企业区块链

-- 备选共识

备选共识

-备选协商一致意见: 除其他核查方法以外的其他核查方法**工作证明(战俘)**.

-在波维发现后创建:

- 大规模的电力吞噬
- 2012年的总性能超过了最高效的超级计算机

采取的证明 (Pos)

- Pos要求用户提供货币的所有权, 即皮尔科恩.
- 节省能源与工作方法的证明, 降低计算过程和所需的功率。
- 以货币计价为网络和区块创建提供信任的 "抵押品"。
- 股权较高, 抵押品较高。

- 使用工作证明, 挖掘块的概率取决于矿工所做的工作 (例如, cpu/gpu 循环使用了检查哈希)。
- 与卡扣证明, 比较的资源是一个矿工持有的比特币的数量-有人持有1% 的比特币可以开采1% 的 " 卡块证明"。

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

活动证明 (Poa)

- 之间的混合Pos和战俘.战俘用于块创建的检查点的机制。
- 块是通过战俘方法, 与Pos类型签名来验证块。
- 只是一个理论, 很少发展。

烧伤证明 (Pob)

- **烧伤证明**是一种分布式共识的方法，也是工作证明和作品证明的替代方法。它还可用于引导一个加密货币离开另一个加密货币。

- 其想法是，矿工应出示证据，证明他们***烧***一些硬币-也就是说，送他们到一个可验证的不可选择地址。从他们个人的角度来看，这是很昂贵的，就像工作证明一样;但它只消耗任何其他资源，而会消耗被烧毁的基础资产。到目前为止，所有燃烧加密货币的证明都是通过燃烧工作开采的加密货币证明来工作的，因此，稀缺性的最终来源仍然是工作开采的 "燃料"。

- 有可能有许多可能的燃烧证明的变种。(https://en.bitcoin.it/wiki/Proof_of_burn)

- 彩票系统，其中硬币被烧毁，以赢得开采块的机会。
- 存放的数字硬币不会燃烧，直到接受块奖励。

经过时间的证明 (加密货币)

- 运行时间证明 (poet) 是一种区块链网络共识机制算法
  - 防止高资源利用率和高能耗
  - 遵循公平的彩票制度, 提高了这一过程的效率。

- 网络中的每个参与节点都需要等待随机选择的时间段, 第一个完成指定等待时间的节点将赢得新的块。
- 区块链网络中的每个节点都会生成一个随机等待时间, 并在指定的持续时间内进入睡眠状态。
- 首先醒来的人--也就是等待时间最短的人--醒来后, 将一个新的区块提交到区块链, 向整个对等网络广播必要的信息
- 然后, 对于下一个块的发现, 重复相同的过程。

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

独奏

- 独奏采矿是一个单独的过程，矿工完全在没有任何帮助的情况下完成采矿作业的任务。
- 这个过程主要是完成的**单独而不加入游泳池**.
- 这些块是以矿工的信用完成的任务的方式开采和生成的。

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

动物园管理员

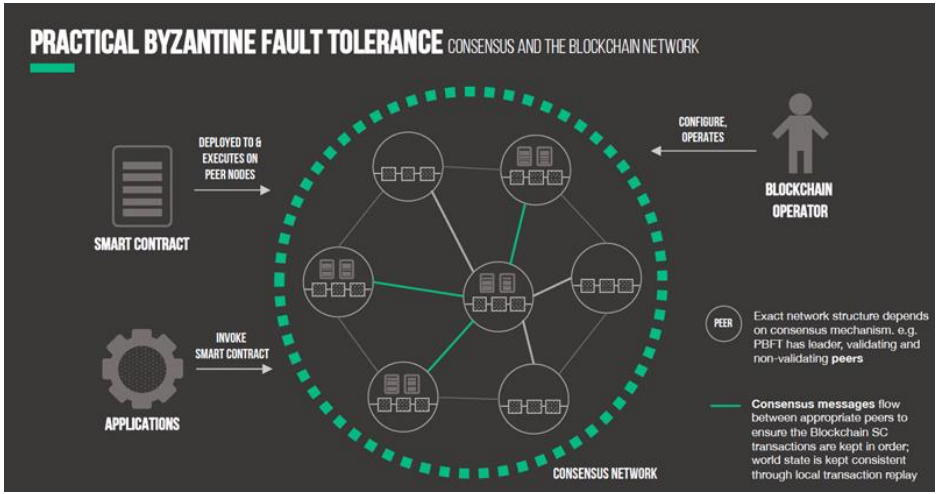
- zookeeper 是一种集中式服务，用于维护配置信息、命名、提供分布式同步和提供组服务。分布式应用程序以某种形式使用所有这些类型的服务。
- 每次实施它们时，都会有很多工作要做，以修复不可避免的错误和比赛条件。由于实现这类服务的难度，应用程序最初通常会对其进行略读，这使得它们在变化的情况下变得脆弱，难以管理。即使执行得正确，这些服务的不同实现也会在部署应用程序时导致管理复杂性。
- 动物园管理员目的是将这些不同服务的本质提炼成一个非常简单的接口，到一个集中的协调服务。服务本身是分布式的，并且非常可靠。
- 一致性、组管理和状态协议将由服务实现，因此应用程序不需要自行实现它们。这些应用的具体用途将包括动物园管理员的特定组件和应用程序特定约定的混合。zookeeper 食谱展示了如何使用这个简单的服务来构建更强大的抽象。

