Blockchain Basics

Ledger Academy

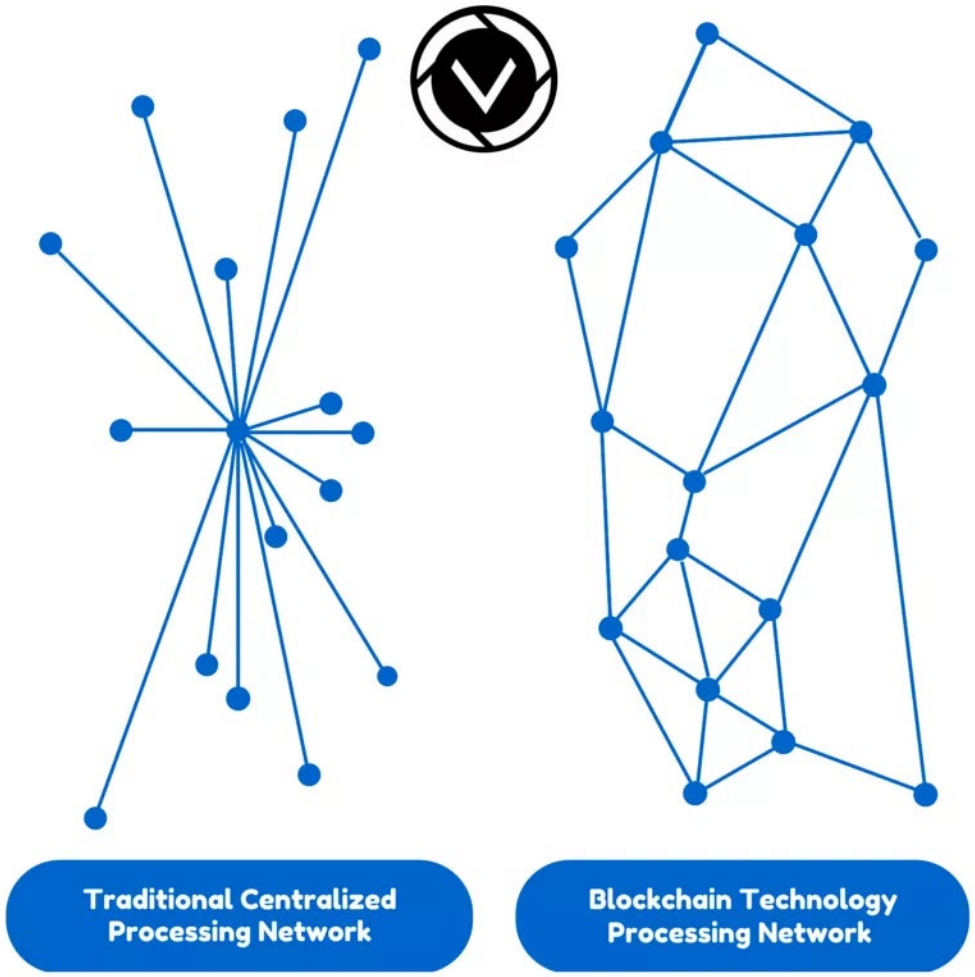
9-23-2019

Introduction

- What Is Blockchain Technology
  - Innovation to Computer Science
  - New way to interact Trade
- History of the Internet
- History Of Bitcoin
- Bitcoin The System
- How It works
- Types of Blockchains

Innovation to Computer Science

- **Blockchain technology is a shared ledger (DLT) that everyone trusts to be accurate and permanent**
- Public registry that stores transactions in append only network system that creates a shared reality between non trusting entities
- Bitcoin was the first to introduce it to the world.
- Cryptoasset – or cryptocurrency or digital asset, Underlying function of a blockchain, Does not have to represent digital cash but digital value.



Distributed Ledger Technology

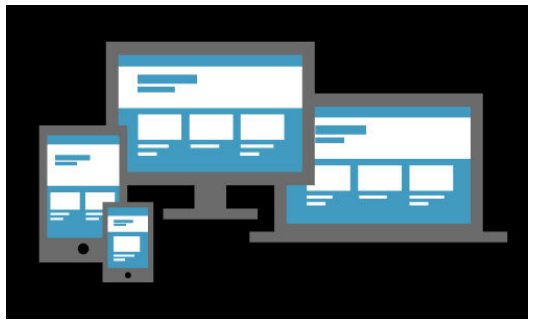
Trade:

First form was bartering , informal rules.

CURRENCY

Purpose of Currency
1. Medium For Exchange.
2. Store of value over time
3. Accepted as a measure of worth.

Fiat currency –Backed by Government (because I said so) .



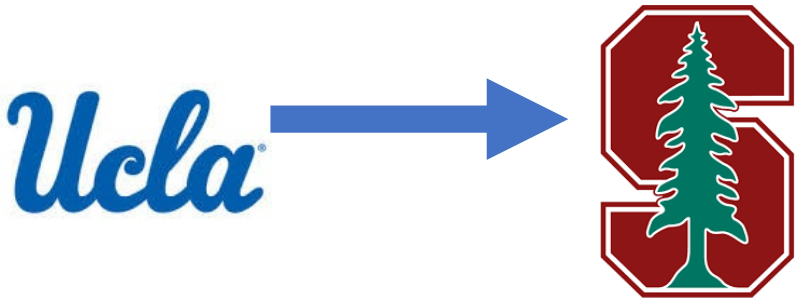
Online transactions. Centralized ledgers Single point of control.

CRYPTOCURRENCY

Because we can prove it.

Distributed Ledger Technology

Origin of Internet



- Electronic computers in the :
- 1960 DARPA attempt to create a decentralized computer system
- in 1969 The first message was sent over the ARPANET, the defense departments first attempt at a WIDE AREA NETWORK, from a laboratory at UCLA to the second network node at Stanford Research Institute.
  - Packet switching, communication protocols were being developed.
- 1970s The INTERNET PROTOCOL SUITE (TCP/IP) was developed by R. Kahn and V. Cerf and became the standard networking protocol.
- 1980s -1990's,CERN in Switzerland, British computer scientist Tim Berners-Lee inventing the World Wide Web and in doing so the first web server, and the first web browser, resulted in a database called the WORLD WIDE WEB that used linking hypertext documents into an information system, accessible from any node on the network.

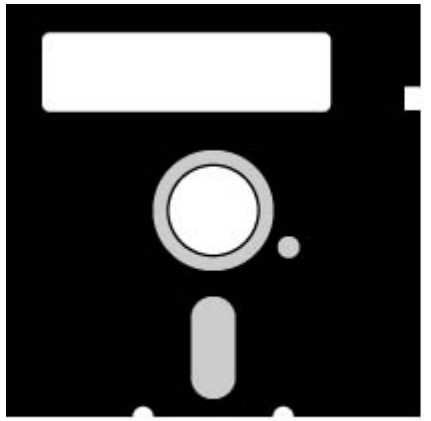
WEB 1.0

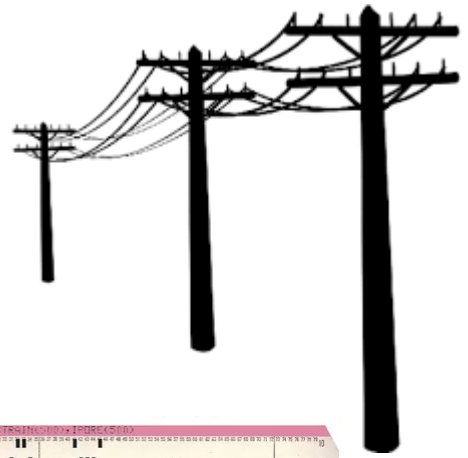
Late 1980s, Commercial Internet Service Providers (ISPs) began to emerge.

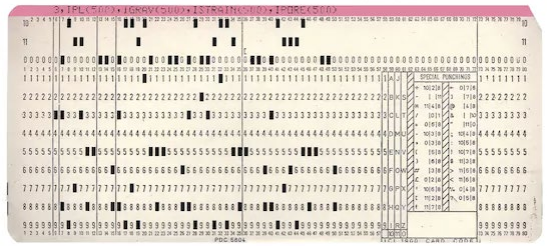
The 1989 implementation of Tim Berners-Lee's Hypertext Transfer Protocol (HTTP) on top of the base-layer Transmission Control and Internet protocols (TCP/IP) paved the way for web-based applications
1993 Marc Andreessen's MOSAIC which we know as NETSCAPE gave us the Commercial BROWSER
Information Revolution, email, messaging, video calls, discussion forums.

WEB 2.0

- First used in 1999
- Marked household adoption: computers and items for connect became necessities
- Technology advancements : computer storage, data access speeds, *hard drives instead of floppies MB turned in GB that turned into TB.*
- Internet Speeds (ethernet technology that allows for TCP/IP) common speeds of kilobits to tens of megabits per second, to gigabits per second.
- RAM grew from hundreds of kilobytes to gigabytes as typical amounts on a system.
- Dot. Com Bubble

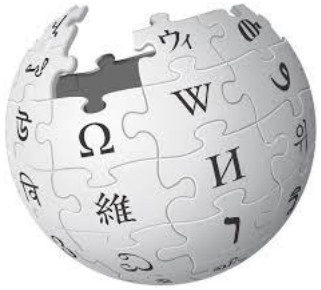


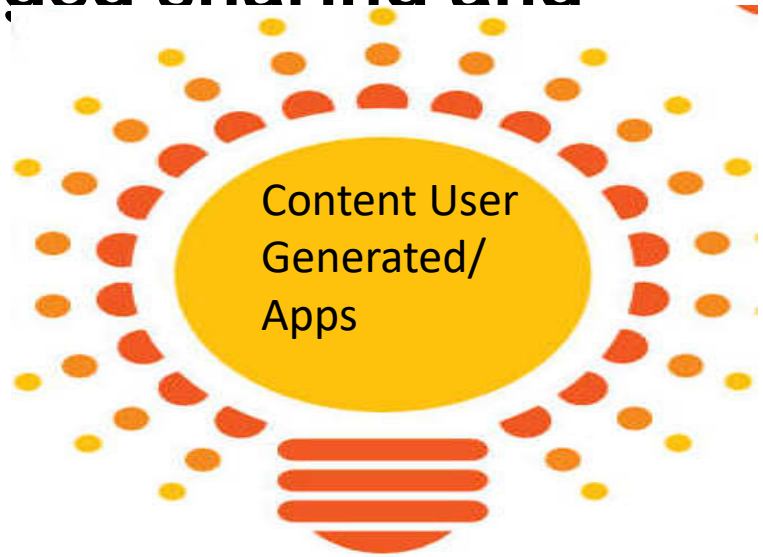




WEB 2.0

- Collaboration
- **The emergence of social media and interactive websites**
- **Instagram, Twitter, Facebook, Wikipedia, Google**
- **Web sites generated content and encouraged sharing and online commerce.**
- **Website with user generated content.**





WEB 3.0

Blockchains
Smart Contracts
D Apps
Artificial Intelligence
Data Mining
Cloud Storage
Tokenization of Value

Internet of Information Web 2.0
Internet Value Web 3.0.

