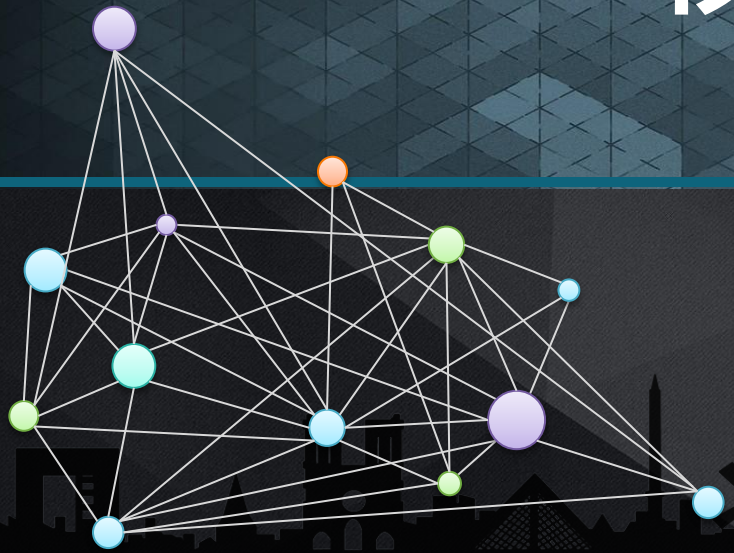
区块链技术
核心本质及社交应用



郑嘉文 - 2018/02

自我介绍

郑嘉文

- 贝尔大型电子商务网站架构师
- 贝尔大数据研发部门经理
- 开源项目从业者
- 独立创业者

- 加拿大麦吉尔大学信息学硕士
- 加拿大多伦多大学罗特曼商学院MBA

多元文化背景

- 中文, 英文, 日文, 法文

多学科交叉背景

- 计算机, 金融, 统计, 数学

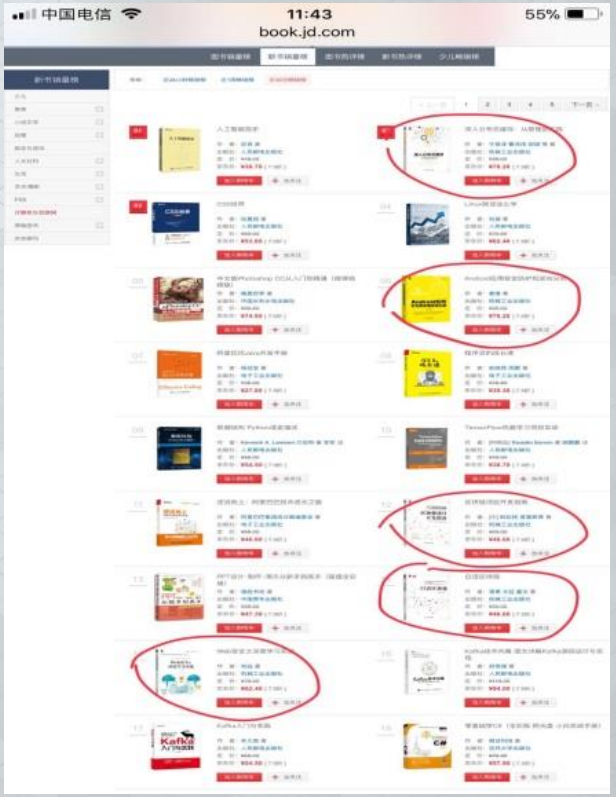
多才多艺技术背景

- Java/J2EE, C#/.Net, C/C++, Python/Django, Go, Rust 前台/后台…

区块链项目历史

- 2012年开始接触比特币
- 2014年开始接触雷欧币（LeoCoin）
- 2015年开始研究以太坊（Ethereum)源代码
- 2016年基于Ripple框架开发了多人签名（Multi-Sign）的支付网关
- 2017年撰写多个数字货币的白皮书
- 2017年开发了基于数字货币的套利程序
- 2017年机械工业出版社《白话区块链》出版, 跻身京东30天新书出版销量Top15
- 2017年12月31号发布了Bitcoin Payment Performance(BPP)分叉币
- 2018年参与发布了Coinmeet上火币交易所交易
- 目前从事基于区块链的量化金融的研究

