Enterprise Blockchain

-- Alternative Consensus

LING Zong, Ph. D.
Senior Software Engineer / Scientist
IBM Almaden Research Center
San Jose, California, U.S.A.

替代的共识

Alternative Consensus

-Alternative consensus: other methods of verification other than **proof of work** (**PoW**).

-Created after downsides of PoW discovered:

- Massive electricity devouring
- Total performance in 2012 surpassed the most productive supercomputer

-替代共识:除工作证明(PoW)外的其他验证方法。
-在发现PoW的缺点后创建:
· 大规模电力吞噬
· 2012年的总性能超过了生产效率最高的超级计算机

权益证明

Proof of Stake (PoS)

· PoS需要用户提供货币的所有权股份，即点点币。
· 节省能源与工作证明方法，降低计算过程和电力需求。
· 股份货币提供信任网络和块的创建的抵押品。
· 赌注越高，抵押品就越高

- PoS requires users to provide ownership stake in currency, i.e. PeerCoin.
- Saves energy vs. proof of work methodology, lowering computing processes and power required.
- Stake in currency provides “collateral” of trust in network and block creation.
- Higher the stake, higher the collateral.

对于工作证明，挖掘一个块的概率取决于挖掘器所做的工作(例如，CPU/GPU检查哈希值的周期)。
有了股权证明，比较的资源是一个矿工所持有的比特币数量——一个持有1%比特币的人可以开采1%的“股权证明块”。

- With Proof of Work, the probability of mining a block depends on the work done by the miner (e.g. CPU/GPU cycles spent checking hashes).
- With Proof of Stake, the resource that's compared is the amount of Bitcoin a miner holds - someone holding 1% of the Bitcoin can mine 1% of the "Proof of Stake blocks".

--https://en.bitcoin.it/wiki/Proof_of_Stake

活动证明

Proof of Activity (PoA)

· 是PoS和PoW的混合体。作为块创建检查点的PoW机制。
· 块是通过PoW方法生成的，并带有验证块的PoS-type签名。
· 只是个理论，没什么进展

- Hybrid between PoS and PoW. PoW mechanisms used as checkpoints for block creation.
- Blocks are generated through PoW methods, with PoS-type signatures to certify blocks.
- Just a theory, little development.

活动证明增加了针对51%攻击的第二道防线，因为攻击者理论上需要同时拥有网络总采矿能力的51%或更多，以及在网络中下注的51%或更多的金币，才能成功实施攻击。

Proof of activity adds a second line of defense against 51% attacks because an attacker would theoretically need to have both 51% or more of the network's total mining power and 51% or more of the coins staked in the network in order to successfully pull off the attack.

燃烧证明

Proof of Burn (PoB)

· 燃烧证明是一种分配共识的方法，是工作证明和权益证明的替代方法。它还可以用于从一种加密货币引导到另一种加密货币。
· 他们的想法是，矿商应该拿出证据，证明他们烧毁了一些硬币——也就是说，把它们送到一个可核实的无法使用的地址。从他们个人的角度来看，这是昂贵的，就像工作证明;但它只消耗燃烧后的基础资产而非任何资源。到目前为止，所有燃烧加密货币的证据都是通过燃烧挖掘工作证明的加密货币来工作的，因此，最终稀缺的来源仍然是挖掘工作证明的“ 燃料 ”。
· 有许多可能的燃烧证据的变种。
· 通过焚烧硬币来赢得开矿机会的彩票系统。
· 存入的数字硬币不会燃烧，直到接受块奖励。

- **Proof of burn** is a method for distributed consensus and an alternative to Proof of Work and Proof of Stake. It can also be used for bootstrapping one cryptocurrency off of another.

- The idea is that miners should show proof that they ***burned*** some coins - that is, sent them to a verifiably unspendable address. This is expensive from their individual point of view, just like proof of work; but it consumes no resources other than the burned underlying asset. To date, all proof of burn cryptocurrencies work by burning proof-of-work-mined cryptocurrencies, so the ultimate source of scarcity remains the proof-of-work-mined "fuel".

- There are likely many possible variants of proof of burn. (https://en.bitcoin.it/wiki/Proof_of_burn)

- Lottery system where coins are burned to win chance of mining a block.
- Digital coins deposited do not burn until accepted for block rewards.

· 消逝时间证明(POET)是一种区块链网络共识机制算法
防止资源的高利用率和能源的高消耗
通过遵循公平的抽签制度，使整个过程更有效率。
· 网络中的每个参与节点都需要等待一个随机选择的时间段，第一个完成指定等待时间的节点赢得新区块。
· 区块链网络中的每个节点都会生成一个随机的等待时间，并在指定的时间内进入睡眠状态。
· 第一个被唤醒的，也就是等待时间最短的那个，会被唤醒并向区块链提交一个新的块，向整个对等网络广播必要的信息
· 然后为发现下一个区块重复相同的过程。

消逝时间证明

Proof of Elapsed Time (Cryptocurrency)

- Proof of elapsed time (POET) is a blockchain network consensus mechanism algorithm
  - prevents high resource utilization and high energy consumption
  - keeps the process more efficient by following a fair lottery system.

- Each participating node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block.
- Each node in the blockchain network generates a random wait time and goes to sleep for that specified duration.
- The one to wake up first – that is, the one with the shortest wait time – wakes up and commits a new block to the blockchain, broadcasting the necessary information to the whole peer network
- The same process then repeats for the discovery of the next block.

https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp

Solo

· 单人采矿是一个单独的过程，矿工完全完成他的采矿作业，没有任何帮手。
· 这个过程主要是单独完成的，不需要加入一个池。
· 挖掘和生成这些块的方式与挖掘人员的信用完成的任务有关

- Solo mining is a solo process where the miner completely does his task of mining operations without any helping hand.
- This process is mainly done **alone without joining a pool**.
- These blocks are mined and generated in a way to the task completed by the miner’s credit.

https://www.blockchain-council.org/blockchain/solo-mining-works/

动物园管理员

ZooKeeper

·ZooKeeper是一个集中的服务，用于维护配置信息、命名、提供分布式同步和提供组服务。所有这些类型的服务都被分布式应用程序以某种形式使用。
·每次实现它们时，都要做大量工作来修复不可避免的bug和竞争条件。由于实现这些类型的服务很困难，应用程序最初通常忽略它们，这使得它们在出现更改时很脆弱，难以管理。即使正确执行，这些服务的不同实现也会在部署应用程序时导致管理复杂性。
·ZooKeeper的目标是将这些不同服务的本质提炼为一个非常简单的接口，从而形成一个集中式的协调服务。服务本身是分布式的，而且高度可靠。
·共识、组管理和到场协议将由服务实现，这样应用程序就不需要自己实现它们。这些应用的具体用途将包括ZooKeeper的具体组件和应用的具体约定的混合物。ZooKeeper Recipes展示了如何使用这个简单的服务来构建功能强大得多的抽象。