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

实用拜占庭容错 (PBFt)

- pbft 模型主要侧重于提供一个实用的拜占庭状态机复制, 通过假设存在独立的节点故障和通过特定传播的操作消息来容忍拜占庭故障 (恶意节点),独立节点。
- 该算法设计为在异步系统中工作, 并经过优化, 具有令人印象深刻的开销运行时性能, 并且延迟仅略有增加。

- 实质上, pbft 模型中的所有节点都按顺序排序, 其中一个节点是主节点 (引线), 另一个节点称为备份节点。
- 系统中的所有节点都相互通信, 目标是让所有诚实的节点通过多数达成系统状态的协议。节点之间进行大量通信, 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。



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

拜占庭将军问题

背景：

-所有将军的共识决定。叛国将领可以破坏计划，也会发出有目的的误传。

-如果有平局，最终 (叛国) 将军可以发送两个单独的消息。

-物理分离

-(空)，或无响应，可以有预定义的值 (后退)。

-将军是计算机，信使是数字通信系统。

拜占庭容错

力学:

-如果有一半或更多的将军叛国, 就不可能解决。

-容错计算机系统中最困难的故障模式。不是故障停止机制。

-"真相" 的方向, 随着网络的发展→更难以反对 (satoshi 白皮书: 最后一节)。

-适用于比特币中使用的现金机制。

备选共识

脉动：

-支付协议，与菲亚特货币和波纹货币 (xrp) 交易。

-金融机构与 "做市商" 之间的支付基础设施。

-成熟的信任系统，利用内部分类帐。所有资产均作为债务债务持有。

备选共识

恒星

-支付系统具有更好的技术比波纹。更多的对等使用。

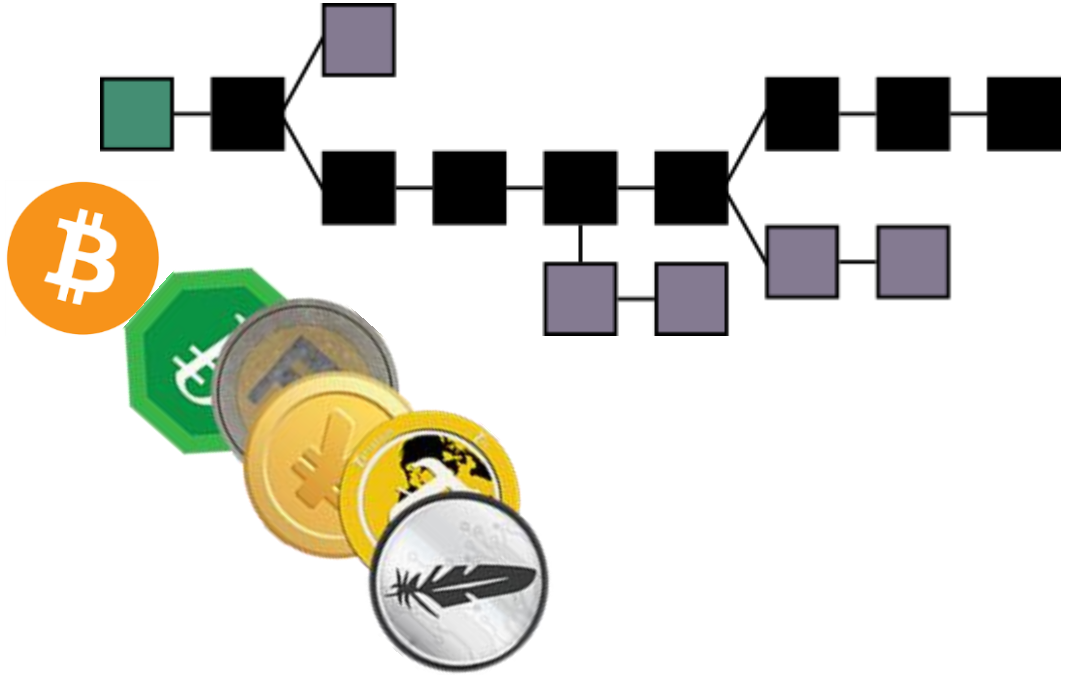
-存储在分类帐中的帐户，计算机网络创建全局价值交换网络。

-选定的公共可信节点，使用仲裁切片来创建连锁反应。

-2 至4秒的持续共识。约80% 的共识。

"企业" 区块链

区块链



区块链 1.0-货币

- 比特币
- 阿尔特币
- iom (货币互联网)