著作



内容

什么是区块链

Introduction of Blockchain & BitCoin

区块链的核心

Understanding of underlying Blockchain technologies

区块链发展以及展望

Development Phase of Blockchain and its prospect

区块链做社交

Blockchain for social

BlockChain

IS CHANGING THE WORLD

区块链是什么

什么是区块链? Blockchain is Distributed Ledger (Database) System

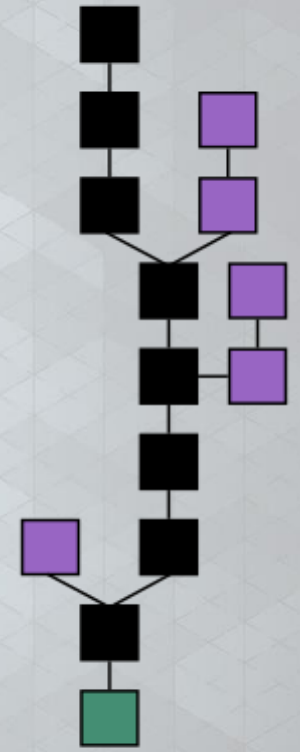
区块链

区块链本质上是在多个分布式节点间传递账本（价值/数据归属权）信息并通过一定的共识机制（公共/联盟）达成一致性，建立信任关系的技术。

01 独特的**遗传式链状数据结构**从本质上保证数据不会被更改。数据块不会被以追溯方式更改以前的时间戳，一旦数据写入不可更改（无论现在发生什么，都不会影响以前发生过的事实）。而且 这样的数据链均匀的分布在点对点的节点网络间。

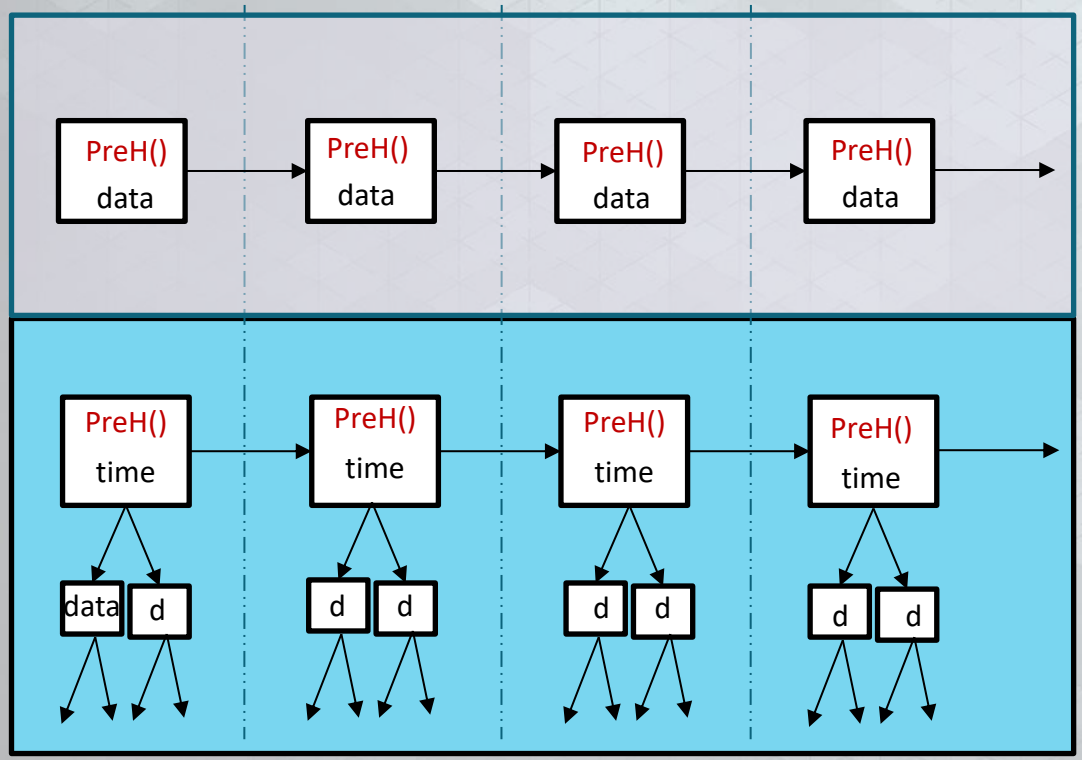
02 **去中心化**，区块链技术可以实现去中心的共识机制。公共账本所记录的事务（transaction）可以通过链上参与节点的多少人投票的方式校验并达成一致共识。

03 **信任机器:** 区块链技术是在彼此不信任的节点间建立信任关系的技术。超越数字货币，区块链是让完全没有信任机制的人民不需要通过集权方式的权威中心授权就可以建立信任并能高效协同达成一致。



什么是区块链?

