/S1877050918313607 Open access.

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.

Kostal, K, Helebrandt, P, Bellus, M, Ries, M, Kotuliak, I. Management and monitoring of IoT devices using blockchain (dagger). Sensors (Basel). 2019;19(4). Epub 2019 Feb 19.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/19/4/856 Open access.

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 this history is available for administrators. Our results show that such a system is possible and dissemination of configuration changes to IoT devices can be secured by the blockchain. The key novelty of our solution is a distributed management of configuration files of IoT devices in enterprise networks utilizing blockchain technology. This is essentially improving security and storage options for configurations in the blockchain.

Kotsiuba, I, Velvkzhanin, A, Yanovich, Y, Bandurova, IS, Dyachenko, Y, Zhygulin, V. Decentralized e-Health architecture for boosting healthcare analytics. In: X. S. Yang, N. Dey and N. Joshi, editors. 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4); Oct 30-31; London, United Kingdom. IEEE; 2018. p. 113-118.

Reference Type: Conference Paper

Available from: https://bitfury.com/content/downloads/research-decentralized-e-health-architecture.pdf Open access; https://ieeexplore.ieee.org/abstract/document/8611621Subscription required to view.

Abstract:

In this paper, we present an overview of the problems associated with the analysis and security of medical data and offer a solution that will provide the basis for improving the quality of medical services. We propose the architecture of a decentralized health data ecosystem based on a blockchain that will allow us to operate with vast volumes of clinical data, while also protecting confidential medical data. An example of a blockchain solution based on Exonum framework for state-scale use in healthcare is discussed. The deployments of such systems will the benefit to medical data safety, extend the base of clinical data collections, and create an effective shared health infrastructure.

Kravitz, DW, Cooper, J. Securing user identity and transactions symbiotically: IoT meets blockchain. 2017 Global Internet of Things Summit (GIoTS); 2017 Jun 6-9; Geneva, Switzerland. Piscataway, NJ: IEEE Computational Intelligence Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8016280 Subscription required to view.

Abstract:
Swarms of embedded devices provide new challenges for privacy and security. We propose Permissioned Blockchains as an effective way to secure and manage these systems of systems. A long view of blockchain technology yields several requirements absent in extant blockchain implementations. Our approach to Permissioned Blockchains meets the fundamental requirements for longevity, agility, and incremental adoption. Distributed Identity Management is an inherent feature of our Permissioned Blockchain and provides for resilient user and device identity and attribute management.

Krishnamurty, S. Blockchain for business. Wilmott. 2018 2018 Jul 19:18-19.

Reference Type: Magazine Article

Available from: https://onlinelibrary.wiley.com/doi/abs/10.1002/wilm.10686 Subscription required to view.

Abstract:
"So, how do we buy some of these Blockchains for our portfolio?"

Kshetri, N. Blockchain's roles in strengthening cybersecurity and protecting privacy. Telecomm Policy. 2017;41(10):1027-1038. Epub 2017 Sep 22.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0308596117302483 Subscription required to view.

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-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.

Kshetri, N. Can blockchain strengthen the internet of things? IT Prof. 2017;19(4):68-72. Epub 2017 Aug 17.

Reference Type: Journal Article

Available from: https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Can_2017.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8012302 Subscription required to view.

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.

Kumar, NM, Mallick, PK. Blockchain technology for security issues and challenges in IoT. Procedia Comput Sci. 2018;132:1815-1823. Epub 2018 Jun 8.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S187705091830872X Open access.

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 there by 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.

Kuo, TT, Kim, HE, Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. J Am Med Inform Assoc. 2017;24(6):1211-1220. Epub 2017 Sep 8.

Reference Type: Journal Article

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

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 crypto-currency 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.

Lamport, L, Shostak, R, Pease, MI. The Byzantine generals problem. TOPLAS. 1982;4(3):382-401.

Reference Type: Journal Article

Available from: http://people.cs.uchicago.edu/~shanlu/teaching/33100_wi15/papers/byz.pdf Open access.

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.

Le Nguyen, T, D. F. Kocaoglu, T. R. Anderson, D. C. Kozanoglu et al., editors. Blockchain in healthcare: a new technology benefit for both patients and doctors. 2018 Portland International Conference on Management of Engineering and Technology (PICMET); 2018 Aug 19-23; Honolulu, HI. Portland, OR: IEEE Technology and Engineering Management Society; 2018.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8481969 Subscription required to view.

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.

Li, H, Zhu, L, Shen, M, Gao, F, Tao, X, Liu, S. Blockchain-based data preservation system for medical data. J Med Syst. 2018;42(8):141. Epub 2018 Jun 28.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0997-3 Subscription required to view.

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.

Li, J, Wu, J, Chen, L. Block-secure: blockchain based scheme for secure P2P cloud storage. Inf Sci (Ny). 2018;465:219-231. Epub 2018 Jul 9.

Reference Type: Journal Article

Available from: http://iranarze.ir/wp-content/uploads/2018/10/E9969-IranArze.pdf Open access;
http://www.sciencedirect.com/science/article/pii/S0020025518305012 Subscription required to view.

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.

Li, P, Nelson, SD, Malin, BA, Chen, Y. DMMS: a decentralized blockchain ledger for the management of medication histories. BHTY [Internet]. 2019 Jan 4 [cited 2019 Mar 12]; 2(38):[15 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/38

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.

Li, X, Jiang, P, Chen, T, Luo, X, Wen, Q. A survey on the security of blockchain systems. arXiv [Internet]. 2018 Mar 6 [cited 2019 Feb 1]; 1802.06993:[25 p.]. Available from: https://arxiv.org/abs/1802.06993

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.

Liang, X, Zhao, J, Shetty, S, Liu, J, Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC); 2017 Oct 8-13; Montreal, QC, Canada. Piscataway, NJ: IEEE eXpress Conference Publishing; 2017.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/document/8292361 Subscription required to view.
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.

Lin, IC, Liao, TC. A survey of blockchain security issues and challenges. IJ Network Security. 2017;19(5):653-659. Epub 2017 Sep 1.

Reference Type: Journal Article

Available from: http://ijns.jalaxy.com.tw/download_paper.jsp?PaperID=IJNS-2017-03-25-1&PaperName=ijns-v19-n5/ijns-2017-v19-n5-p653-659.pdf Open access.

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.

Lin, Q, Yan, H, Huang, Z, Chen, W, Shen, J, Tang, Y. An ID-based linearly homomorphic signature scheme and its application in blockchain. IEEE Access. 2018;6:20632-20640. Epub 2018 Feb 2018.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8302552 Open access.

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.

Lindman, J, Tuunainen, VK, Rossi, M. Opportunities and risks of blockchain technologies–a research agenda. In: Proceedings of the 50th Hawaii International Conference on System Sciences; Jan 4-7; Waikoloa, HI. Honolulu, HI: University of Hawaii at Manoa; 2017. p. 1533-1542.

Reference Type: Conference Paper

Available from: https://aisel.aisnet.org/hicss-50/da/open_digital_services/3/ Open access;
https://scholarspace.manoa.hawaii.edu/handle/10125/41338 Open access.