"智能合同作为智能合同代码"

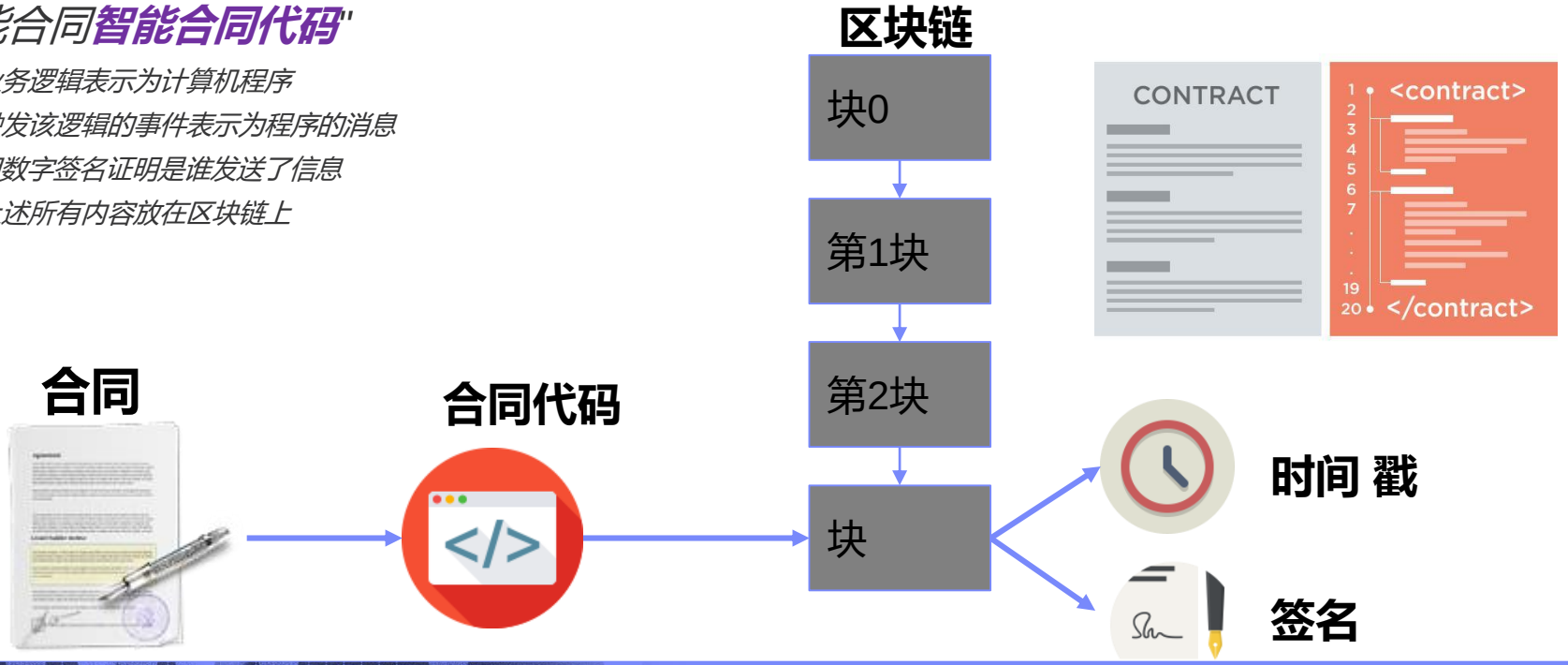
*"智能合同**智能合同代码**"*

(a) 将业务逻辑表示为计算机程序

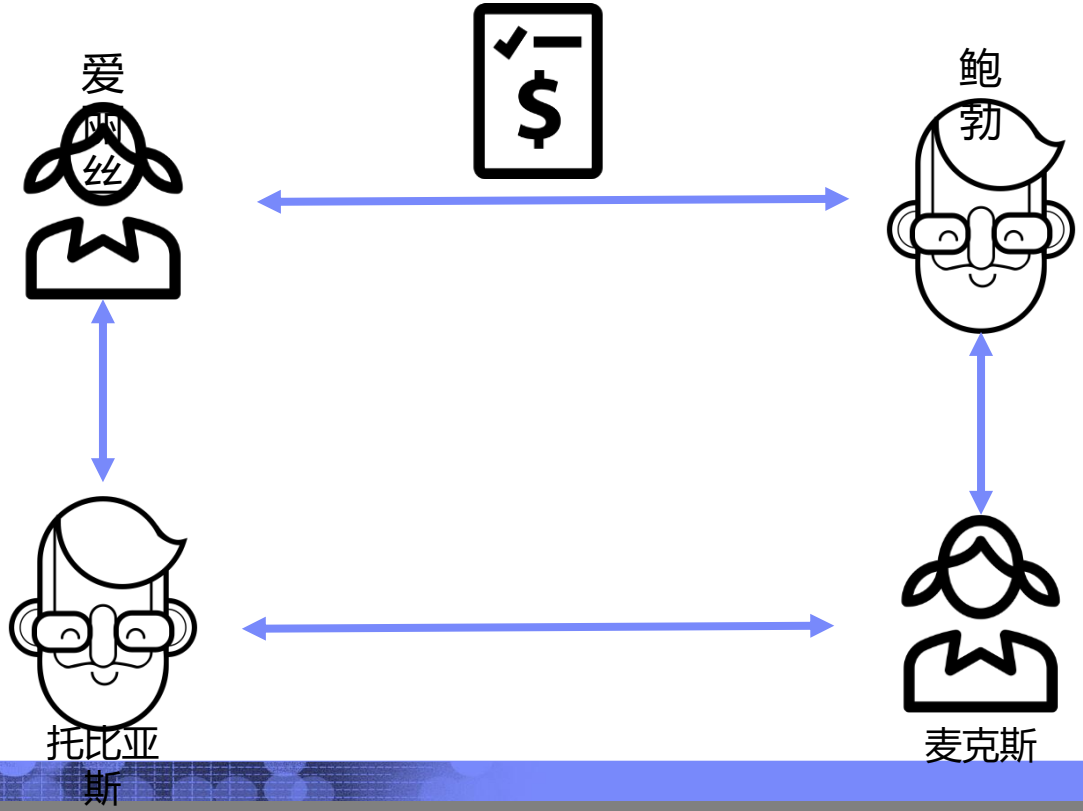
(b) 将触发该逻辑的事件表示为程序的消息

(c) 使用数字签名证明是谁发送了信息

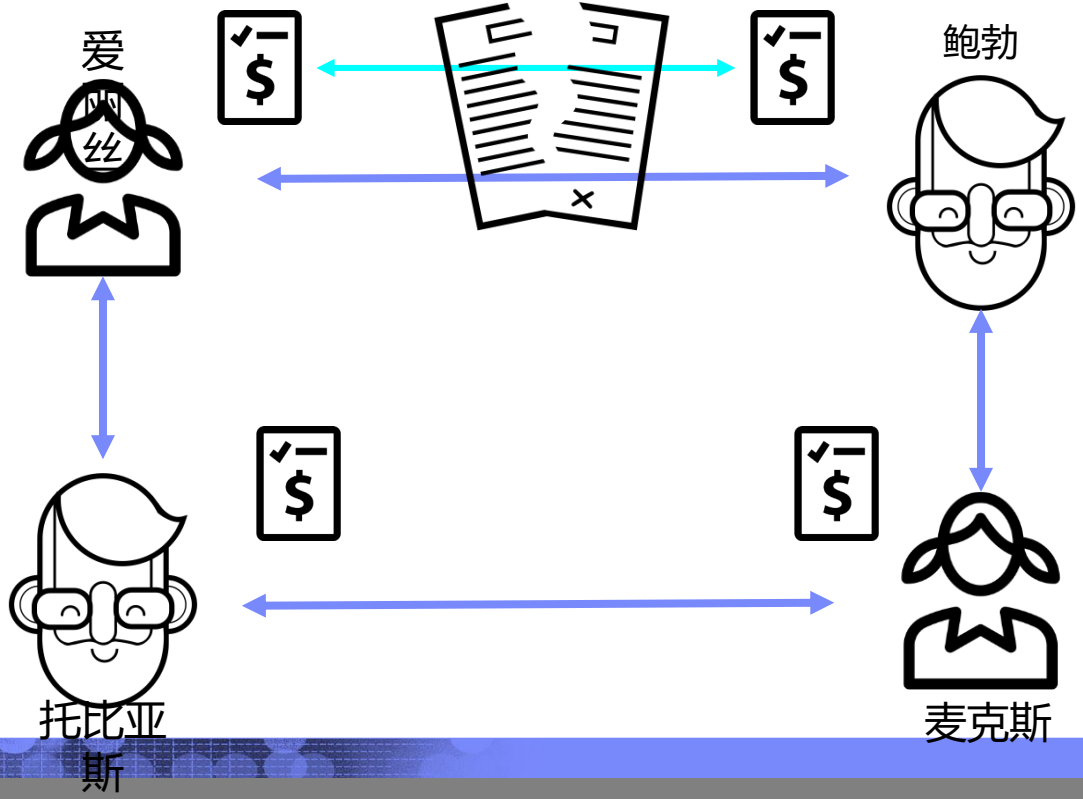
(d) 将上述所有内容放在区块链上



智能合同-示例

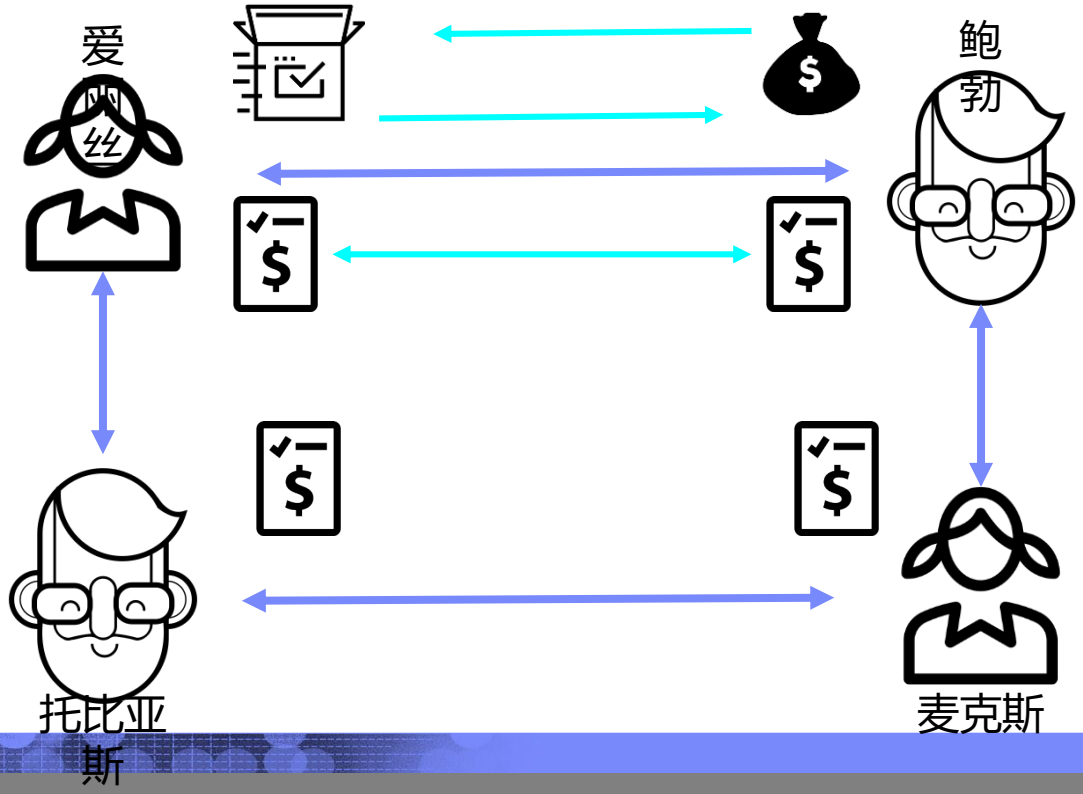