1 区块链底层通过使用哈希指针连接的数据链表。而这个哈希指针是数据加数据本身通过加密产生的特征值在特定的时间产生的唯一的指向下一个链接数据块的。



区块链数据块是用哈希值做指针的特殊数据链表

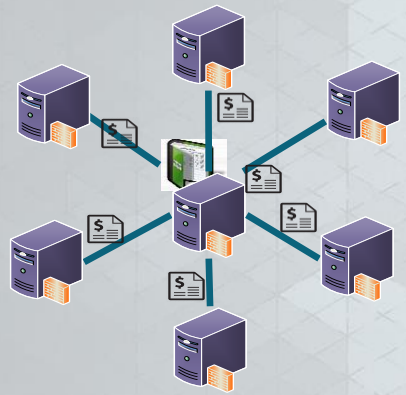
特殊的区块链可以是把哈希指针和时间放在数据块中而把数据块放在以此特征值为指针的侧链上。这样可以提高链式数据操作性能

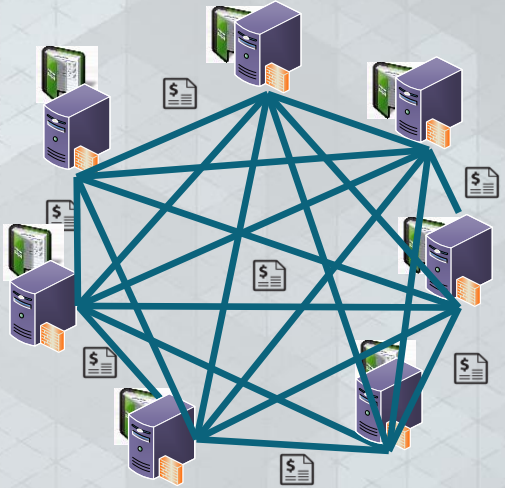
什么是区块链?

2

区块链是一种在完全分布式的点对点分网络间存在和传递的分布式账本系统。

可以完全实现去中心化。





Centralized computing is computing done at a central location, using terminals(Clients) that are attached to and request resource from a centralized Server. C/S model, more secured, authentication & encryption are easier.

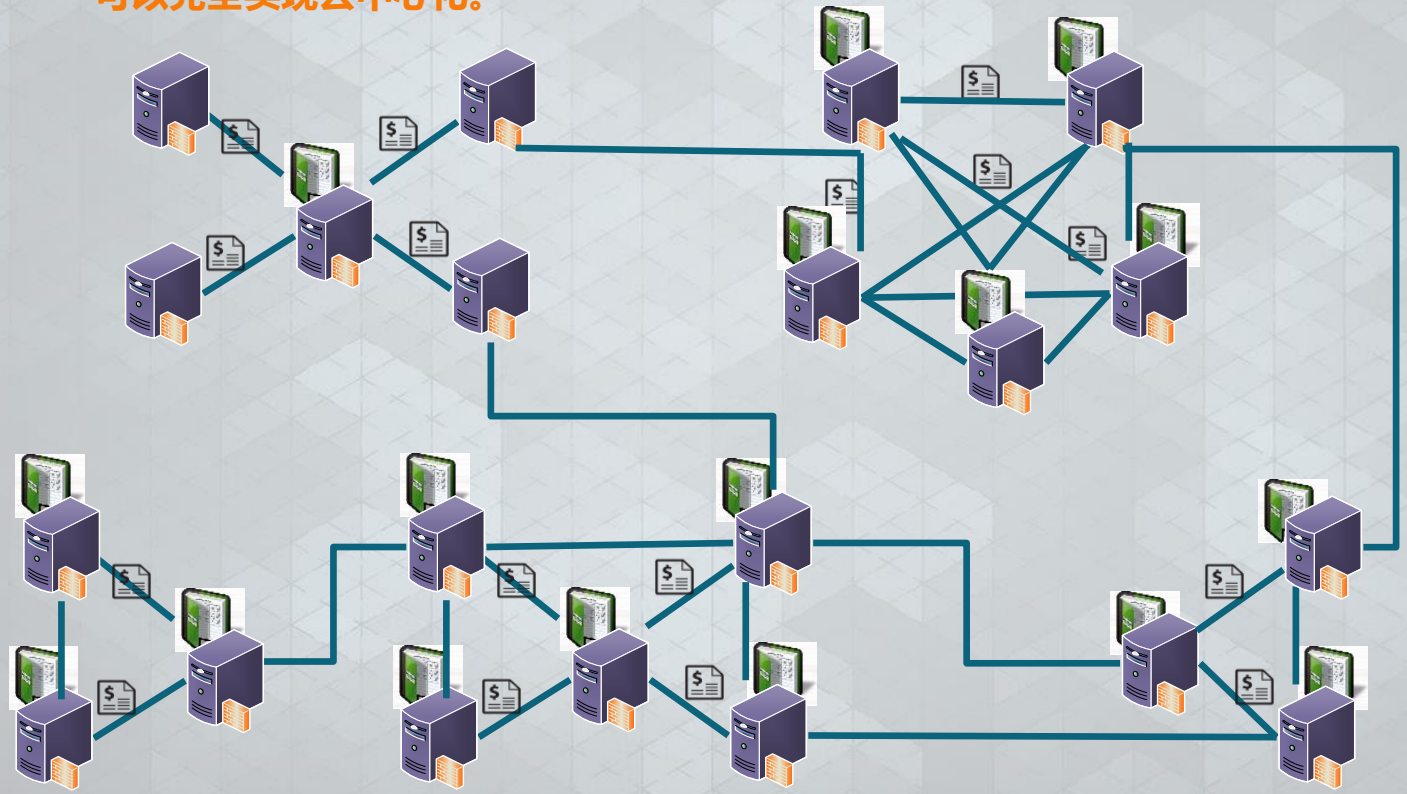
A peer-to-peer (P2P) network in which interconnected nodes ("peers") share resources amongst each other without the use of a centralized administrative system. P2P systems pose unique challenges from a computer security perspective.