- ZooKeeper is a centralized service for maintaining configuration information, naming, providing distributed synchronization, and providing group services. All of these kinds of services are used in some form or another by distributed applications.
- Each time they are implemented there is a lot of work that goes into fixing the bugs and race conditions that are inevitable. Because of the difficulty of implementing these kinds of services, applications initially usually skimp on them ,which make them brittle in the presence of change and difficult to manage. Even when done correctly, different implementations of these services lead to management complexity when the applications are deployed.
- ZooKeeper aims at distilling the essence of these different services into a very simple interface to a centralized coordination service. The service itself is distributed and highly reliable.
- Consensus, group management, and presence protocols will be implemented by the service so that the applications do not need to implement them on their own. Application specific uses of these will consist of a mixture of specific components of Zoo Keeper and application specific conventions. ZooKeeper Recipes shows how this simple service can be used to build much more powerful abstractions.

https://cwiki.apache.org/confluence/display/ZOOKEEPER/Index/

实用拜占庭容错

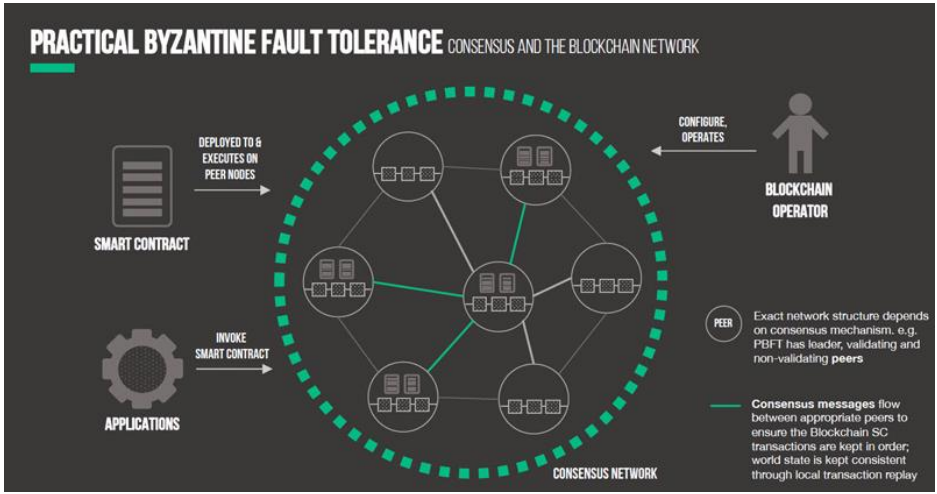
Practical Byzantine Fault Tolerance(PBFT)

· PBFT模型主要侧重于提供一个实用的错综复杂的状态机复制,容忍拜占庭错误(恶意节点)通过假设存在独立节点故障和由特定的独立节点传播的操纵消息
· 该算法被设计为在异步系统中工作，并被优化为高性能，具有令人印象深刻的运行时开销和延迟仅略有增加

- The PBFT model primarily focuses on providing a practical Byzantine state machine replication that tolerates Byzantine faults (malicious nodes) through an assumption that there are independent node failures and manipulated messages propagated by specific, independent nodes.
- The algorithm is designed to work in asynchronous systems and is optimized to be high-performance with an impressive overhead runtime and only a slight increase in latency.

· 本质上，PBFT模型中的所有节点都是按顺序排列的，其中一个节点是主节点(leader)，其他节点称为备份节点。
· 系统内的所有节点相互通信，其目标是让所有诚实的节点通过多数方式就系统的状态达成一致。
· 节点之间的通信非常频繁，不仅需要证明消息来自特定的对等节点，还需要验证消息在传输过程中没有被修改。

- Essentially, all of the nodes in the PBFT model are ordered in a sequence with one node being the primary node (leader) and the others referred to as the backup nodes.
- All of the nodes within the system communicate with each other and the goal is for all of the honest nodes to come to an agreement of the state of the system through a majority.
- Nodes communicate with each other heavily, and not only have to prove that messages came from a specific peer node, but also need to verify that the message was not modified during transmission.



https://blockonomi.com/practical-byzantine-fault-tolerance/

拜占庭将军问题

Byzantine Generals Problem

背景:
-全体将军一致决定。叛国将领可以破坏计划，也可以故意发出误传。
-如果有一个平局，最终(叛国)将军可以发送两个不同的信息。
-物理分离。
-(Null)或不响应，可以有预定义值(撤退)。
-将军是计算机，信使是数字通信系统。

Background:

-Consensus decision made by all generals. Traitorous generals can sabotage plan, also send out purposeful miscommunication.

-If there’s a tie, the final (traitorous) general can send two separate messages.

-Physical separation.

-(Null), or no response, can have predefined value (retreat).

-**Generals are computers, messengers are digital communication systems.**

Byzantine Fault Tolerance

技术细节:
-不可能解决，如果1/3或更多的将军是叛国。
-在容错计算机系统中最困难的故障模式。不是故障停止机制。
-“真理”的方向随着网络增长，越来越难反对(Satoshi白皮书:最后一部分)。
-适用于比特币中的hashcash机制。

Mechanics:

-Impossible to solve if ⅓ or more of generals are traitorous.

-Most difficult of failure modes in fault-tolerant computer systems. Not a fail-stop mechanism.

-Direction of “truth” as network grows → more difficult to oppose (Satoshi white paper: final section).

-Applies to hashcash mechanism used in bitcoin.

Alternative Consensus

波纹：
-支付协议，使用菲亚特货币和波纹货币(XRP)进行交易。
-金融机构与做市商之间的支付基础设施。
-波纹信托系统，利用内部分类帐。所有的资产都以债务的形式持有。

Ripple:

-Payment protocol, trading with fiat currency and Ripple currency (XRP).

-Infrastructure for payments between financial institutions and “market makers”.

-Rippled trust system, makes use of internal ledger. All assets are held as debt obligations.

Ripple

Ripple让银行对支付世界有了不同的看法

Ripple allows banks to think differently about the payment world.

Let’s watch the video!

How Ripple Works.mp4

Alternative Consensus

恒星币

Stellar

-比Ripple技术更好的支付系统。更多的点对点使用。
-账户存储在总账中，计算机网络创造全球价值交换网络。
-二十三公共可信节点,使用群体片产生涟漪效应。
-二到四秒的一致意见。~ 80%的共识

-Payment system with better technology than Ripple. More peer-to-peer use.

-Accounts stored in ledger, with network of computers creating global value exchange network.