History Of Bitcoin

- In 1983, David Chaum introduced the idea of digital cash. In 1990, he founded DigiCash, an electronic payment system. Chaum wrote a paper describing the technological of public and private key generation order to create this Blind Signature Technology. Chaum's Blind Signature Technology was designed to ensure the complete privacy of users who conduct online transactions.
- 1990 Dot Com bubble and business mis-management discouraged digital cash mechanisms
- In 1998, Wei Dai / Nick Szabo created (bitgold) electronic currency system which required users to complete a proof of work function with solutions being cryptographically put together and published.
- A currency system based on a proof of work was later created by Hal Finney who followed the work of Dai and Szabo(smart contract 1996).
- **Satoshi Nakamoto**, the unknown inventor of Bitcoin, never intended to invent a currency. In his announcement of Bitcoin in late 2008, **Satoshi** said she developed “A Peer-to-Peer Electronic Cash System.“

Bitcoin:

A Peer-to-Peer Electronic Cash System Satoshi Nakamoto. A purely peer-to-peer version of electronic cash would allow **ONLINE PAYMENTS** to be **SENT DIRECTLY** from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network. **THE NETWORK TIMESTAMPS TRANSACTIONS BY HASHING THEM INTO AN ONGOING CHAIN OF HASH-BASED PROOF-OF-WORK, FORMING A RECORD THAT CANNOT BE CHANGED WITHOUT REDOING THE PROOF-OF-WORK.** The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself **REQUIRES MINIMAL STRUCTURE**. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

The White Paper

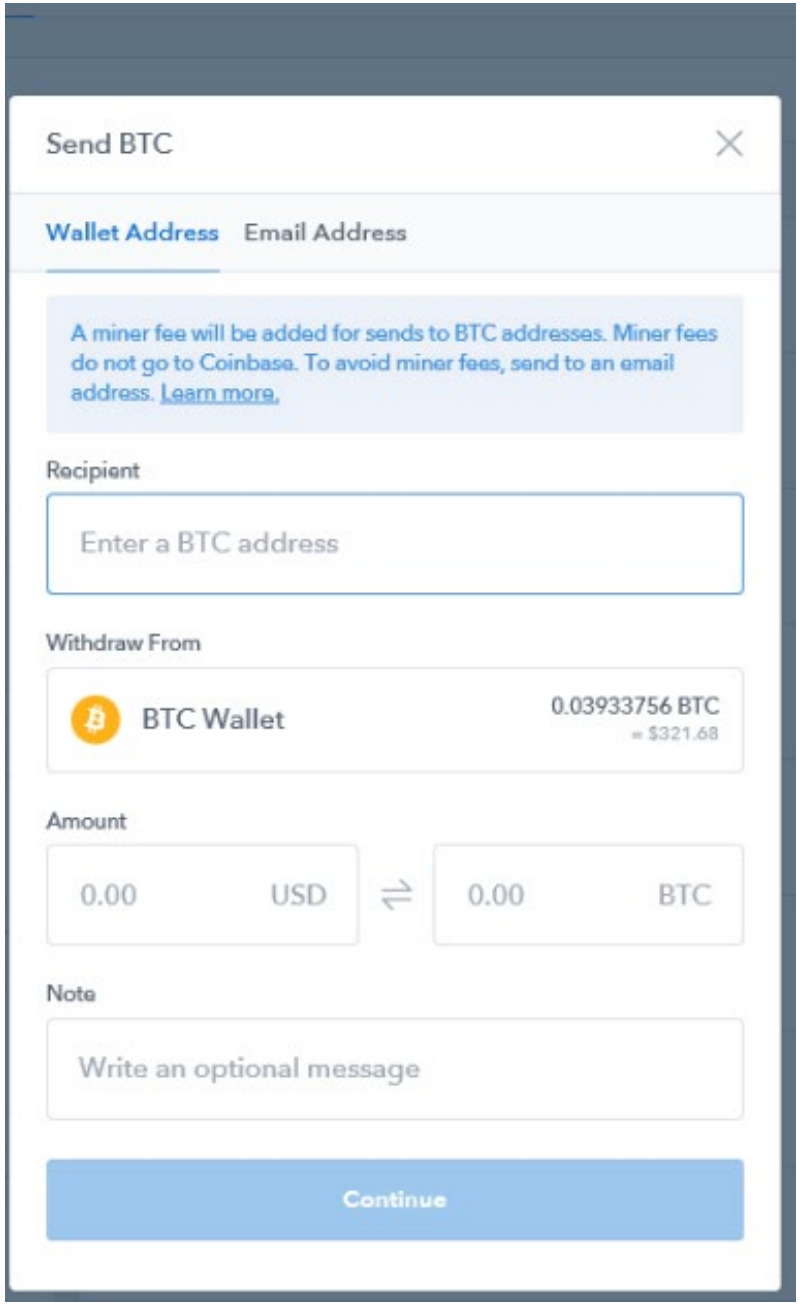
- Introduced to a Crypto Mailing list by publishing the White Paper “ **Bitcoin: A Peer-to-Peer Electronic Cash System** ”, and released as open-source software in 2009.
- The system is peer-to-peer, and transactions take place between users directly, without an intermediary.
- These transactions are verified by network nodes and recorded in a public distributed ledger called the *blockchain* , which uses bitcoin as its native currency.
- Bitcoins are created as a reward in a competition in which users offer their computing power to verify and record bitcoin transactions into the blockchain. This activity is referred to as *mining* and successful miners are rewarded with transaction fees and newly created bitcoins.
- Bitcoin can be exchanged for other currencies. products, and services. When sending bitcoins, users can pay an optional transaction fee to the miners. This may expedite the transaction being confirmed.

BITCOIN ECOSYSTEM

- **bitcoin the Unit:** the denominations of bitcoin
- Bitcoin (capitalized B) : associated with Bitcoin the protocol and payment network. The uppercase form, “Bitcoin,” is also often used to refer to as the ecosystem as a whole. Using Bitcoin with a capital “B” is the common way of referencing Bitcoin when writing about it in general terms.
- bitcoin. lowercase “b” written as “bitcoin” is usually associated with bitcoin as the currency
- **Bitcoin the Network:** the network is connected by independent nodes. Network is secure from from attacks (such as DDoS) but not 51% Attack.
- **Bitcoin Improvement Proposals (BIPs):** a BIP is the basic process of submitting, evaluating, and implementing updates to the system. BIP Reviews are posted in Github and community votes on the Bitcoin Improvement Proposals

How it works

- User Makes Request of system:
  - New to system, set up account, returning user, open blockchain and login
  - Fill out Ticket
  - Request goes to the system
  - Verification and consensus process by miners (or other mechanism)
  - Value gets transferred and confirmed.

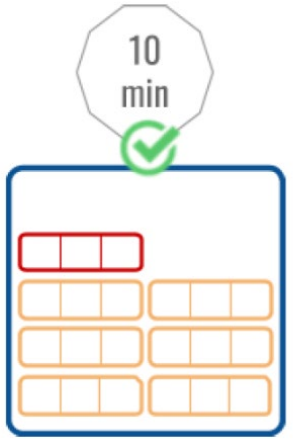


Denominations of Bitcoin

- .012 BTC = $ 100.
- Satoshi, which is the name of the creator of bitcoin, is also the smallest denomination available at 0.00000001 BTC.

DENOMINATION	ABBREVIATION	VALUE IN BTC
Megabit (coin)	MBTC	1,000,000. BTC
Kilobit (coin)	kBTC	1,000. BTC
Hectobit (coin)	hBTC	100. BTC
DecaBit (coin)	daBTC	10. BTC
BITCOIN	BTC	1. BTC
Decibit (coin)	dBTC	0.1 BTC
Centibit (coin)	cBTC	0.01 BTC
Millibit (coin)	mBTC	0.001 BTC
Micrbit (coin)	uBTC	0.000001 BTC
SATOSHI	SAT	00000001 BTC