什么是区块链?

2

区块链是一种在完全分布式的点对点分网络间存在和传递的分布式账本系统。

可以完全实现去中心化。

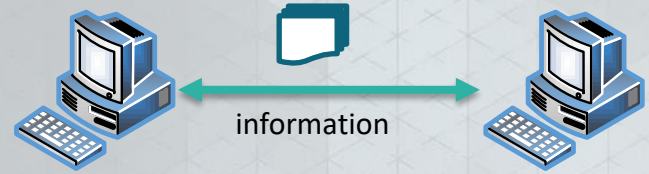


什么是区块链?

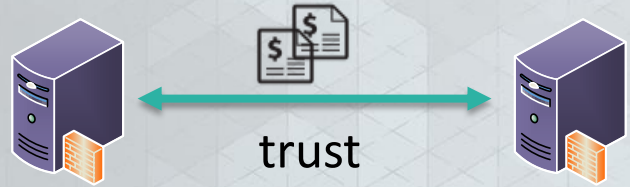
3

区块链是信任机器，是在完全不信任节点间建立信任机制的技术。

是价值网络，是传递价值的互联网（Internet Of Value, IOV)



互联网在节点间传递信息



区块链交换的是价值，是价值网络，是在不信任节点间建立信任关系，传递的是信任。是信任机器

Blockchain is a trust machine

陈
命运要掌握在我自己手里，根据这个原则，我按与黄督察约定好的条款写了一份卧底证明，即我的掩护名为“阿仁”，韩琛帮覆灭后就回警局工作，升两级且获奖金50万元，并要求黄督察签字盖章。但是，我不能让他看到这份证明，因为黄督察有可能事后变节，把“阿仁”是卧底的情况泄露给黑帮。

我把证明打印好后，把文字部分遮挡住，只留下空白处让黄督察签字盖章

黄警司
我不干，因为我对陈写的证明内容没信心，我认为陈可能写的是“卧底1个月即退休，退休金2000万”。

如何才能让黄督察既看不到我写的证明内容，又让他确信他已经知道了我的证明内容呢

用数学和计算机技术建立信任 – 盲签

1、写了10份掩护名不同的证明，有的叫“阿仁”，有的叫“阿德”等等，其它内容都完全一致，用同一种加密方法进行加密，得到十份不同的密文。特别的是，这种加密方法对明文的变化很敏感，即使两份证明中仅有“仁”“德”两个字不同，那密文也显得毫无关系的样子，这叫作雪崩效应，即一丁点的扰动就会引起结果巨大的差别。

2、我找黄督察签字盖章，他随机挑出9份，让我当场解密，他看到解密后的明文与我们的约定相同，只是掩护名不同而矣。于是，黄督察放心地在第10张密文上签了字盖了章，他当然不知道我的掩护名是什么，现在我放心了。