Abstract:

Blockchain technologies offer new open sourcebased opportunities for developing new types of digital platforms and services. While research on the topic is emerging, it has this far been predominantly focused to 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 question 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

Available from: https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf Open access.

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.

Liu, L, Xu, B. Research on information security technology based on blockchain. In: 2018 IEEE 3rd International Conference on Cloud Computing and Big Data Analysis (ICCCBDA); Apr 20-22; Chengdu, China. Piscataway, NJ: IEEE; 2018. p. 380-384.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8386546 Subscription required to view.

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.

Liu, W, Zhu, SS, Mundie, T, Krieger, U. Advanced block-chain architecture for e-health systems. In: 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom); Oct 12-15; Dalian, China. Piscataway, NJ: IEEE; 2017. p. 37-42.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/document/8210847 Subscription required to view.

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.

Liu, Y, Zhao, Z, Guo, G, Wang, X, Tan, Z, Wang, S. An identity management system based on blockchain. In: 2017 15th Annual Conference on Privacy, Security and Trust (PST); Aug 28-30; Calgary, AB, Canada. Los Alamitos, CA: IEEE Computer Society; 2017. p. 44-53.

Reference Type: Conference Paper

Available from: https://www.ucalgary.ca/pst2017/files/pst2017/paper-8.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8476877 Subscription required to view.

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.

Lone, AH, Mir, RN. Forensic-chain: blockchain based digital forensics chain of custody with PoC in Hyperledger Composer. Digit Invest. 2019;28:44-55. Epub 2019 Jan 10.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S174228761830344X Open access.

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.

Ma, C, Kong, X, Lan, Q, Zhou, Z. The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance. Cybersecurity. 2019;2(1):5. Epub 2019 Jan 30.

Reference Type: Journal Article

Available from: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0022-2 Open access.

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.

Magyar, G. Blockchain: solving the privacy and research availability tradeoff for EHR data: a new disruptive technology in health data management. In: 2017 IEEE 30th Jubilee Neumann Colloquium (NC); 2017 Nov 24-25; Budapest, Hungary. Piscataway, NJ: IEEE; 2017. p. 135-140.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/document/8263269 Subscription required to view.

Abstract:

A blockchain powered Health information ecosystem can solve a frequently discussed problem of the lifelong recorded patient health data, which seriously could hurdle the privacy of the patients and 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 full-featured EHR system.

Mamoshina, P, Ojomoko, L, Yanovich, Y, Ostrovski, A, Botezatu, A, Prikhodko, P, et al. Converging blockchain and next-generation artificial intelligence technologies to decentralize and accelerate biomedical research and healthcare. Oncotarget. 2018;9(5):5665-5690. Epub 2017 Nov 9.

Reference Type: Journal Article

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

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.

Mannaro, K, Baralla, G, Pinna, A, Ibba, S. A blockchain approach applied to a teledermatology platform in the Sardinian Region (Italy). Info CG. 2018;9(2):44. Epub 2018 Feb 23.

Reference Type: Journal Article

Available from: https://www.mdpi.com/2078-2489/9/2/44 Open access.

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.

Manski, S, Manski, B. No Gods, no masters, no coders? The future of sovereignty in a blockchain world. Law Critique. 2018;29(2):151-162. Epub 2018 May 17.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10978-018-9225-z Subscription required to view.

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. 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.

Marceglia, S, Fontelo, P, Rossi, E, Ackerman, MJ. A standards-based architecture proposal for integrating patient mHealth apps to electronic health record systems. Appl Clin Inform. 2015;6(3):488-505. Epub 2015 Aug 5.

Reference Type: Journal Article

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

Abstract:

BACKGROUND: Mobile health Applications (mHealth Apps) are opening the way to patients' responsible and active involvement with their own healthcare management. However, apart from Apps allowing patient's access to their electronic health records (EHRs), mHealth Apps are currently developed as dedicated "island systems". OBJECTIVE: Although much work has been done on patient's access to EHRs, transfer of information from mHealth Apps to EHR systems is still low. This study proposes a standards-based architecture that can be adopted by mHealth Apps to exchange information with EHRs to support better quality of care. METHODS: Following the definition of requirements for the EHR/mHealth App information exchange recently proposed, and after reviewing current standards, we designed the architecture for EHR/mHealth App integration. Then, as a case study, we modeled a system based on the proposed architecture aimed to support home monitoring for congestive heart failure patients. We simulated such process using, on the EHR side, OpenMRS, an open source longitudinal EHR and, on the mHealth App side, the iOS platform. RESULTS: The integration architecture was based on the bi-directional exchange of standard documents (clinical document architecture rel2 - CDA2). In the process, the clinician "prescribes" the home monitoring procedures by creating a CDA2 prescription in the EHR that is sent, encrypted and de-identified, to the mHealth App to create the monitoring calendar. At the scheduled time, the App alerts the patient to start the monitoring. After the measurements are done, the App generates a structured CDA2-compliant monitoring report and sends it to the EHR, thus avoiding local storage. CONCLUSIONS: The proposed architecture, even if validated only in a simulation environment, represents a step forward in the integration of personal mHealth Apps into the larger health-IT ecosystem, allowing the bi-directional data exchange between patients and healthcare professionals, supporting the patient's engagement in self-management and self-care.

Maslove, DM, Klein, J, Brohman, K, Martin, P. Using blockchain technology to manage clinical trials data: a proof-of-concept study. JMIR Med Inform. 2018;6(4):e11949. Epub 2018 Dec 21.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/PMC6320404/ Open access.

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.

Mears, J. The rise and rise of ID as a Service. Biometric Technology Today. 2018 February 15:5-8.

Reference Type: Magazine Article

Available from: http://www.sciencedirect.com/science/article/pii/S0969476518300237 Subscription required to view.

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.

Meinert, E, Alturkistani, A, Foley, KA, Osama, T, Car, J, Majeed, A, et al. Blockchain implementation in health care: protocol for a systematic review. JMIR Res Protoc. 2019;8(2):e10994. Epub 2018 May 8.

Reference Type: Journal Article

Available from: http://www.researchprotocols.org/2019/2/e10994/ Open access.

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.

Mendes, D, Rodrigues, I, Fonseca, C, Lopes, M, García-Alonso, JM, Berrocal, J. Anonymized distributed PHR using blockchain for openness and non-repudiation guarantee. In: E. Méndez, F. Crestani, C. Ribeiro, G. David and J. C. Lopes, editors. International Conference on Theory and Practice of Digital Libraries; Sep 10-13; Porto, Portugal. Cham, Switzerland: Springer International Publishing; 2018. p. 381-385.

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.

Mendes, D, Rodrigues, IP, Fonseca, C, Lopes, MJ, Garcia-Alonso, JM, Berrocal, J. Anonymized distributed PHR using blockchain for openness and non-repudiation guarantee. Stud Health Technol Inform. 2018;255:170-174. Epub 2018 Sep 5.