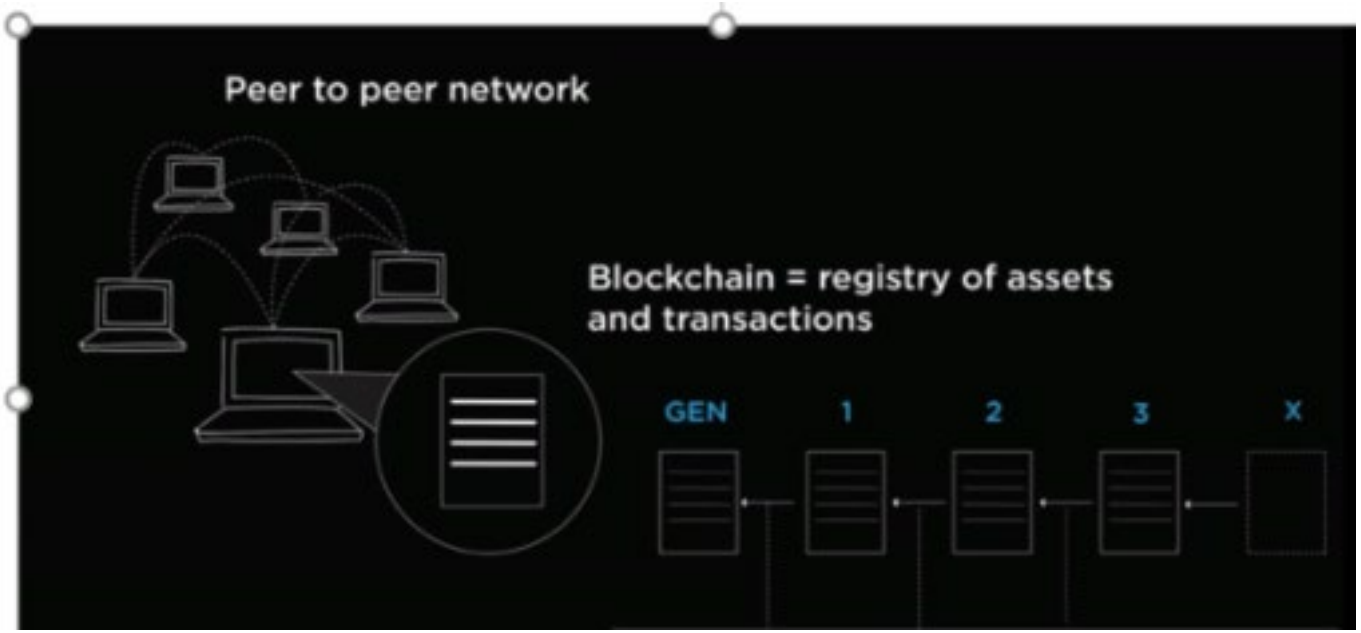
How It works



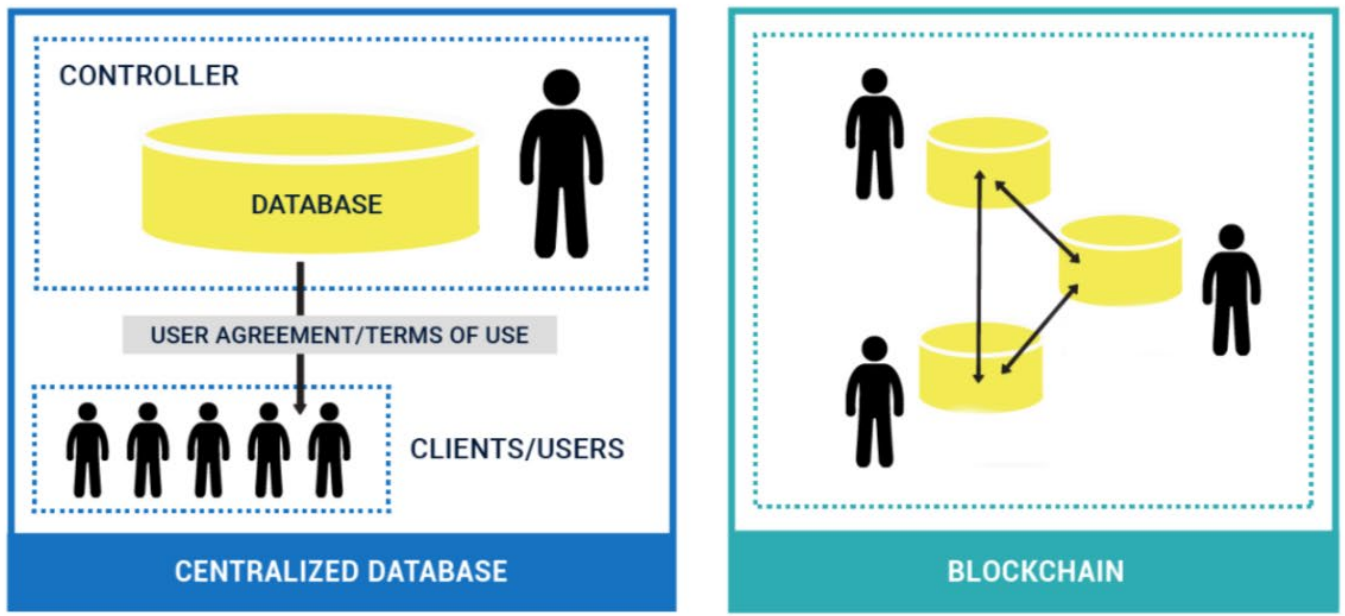
- *Parts of a Bitcoin blockchain:*
- *Header (Version, Previous Block Hash, Merkle Root, Timestamp, Difficulty Target, Nonce)*
- **Description**
- Version number to track software/protocol upgrades
- **HASH**
- A reference to the hash of the previous (parent) block in the chain
- Merkle Root A hash of the root of the Merkle tree of this block's transactions
- Timestamp The approximate creation time of this block
- Difficulty Target The proof-of-work algorithm difficulty target for this block (Nonce A counter used for the proof-of-work algorithm)
- *Transactions in the block.*

Bitcoins Blockchain System

- Technologies :
- Cryptography
- Mathematical Hashing
- Consensus Algorithms
- Public / Private Keys



CENTRALIZED DATABASES VS. BLOCKCHAIN



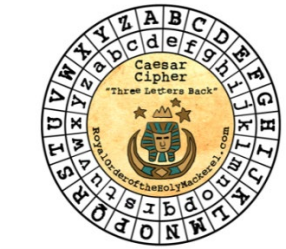
Consensus

- Consensus is a process whereby the peers synchronize the data on the blockchain.
- There are a number of consensus mechanisms or algorithms.
- One is Proof of Work. Another is Proof of Stake.
- There's also Proof of Elapsed Time, as well as Simplified Byzantine Fault Tolerance.
- Bitcoin uses Proof of Work, while Ethereum uses Proof of Work currently, but is moving towards Proof of Stake.
- **The Hyperledger Sawtooth uses Proof of Elapsed Time.**

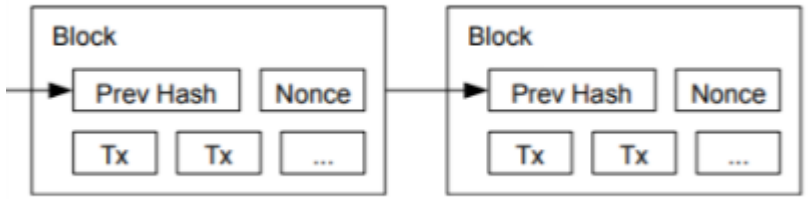
- **Immutability of Data**
- his **immutability**, or '**unchanging over time**' feature makes the blockchain useful for accounting, financial transactions, identity management, and asset ownership, management and transfer, just to name a few examples. Once a transaction is written onto the blockchain, no one can change it, or, at least, it would be extremely difficult to change it.

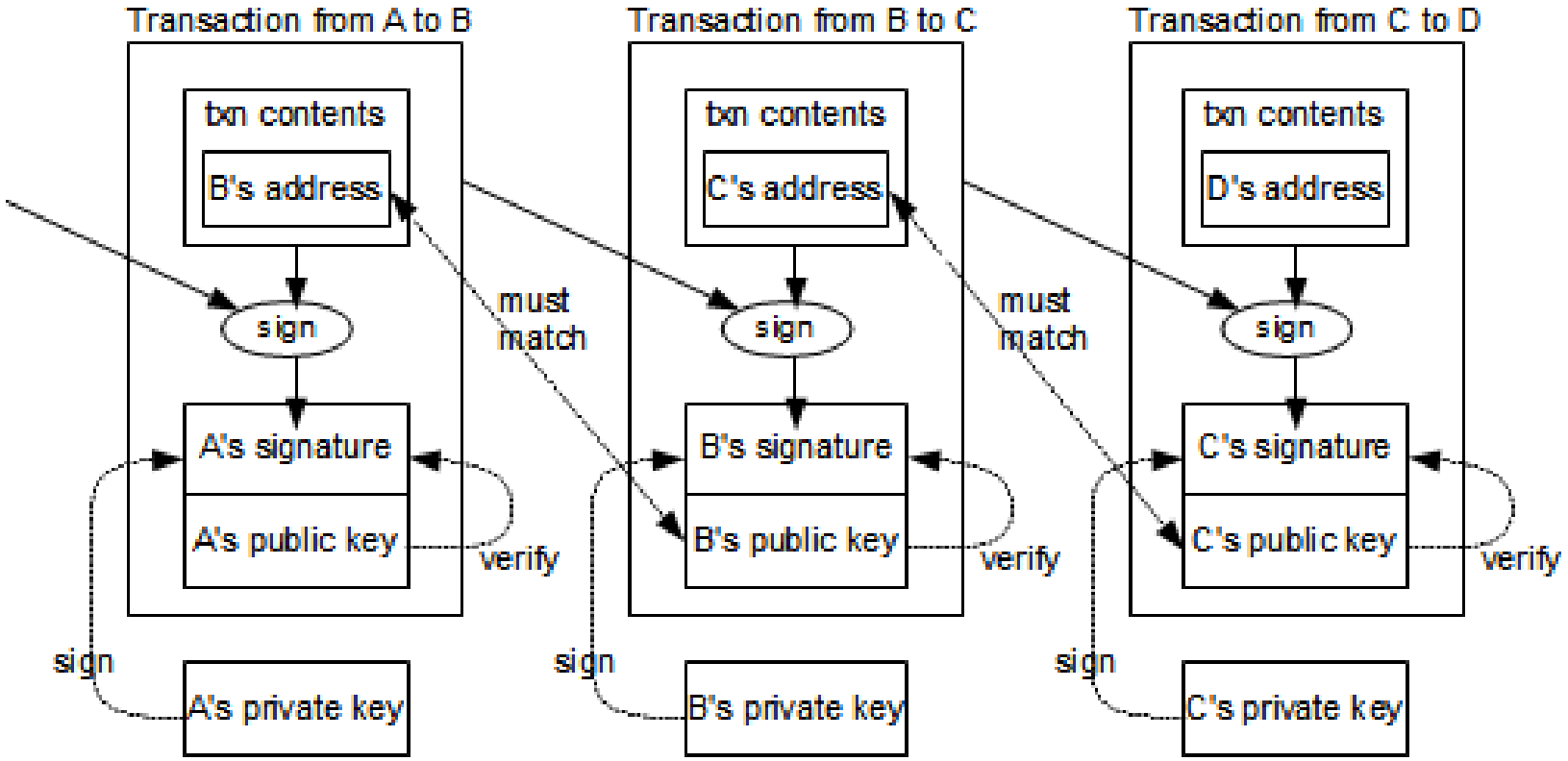
Cryptography DIGITAL SECRETS

- **Cryptography** has a key role to play both in the security, as well as in the immutability
- For blockchain technologies, cryptography is used
  - to prove that a transaction was created by the right person.
  - It is used to link transactions into a block in a tamper-proof way, as well as create the links between blocks, to form a blockchain.
- Hash: Cryptographic hash functions are mathematical operations run on digital data. (SHA 256) Elliptic Curves Cryptography
  - Proof-of-Work



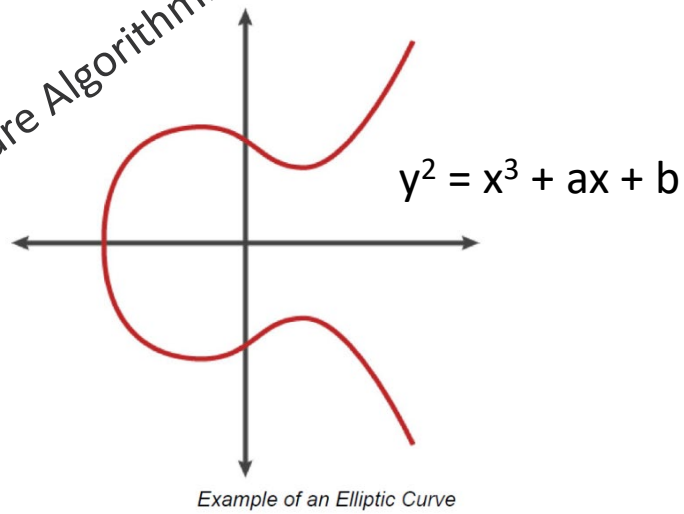
Procedure


Block
Prev Hash
Nonce
Tx
Tx
...
Block
Prev Hash
Nonce
Tx
Tx
...