区块链核心技术原理

区块链核心 – 数字加密 & 数字货币

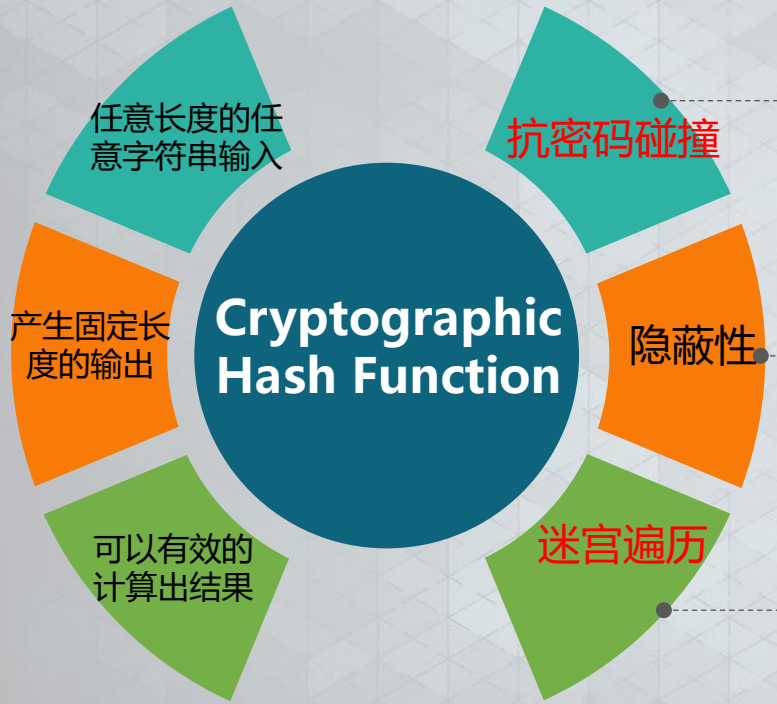
密码通过哈希函数加密后，拿到的结果没有人可以反向计算出加密前的密码，但是可以校验

保证哈希指针链接的数据链一旦产生不可更改

只有自己可以签名，任何人可校验但是又没有人能修改，移动或删除。

数字加密技术通过加密操作把信息和交易数据封装在不可修改的数据块中。严格安全加密的数据块在分布式的网络间传递数字货币和数字资产。

区块链核心 – 数字加密哈希函数

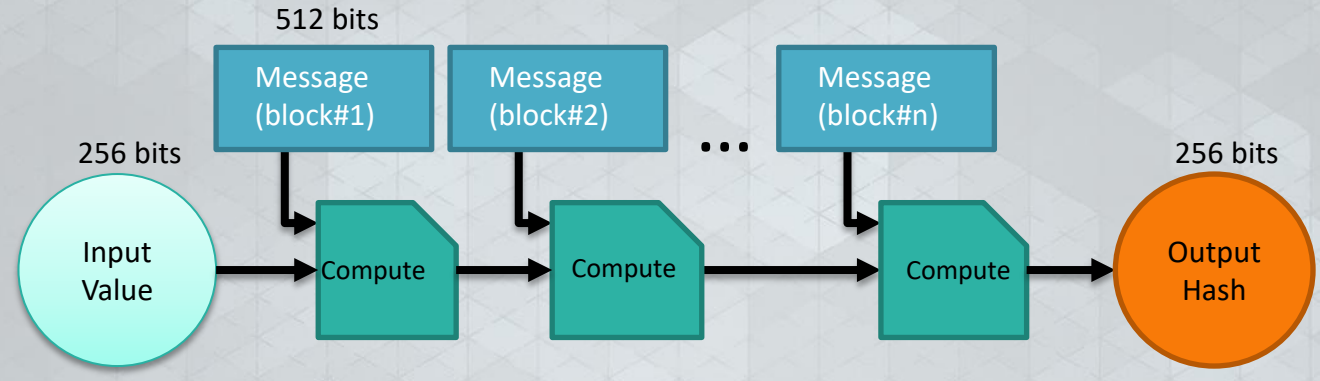


there are no hash functions *proven* to be collision-resistant. The cryptographic hash functions that we rely on in practice are just functions for which people have tried really, really hard to find collisions and have not yet succeeded.

The hiding property asserts that if we’re given the output of the hash function $y = H(x)$, there’s no feasible way to figure out what the input, x, was.