Reference Type: Journal Article

Available from: http://ebooks.iospress.nl/publication/50496 Open access.

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.

Mertz, L. (Block) chain reaction: a blockchain revolution sweeps into health care, offering the possibility for a much-needed data solution. IEEE Pulse. 2018;9(3):4-7. Epub 2018 May 11.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8358054 Subscription required to view.

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.

Mertz, L. Hospital CIO explains blockchain potential: an interview with Beth Israel Deaconess Medical Center's John Halamka. IEEE Pulse. 2018;9(3):8-9. Epub 2018 May 11.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8358056 Subscription required to view.

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

Available from: https://ieeexplore.ieee.org/abstract/document/7749510 Subscription required to view.

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.

Mikula, T, Jacobsen, RH. Identity and access management with blockchain in electronic healthcare records. In: M. Novotný, N. Konofaos, A. Skavhaug and IEEE Computer Society, editors. 2018 21st Euromicro Conference on Digital System Design (DSD); Aug 29-31; Prague, Czech Republic. Los Alamitos, CA: IEEE Computer Society; 2018. p. 699-706.

Reference Type: Conference Paper

Available from:

https://www.researchgate.net/profile/Rune_Jacobsen2/publication/328313216_Identity_and_Access_Management_with_Blockchain_in_Electronic_Healthcare_Records/links/5be00e76a6fdcc3a8dbedfcf/Identity-and-Access-Management-with-Blockchain-in-Electronic-Healthcare-Records.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8491888 Subscription required to view.

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.

Min, H. Blockchain technology for enhancing supply chain resilience. Bus Horiz. 2019;62(1):35-45. Epub 2018 Oct 25.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0007681318301472 Subscription required to view.

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.

Mougayar, W. The business blockchain: promise, practice, and application of the next internet technology [Internet]. New York, NY: John Wiley & Sons, Incorporated. 2016 [updated 2016 Apr 26; cited 2019 Mar 14]. 141 p. Available

from: https://www.wiley.com/en-us/The+Business+Blockchain%3A+Promise%2C+Practice%2C+and+Application+of+the+Next+Internet+Technology-p-9781119300311 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 way by the force of its progression. 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.

Mudliar, K, Parekh, H, Bhavathankar, P, Sardar Patel Institute of Technology and IEEE, editors. A comprehensive integration of national identity with blockchain technology. 2018 International Conference on Communication information and Computing Technology (ICCICT); 2018 Feb 2-3; Mumbai, India. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8325891 Subscription required to view.

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.

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

Available from: https://www.centerwatch.com/cwweekly/2018/05/29/blockchain-is-coming-ready-or-not-expert-warns-clinical-research-site-executives/ Open access.

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.”

Nasrulin, B, Muzammal, M, Qu, Q. ChainMOB: mobility analytics on blockchain. In: 2018 19th IEEE International Conference on Mobile Data Management (MDM); Jun 25-28; Aalborg, Denmark. Piscataway, NJ: IEEE Computer Society; 2018. p. 292-293.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/document/8411296 Subscription required to view.

Abstract:

Mobile devices generate massive amounts of data that is used to get an insight into the user behavior by enterprise systems. Data privacy is a concern in such systems as users have little control over the data that is generated by them. Blockchain systems offer ways to ensure privacy and security of the user data with the implementation of an access control mechanism. In this demonstration, we present ChainMOB, a mobility analytics application that is built on top of blockchain and addresses the fundamental privacy and security concerns in enterprise systems. Further, the extent of data sharing along with the intended audience is also controlled by the user. Another exciting feature is that user is part of the business model and is incentivized for sharing the personal mobility data. The system also supports queries that can be used in a variety of application domains.

Nguyen, B. Exploring applications of blockchain in securing electronic medical records. J Health Care L Pol. 2017;20(1):99-115.

Reference Type: Journal Article

Available from: https://digitalcommons.law.umaryland.edu/jhclp/vol20/iss1/5/ Open access.

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.

Nikolić, I, Kolluri, A, Sergey, I, Saxena, P, Hobor, A. Finding the greedy, prodigal, and suicidal contracts at scale. Proceedings of the 34th Annual Computer Security Applications Conference; 2018; San Juan, PR, USA. 3274743: ACM.

Reference Type: Conference Proceedings

Available from: https://arxiv.org/pdf/1802.06038.pdf Open access; https://dl.acm.org/citation.cfm?id=3274743 Subscription required to view.

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.

Nugent, T, Upton, D, Cimpoesu, M. Improving data transparency in clinical trials using blockchain smart contracts. F1000Res. 2016;5:2541. Epub 2016 Oct 20.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5357027/ Open access.

Abstract:

The scientific credibility of findings from clinical trials can be undermined by a range of problems including missing data, endpoint switching, data dredging, and selective publication. Together, these issues have contributed to systematically distorted perceptions regarding the benefits and risks of treatments. While these issues have been well documented and widely discussed within the profession, legislative intervention has seen limited success. Recently, a method was described for using a blockchain to prove the existence of documents describing pre-specified endpoints in clinical trials. Here, we extend the idea by using smart contracts - code, and data, that resides at a specific address in a blockchain, and whose execution is cryptographically validated by the network - to demonstrate how trust in clinical trials can be enforced and data manipulation eliminated. We show that blockchain smart contracts provide a novel technological solution to the data manipulation problem, by acting as trusted administrators and providing an immutable record of trial history.

Ogiela, MR, Majcher, M. Security of distributed ledger solutions based on blockchain technologies. In: L. Barolli, Fukuoka Institute of Technology Japan and IEEE Technical Committee on Distributed Processing, editors. 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA); May 16-18; Krakow, Poland. Los Alamitos, CA: IEEE Computer Society; 2018. p. 1089-1095.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8432358 Subscription required to view.

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.

Orel, A, Bernik, I. GDPR and health personal data; tricks and traps of compliance. In: J. Mantas, Z. Sonicki, M. Crişan-Vida et al., editors. Special Topic Conference of the European Federation for Medical Informatics (EFMI STC); 2018 Oct 15-16; Zagreb, Croatia. Amsterdam, the Netherlands: IOS Press BV; 2018. p. 155-159.

Reference Type: Conference Paper

Available from: http://ebooks.iospress.nl/publication/50493 Open access.

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.

Orman, H. Blockchain: the emperors new PKI? IEEE Internet Comput. 2018;22(2):23-28. Epub 2018 Apr 24.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8345567 Subscription required to view.

Abstract:

I would like to jump on the blockchain bandwagon. I would like to be able to say that blockchain is the solution to the longstanding problem of secure identity on the Internet. I would like to say that everyone in the world will soon have a digital identity. Put yourself on the blockchain and never again ask yourself, Who am I? - you are your blockchain address.

Othman, A, Callahan, J, IEEE Computational Intelligence Society and International Neural Networks Society, editors. The Horcrux Protocol: a method for decentralized biometric-based self-sovereign identity. 2018 International Joint Conference on Neural Networks (IJCNN); 2018 Jul 8-13; Rio de Janeiro, Brazil. Piscataway, NJ: IEEE Computational Intelligence Society.