智能合同-示例



因此, 如果 max 想要做出改变, 整个链都会得到一条信息。每个人都需要批准。

智能合同-示例



优点/缺点

优点:
-它是安全的

- 如果有人想改变合同, 每个人都会得到警告

-自我执行,
-分发/分散
-m2m (机器到机器)

缺点:
-链条的可扩展性
-法律合同的困难, 需要人的解释
-计算能力
-很难更新智能合同

dapp、dao、dac、das

分散应用 (**dapp**)
-它是一个以分布式方式在网络上运行的应用程序, 参与者信息得到安全保护, 并且在网络节点上分散执行操作。

分散的自治组织和公司 (**dao 和 dac**)
-在 dao只能 dac 中, 有智能合约作为在区块链上运行的代理, 它们根据事件和不断变化的条件执行预先指定或预先批准的任务范围。
-storj, 智能合同运营, 分散的文件存储

权力下放的自治社会 (**das**)
-在未来, 这可以是一个 das, 一个智能合同车队, 或整个生态系统的 dapp, dao, dac 自主运作

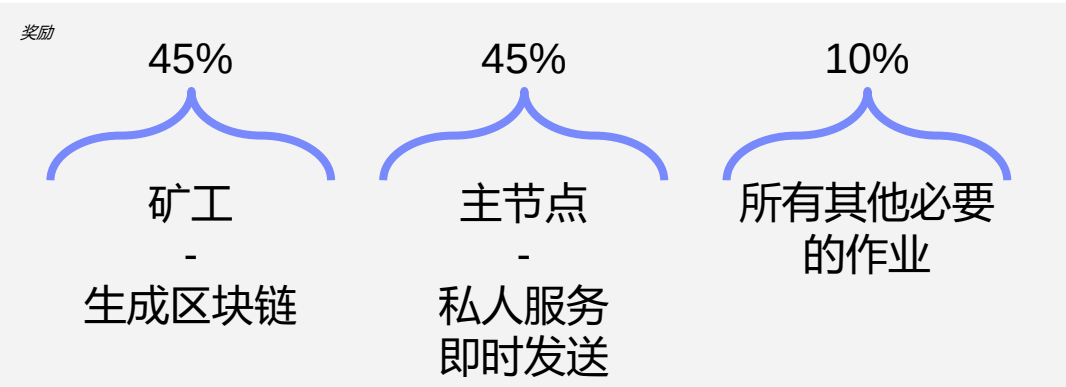
DAO-DASH

分散自治组织 (dao), 有时被标记为分散自治公司 (dac), 是一个组织通过编码为计算机程序叫智能合约.dao 的财务交易记录和程序规则保留在区块链.