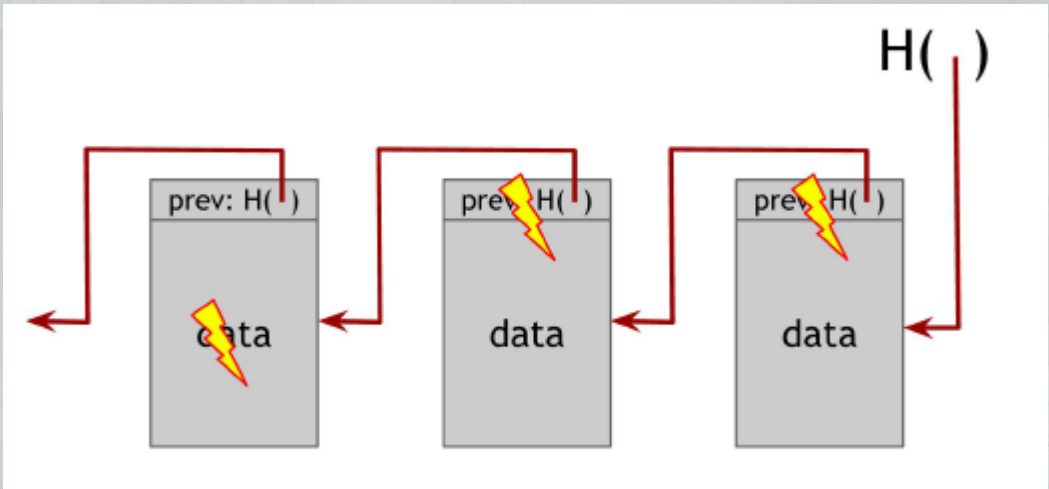
search puzzle, a mathematical problem which requires searching a very large space in order to find the solution

区块链核心 – 比特币采用的哈希函数SHA-256



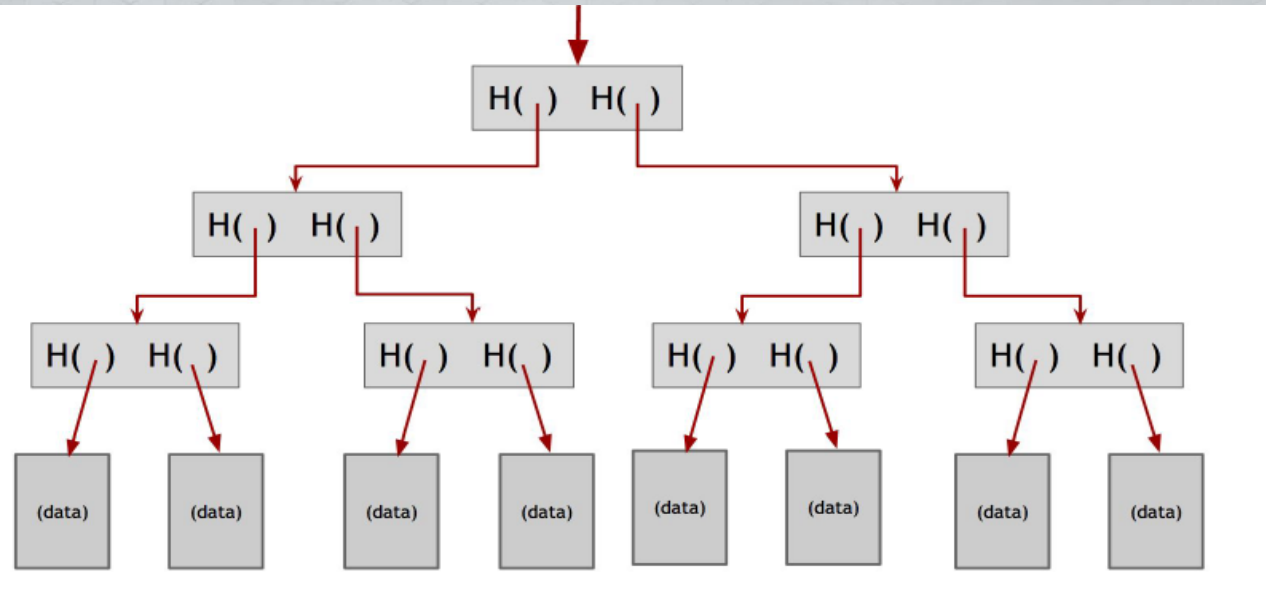
***SHA-256 哈希函数*. SHA-256 通过 Merkle-Damgard 变换把任意长度的信息/字符转换成多个哈希函数的512个字节的输入值不断迭代加密产生256个字节的加密后的字符串。**