Reference Type: Conference Proceedings

Available from: https://arxiv.org/abs/1711.07127 Open access;
https://ieeexplore.ieee.org/abstract/document/8489316 Subscription required to view.

Abstract:

Most user authentication methods and identity proving systems rely on a centralized database. Such information storage presents a single point of compromise from a security perspective. If this system is compromised it poses a direct threat to users digital identities. This paper proposes a decentralized authentication method, called the Horcrux protocol, in which there is no such single point of compromise. The protocol relies on decentralized identifiers (DIDs) under development by the W3C Verifiable Claims Community Group and the concept of self-sovereign identity. To accomplish this, we propose specification and implementation of a decentralized biometric credential storage option via blockchains using DIDs and DID documents within the IEEE 2410–2017 Biometric Open Protocol Standard (BOPS).1The term “horcrux” comes from the Harry Potter book series in which the antagonist (Lord Voldemort) places copies of his soul into physical objects. Each object is scattered and/or hidden to disparate places around the world. He cannot be killed until all horcruxes are found and destroyed.

Ozercan, HI, Ileri, AM, Ayday, E, Alkan, C. Realizing the potential of blockchain technologies in genomics. Genome Res. 2018;28(9):1255-1263. Epub 2018 Aug 3.

Reference Type: Journal Article

Available from: https://genome.cshlp.org/content/28/9/1255.long Open access.

Abstract:

Genomics data introduce a substantial computational burden as well as data privacy and ownership issues. Data sets generated by high-throughput sequencing platforms require immense amounts of computational resources to align to reference genomes and to call and annotate genomic variants. This problem is even more pronounced if reanalysis is needed for new versions of reference genomes, which may impose high loads to existing computational infrastructures. Additionally, after the compute-intensive analyses are completed, the results are either kept in centralized repositories with access control, or distributed among

stakeholders using standard file transfer protocols. This imposes two main problems: (1) Centralized servers become gatekeepers of the data, essentially acting as an unnecessary mediator between the actual data owners and data users; and (2) servers may create single points of failure both in terms of service availability and data privacy. Therefore, there is a need for secure and decentralized platforms for data distribution with user-level data governance. A new 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.

Park, HJ, Park, HJ. Blockchain security in cloud computing: use cases, challenges, and solutions. Symmetry (Basel). 2017;9(8):164. Epub 2017 Aug 18.

Reference Type: Journal Article

Available from: https://www.mdpi.com/2073-8994/9/8/164 Open access.

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.

Park, YR, Lee, E, Na, W, Park, S, Lee, Y, Lee, JH. Is blockchain technology suitable for managing personal health records? Mixed-methods study to test feasibility. J Med Internet Res. 2019;21(2):e12533. Epub 2019 Feb 8.

Reference Type: Journal Article

Available from: https://www.jmir.org/2019/2/e12533/ Open access.

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 visit data less than 1 year old), B (84 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 (128.7 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 1494.2 seconds, 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.

Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus.

Health Inform J. 2018;doi: 10.1177/1460458218769699. Epub 2018 Apr 25.

Reference Type: Journal Article

Available from: https://journals.sagepub.com/doi/abs/10.1177/1460458218769699 Subscription required to view.

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.

Pauwels, E, Grevatt, N. The social benefits of blockchain for health data: securing patient privacy & control. Washington, DC: Woodrow Wilson International Center for Scholars, 2017 Dec 5.

Reference Type: Report

Available from: https://www.wilsoncenter.org/publication/the-social-benefits-blockchain-for-health-data-securing-patient-privacy-and-control Open access.

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 Spectrum. 2017;54(10):38-60. Epub 2017 Sep 28.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8048838 Subscription required to view.

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.

Peters, AW, Till, BM, Meara, JG, Afshar, S. Blockchain technology in health care: a primer for surgeons. Bull Am Coll Surg. 2017;12:1-5. Epub 2017 Dec 6.

Reference Type: Journal Article

Available from: http://bulletin.facs.org/2017/12/blockchain-technology-in-health-care-a-primer-for-surgeons/ Open access.

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.1 More than 130 million secure Bitcoin transactions have occurred since the digital currency launched in 2009.2 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 technoology 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).

Pilkington, M. Blockchain technology: principles and applications. In: F. X. Olleros and M. Zhegu, editors. Research handbook on digital transformations [Internet]. Northampton, MA: Edward Elgar. 2015 Sep 18. cited 2019 Feb 27]. [39]. Available from: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2662660

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.

Pirtle, C, Ehrenfeld, J. Blockchain for healthcare: the next generation of medical records? J Med Syst. 2018;42(9):172. Epub 2018 Aug 10.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-1025-3 Open access.

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.

Popielarski, M. Blockchain research: bitcoins, cryptocurrency, and distributed ledgers. Colo Lawyer. 2018 June:10-14.

Reference Type: Magazine Article

Available from: https://www.cobar.org/Portals/COBAR/TCL/June%202018/CL_June_Departments_LRC.pdf Open access.

Abstract:
The rapid development and implementation of blockchain technology throughout the global 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.

Pouwelse, J, de Kok, A, Fleuren, J, Hoogendoorn, P, Vliegendhart, R, de Vos, M. Laws for creating trust in the blockchain age. Eur J Intl L. 2017;6(3):321-356. Epub 2017 Dec 7.

Reference Type: Journal Article

Available from: http://pure.tudelft.nl/ws/files/41225519/article.pdf Open access;
https://www.degruyter.com/view/j/eplj.2017.6.issue-3/eplj-2017-0022/eplj-2017-0022.xml Subscription required to view.

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 devises trust, new acts, principles and rules beyond the possibilities in current economic, legal and political systems.

Price, E. Regulatory divergence could hamper blockchain. Int Fin Law Rev. 2016;35(41):1. Epub 2016 Sep 1.

Reference Type: Journal Article

Available from: https://search.proquest.com/openview/bc1594ace75fc74f55660832a0e3e1c0/1 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.

Priisalu, J, Ottis, R. Personal control of privacy and data: Estonian experience. Health Technol (Berl). 2017;7(4):441-451. Epub 2017 Jun 15.

Reference Type: Journal Article

Available from: https://www.ncbi.nlm.nih.gov/pmc/PMC5741780/ Open access.

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 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.

Puthal, D, Malik, N, Mohanty, SP, Kougianos, E, Das, G. Everything you wanted to know About the blockchain: its promise, components, processes, and problems. IEEE Trans Consum Electron. 2018;7(4):6-14. Epub 2018 Jun 15.

Reference Type: Journal Article

Available from:

https://www.researchgate.net/profile/Saraju_Mohanty/publication/326102908_Everything_You_Wanted_to_Know_About_the_Blockchain_Its_Promise_Components_Processes_and_Problems/links/5b394ed74585150d23ee03a7/Everything-You-Wanted-to-Know-About-the-Blockchain-Its-Promise-Components-Processes-and-Problems.pdf Open access; https://ieeexplore.ieee.org/abstract/document/8386948 Subscription required to view.