Transaction from A to B
txn contents
B's address
sign
A's signature
A's public key
verify
must match
sign
A's private key
Transaction from B to C
txn contents
C's address
sign
B's signature
B's public key
verify
must match
sign
B's private key
Transaction from C to D
txn contents
D's address
sign
C's signature
C's public key
verify
sign
C's private key

Elliptical Curve Cryptography

Elliptic Curve Digital Signature Algorithm.



Example of an Elliptic Curve

- create the public key derived from the private key, approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields.
- Cryptocurrency mining is the process of adding sets, or “blocks” of new transactions to the blockchain. Miners use large amounts of computing power to guess a specific number that cryptographically links the new block to the preceding one—the key to making the record tamper-proof. By finding the number, a miner proves that it did the work required to secure the chain and reaps a cryptocurrency reward.

ECDSA has separate procedures for signing and verification. Each procedure is an algorithm composed of a few arithmetic operations.

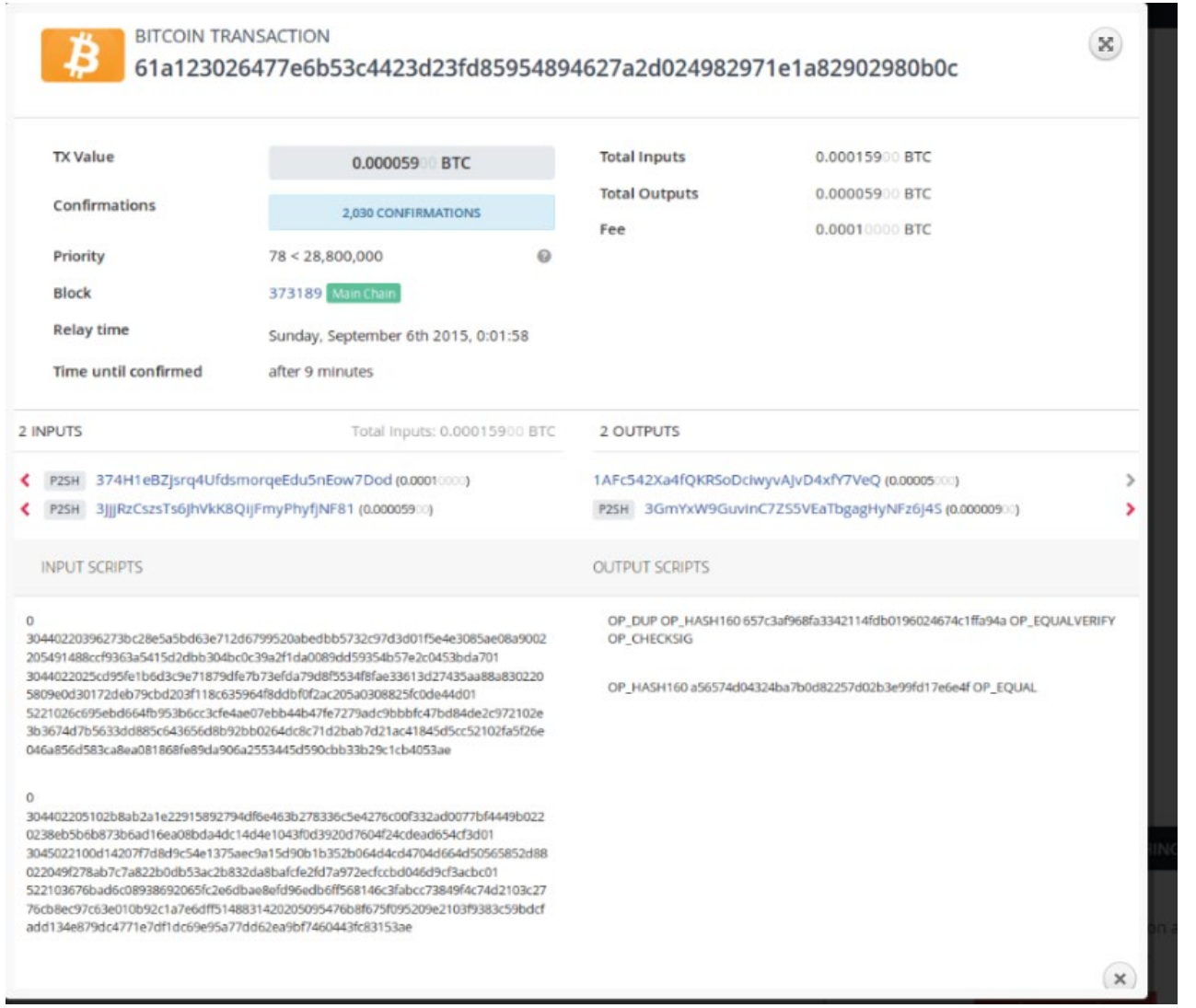
Proof of Work

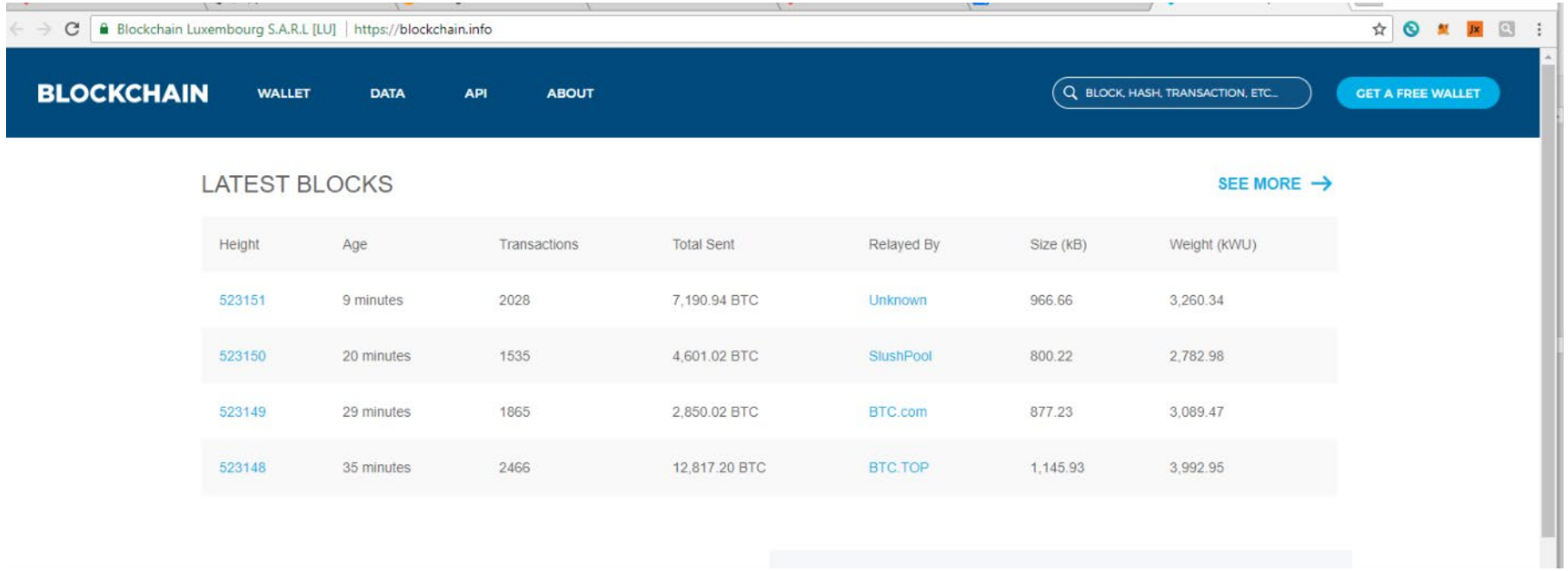
- A piece of data that requires a significant computer computational power to find.
- Bitcoin miners (node operators) must agree (consensus) to the solution to a SHA 256 algorithm to make the hash label that is required to add block to the chain. The label is the proof of work that the algorithm was solved. And consensus was reached as to it accuracy.
- Once that label is added it is mathematically linked (hashed) to the previous validated block creating an immutable chain of reference.
- Every Bitcoin can be cryptographically traced back to its origin (genesis block NO DOUBLE SPENDING>.

Public Keys and Private Keys Address

- Bitcoin Address: To keep information secure, these keys are crypto secure.
- **PRIVATE KEY**
- The private key is crucial to keeping your bitcoins safe. This is unique to you, and only you should know your private key. It takes the form of a string that signs a digital communication once hashed with your public key.
- **PUBLIC KEY**
- A public key is a bitcoin address, the information of which is accessible to all. When hashed with a private key it secures a digital communication.
- Public / Private Keys / Wallets
- Passphrase-Encrypted Wallets (AKA BIP38)
- Multisig

Stored on the blockchain




Blockchain Luxembourg S.A.R.L [LU] | https://blockchain.info
BLOCKCHAIN
WALLET
DATA
API
ABOUT
BLOCK, HASH, TRANSACTION, ETC...
GET A FREE WALLET
LATEST BLOCKS
SEE MORE
Height Age Transactions Total Sent Relayed By Size (kB) Weight (kWU)
523151 9 minutes 2028 7,190.94 BTC Unknown 966.66 3,260.34
523150 20 minutes 1535 4,601.02 BTC SlushPool 800.22 2,782.98
523149 29 minutes 1865 2,850.02 BTC BTC.com 877.23 3,089.47
523148 35 minutes 2466 12,817.20 BTC BTC.TOP 1,145.93 3,992.95

Blockchain Explorers

- Block explorer
- Etherscan
- Etherchain.org

- **stamp.io is a tool that can be used to put and verify document hashes onto both the Ethereum and Bitcoin blockchains.**
-

Dapps

- **Dapps**: Distributed apps - applications that use blockchain storage and computing power through Ethereum. Generally, dapps look and feel like existing apps you know and use every day
- **Gas**: The small amount of money you pay for each transaction that rewards nodes for providing their
- **Web 3.0 browsers**: New browsers are being built that help you manage your cryptocurrency, keys, passwords, blockchain, identity, permissions, etc. In general, they will use the familiar web front-end toolkits: JavaScript, AJAX, HTML, etc.