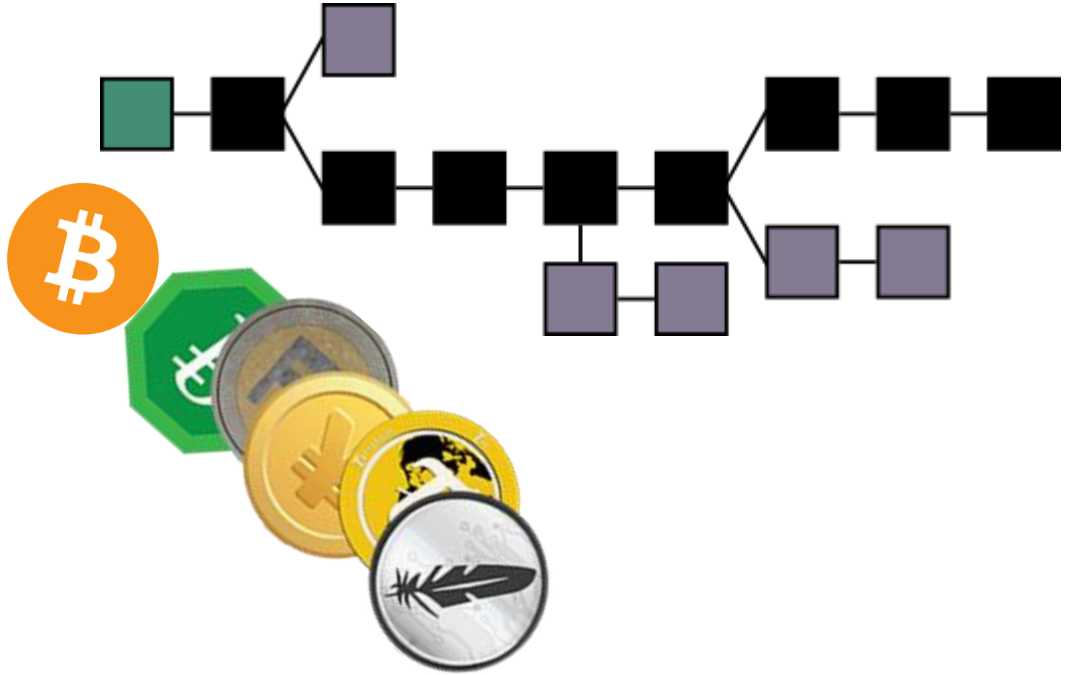
-Selected public trustworthy nodes, use of quorum slices to create ripple effect.

-Two to four second constant consensus. ~80% consensus.

Video: how-money-moves-on-stellar.mp4

“Enterprise” Blockchain

Blockchain



Blockchain 1.0 - Currency

- Bitcoins
- Altcoins
- IoM (Internet of Money)

Blockchain 2.0 - Contracts

- Smart Property
- Smart contracts (Programmable money)
- Dapps, DAOs, DACs, DASs

智能合同是智能合同代码

“Smart contracts as smart contract code”

*“Smart contracts as **smart contract code**”*

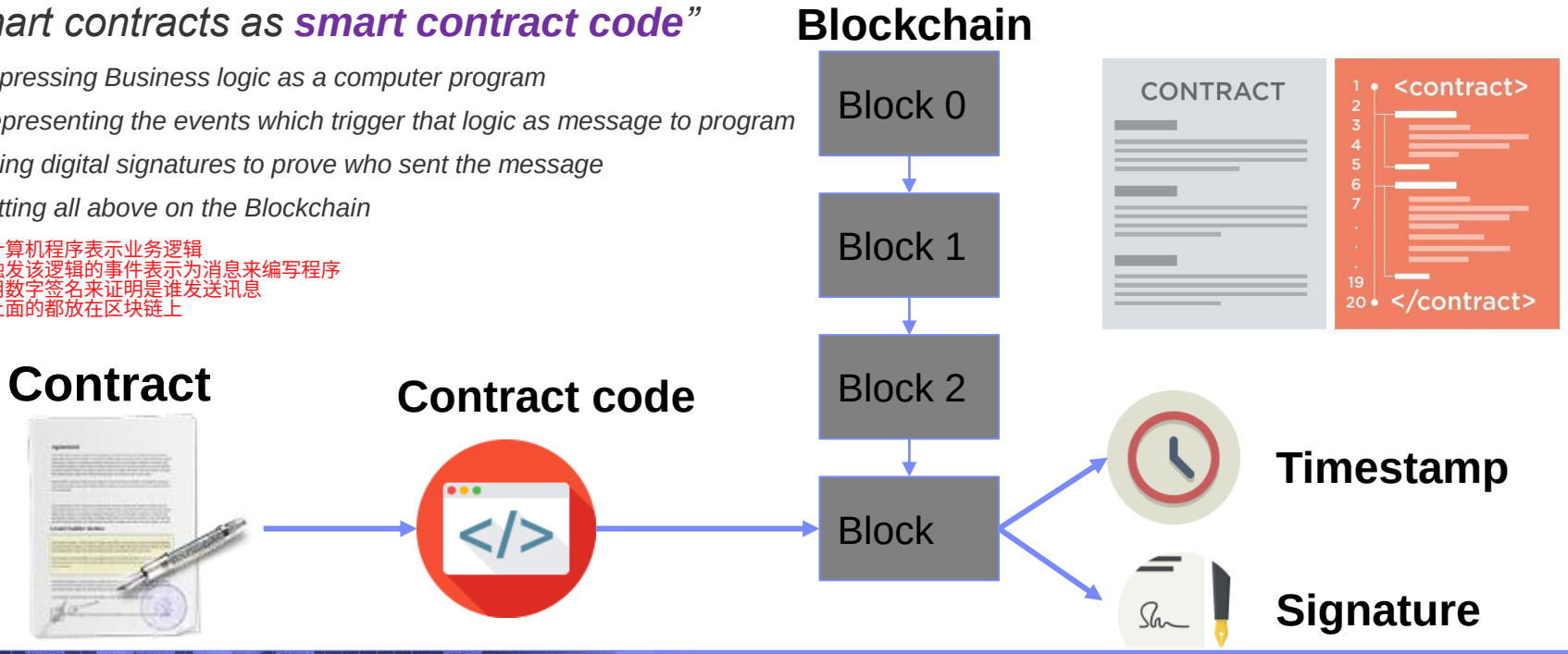
(a) Expressing Business logic as a computer program