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.

Queiroz, MM, Telles, R, Bonilla, SH. Blockchain and supply chain management integration: a systematic review of the literature. Supply Chain Manag [Internet]. 2018 Dec 6 [cited 2019 Mar 12]:[14 p.]. Available from: https://www.emeraldinsight.com/doi/abs/10.1108/SCM-03-2018-0143 Subscription required to view.

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.

Rabah, K. Challenges and opportunities for blockchain powered healthcare systems: a review. MR Res J Med Health Sci. 2017;1(1):45-52. Epub 2017 Oct 16.

Reference Type: Journal Article

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

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.

Radanović, I, Likić, R. Opportunities for use of blockchain technology in medicine. Appl Health Econ Health Policy. 2018;16(5):583-590. Epub 2018 Jul 18.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s40258-018-0412-8 Subscription required to view.

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.

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. BHTY [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.

Rahman, MA, Hossain, MS, Hassanain, E, Rashid, M, Barnes, S. Spatial blockchain-based secure mass screening framework for children with dyslexia. IEEE Access. 2018;2875242:1-11. Epub 2018 Oct 10.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8488459 Open access.

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.

Randall, D, Goel, P, Abujamra, R. Blockchain applications and use cases in health information technology. J Health Med Informat [Internet]. 2017 [cited 2019 Feb 22]; 8(276):[4 p.]. Available from: http://arapi.org/?news=blockchain-applications-and-use-cases-in-health-information-technology

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 health care 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.

Ribitzky, R, St. Clair, J, Houlding, DI, McFarlane, CT, Ahier, B, Gould, M, et al. Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: paving the future for healthcare. BHTY [Internet]. 2018 Mar 23 [cited 2018 Jul 18]; 1(24):[15 p.]. Available from: https://blockchainhealthcaretoday.com/index.php/journal/article/view/24

Reference Type: Electronic Article

Abstract:

Background: Blockchain and distributed ledger technology is a disruptive force in healthcare.
Methods: 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.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8167555 Subscription required to view.

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.

Rivera, R, Robledo, JG, Larios, VM, Avalos, JM. How digital identity on blockchain can contribute in a smart city environment. 2017 International Smart Cities Conference (ISC2); 2017 Sep 14-17; Wuxi, China. Piscataway, NJ: IEEE Power & Energy Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8090839 Subscription required to view.

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 characteristics like health status, hobbies and others. That is why Digital Identity has taken a significantly important role in this area and becoming as a crucial security measure in this interconnected environment. This research is a

systematic mapping review with the goal of collecting all relevant existing research of Digital Identity on Blockchain technology implemented in a smart city environment. The objective of this paper is to understand the current research topics, challenges and future directions of these areas from the technical point of view. It is expected that this paper can stimulate interest in theory and practice to further discussions and research in these areas.

Roehrs, A, da Costa, CA, da Rosa Righi, R. OmniPHR: a distributed architecture model to integrate personal health records. J Biomed Inform. 2017;71:70-81. Epub 2017 May 22.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S1532046417301089 Open access.

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.

Roman-Belmonte, JM, De la Corte-Rodriguez, H, Rodriguez-Merchan, EC. How blockchain technology can change medicine. Postgrad Med. 2018;130(4):420-427. Epub 2018 May 10.

Reference Type: Journal Article

Available from: https://www.tandfonline.com/doi/abs/10.1080/00325481.2018.1472996 Subscription required to view.

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.

Ryan, P. Smart contract relations in e-commerce: Legal implications of exchanges conducted on the blockchain. Technol Innov Manag Rev. 2017;7(10):10-17. Epub 2017 Oct 27.

Reference Type: Journal Article

Available from: https://opus.lib.uts.edu.au/handle/10453/127958 Open access.

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. Internal Auditor. 2018 Dec:17-18.

Reference Type: Magazine Article

Available from: https://iaonline.theiia.org/2018/Pages/Internal-Audit-and-the-Blockchain.aspx Subscription required to view.

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.

Salahuddin, MA, Al-Fuqaha, A, Guizani, M, Shuaib, K, Sallabi, F. Softwarization of internet of things infrastructure for secure and smart healthcare. Computer. 2017;50(7):74-79. Epub 2018 May 28.

Reference Type: Journal Article

Available from: https://arxiv.org/abs/1805.11011 Open access;
https://ieeexplore.ieee.org/abstract/document/7971867 Subscription required to view.

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.

Saleem, JJ, Savoy, A, Etherton, G, Herout, J. Investigating the need for clinicians to use tablet computers with a newly envisioned electronic health record. Int J Med Inform. 2018;110:25-30. Epub 2017 Nov 23.

Reference Type: Journal Article

Available from: https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1119&context=veterans Open access;
https://www.sciencedirect.com/science/article/pii/S1386505617304276 Subscription required to view.

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.

Saraf, C, Sabadra, S. Blockchain platforms: a compendium. 2018 IEEE International Conference on Innovative Research and Development (ICIRD); 2018 May 11-12; Bangkok, Thailand. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/document/8376323 Subscription required to view.

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, Ethereum, Corda to make a choice of the platform easily according to the requirement.

Saravanan, M, Shubha, R, Marks, AM, Iyer, V. SMEAD: a secured mobile enabled assisting device for diabetics monitoring. 2017 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS); 2017 Dec 17-20; Bhubaneswar, India. Piscataway, NJ: IEEE Communications Society.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8384099 Subscription required to view.

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.

Sato, T, Himura, Y. Smart-contract based system operations for permissioned blockchain. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS); 2018 Feb 26-28; Paris, France. Red Hook, NY: Curran Associates, Inc.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/document/8328745 Subscription required to view.

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.

Savelyev, A. Copyright in the blockchain era: Promises and challenges. CLSR. 2017;34(3):550-561. Epub 2017 Dec 8.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0267364917303783 Subscription required to view.

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.

Schanzenbach, M, Bramm, G, Schütte, J. ReclaimID: secure, self-sovereign identities using name systems and attribute-based encryption. arXiv [Internet]. 2018 May 16 [cited 2019 Feb 17]; 1805.06253:[12 p.]. Available from: https://arxiv.org/abs/1805.06253

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.

Scheuer, E. Health information traceability foundation: a blockchain-based online marketplace for personal health data. HIT Foundation Zug, 2017 Dec 3.

Reference Type: Report

Available from: https://hit.foundation/wp-content/uploads/hit_foundation_tge_terms.pdf Open access.

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.

Scriber, BA. A framework for determining blockchain applicability. IEEE Softw. 2018;35(4):70-77. Epub 2018 Jul 6.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8405623 Subscription required to view.

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.

Shabani, M. Blockchain-based platforms for genomic data sharing: a de-centralized approach in response to the governance problems? J Am Med Inform Assoc. 2019;26(1):76-80. Epub 2018 Nov 28.

Reference Type: Journal Article

Available from: https://academic.oup.com/jamia/article-abstract/26/1/76/5211361 Subscription required to view.

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.