Permissioned versus Permission less

Characteristic	Ethereum	Hyperledger Fabric	R3 Corda
Description of platform	– Generic blockchain platform	– Modular blockchain platform	– Specialized distrib-uted ledger platform for financial industry
Governance	– Ethereum developers	– Linux Foundation	– R3
Mode of operation	– Permissionless, public or private[4]	– Permissioned, private	– Permissioned, private
Consensus	– Mining based on proof-of-work (PoW) – Ledger level	– Broad understand-ing of consensus that allows multiple approaches – Transaction level	– Specific understand-ing of consensus (i.e., notary nodes) – Transaction level
Smart contracts	– Smart contract code (e.g., Solidity)	– Smart contract code (e.g., Go, Java)	– Smart contract code (e.g., Kotlin, Java) – Smart legal contract (legal prose)
Currency	– Ether – Tokens via smart contract	– None – Currency and tokens via chaincode	– None

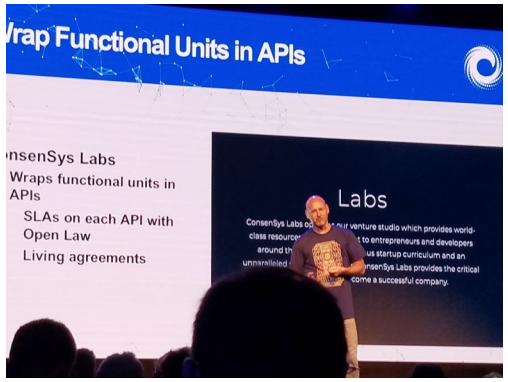
Ethereum
An open-source virtual machine that allows programmers to build dapps using blockchain. Includes ETH, its own native currency

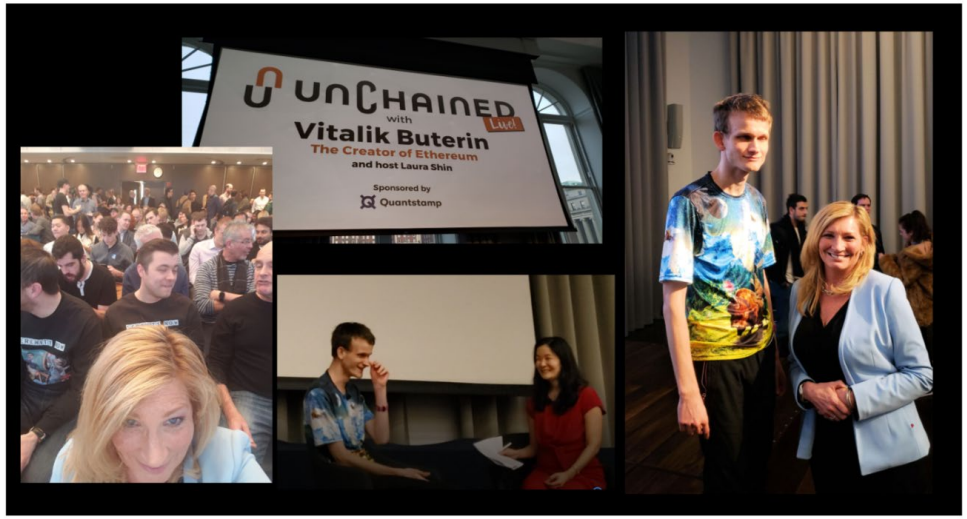
The EVM
With Ethereum, servers and clouds are replaced by thousands of so-called "nodes" run by volunteers from across the globe (thus forming a "world computer").

The vision is that Ethereum would enable this same functionality to people anywhere around the world, enabling them to compete to offer services on top of this infrastructure.

Vitalik Buterin

- **Ethereum**
  Ethereum, which was first described in a white paper in 2013, is the operating system that adds programming to blockchains, effectively turning the network of “miners” into the world’s largest computer.
- Ethereum can be programmed just like any general-purpose computer, and apps built on Ethereum can grow to any size, are incredibly secure, preserve anonymity, are auditable, and provide the same service at the same scale for less than 1% of the centralized price
- The Ethereum Virtual Machine or EVM is the virtual machine in which all the smart contracts function in Ethereum.
- It is a simple yet powerful Turing Complete 256-bit virtual machine. Turing Complete means that given the resources and memory, any program executed in the EVM can solve any problem.
- Because it has the ability to build platforms, its both a cryptoasset and a cryptocurrency





Smart Contracts

- a smart contract within the blockchain may allow automatic execution of transactions upon meeting predefined criteria
- The Enterprise Ethereum Architecture Stack will serve as a guidepost for corporations, providing infrastructure tools and frameworks designed to empower the next generation of Enterprise Ethereum applications. The new EEA specifications have been under development by the EEA's technical committee, in partnership with member companies, for the past year and a half.

Crypto Assets versus Crypto Commodities

Crypto-asset is the currency used on a blockchain, a crypto-commodity is a platform by which blockchains can be generated.

- INVESTMENT ISSUES:
  - Supply of Native currency
  - How its release into the system
  - Who owns it

7 classification of crypto assets::

ICO and Tokens

- **Tokens**: represent value inside various systems. tokens will bridge systems, interoperable.
- https://youtu.be/rIMKNkF6d28
- Unit of value that an organization creates to
  - Self govern business model
  - Empower users to interact with product/service
  - Facilitates sharing of rewards to ecosystem

Token Values:

Each token represents some value for the company:

1. Who will use it
2. How will they use it
3. What will it cost
4. What is the benefit
5. What's the value
6. Can it be exchanged

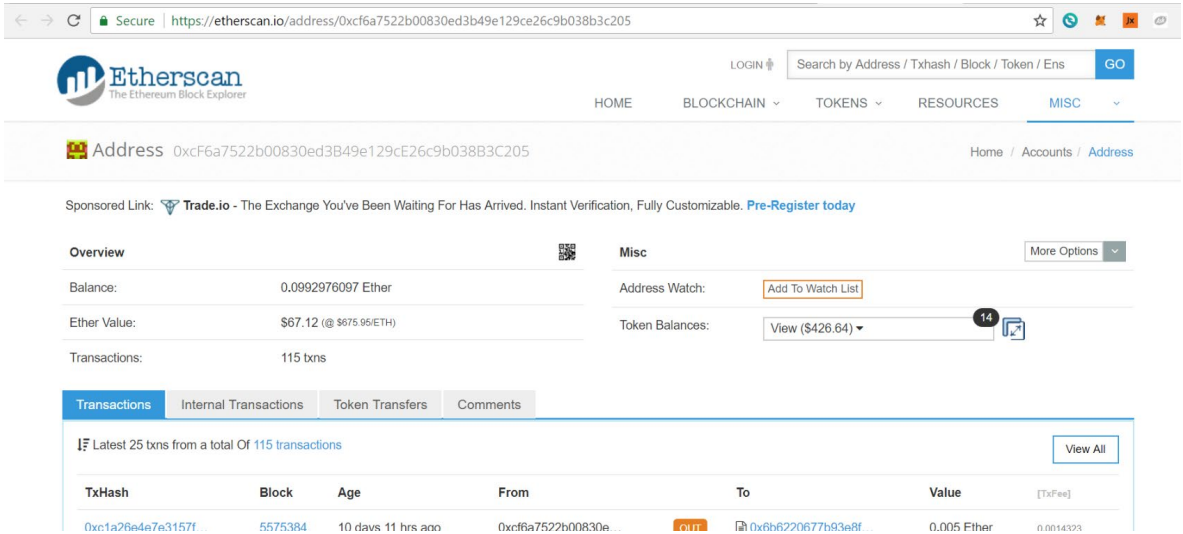
Tokens create private economies

Future:

Standards
Scalability
Interoperability
Reliable Exchanges
Native Assets
Token Types
New Economic Models
Easy Dapps
Consumer Applications

Ethereum

“Ethereum is a decentralized platform that runs smart contracts: applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third-party **interference. These apps run on a custom built blockchain, an enormously powerful shared global infrastructure that can move value around and represent the ownership of property.”**



GAS

https://media.consensys.net/a-guide-to-gas-12b40d03605d

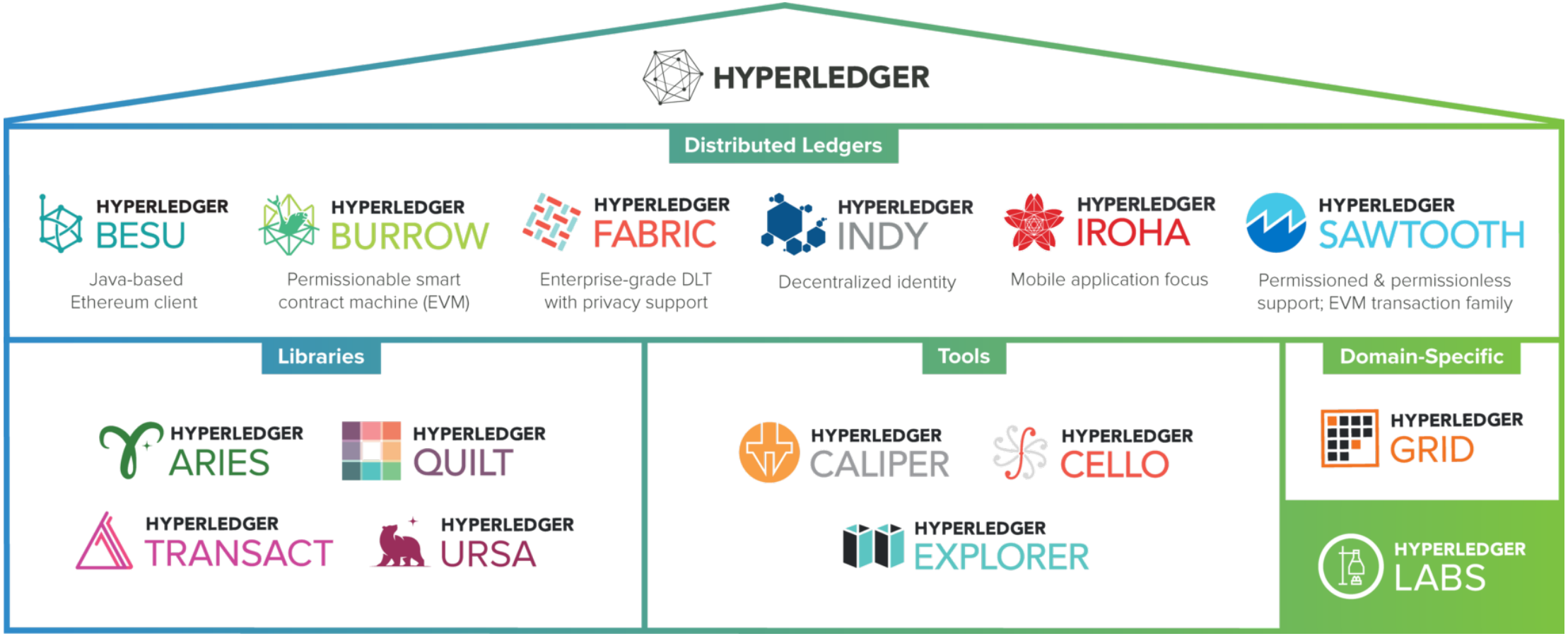
- "Gas" is the lifeblood of the Ethereum ecosystem, there is no other way of putting that. Gas is a unit that measures the amount of computational effort that it will take to execute certain operations.
- Every single operation that takes part in Ethereum, be it a simple transaction, or a smart contract, or even an ICO takes some amount of gas. Gas is what is used to calculate the number of fees that need to be paid to the network in order to execute an operation.
- When someone submits a smart contract, it has a pre-determined gas value. When the contract is executed each and every step of the contract requires a certain amount of gas to execute.