(b) Representing the events which trigger that logic as message to program

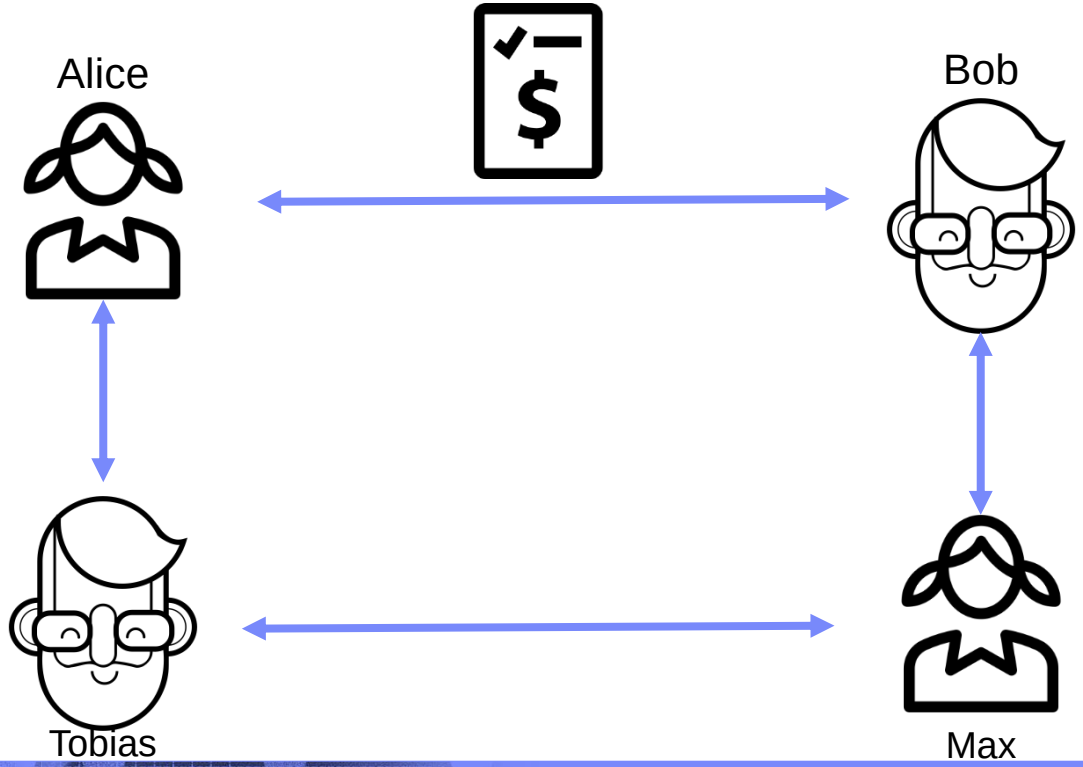
(c) Using digital signatures to prove who sent the message

(d) putting all above on the Blockchain

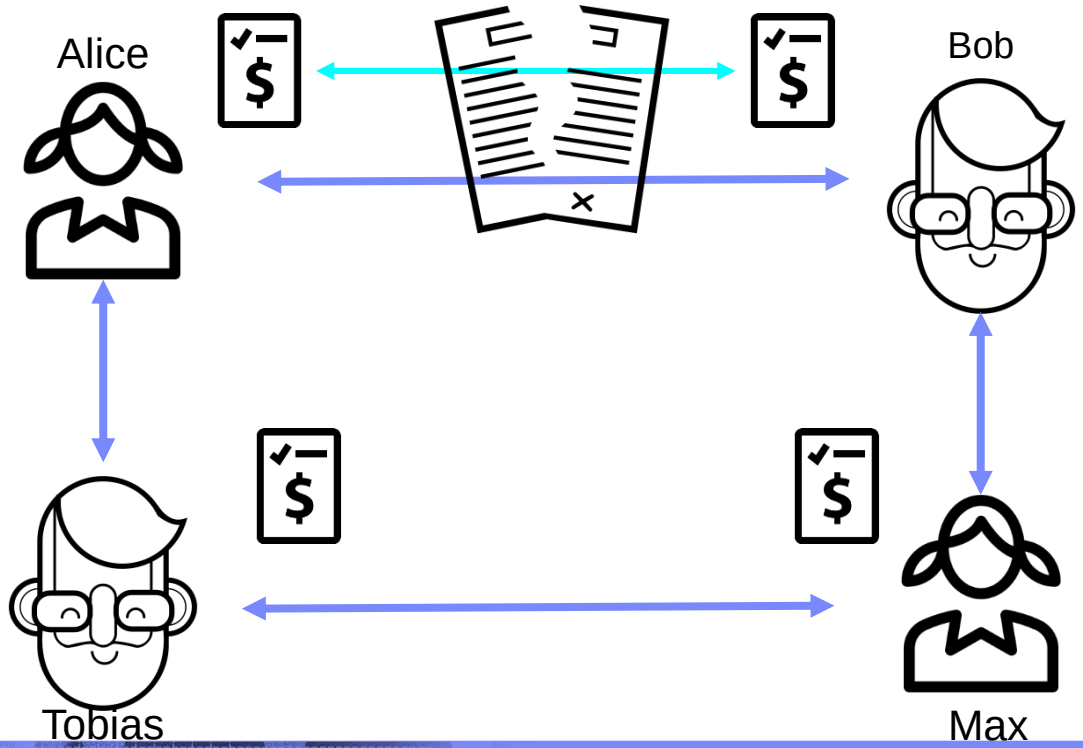
(a)用计算机程序表示业务逻辑
(b)将触发该逻辑的事件表示为消息来编写程序
(c)使用数字签名来证明是谁发送讯息
(d)把上面的都放在区块链上