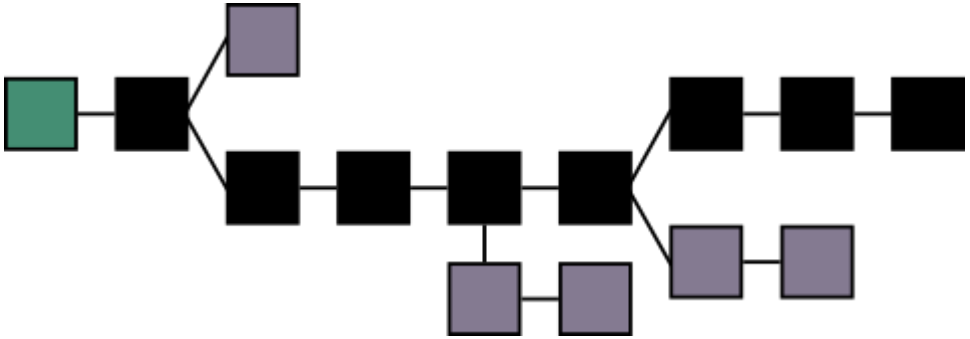
- 破折号以前被称为达克科尔和xcoin, 2015年更名
- 通过网络协议进行通信的人员

两个原则:
1. 共识
2. 执行

是什么让它如此特别? →



区块链



区块链 1.0-货币
- 比特币
- 阿尔特币
- iom

区块链 2.0-合同
- 智能物业
- 智能合同 (可编程货币)
- dapp、dao、dac、das

区块链 3.0-公正应用 (*超越货币、经济和市场*)
- 新的组织模式 (共识)
- 数字身份验证
- 知识产权保护
- 媒体管理
- 虚拟公证员, bitnotar, 编年史
- 政府和医疗保健

应用

我们所说的企业封锁是什么意思？

医疗

- 患者注册
- 假药
- 医学研究数据

政府

- 身份证注册
- 纳税

金融和投资

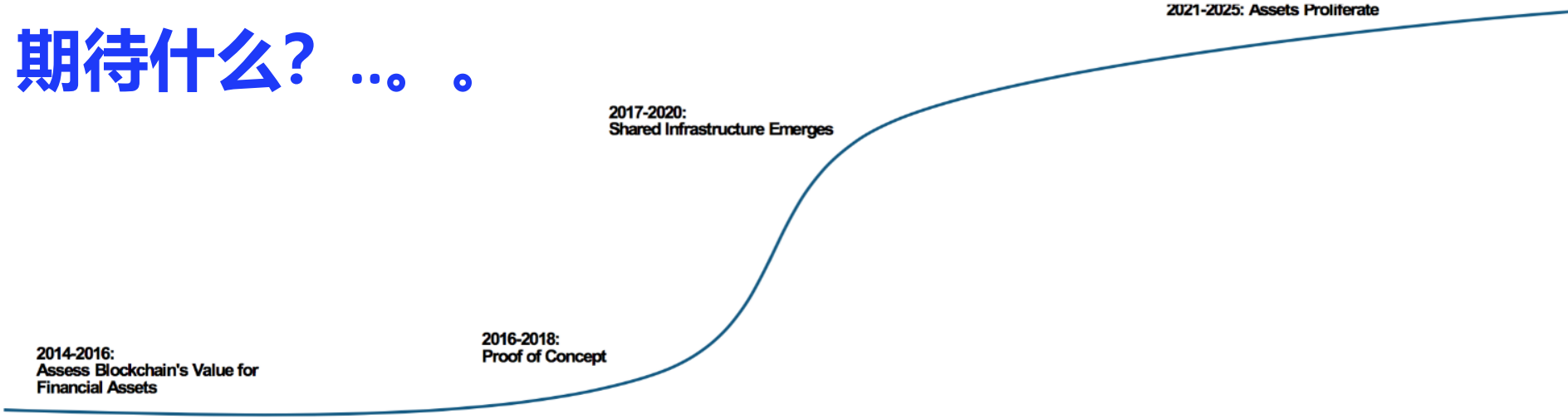
- 交易
- 贸易融资
- 商品交易
- 内部交易记录
- 交叉船

医疗保健-用户案例

- epic 是医疗保健领域的大型软件提供商
- 只有没有区块链, 所以一切都集中存储

让我们将区块链应用到医疗保健领域:

期待什么？…。



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

私有与开放区块链

区块链..。

公共区块链- 公共封锁链是世界上每个人都能阅读的区块链，世界上任何人都可以向其发送交易，如果交易有效，希望看到交易被包括在内，世界上任何人都可以参与共识进程。

集团区块链-联盟区块链是一个区块链，其中的共识过程由一组预先选定的节点控制；例如，人们可以想象一个由15个金融机构组成的财团，每个金融机构经营一个节点，其中10个机构必须对每个区块进行签名，才能使该区块有效。

完全私有的区块链-完全私有的区块链是一个区块链，其中写入权限被集中到一个组织。读取权限可能是公共的，也可能是任意范围的。

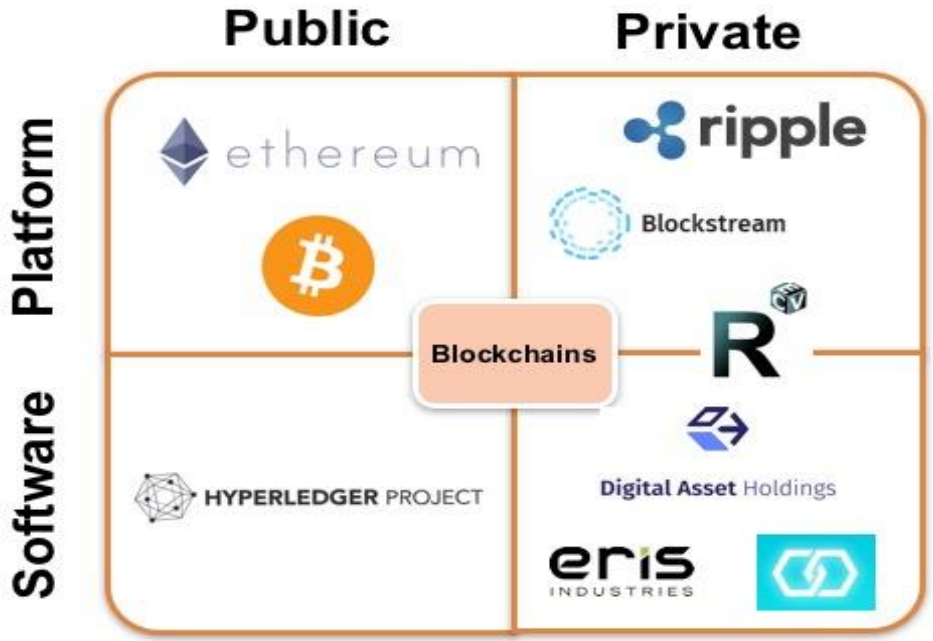
公共 (开放) 与专用区块链 (关闭)

	公共	私人
访问	打开对数据库的读取/写入访问	已保护对数据库的写入访问
速度	慢	更快
安全	工作证明/国家证明	预先核准的参与人
身份	匿名/假名	已知标识
资产	原生资产	任何资产
成本	昂贵	便宜

限制

- 技术挑战
  - 吞吐量
  - 延迟
  - 大小和带宽
  - 安全
  - 可用 性
  - 版本控制, 硬叉, 多个链
- 业务模式更改
- 政府条例
- 隐私法规

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



- *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

Sources: Chain, Chris Skinner's blog

http://www.coindesk.com/state-of-blockchain-q1-2016/

脉动

波纹允许银行对支付世界有不同的看法。

让我们看视频吧!

波纹是如何工作的。

大分类账-项目

HYPERLEDGER PROJECT

让我们看2个视频!

视频: 什么是超级分类帐结构?
什么是超级分类帐法。

视频: 以太与超分类帐, 选择哪种区块链技术?
以太 vs 超细条. mp4

r3-项目 (私有)

1. 软件平台
2. 由世界上50家最大银行组成的联盟
3. corda 项目-所有50家银行的分布式分类账

让我们一起来看一段视频!

r3 corda–ha.mp4

chain. com (私有)

为公司提供三种不同的选择:

1. 打开标准-*金融资产注册*
2. 链芯-*企业级分布式系统, 为安全、 可扩展和高可用性的区块链网络提供支持.* ***区块链中的企业软件.***
3. 链式沙盒-*专为快速原型设计的专用区块链网络。 它允许开发团队在托管环境中开始构建区块链应用程序, 而无需在内部部署链核心。*

让我们一起来看一段视频!