区块链核心 – 哈希指针和数据结构



如果攻击者篡改了区块链上的任何数据，篡改过的数据都无法产生正确的（唯一的）指向下一个数据块的哈希指针。就是篡改者把整个区块链的数据和指针，也因为不知道原始输入密码而无法产生第一个头指针。从而导致网络上所有的节点都会探测到这样的篡改企图。

区块链核心 – 哈希指针和数据结构Merkle Tree



Merkle树, 所有的数据块按配对存储然后哈希指针存储在树结构上的父节点。父节点的哈希指针又再配对作为输入产生新的哈希指针作为父节点，这样一直到把所有叶节点的数据都能存储在这个树结构里。

区块链核心 – 哈希指针和数据结构

Blockchain Explorer

101 | 102 | 103 | 104 | 105

Block Hash:
SzAnUVgxQbhJlsq7Ev1PfwGfnhLoaugH+QO8BjaRCzdjmBh74L61aEzwfW21fLQzaNV6U5nIlptLB4fXsAXDiw==

Previous Block Hash:
N/SH6xkdYz7ThCu8ngHtaYNvsS8wIxrx13dFFqjBTk8ZbH5BTAugHypF4baj13dlc5+hvKaIPbt9sNs2r8qAyA==

Added to Chain:
9 Dec 2016 1:54:38

Transactions:
5c955641-1a00-4c3b-8b60-88d0c30a7d7b

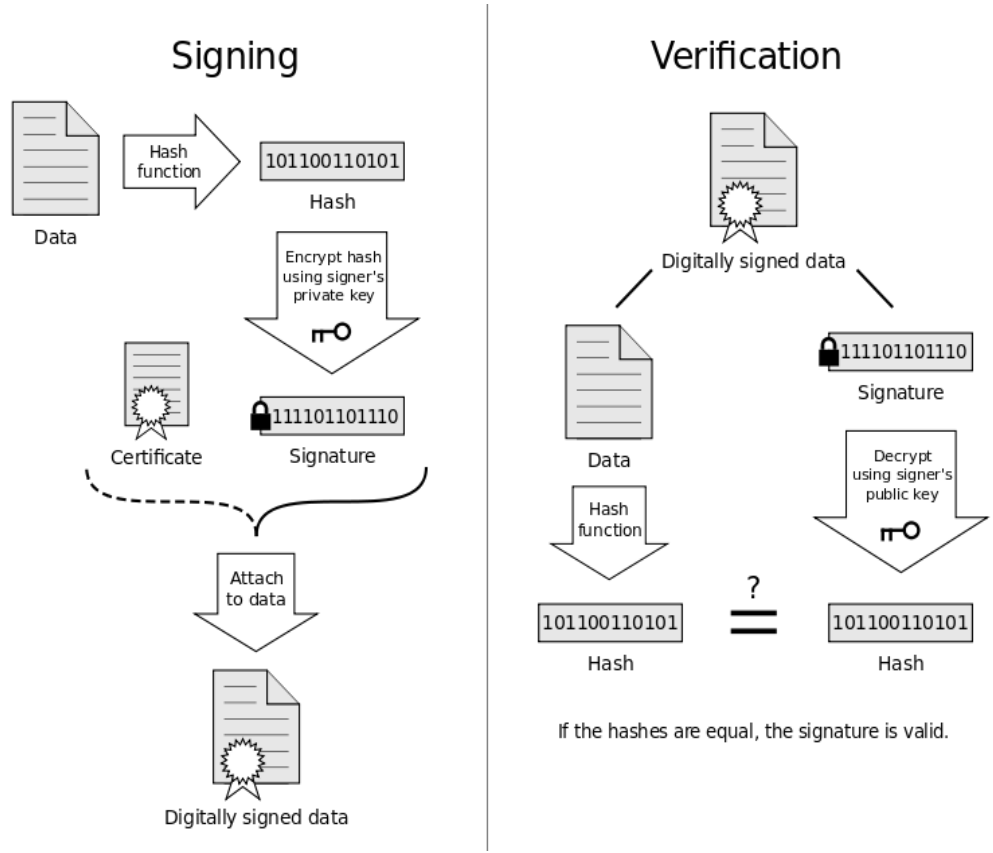
Block Hash:
1ZJJ+6ck+B4XqzLFvQ0kS3Iv3IB5xdt60W7IuYeSWL6S9eB1zIBbSjsJeRhwbj9WN41thh8PbI4haTnnpRZ1oA==

Previous Block Hash:
SzAnUVgxQbhJlsq7Ev1PfwGfnhLoaugH+QO8BjaRCzdjmBh74L61aEzwfW21fLQzaNV6U5nIlptLB4fXsAXDiw==