Digital Promises
Smart Contracts

- Because Ethereum has its own currency, it lets us write smart contracts. You program business logic into a smart contract and let it execute automatically. Now the system will make sure that only allowed actions can take place, whether it’s escrow, payment for services, scheduling an appointment, heating a building, landing an airplane, checking out at the grocery store, harvesting potatoes, etc. Renting or using a shared car in the future will involve no human contact. No need to check in at the hotel - just go straight to your room. Software makes most of the decisions using sensors and event-driven data feeds as input.

- **History of smart contracts**
- Computer scientist Nick Szabo In 1993, originally designed for a vending machine.
- The object of the contract was a physical good — a snack.
- **Basics of operation**
- The modern use of smart contract was initially started by Bitcoin. The idea was to enable transfer of information from one person to another. The information itself was rather simplistic and included only few pieces of data: the sender, the number of bitcoins being sent, and the recipient.
- Nodes of the Bitcoin network would only approve this transfer of information if certain pre-coded conditions were met.
- **The Ethereum network took this idea and extended it further.** It is not restricted to act merely as a decentralized register of transactions but can include whole pieces of computer code which is executed upon meeting certain, predetermined conditions.
- This platform was created to enable developers to create additional programs and applications with their own internal logic.
- And since everyone can create their own smart contract, there is little to restrict what it can be used for: commercial transactions, blockchain based applications or currencies.

The Greenhouse



Hyperledger Momentum

3.5

Years since launch

4

Libraries

4

Tools

5

Distributed Ledgers

3

1.0+ Production Releases

275+

Members
(50+ in AsiaPac)

14

Active Community Working Groups & Special Interest Groups

175+

Meetups Worldwide
(75+ countries)

62K+

Meetup Participants

2,000+

Media Clips Per Month

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Hyperledger has a modular approach to hosting projects. Think of Hyperledger as a **greenhouse** growing and sustaining business blockchain projects from seed to fruition. The Linux Foundation and Hyperledger provide the infrastructure for open development to occur among a diverse and thriving community.

Major Project Releases

The Alpha release of Hyperledger Fabric v2.0 allows users to try out the new support for decentralized governance of smart contracts.

The Iroha 1.0 release happened in May and included YAC Consensus, Fully Operational Multisignature, updated client libraries and Windows support

Our Newest Projects

HYPERLEDGER ARIES

Infrastructure for blockchain-rooted, peer-to-peer interactions. Includes a shared cryptographic wallet (the secure storage tech, not a UI) + a protocol for off-ledger interaction between clients.

HYPERLEDGER TRANSACT

Hyperledger Transact will reduce the development effort for writing distributed ledger software by providing a standard interface for executing smart contracts that is separate from the distributed ledger implementation. A shared software library handles all aspects of scheduling, transaction dispatch, and state management.

Special Interest Groups (SIG)

Newest SIGs:

HYPERLEDGER

Supply Chain Special Interest Group

Focused on the implementation of enterprise-grade solutions utilizing the Hyperledger greenhouse of business blockchain frameworks and tools (launched May)

HYPERLEDGER

Capital Markets Special Interest Group

Focused on studying how Hyperledger DLTs interact with Capital Markets use cases and exploring architecture, identity and performance related considerations (launched July)

Current SIG Proposals:

- **Education Architecture**

For more information or to get involved, please visit: https://wiki.hyperledger.org/display/HYP/Special+Interest+Groups

New Technical Working Groups

HYPERLEDGER

Diversity, Civility and Inclusion Working Group

This group is focused on measuring and improving the health of our open source community. We seek to provide constructive recommendations to the TSC, projects, and working groups. All are welcome to join us and help Hyperledger continue to grow in a diverse, civil, and inclusive way.

For more information or to get involved, please visit: https://wiki.hyperledger.org/display/DCI/

Training and Certifications

THE LINUX FOUNDATION

Technical training courses and professional certifications to get you up-to-speed on Hyperledger with the highest quality training from The Linux Foundation and Hyperledger Training Partners.

- Blockchain: Understanding Its Uses and Implications
- Introduction to Hyperledger Technologies
- Hyperledger Fabric Fundamentals
- Hyperledger Sawtooth Administration
- Hyperledger Fabric Administration

New Professional Certifications!

- **Certified Hyperledger Sawtooth Administrator (CHSA)**
- **Certified Hyperledger Fabric Administrator (CHFA).**
- **Certified Hyperledger Fabric Developer (CHFD) (coming soon Q1 2020!)**

HYPERLEDGER
TRAINING PARTNER

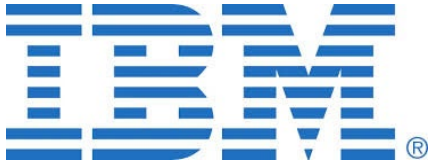
HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Visit: https://www.hyperledger.org/resource

Hyperledger
Now Available Across All Major Clouds

Google Cloud

Microsoft Azure
Tencent 腾讯
Baidu 百度
Alibaba Cloud



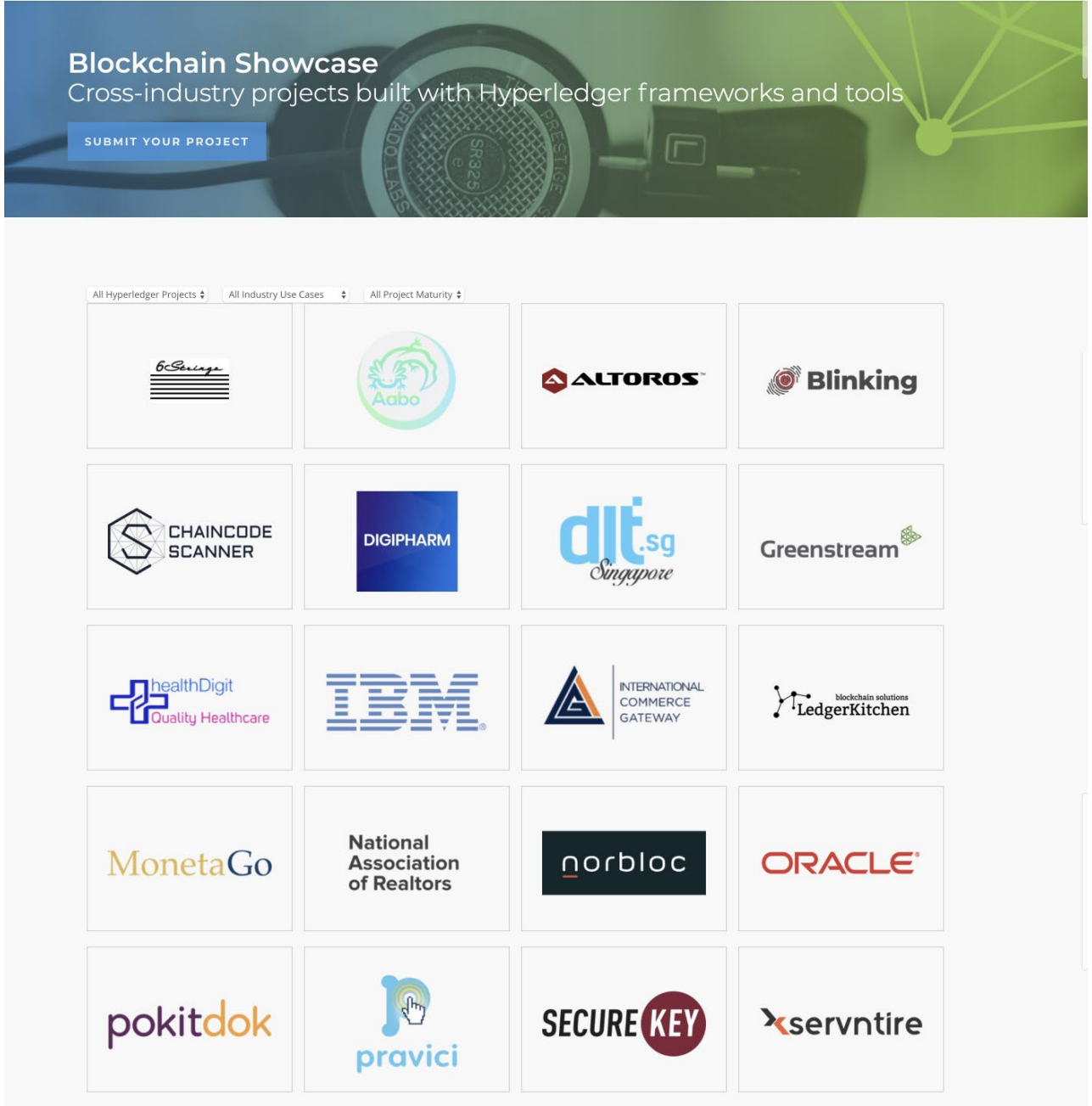
ORACLE

Blockchain Showcase

Cross-industry projects built with Hyperledger frameworks and tools.

65+

Community self submitted projects!



HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

Submit your showcase

Hyperledger Global Forum 2020

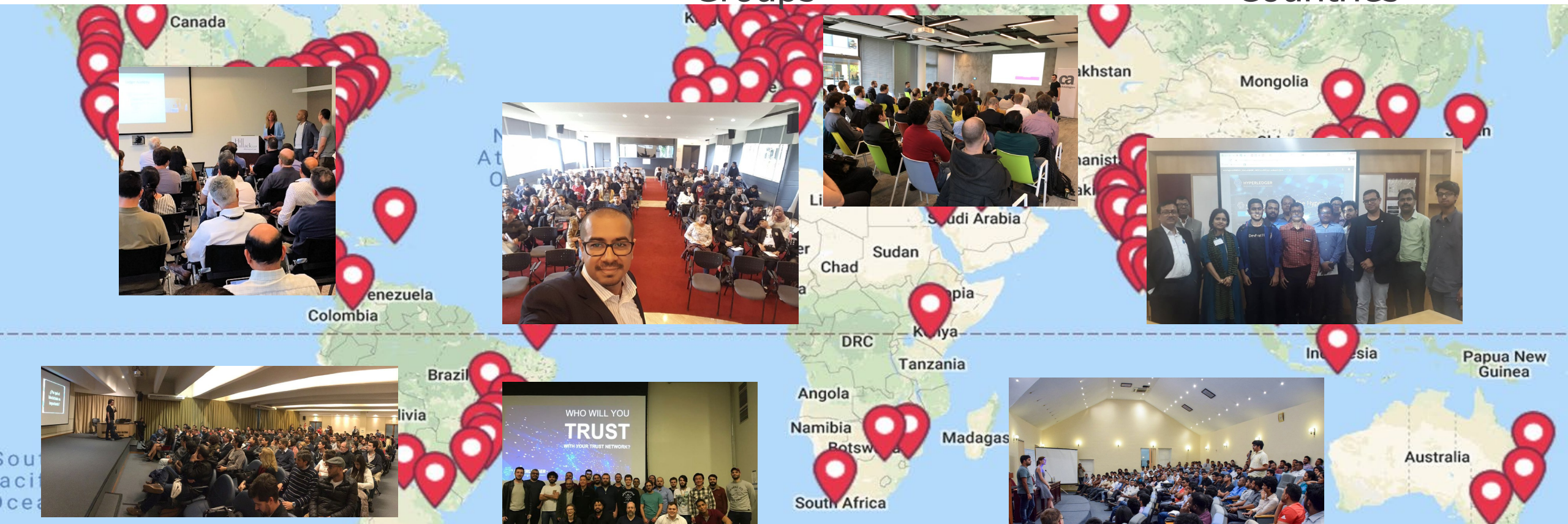
- More than 1,000 users and contributors of Hyperledger projects from across the globe to meet, align, plan and hack together in-person. Phoenix, AZ, March 3-6, 2020
- Registration is now open! individual, academic, Govt rates available.
- We encourage you to submit a talk by Sept 27!
- Please help us promote the event on your channels using #HyperledgerForum