Shae, Z, Tsai, J. Transform blockchain into distributed parallel computing architecture for precision medicine. In: IEEE Computer Society, editor. 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS); Jul 2-6; Vienna, Austria. Piscataway, NJ: IEEE Computer Society; 2018. p. 1290-1299.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8416392 Subscription required to view.

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.

Shae, Z, Tsai, JJP. On the design of a blockchain platform for clinical trial and precision medicine. In: A. Musaev, J. E. Ferreira, T. Higashino and IEEE Computer Society, editors. 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS); Jun 5-8; Atlanta, GA. Piscataway, NJ: IEEE Computer Society; 2017. p. 1972-1980.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/7980138 Subscription required to view.

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.

Shbair, WM, Steichen, M, François, J, State, R. Blockchain orchestration and experimentation framework: a case study of KYC. NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium; 2018 Apr 23-27; Taipei, Taiwan. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: http://publications.uni.lu/bitstream/10993/35467/1/blockchain-orchestration-experimentation.pdf Open access; https://ieeexplore.ieee.org/document/8406327 Subscription required to view.

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.

Shubbar, S. Ultrasound medical imaging systems using telemedicine and blockchain for remote monitoring of responses to neoadjuvant chemotherapy in women's breast cancer: concept and implementation [Master's Thesis]: Kent State University; 2017.

Reference Type: Thesis

Available from: https://etd.ohiolink.edu/!etd.send_file?accession=kent1493646959335823&disposition=attachment Open access.

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.

Siyal, AA, Junejo, ZA, Zawish, M, Ahmed, K, Khalil, A, Soursou, G. Applications of blockchain technology in medicine and healthcare: challenges and future perspectives. Cryptogr. 2019;3(1):1-16. Epub 2019 Jan 2.

Reference Type: Journal Article

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

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.

Skiba, DJ. The potential of blockchain in education and health care. Nurs Educ Perspect. 2017;38(4):220-221. Epub 2017 Jun 18.

Reference Type: Journal Article

Available from:
https://journals.lww.com/neponline/Citation/2017/07000/The_Potential_of_Blockchain_in_Education_and.17.aspx
Subscription required to view.

Abstract:

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.

Stawicki, S, Firstenberg, M, Papadimos, T. What's new in academic medicine? Blockchain technology in health-care: bigger, better, fairer, faster, and leaner. Int J Acad Med. 2018;4(1):1-11. Epub 2018 Apr 23.

Reference Type: Journal Article

Available from: http://www.ijam-web.org/text.asp?2018/4/1/1/230844 Open access.

Abstract:

Computers and other electronic devices permeate our lives. The world as we know it would not be possible without the increasingly pervasive incorporation of technological advances into essentially every single facet of our daily routines. Although steady and relentless progress in this area can be traced back to the 1950's, accelerated growth began in the late 1990s and early 2000s with the so-called “internet revolution.” As a result, previously unforeseen increases in productivity, automation, and standards of living became possible. Beyond obvious economic effects of this tremendous paradigm shift, the incorporation of technological advances into various aspects of our daily lives led to the transformation of our social fabric and the way we see (and interact with) the world.

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.

Sulkowski, AJ. Blockchain, business supply chains, sustainability, and law: the future of governance, legal frameworks, and lawyers? DJCL [Internet]. 2018 Oct 7 [cited 2019 Feb 27]; 43(Forthcoming):[25 p.]. Available from: https://ssrn.com/abstract=3262291

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.

Sullivan, C, Burger, E. E-residency and blockchain. CLSR. 2017;33(4):470-481. Epub 2017 May 3.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0267364917300845 Subscription required to view.

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.

Sun, Y, Zhang, R, Wang, X, Gao, K, Liu, L. A decentralizing attribute-based signature for healthcare blockchain. 2018 27th International Conference on Computer Communication and Networks (ICCCN); 2018 Jul 30-Aug 2; Hangzhou, China. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8487349 Subscription required to view.

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.

Sylim, P, Liu, F, Marcelo, A, Fontelo, P. Blockchain technology for detecting falsified and substandard drugs in distribution: pharmaceutical supply chain intervention. JMIR Res Protoc. 2018;7(9):e10163. Epub 2018 Sep 15.

Reference Type: Journal Article

Available from: https://www.researchprotocols.org/2018/9/e10163/ Open access.

Abstract:

BACKGROUND: Drug counterfeiting is a global problem with significant risks to consumers and the general public. In the Philippines, 30% of inspected drug stores in 2003 were found with substandard/spurious/falsely-labeled/falsified/counterfeit drugs. The economic burden on the population drug expenditures and on governments is high. The Philippine Food and Drug Administration (FDA) encourages the public to check the certificates of product registration and report any instances of counterfeiting. The National Police of Philippines responds to such reports through a special task force. However, no literature on its impact on the distribution of such drugs were found. Blockchain technology is a cryptographic ledger that is allegedly immutable through repeated sequential hashing and fault-tolerant through a consensus algorithm. This project will develop and test a pharmacosurveillance blockchain system that will support information sharing along the official drug distribution network. OBJECTIVE: This study aims to develop a pharmacosurveillance blockchain system and test its functions in a simulated network. METHODS: We are developing a Distributed Application (DApp) that will run on smart contracts, employing Swarm as the Distributed File System (DFS). Two instances will 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.

Takemiya, M, Vanieiev, B. Sora identity: secure, digital identity on the blockchain. In: S. Reisman and IEEE Computer Society, editors. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC); Jul 23-27; Tokyo, Japan. Piscataway, NJ: IEEE Computer Society; 2018. p. 582-587.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8377927 Subscription required to view.

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.

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. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://hoticn.com/files/hoticnPapers/043-paper%20113.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8605956 Subscription required to view.

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.

Theodouli, A, Arakliotis, S, Moschou, K, Votis, K, Tzovaras, D. On the design of a blockchain-based system to facilitate healthcare data sharing. In: IEEE Computer Society, editor. 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications ; the 12th IEEE International Conference on Big Data Science and Engineering; Jul 31-Aug 3; New York, NY. Los Alamitos, CA: IEEE Computer Society; 2018. p. 1374-1379.

Reference Type: Conference Paper

Available from: https://konfido-project.eu/system/files/private/konfido/on_the_design_of_a_blockchain-based_system_to_facilitate_healthcare_data_sharing.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8456059/ Subscription required to view.

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.

Till, BM, Peters, AW, Afshar, S, Meara, JG. From blockchain technology to global health equity: can cryptocurrencies finance universal health coverage? BMJ Glob Health. 2017;2(4):e000570. Epub 2017 Dec 1.

Reference Type: Journal Article

Available from: https://gh.bmj.com/content/2/4/e000570.abstract Open access.

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.

Tosh, DK, Shetty, S, Liang, X, Kamhoua, C, Njilla, L. Consensus protocols for blockchain-based data provenance: challenges and opportunities. In: S. Chakrabarti, editor. 2017 IEEE 8th Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON); Oct 19-21; New York, NY. Piscataway, NJ: IEEE; 2017. p. 469-474.