Smart Contract - Example



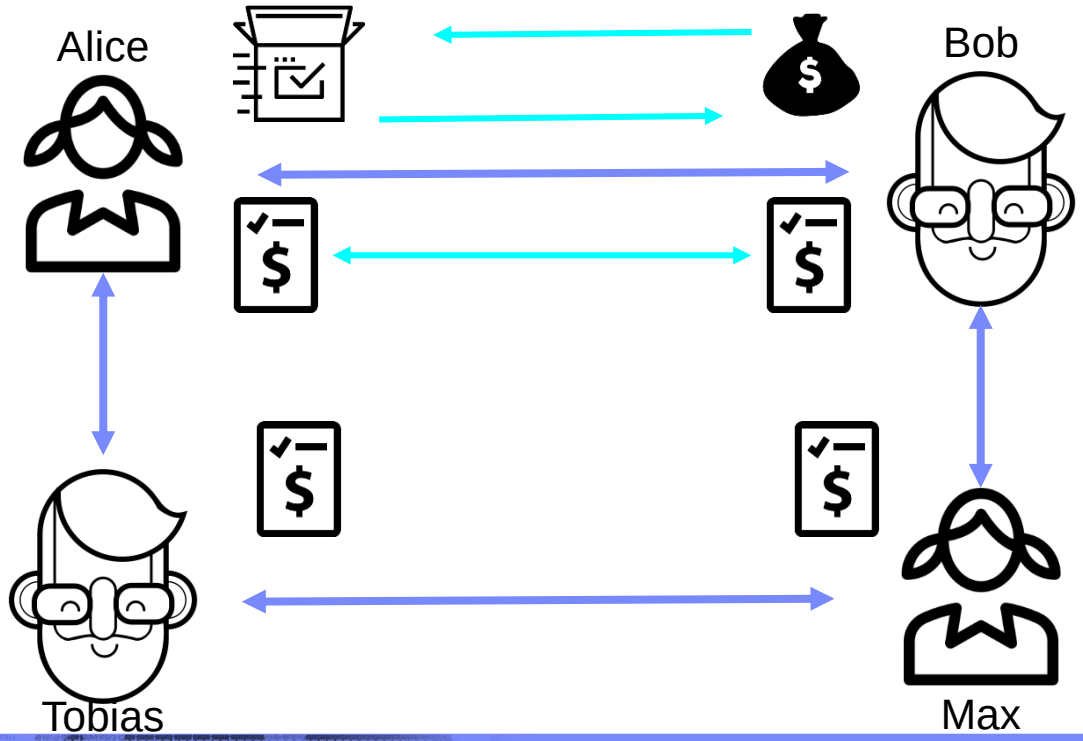
Smart Contract - Example



所以如果Max想改变，整个链都会得到消息。每个人都需要批准

So if Max wants to make a change the whole chain gets a message. Everybody needs to approve.

Smart Contract - Example



Pros / Cons

Pros:

-它是安全的
  •如果有人想更改合同，每个人都会得到警告
-自我执行，
-分布式/分散
- M2M(机器对机器)

- It is secure
    - if somebody wants to change a contract **everybody** gets a warning
- Self executing,
- Distributed/Decentralized
- M2M (Machine to Machine)

Cons:

-链的可伸缩性
-法律合同困难，需要人的解释
-计算能力
-难以更新的智能合同

- Scalability of the chain
- Difficult for legal contracts, which need human interpretation
- Computation power
- Difficult to update a smart contract

Dapps, DAOs, DACs, DASs

· 分散的应用程序(Dapps)
-这是一个运行在分布式网络上的应用程序，参与者信息被安全保护，操作执行分散跨网络节点。
· 分权自治组织&公司(DAOs和DACs)
-在DAO/DAC中，智能合同作为运行在区块链上的代理，根据事件和变化的条件执行预先指定或预先批准的任务范围。
- Storj，智能合同操作，分散文件存储
· 分权自治社会(DASs)
-在未来，这可以是一系列智能合同的DAS，或整个一个自动运行的Dapp、DAOs、DACs生态系统

Decentralized applications (**Dapps**)

- It is an application that runs on a network in a distributed fashion with participant information securely protected and operation execution decentralized across network nodes.

Decentralized Autonomous Organizations & Corporations (**DAOs & DACs**)

- In a DAO/DAC, there are smart contracts as agents running on Blockchains that execute ranges of prespecified or preapproved tasks based on events and changing condition.
- Storj, Smart Contracts operated, decentralized file storage

Decentralized Autonomous Societies (**DASs**)

- In the future this can be a DAS where a fleet of smart contracts, or entire ecosystems of Dapps, DAOs, DACs operating autonomously

DAO - DASH

A decentralized autonomous organization (DAO), sometimes labeled a decentralized autonomous corporation (DAC), is an organization that is run through rules encoded as computer programs called smart contracts. A DAO's financial transaction record and program rules are maintained on a blockchain.

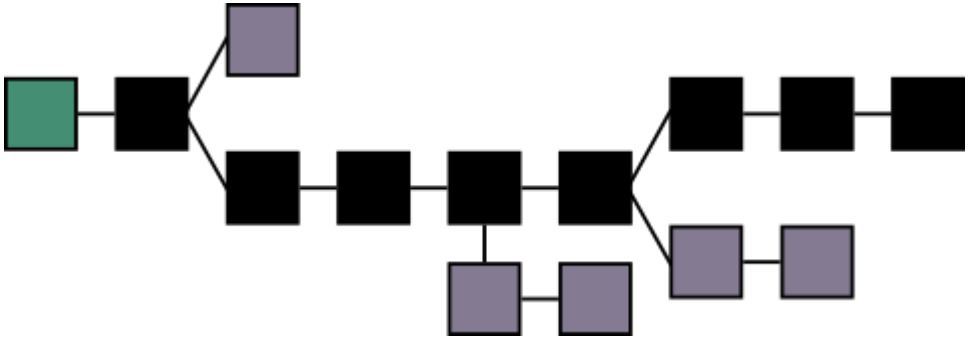
- Dash formerly known as Darkcoin and XCoin, rebranded in 2015
- People who communicate via a network protocol

分散式自治组织(DAO)，有时也被称为分散式自治公司(DAC)，是一种通过被称为智能合同的计算机程序编码的规则运行的组织。DAO的财务交易记录和程序规则在区块链上维护。
·Dash原名Darkcoin XCoin，2015年更名
·人通过网络协议通信
两个原则：
1. 共识
2. 执行
是什么让它如此特别？

Two principles:
1. Consensus
2. Execution

What makes it so special? →

Blockchain



Blockchain 1.0 - Currency
- Bitcoins
- Altcoins
- IoM

Blockchain 2.0 - Contracts
- Smart Property
- Smart contracts (Programmable money)
- Dapps, DAOs, DACs, DASs

司法应用(不限于货币、经济和市场)

Blockchain 3.0 - Justice applications (*Beyond currency, economics and market)*
- New model of organizing (consensus)
- Digital ID Verification
- IP Protection
- Media Management
- Virtual Notary, Bitnotar, Chronobit
- Government and Healthcare

-组织新模式(共识)
-数码身份验证
-知识产权保护
-媒体管理
-虚拟公证人，Bitnotar，Chronobit
-政府和医疗保健

Applications

What do we mean by enterprise blockchain?

Healthcare

- Patient registration
- Fake pharmaceuticals 假药
- Medical Research data

Government

- ID Registration
- Tax payments

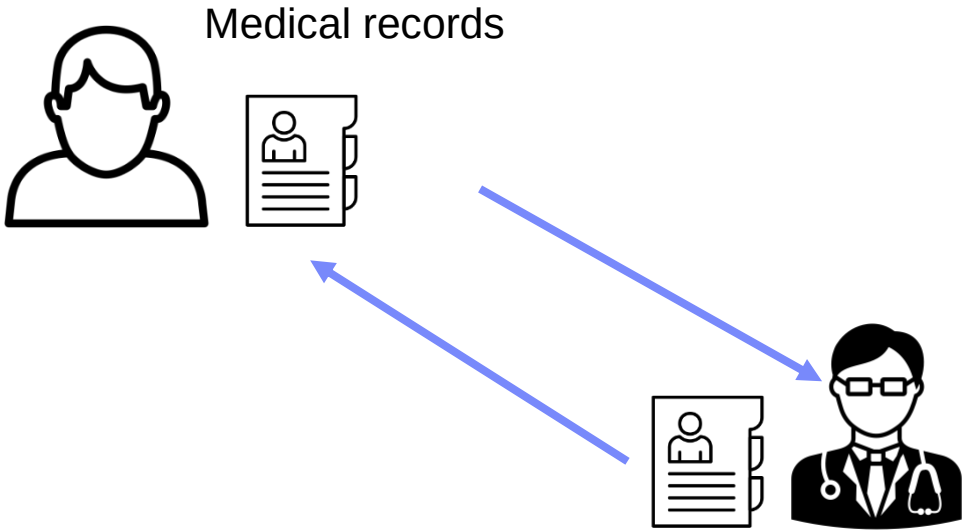
Finance & Investments

- Transactions
- Trade Finance
- Commodity trading
- Internal transactions
- Cross Boarder