链介绍. mp4

结束！

धन्यवाद
Hindi印地语

多謝
繁体中文

ขอบคุณ
泰语

Спасибо
俄语

谢谢
西班牙语

谢谢
英语

شكرا
阿拉伯语

奥布里加多
巴西葡萄牙语

多谢
简体中文

丹克
德语

格拉齐
意大利语

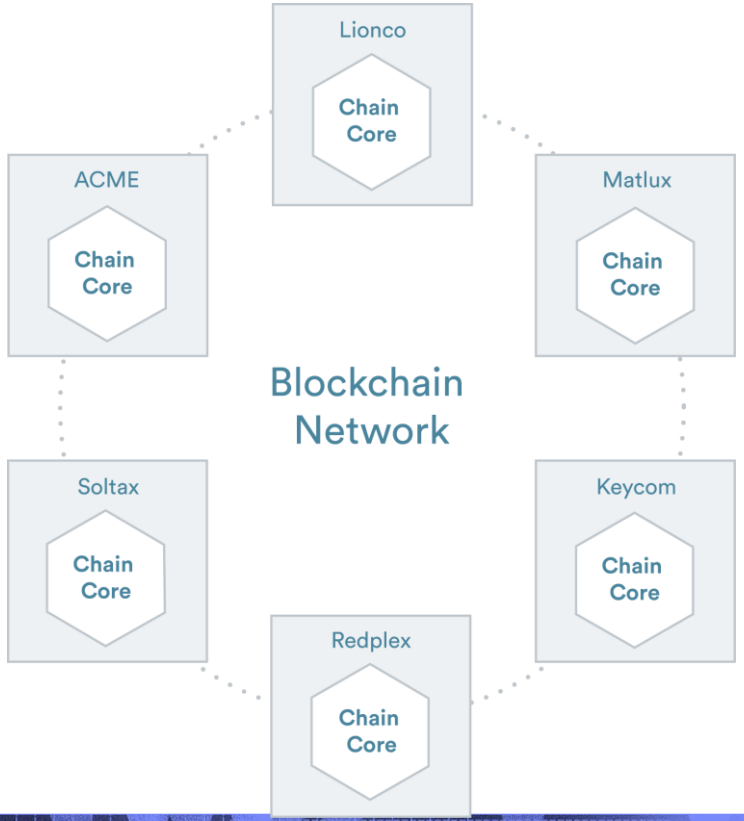
谢谢
法语

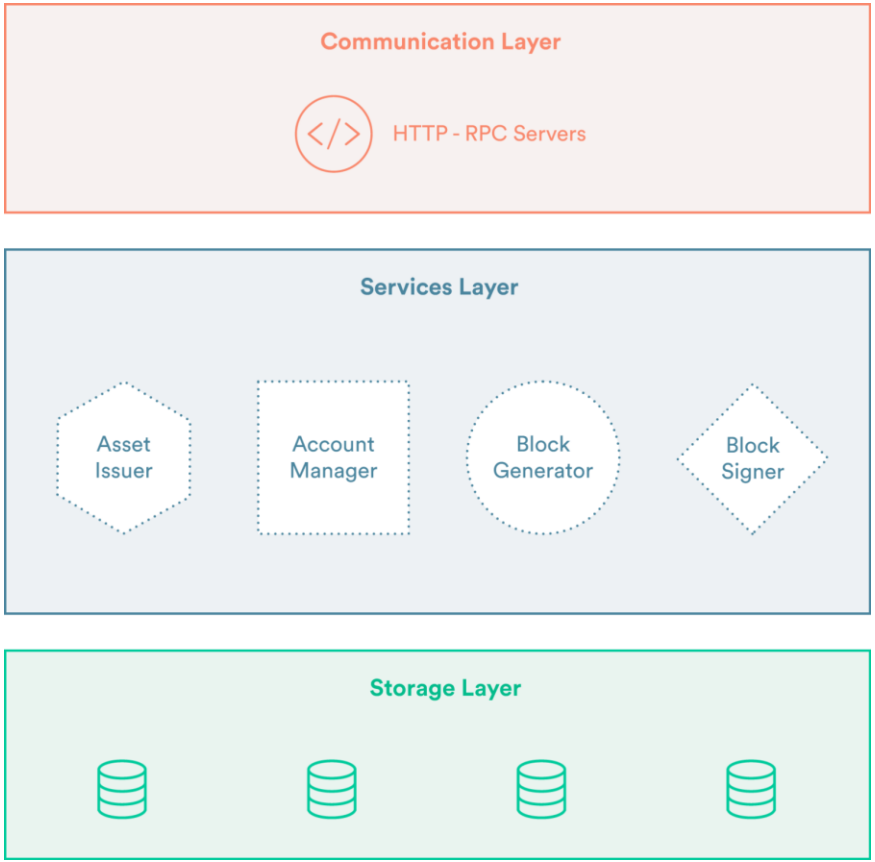
நன்றி
Tamil
泰米尔语

ありがとうございました
日语

감사합니다
朝鲜语

链核


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