Reference Type: Conference Paper

Available from:
https://www.researchgate.net/profile/Sachin_Shetty11/publication/323203891_Consensus_protocols_for_blockchain-based_data_provenance_Challenges_and_opportunities/links/5b4e54f6a6fdcc8dae27a46e/Consensus-protocols-for-blockchain-based-data-provenance-Challenges-and-opportunities.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8249088 Subscription required to view.

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.

Treiblmaier, H. The impact of the blockchain on the supply chain: a theory-based research framework and a call for action. Supply Chain Manage. 2018;23(6):545-559. Epub Aug 7.

Reference Type: Journal Article

Available from: https://www.emeraldinsight.com/doi/full/10.1108/SCM-01-2018-0029 Subscription required to view

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.

Tse, D, Zhang, B, Yang, Y, Cheng, C, Mu, H. Blockchain application in food supply information security. In: IEEE Technology and Engineering Management Society and IEEE Singapore Section, editors. 2017 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM); Dec 10-13; Singapore. Piscataway, NJ:

IEEE Technology and Engineering Management Society; 2017. p. 1357-1361.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8290114 Subscription required to view.

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.

Tseng, JH, Liao, YC, Chong, B, Liao, SW. Governance on the drug supply chain via Gcoin blockchain. Int J Environ Res Public Health. 2018;15(6):1055. Epub 2018 May 23.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1660-4601/15/6/1055 Open access.

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.

Tung, JK, Nambudiri, VE. Beyond bitcoin: potential applications of blockchain technology in dermatology. Br J Dermatol. 2018;179(4):1013-1014. Epub 2018 Jun 26.

Reference Type: Journal Article

Available from: https://onlinelibrary.wiley.com/doi/abs/10.1111/bjd.16922 Subscription required to view.

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.

U. S. Government Accountability Office. Urgent actions are needed to address cybersecurity challenges facing the nation. Washington, D.C.: 2018. Report No.: GAO-18-622.

Reference Type: Report

Available from: http://media.proquest.com/media/hms/PFT/1/EHP07?_s=h7D1qexAHJOqnGYfNjXKiA75J8k%3D Open access.

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.

Uddin, MA, Stranieri, A, Gondal, I, Balasubramanian, V. Continuous patient monitoring with a patient centric agent: a block architecture. IEEE Access. 2018;6:32700-32726. Epub 2018 Jun 13.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8383967 Open access.

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.

Vazirani, AA, O'Donoghue, O, Brindley, D, Meinert, E. Implementing blockchains for efficient health care: systematic review. J Med Internet Res. 2019;21(2):e12439. Epub 2018 Oct 7.

Reference Type: Journal Article

Available from: https://www.jmir.org/2019/2/e12439/ Open access.

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.

Wang, H, Song, Y. Secure cloud-based EHR system using attribute-based cryptosystem and blockchain. J Med Syst. 2018;42(8):152. Epub 2018 Jul 5.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0994-6 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.

Wang, J, Wang, S, Guo, J, Du, Y, Cheng, S, Li, X. A summary of research on blockchain in the field of intellectual property. In: 2018 International Conference on Identification, Information and Knowledge in the Internet of Things; 2018 Oct 19-21; Beijing, China. Cambridge, MA: Elsevier; 2019. p. 191-197.

Reference Type: Conference Paper

Available from: http://www.sciencedirect.com/science/article/pii/S187705091930239X Open access.

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.

Wang, S, Wang, J, Wang, X, Qiu, T, Yuan, Y, Ouyang, L, et al. Blockchain-powered parallel healthcare systems based on the ACP approach. IEEE Trans Comput Soc Sys. 2018;5(4):942-950. Epub 2018 Aug 28.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8449329 Subscription required to view.

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 auditability. 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.

Wang, Y, Han, JH, Beynon-Davies, P. Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. Supply Chain Manag. 2018;24(1):62-84. Epub 2018 Oct 4.

Reference Type: Journal Article

Available from: https://www.emeraldinsight.com/doi/full/10.1108/SCM-03-2018-0148 Subscription required to view.

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.

Wang, Y, Singgih, M, Wang, J, Rit, M. Making sense of blockchain technology: How will it transform supply chains? International Journal of Production Economics. 2019;211:221-236. Epub 2019 Feb 6.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S0925527319300507 Subscription required to view.

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.

Weber, I, Gramoli, V, Ponomarev, A, Staples, M, Holz, R, Tran, AB, et al. On availability for blockchain-based systems. In: IEEE Computer Society and Hong Kong Polytechnic University, editors. 2017 IEEE 36th Symposium on

Reliable Distributed Systems (SRDS); Sep 26-29; Hong Kong. Los Alamitos, CA: IEEE Computer Society; 2017. p. 64-73.

Reference Type: Conference Paper

Available from: https://research.csiro.au/data61/wp-content/uploads/sites/85/2016/08/OnAvailabilityForBlockchain-BasedSystems-SRDS2017-authors-copy.pdf Open access;
https://ieeexplore.ieee.org/abstract/document/8069069 Subscription required to view.

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

Wong, MC, Yee, KC, Nohr, C. Socio-technical considerations for the use of blockchain technology in healthcare. Stud Health Technol Inform. 2018;247:636-640. Epub 2018 Apr 22.

Reference Type: Journal Article

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

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.

Wright, A, De Filippi, P. Decentralized blockchain technology and the rise of lex cryptographia. SSRN. 2015;https://dx.doi.org/10.2139/ssrn.2580664. Epub 2015 Mar 20.

Reference Type: Journal Article

Available from:
https://papers.ssrn.com/sol3/Delivery.cfm/SSRN_ID2580664_code2373233.pdf?abstractid=2580664&mirid=1 Open access.

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.

Wu, HT, Tsai, CW. Toward blockchains for health-care systems: applying the bilinear pairing technology to ensure privacy protection and accuracy in data sharing. IEEE Consum Electron. 2018 July:65-71.

Reference Type: Magazine Article

Available from: https://ieeexplore.ieee.org/abstract/document/8386918 Subscription required to view.

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.nhri.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.

Xia, Q, Sifah, EB, Asamoah, KO, Gao, J, Du, X, Guizani, M. MeDShare: trust-less medical data sharing among cloud service providers via blockchain. IEEE Access. 2017;5:14757-14767. Epub 2017 Jul 24.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/7990130 Open access.

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 proved 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.

Xu, JJ. Are blockchains immune to all malicious attacks? Financ Innov. 2016;2(25):1-9. Epub 2016 Dec 10.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1186/s40854-016-0046-5 Open access.

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.

Yaeger, K, Martini, M, Rasouli, J, Costa, A. Emerging blockchain technology solutions for modern healthcare infrastructure. J Sci Innov Med [Internet]. 2019 Jan 24 [cited 2019 Feb 28]; 2(1):[7 p.]. Available from: https://journalofscientificinnovationinmedicine.org/articles/10.29024/jsim.7/#

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.