Healthcare - user cases

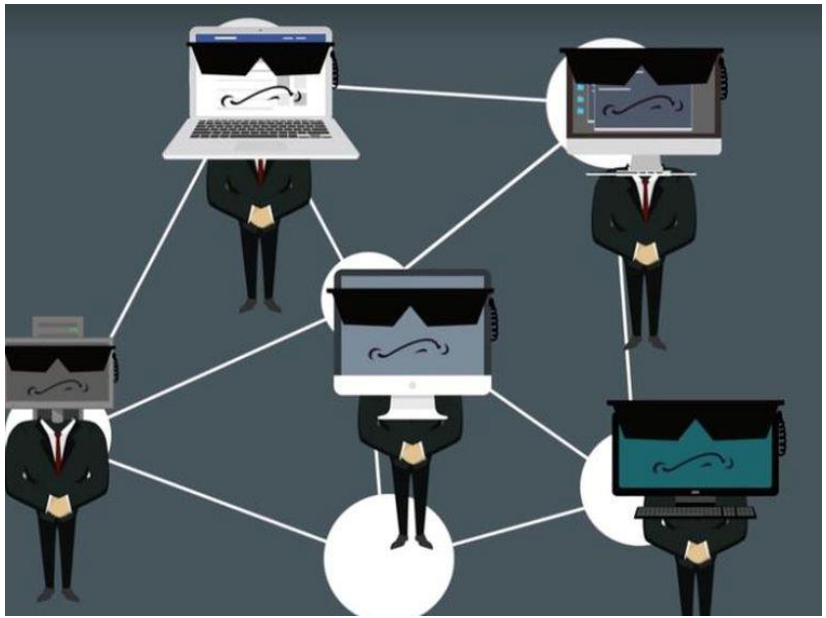
Let’s apply blockchain to Healthcare.

Video: how-blockchain-can-streamline-healthcare.mp4



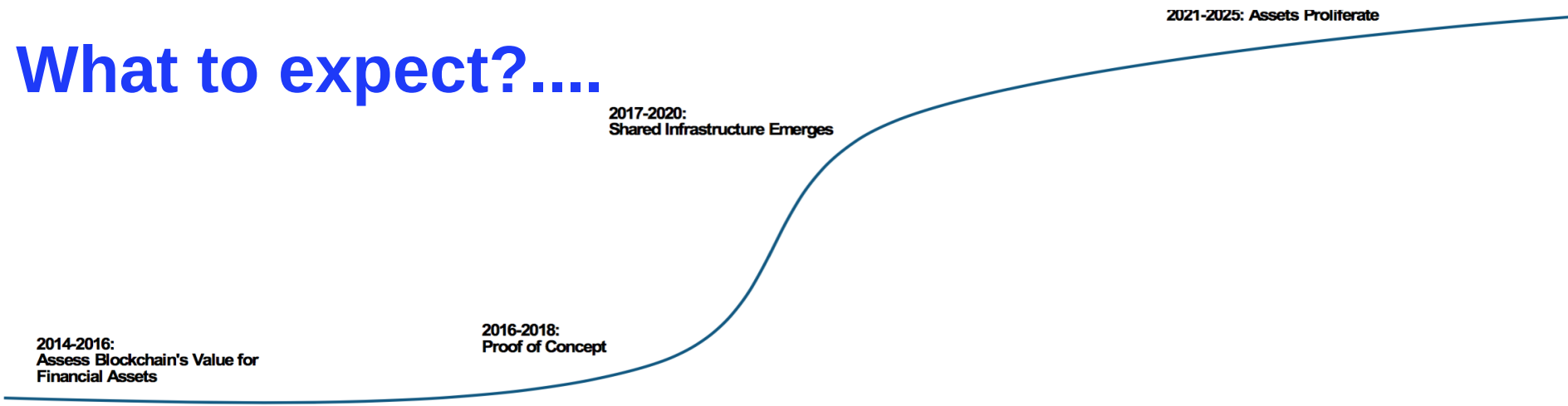
Government - user cases

Let’s apply blockchain to government.



Video: blockchain-for-government-services.mp4

What to expect?....



2014-2016: Assess Blockchain's Value for Financial Assets
- Banks and other financial infrastructure intermediaries (FIIs), including Central Depositories, Exchanges, & Technology Vendors, size potential efficiencies from permissioned, shared, secure distributed ledgers
- Banks and financial infrastructure intermediaries form industry groups to discuss opportunities
- R3
- Linux Hyperledger Foundation

2016-2018: Proof of Concept
- Banks and FIIs tee up specific assets as a test case for Blockchain
- CDS
- Repo settlement
- Corporate syndicated loan settlement
- Trade finance
- International currency transfer
- Exchanges for post trade settlement

- POC Goal: Assess if Blockchain can scale and reduce costs
1) Does Tech work and scale
- Does the asset transact between buyer and seller smoothly
- Does it offer benefits beyond existing technologies on a performance, cost, speed, scale analysis
- Fails are de minimis
2) Can buyer, seller, and their 3rd parties (i.e., lawyers, auditors, regulators) validate the transaction with few human touch points, replacing teams of people
3) Does it offer benefits beyond existing technologies on a performance, cost, speed, scale analysis

- POC Tiering: Segment into most to least important assets to address
- Focus resources on most important assets, most inefficient processes
- Engage regulators, lawyers, auditors

2017-2020: Shared Infrastructure Emerges
- Proven assets adopted well beyond initial POC group
- Develop interface for external users
- Leverage APIs
- Reduce costs with fewer heads and increased mutualization of infrastructure costs

2021-2025: Assets Proliferate
- More assets move onto Blockchain as efficiencies prove out

Private vs. Open blockchains

Blockchains…

公共区块链
· 一个公开的区块链是一个区块链，世界上的每个人都可以阅读，世界上的每个人都可以向其中发送交易，如果它们是有效的，就期望看到它们，世界上的每个人都可以参与到共识过程中。
联合体区块链
· 联合体区块链是区块链，其中共识过程由预先选择的一组节点控制;例如，我们可以想象一个由15家金融机构组成的联合体，每个机构都有一个节点，其中的10家机构必须在每个区块上签名，才能使区块有效。
完全私有区块链
· 一个完全私有的区块链是一个区块链，它的写权限集中在一个组织。读取权限可以是公开的，也可以是任意限制的。

Public Blockchain - A public blockchain is a blockchain that everybody in the world can read, anyone in the world can send transactions to and expect to see them included if they are valid, and anyone in the world can participate in the consensus process.