Growing Global Meetup Community

62,000+ Members

175+ Groups

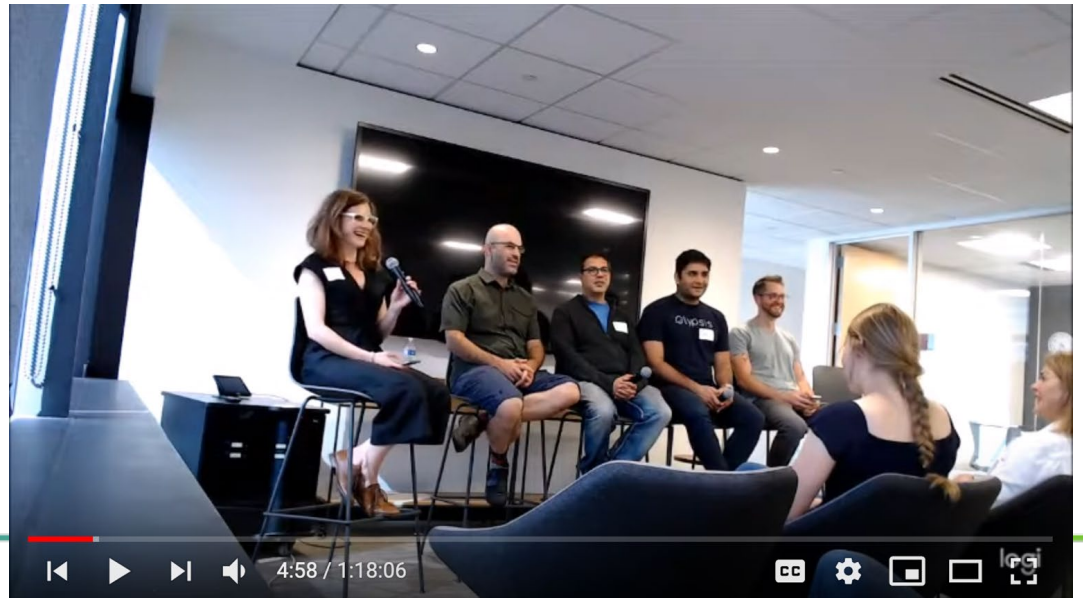
75+ Countries



Meetup Highlights

- India Chapter ran a nation wide meetup that included several local groups across India holding events at the same time and streaming presentations to each location and online. This is a great template for other regional groups to consider doing.

- There are now over 25 recorded talks from Hyperledger meetups around the world on the Hyperledger YouTube channel. Thanks to Hyperledger Seattle for recording and sharing each of their meetups. If you record your meetup and would like it posted, please reach out to meetup@hyperledger.org.



Hyperledger Bootcamps

- An event where we help get community members up to speed on how to contribute
- For existing community members this is the ideal place to recruit more help for your project, lab, or group
- Bootcamps were held in Hong Kong and São Paulo earlier this year
- The next Bootcamp is in Moscow on October 14 and 15
- If your local community is interested in hosting a Bootcamp, look more about the next steps at:

  https://wiki.hyperledger.org/display/events/Bootcamps

Other Upcoming Events

Hyperledger will be active at the following upcoming events. If you will be attending any of these events, we are looking forward to meeting you there.

Conference	Focus	Location	Dates
Sibos 2019	FinTech	London	Sept. 23-26
Devcon	OSS	Osaka, Japan	Oct 8-11
All Things Open	OSS	Raleigh, NC	Oct. 13-15
Singapore FinTech	APAC FinTech	Singapore	Nov. 11-15
Blockchain World Series NA	Enterprise Blockchain	Santa Clara	Nov. 12 - 13
Open FinTech	OSS, DLT	New York	Dec. 9
Mobile World Congress	Telecom, OS	Barcelona	Feb. 24 - 27

Hyperledger embraces the full spectrum of industry use cases, especially enterprise scenarios with widely varied requirements for decentralization, trust, continuity and confirmation times. Each represents a potentially unique optimization point for the technology.

HYPERLEDGER

BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

"Hyperledger immediately established itself as the gold standard for corporate blockchain projects." - Forbes

Half of the 'Forbes Blockchain 50' is building on Hyperledger

Allianz, amazon, BBVA, BNP PARIBAS, Broadridge, Cargill, COMCAST, CVSHealth, gsf golden state foods, Hewlett Packard Enterprise, IBM, ING, intel, MAERSK, Microsoft, Nasdaq, Nestlé, NORTHERN TRUST, PNCBANK, Santander, SAP, SEAGATE, SIEMENS, StateFarm, UBS, VISA, Walmart

https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/

Forbes

BLOCKCHAIN 50

EDITOR'S PICK | 87,461 views | Apr 16, 2019, 06:00am

Blockchain 50: Billion Dollar Babies

Michael del Castillo Forbes Staff
Crypto & Blockchain
I cover enterprise adoption of blockchain and cryptocurrency.

Cryptocurrencies may be in the depths of winter, but it's early spring for business applications using the technology underlying bitcoin. Take the case o financial record keeping behemoth Depository Trust & Clearing Corp, otherwi known as "DTCC." It's responsible for keeping the books on 90 million transa day, representing most of the world's $48 trillion in securities —from stocks a

So who's using what?

Of the Forbes Blockchain 50:

- 23 HL Fabric
  - +5 IBM Blockchain
  - +2 DTCC & Google
  - +1 Oracle Blockchain
  - +1 Samsung Nexledger
- 21 (Public?) Ethereum
- 13 Corda
- 12 Quorum
- 3 HL Indy
- 3 HL Sawtooth

https://www.forbes.com/sites/michaeldelcastillo/2019/04/16/blockchain-50-billion-dollar-babies/

Newest Cross Industry Case Studies

Change Healthcare using Hyperledger Fabric to improve claims lifecycle throughput and transparency
Industry: Healthcare
Topics: Hyperledger Fabric, Healthcare, Blockchain
Project(s): Hyperledger Fabric

When Hyperledger Sawtooth Met Kubernetes – Simplifying Enterprise Blockchain Adoption
Industry: Blockchain, Cloud Computing, Technology, IT Services
Topics: Hyperledger Sawtooth, Kubernetes, Blockchain, Containers, Cloud computing
Project(s): Hyperledger Sawtooth

BC aims to cut government red tape with Hyperledger Indy
Industry: Blockchain, Tech, Small Business, Government
Topics: Blockchain, Open Source, Digital Identity, Self Sovereign Identity, Bureaucracy, Small Businesses, Business Development, Government
Project(s): Hyperledger Indy

Kiva: Implementing SSI and a privacy-first credit bureau for Sierra Leone

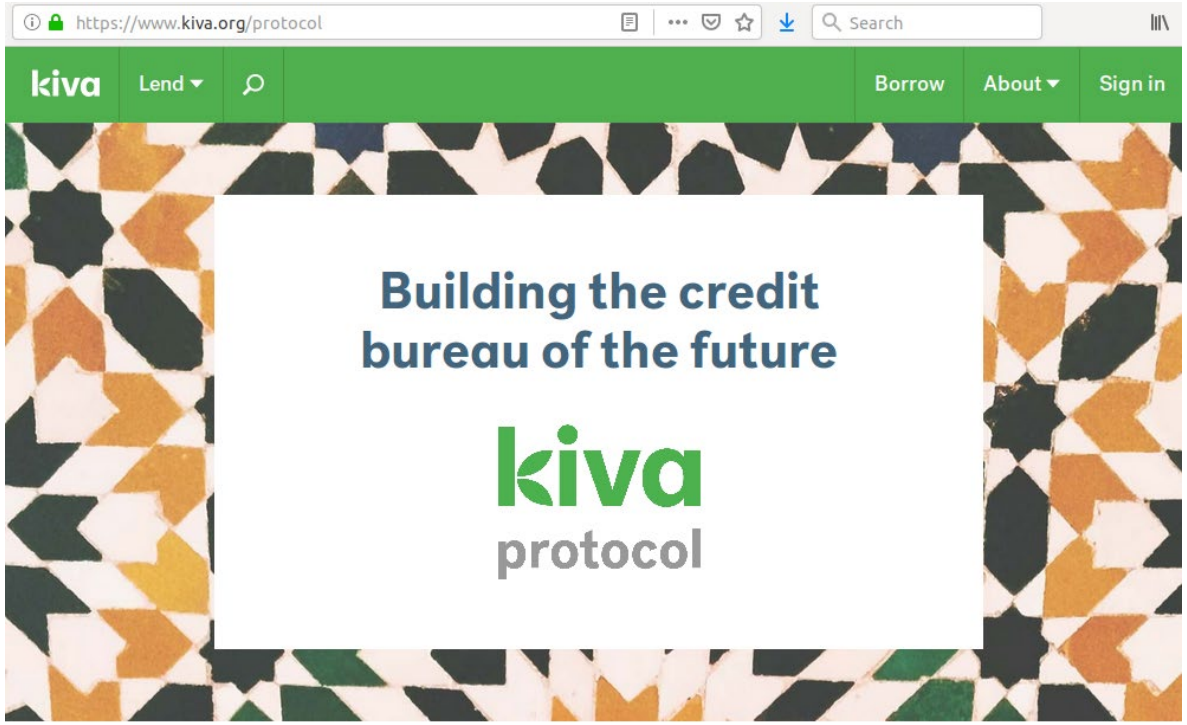
Challenge:

1. There is no effective digital identity system or credit bureau for SL's 7.5M citizens
2. As a result, Kiva's lending rates are 30%, much higher than in other countries and a blocker to financial participation.

Solution:

1. 2019-Q2 NCRA (SL government ID agency) will issue credentials on a Hyperledger-Indy based network.
2. 2019-Q4 BSL (central bank) will use Hyperledger Fabric for a shared, decentralized credit reporting bureau.