Yaga, D, Mell, P, Roby, N, Scarfone, K. Blockchain technology overview. Gaithersburg, MD: National Institute of Standards and Technology, 2018 Oct 3. Report No.: NISTIR 8202.

Reference Type: Report

Available from: https://www.nist.gov/publications/blockchain-technology-overview Open access.

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.

Yang, C, Chen, X, Xiang, Y. Blockchain-based publicly verifiable data deletion scheme for cloud storage. J Netw Comput Appl. 2018;103:185-193. Epub 2017 Dec 7.

Reference Type: Journal Article

Available from: http://www.sciencedirect.com/science/article/pii/S1084804517303910 Subscription required to view.

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.

Yeoh, P. Regulatory issues in blockchain technology. JFRC. 2017;25(2):196-208. Epub 2017 May 8.

Reference Type: Journal Article

Available from: https://www.emeraldinsight.com/doi/abs/10.1108/JFRC-08-2016-0068 Subscription required to view.

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.

Yli-Huumo, J, Ko, D, Choi, S, Park, S, Smolander, K. Where is current research on blockchain technology? A systematic review. PLoS ONE. 2016;11(10):e0163477. Epub 2016 Oct 3.

Reference Type: Journal Article

Available from: https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0163477 Open access.

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.

Yu, B, Wright, J, Nepal, S, Zhu, L, Liu, J, Ranjan, R. IoTChain: establishing trust in the internet of things ecosystem using blockchain. IEEE Trans Cloud Comput. 2018;5(4):12-23. Epub 2018 Aug 14.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8436081 Subscription required to view.

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.

Yue, X, Wang, H, Jin, D, Li, M, Jiang, W. Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J Med Syst. 2016;40(10):218. Epub 2016 Aug 26.

Reference Type: Journal Article

Available from: http://download.xuebalib.com/3drsLUt9gNI2.pdf Open access;
https://link.springer.com/article/10.1007/s10916-016-0574-6 Subscription required to view.

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.

Zamani, E, He, Y, Phillips, M. On the security risks of the blockchain. J Comput Inform Syst. 2018;DOI: 10.1080/08874417.2018.1538709. Epub 2018 Dec 11.

Reference Type: Journal Article

Available from: https://www.tandfonline.com/doi/abs/10.1080/08874417.2018.1538709 Subscription required to view.

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 exists. 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.

Zhang, A, Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. J Med Syst. 2018;42(8):140. Epub 2018 Jun 28.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0995-5 Subscription required to view.

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.

Zhang, J, Xue, N, Huang, X. A secure system for pervasive social network-based healthcare. IEEE Access. 2016;4:9239-9250. Epub 2016 Dec 29.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/7801940 Open access.

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.

Zhang, M, Ji, Y. Blockchain for healthcare records: a data perspective. PeerJ PrePrints. 2018;6:e26942v26941. Epub 2018 May 17.

Reference Type: Journal Article

Available from: https://peerj.com/preprints/26942/ Open access.

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.

Zhang, P, Walker, MA, White, J, Schmidt, DC, Lenz, G. Metrics for assessing blockchain-based healthcare decentralized apps. 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom); 2017 Oct 12-15; Dalian, China. Piscataway, NJ: IEEE.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8210842 Subscription required to view.

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.

Zhang, P, White, J, Schmidt, DC, Lenz, G, Rosenbloom, ST. FHIRChain: applying blockchain to securely and scalably share clinical data. Comput Struct Biotechnol J. 2018;16:267-278. Epub 2018 Aug 16.

Reference Type: Journal Article

Available from: https://www.sciencedirect.com/science/article/pii/S2001037018300370 Open access.

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.

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.

Reference Type: Conference Proceedings

Available from: https://ieeexplore.ieee.org/abstract/document/8422883 Subscription required to view.

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.

Zhao, H, Bai, P, Peng, Y, Xu, R. Efficient key management scheme for health blockchain. CAAI Trans Intell Technol. 2018;3(2):114-118. Epub 2018 Jun 28.

Reference Type: Journal Article

Available from: https://ieeexplore.ieee.org/abstract/document/8396896 Open access.

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.

Zhao, H, Zhang, Y, Peng, Y, Xu, R. Lightweight backup and efficient recovery scheme for health blockchain keys. In: IEEE Computer Society, editor. 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS); Mar 22-24; Bangkok, Thailand. Piscataway, NJ: IEEE Computer Society; 2017. p. 229-234.

Reference Type: Conference Paper

Available from: https://www.computer.org/csdl/proceedings/isads/2017/4042/00/07940245.pdf Open access; https://ieeexplore.ieee.org/abstract/document/7940245 Subscription required to view.

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 no-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 blockchain. 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.

Zhou, L, Wang, L, Ai, T, Sun, Y. BeeKeeper 2.0: confidential blockchain-enabled IoT system with fully homomorphic computation. Sensors (Basel). 2018;18(11):3785. Epub 2018 Nov 5.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/11/3785 Open access.

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.

Zhou, L, Wang, L, Sun, Y. MIStore: a blockchain-based medical insurance storage system. J Med Syst. 2018;42(8):149. Epub 2018 Jul 2.

Reference Type: Journal Article

Available from: https://link.springer.com/article/10.1007/s10916-018-0996-4 Open access.

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.

Zhu, L, Zheng, B, Shen, M, Yu, S, Gao, F, Li, H, et al. Research on the security of blockchain data: a survey. arXiv [Internet]. 2018 Dec 7 [cited 2019 Feb 1]; 1812.02009:[48 p.]. Available from: https://arxiv.org/abs/1812.02009

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.

Zhu, X, Badr, Y. Identity management systems for the internet of things: a survey towards blockchain solutions. Sensors (Basel). 2018;18(12):4215. Epub 2018 Dec 1.

Reference Type: Journal Article

Available from: https://www.mdpi.com/1424-8220/18/12/4215 Open access.

Abstract:

The Internet of Things aims at connecting everything, ranging from individuals, organizations, and companies to things in the physical and virtual world. The digital identity has always been considered as the keystone for all online services and the foundation for building security mechanisms such as authentication and authorization. However, the current literature still lacks a comprehensive study on the digital identity management for the Internet of Things (IoT). In this paper, we firstly identify the requirements of building identity management systems for IoT, which comprises scalability, interoperability, mobility, security and privacy. Then, we trace the identity problem back to the origin in philosophy, analyze the Internet digital identity management solutions in the context of IoT and investigate recent surging blockchain sovereign identity solutions. Finally, we point out the promising future research trends in building IoT identity

management systems and elaborate challenges of building a complete identity management system for the IoT, including access control, privacy preserving, trust and performance respectively.

Zhu, X, Badr, Y, Pacheco, J, Hariri, S. Autonomic identity framework for the internet of things. In: University of Arizona and IEEE Computer Society, editors. 2017 International Conference on Cloud and Autonomic Computing (ICCAC); Sep 18-22; Tucson, AZ. IEEE Computer Society; 2017. p. 69-79.

Reference Type: Conference Paper

Available from: https://ieeexplore.ieee.org/abstract/document/8064055 Subscription required to view.

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.