Consortium Blockchain - A consortium blockchain is a blockchain where the consensus process is controlled by a preselected set of nodes; for example, one might imagine a consortium of 15 financial institutes, each of which operates a node and of which 10 must sign every block in order for the block to be valid.

Fully Private Blockchain - A fully private blockchain is a blockchain where write permissions are kept centralized to one organization. Read permissions may be public or restricted to an arbitrary extent.

Public vs. Private Blockchain

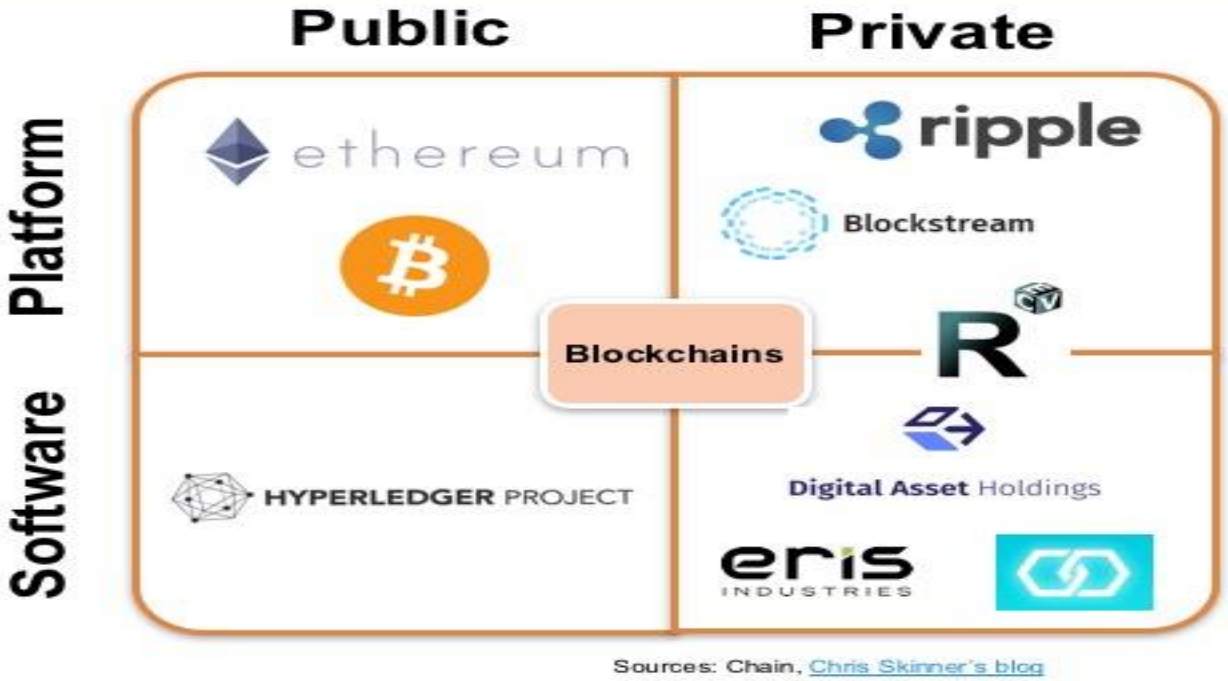
	Public (open) Blockchain	**Private (closed) Blockchain**
Access	Open read/write access to database	Permissioned read/write access to database
Speed	Slower	Faster
Security	Proof-of-Work/Proof-of-State	Pre-approved participants (预先核准的)
Identity	Anonymous/Pseudonymous (匿名的)	Known identities
Asset	Native Assets (原生资产)	Any asset
Costs	Expensive	Cheaper

Limitations

- Technical challenges
  - Throughput
  - Latency
  - Size and Bandwidth
  - Security
  - Usability
  - Versioning, Hard forks, Multiple chains
- Business Model Changes
- Government Regulations
- Privacy Regulation

技术挑战
· 吞吐量
· 延迟
· 尺寸和带宽
· 安全
· 可用性
· 版本化，硬分叉，多链
➢商业模式变化
➢政府规定
➢隐私监管

Blockchains Can Be Further Distinguished Between 'Platform' and 'Software' Providers



Sources: Chain, Chris Skinner's blog

- *Platforms* (ie Facebook, iOS) enable outside developers to build applications on top
- *Software* (eg Oracle 12c DB) is often run privately inside an organization, not open to outside developers
- Unclear whether R3, DAH, etc will become platforms

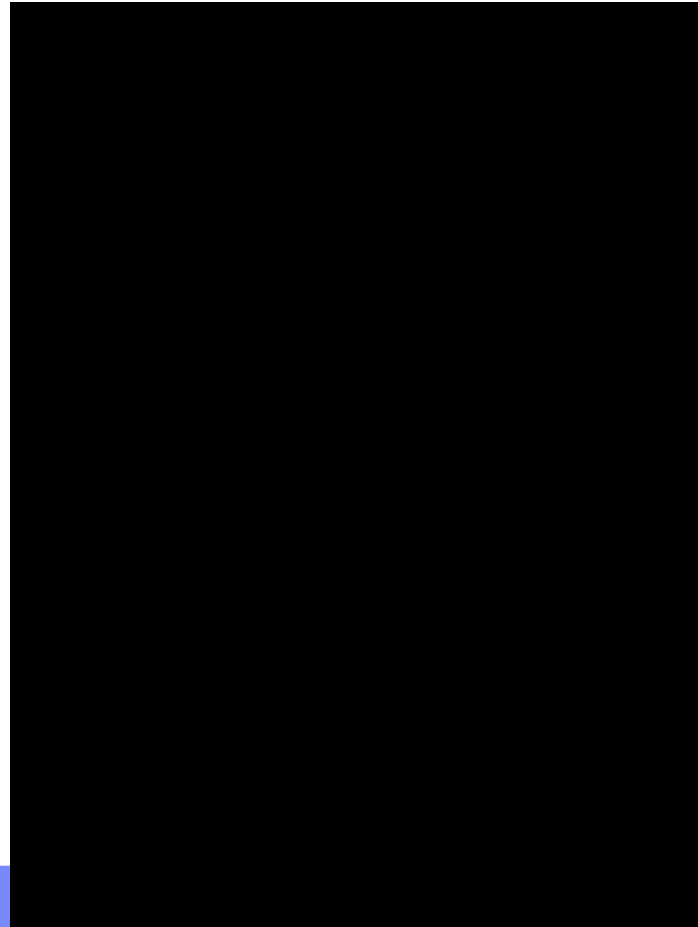
Hyperledger - project

HYPERLEDGER PROJECT

Let’s watch 2 videos!