Partnership between Kiva, SL government, UNDP and UNCDF.



Introducing Kiva Protocol, an exciting new initiative to give unbanked people digital identity and secure control over their own credit information.

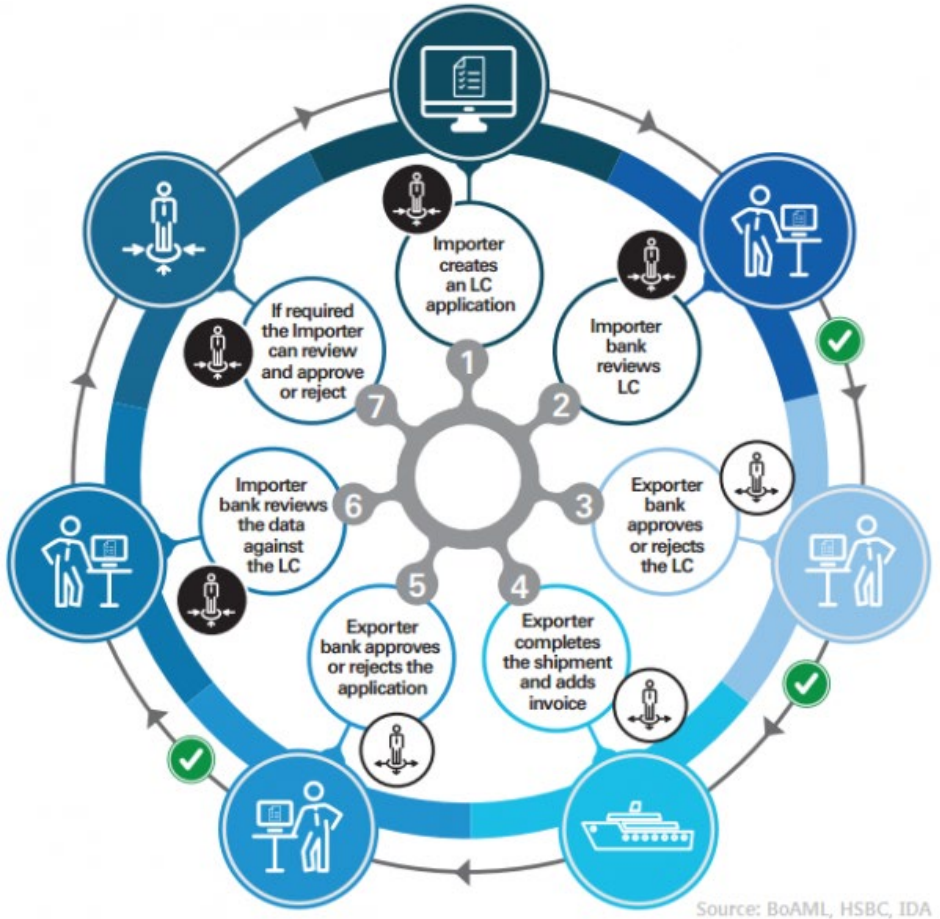
Kiva, Sierra Leone and U.N. agencies announced the first implementation of the Kiva Protocol on Sept. 27, 2018, at the U.N. General Assembly. The Kiva Protocol will be used to create a nationwide digital identification system designed to help the country's 7 million citizens access the financial services they need to improve their lives.

Social Impact SIG presentation: https://wiki.hyperledger.org/display/SISIG/2019-08-06+Meeting+notes

Trade Finance: we.trade

we.trade
more trust. more trade.

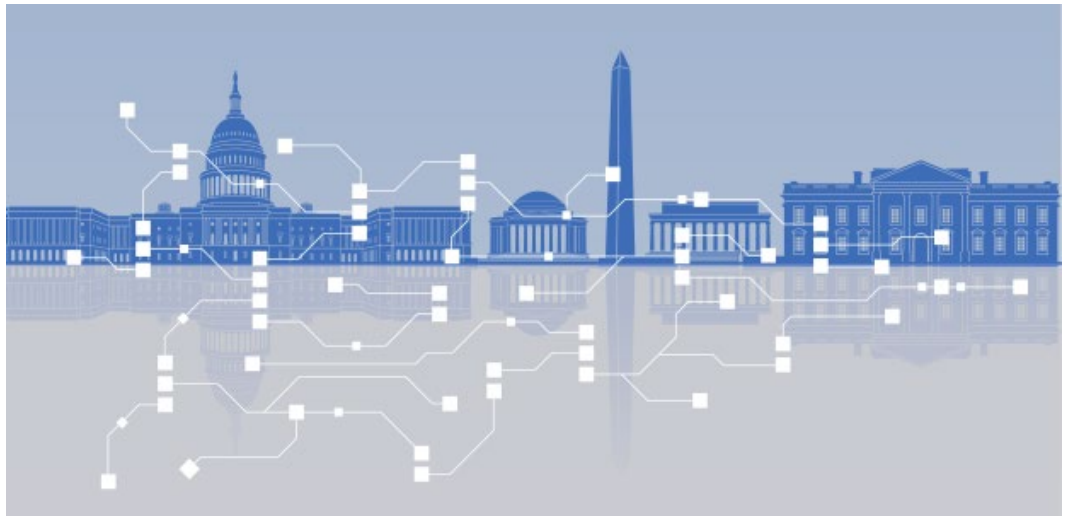
- we.trade is a blockchain-based international trading system for a consortium of major world banks including: **HSBC, Deutsche Bank, KBC, Natixis, Rabobank, Société Générale, Santander, UniCredit and Nordea**
- SMEs generate 85% of employment growth in Europe, but only ~50% of them have access to formal credit.
- Went into production July 2018 conducting **seven live trade transactions by ten companies via four partner banks**
- Enables accurate trading position information, order to settlement control, risk coverage, track and trace options
- **Near-real time exchange of information** on a **secure** platform that digitizes transactional financing
- Continual business and **compliance readiness** in any relevant regulatory environment
- **Scalability** that allows for rapid international expansion as business, regulatory, and security opportunities converge



https://we-trade.com/

Government Procurement: GSA

- Today's procurement processes take upto 35 days even when the requirements are very clear.
- The General Services Administration designed a FASt Lane process for IT Schedule 70 contracts.
- Blockchain-based software layer over the agency's existing infrastructure that aims to make the GSA Schedules **review process transparent and automate financial reviews and processes, creating savings in fixed costs.**
- Vendors' financial information is analyzed through a "smart contract" that compares their financial ratios to the average of companies with the same NAICS code.
- Agency estimates that the blockchain pilot will save a financial analyst 10 to 15 days when it comes to reviewing each proposal. Lowering the OpEx costs by 80-90%.



GSA

Digital Identity: The OrgBook

VON
Verifiable Organizations Network

- The OrgBook serves as a **trusted digital network of verifiable data** about organizations which is globally connected, **interoperable, secure, and easy to join**
- Why? So business/government can quickly access evidence of that a potential partner is legally incorporated
- The new enrollment experience is **more convenient** and use an open global blockchain registry
- Reduced single point of failure for database, **reduced fraud** from counterfeit IDs, reduces bottlenecks, and **improves privacy** which a complex verification system can expose
- As more businesses establish their Self-Sovereign Identity, more Services will become Self-Sovereign Identity-aware
- **Live**, public, **globally accessible network** using the Sovrin Provisional Network built on Hyperledger Indy.

HYPERLEDGER
BLOCKCHAIN TECHNOLOGIES FOR BUSINESS

https://www.hyperledger.org/resources/publications/orgbook-case-study

Project	HYPERLEDGER FABRIC
Status	ACTIVE
CII Badge	cii best practices passing
Description	Distributed ledger in Golang

Hyperledger Fabric is an enterprise-grade permissioned distributed ledger framework for developing solutions and applications.
Its modular and versatile design satisfies a broad range of industry use cases.
It offers a unique approach to consensus that enables performance at scale while preserving privacy.
Fabric v1.4.3 is the current long-term support (LTS) release, which includes RAFT consensus.
2.0-alpha was released in April with support for decentralized governance of smart contracts.
200+ devs across 100+ companies contributing.
Hundreds of pilot and production networks deployed.

Learn more at: https://wiki.hyperledger.org/display/fabric/Hyperledger+Fabric

Project	HYPERLEDGER SAWTOOTH
Status	ACTIVE
CII Badge	cii best practices passing
Description	Distributed ledger with Multi-Language Support

A modular platform for building, deploying, and running distributed ledgers. Hyperledger Sawtooth includes a novel consensus algorithm, Proof of Elapsed Time (PoET), which targets large distributed validator populations with minimal resource consumption. Hyperledger's second project, released as 1.0 in January 2018 and 1.1 in Dec 2018. Supports Solidity/EVM smart contracts by linking with HL Burrow.

Learn more at: https://wiki.hyperledger.org/display/sawtooth/Hyperledger+Sawtooth

Project	HYPERLEDGER INDY
Status	ACTIVE
CII Badge	cii best practices passing
Description	Distributed ledger purpose-built for decentralized identity

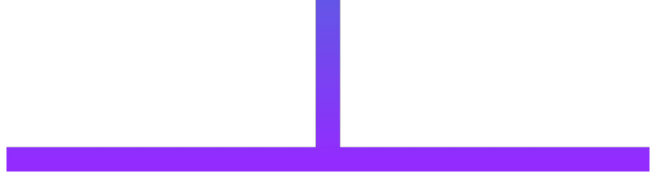
Tools, libraries, and reusable components for providing digital identities rooted on blockchains or other distributed ledgers so that they are interoperable across administrative domains, applications, and any other silo. Utilizes zero-knowledge proofs to provide verifiable claims which can be used to prove something about the identity without providing access to the underlying data

Learn more at: https://wiki.hyperledger.org/display/indy/Hyperledger+Indy

Project	HYPERLEDGER BURROW
Status	INCUBATION
CII Badge	cii best practices in progress 82%
Description	Permissioned Ethereum smart-contract blockchain

Burrow provides a modular blockchain client with a permissioned smart contract interpreter built in part to the specification of the Ethereum Virtual Machine (EVM). It is the only Apache-licensed EVM. Uses Tendermint as its default consensus mechanism, but has also been ported to Fabric and Sawtooth.

Learn more at: https://wiki.hyperledger.org/display/burrow/Hyperledger+Burrow



Project	HYPERLEDGER IROHA
Status	ACTIVE
CII Badge	cii best practices passing
Description	Distributed ledger in C++

1.0 release in May. A business blockchain framework designed to be simple and easy to incorporate into infrastructural projects requiring distributed ledger technology. Written in C++ incorporating unique chain-based Byzantine Fault Tolerant consensus. Mobile SDKs. Multisig support for transactions.

Learn more at: https://wiki.hyperledger.org/display/iroha/Hyperledger+Iroha

Thank You