Video: What is Hyperledger Fabric?
What is Hyperledger Fabric.mp4

Video: Which Blockchain Technology to Choose?
Ethereum vs Hyperledger.mp4



R3 - Project (Private)

1. Software/Platform
2. Consortium of 50 of the largest banks in the world
3. Corda Project - the distributed ledger for all 50 banks

1.软件/平台
2.由世界上最大的50家银行组成的财团
3.Corda项目——所有50家银行的分布式账本

Let’s watch a video!

Corda.mp4

Chain.com (Private)

Chain

Delivers three different options for companies:

1. Open Standard - *Financial Asset registration*
2. Chain Core - *An enterprise-grade distributed system that powers secure, scalable, and highly available blockchain networks.*
   Enterprise software in the blockchain.
3. Chain Sandbox - private blockchain network designed for rapid prototyping. It allows development teams to begin building blockchain applications in a hosted environment without deploying Chain Core on-premise.

为公司提供三种不同的选择：
1.开放标准--金融资产登记
2.链核心--一个企业级分布式系统，支持安全、可扩展和高可用的区块链网络。企业软件在区块链。
3.链沙盒-专用区块链网络设计的快速原型。它允许开发团队在托管环境中开始构建区块链应用程序，而无需部署链核心内部。

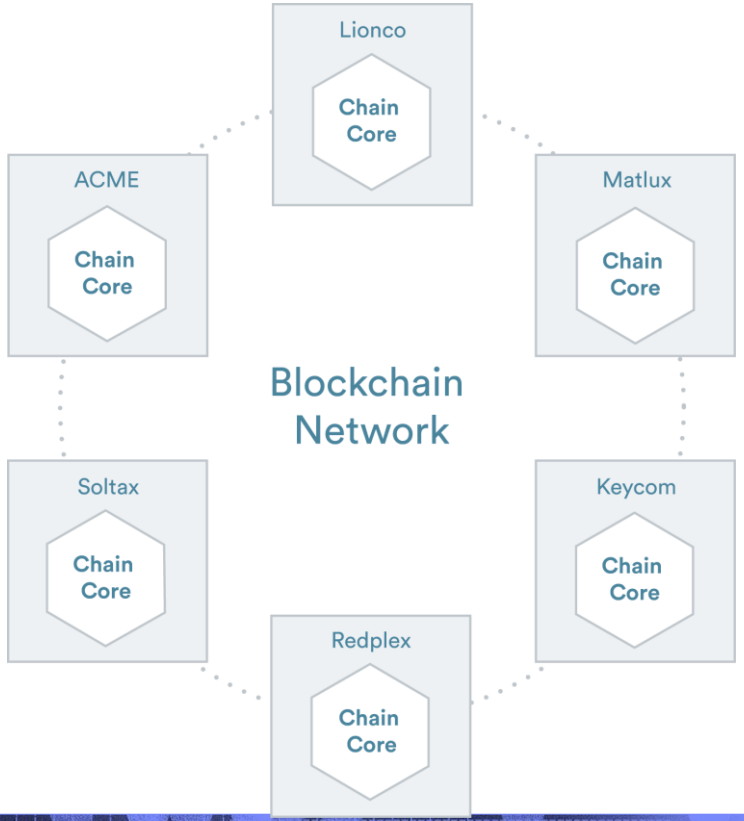
Let’s watch a video!

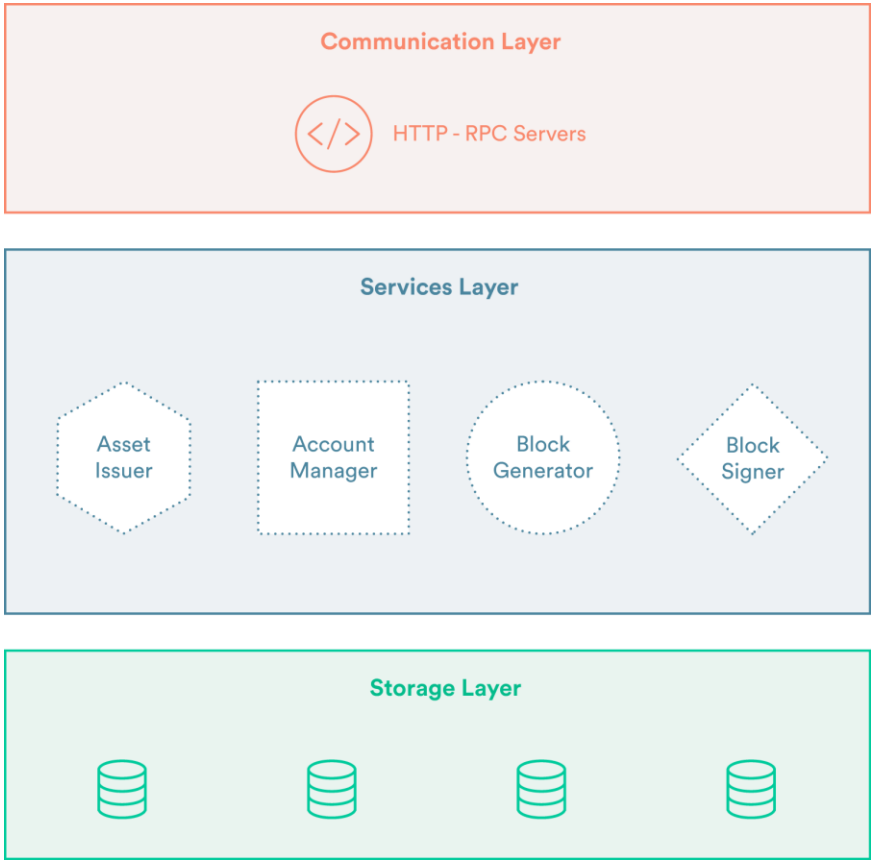
Introduction to Chain.mp4

END !


धन्यवाद
Hindi
多謝
Traditional Chinese
ขอบคุณ
Thai
Спасибо
Russian
Gracias
Spanish
Thank You
English
شكراً
Arabic
Obrigado
Brazilian Portuguese
多谢
Simplified Chinese
Danke
German
Grazie
Merci
நன்றி
Tamil
ありがとうございました
Japanese
감사합니다
Korean

Chain Core


Lionco
Chain Core
ACME
Chain Core
Matlux
Chain Core
Blockchain Network
Soltax
Chain Core
Keycom
Chain Core
Redplex
Chain Core


Communication Layer
HTTP - RPC Servers
Services Layer
Asset Issuer
Account Manager
Block Generator
Block Signer
Storage Layer