Added to Chain:
9 Dec 2016 1:54:41

Transactions:
9f1c2481-7d96-4e2d-bbab-978657470526

区块链核心 – 数字签名



数字签名模式：一个数字签名模式有下面三个算法组成:

- **(sk, pk) := generateKeys(*keysize*)**

密钥生成函数将任意输入产生一对密钥，私钥sk 被私藏并用来对数据签名。公钥pk 可以分发给所有人拿来做校验用，任何人拿到公钥都可以校验出签名者。

- **sig := sign(*sk* , *message*)**

签名函数用私钥sk和需要签名的数据产生数字签名

- **isValid := verify(*pk* , *message* , *sig*)**

校验函数用签名者的公钥，签名的数据，签名本身可以校验出签名的真实性。

要求:

- 真实的签名一定可以通过校验函数校验
  verify (*pk* , *message* , **sign** (*sk* , *message*)) == **true**
- 数字签名不可伪造

区块链核心技术和原理

分布式共识机制

- 所有节点同意全网校验过的交易记录

区块链通过不同的分布式共识协议获得自己特有的去中心化结果

区块链通讯协议实现的去中心化通过如下五个逻辑来实现差异化：

01 谁维护（存储/交换）交易记录账本?

02 谁有权限决定一笔交易是合法的？

03 谁是初始数字资产的产生者?

04 谁可以修改系统规则?

05 数字资产交换谁怎么获利?

区块链 – 去中心化和分布式共识机制 – 常见类型

所有人可访问，完全去中心化，任何人任何时间都可以访问系统读数据确认交易并竞争交易记录修改权

Public Chain 1

Private Chain 2

严格限制的参与节点，指定的组织控制区块数据写权限。高效，高私密性，低成本减少被攻击的可能。很多大型的金融机构偏好这种类型。

由多家机构管理，管理机构运营的多个节点，只有这些特定节点可以有读写交易数据，数据在这些节点间传递，共同记账。

Consortium Chain 3

Permissioned Chain 4

每一个参与节点都必须得到许可，没有许可不可以访问系统。私有链和联盟链属于许可链。许可链上的可以不需要指令牌。

也存在混合链，所有的节点根据情况有不同的许可和权限。

（Enterprise Blockchain）

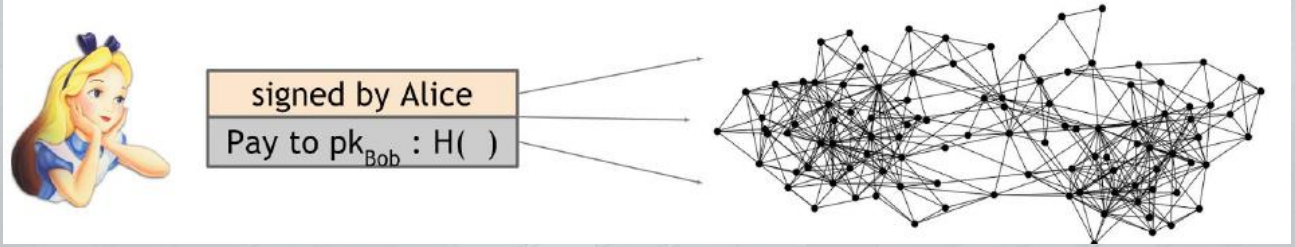
分布式同时协议：

假设有n个节点每个节点都有一个输入值，有些节点是存在故障或有意进行恶意攻击

一个有效的分布式共识机制必须做到：

1. 价值共识是由所有的诚实节点做出的
2. 价值必须是由诚实节点产生

交易记录广播： 如果Alice要支付数字货币给Bob，Alice必须把交易记录向整个点对点分布的比特币网络广播这笔交易. 1. 激励机制 2. 合理的延迟保证随机性



比特币共识算法(简化版)

假设随机选取的节点不是被攻击的假身份节点。

01 新交易记录向所有节点全网广播

02 每个节点都将接收到的交易数据写到区块链数据块中

03 写节点是随机的并马上把结果数据块全网广播

04 任一节点接受新的数据块前必须对所有的交易记录校验通过(未支付，签名合法）

05 接受节点将自己的哈希加到所认可的数据块中做背书

为什么比特币共识机制有效？因为它成功的防止了如下几种攻击：

Stealing Asset

要花掉币必须有所有权产生合法的交易记录。需要篡改持币人的数字签名。只要数字签名模式足够安全，外人无法通过篡改数字签名来盗窃数字资产（比特币）

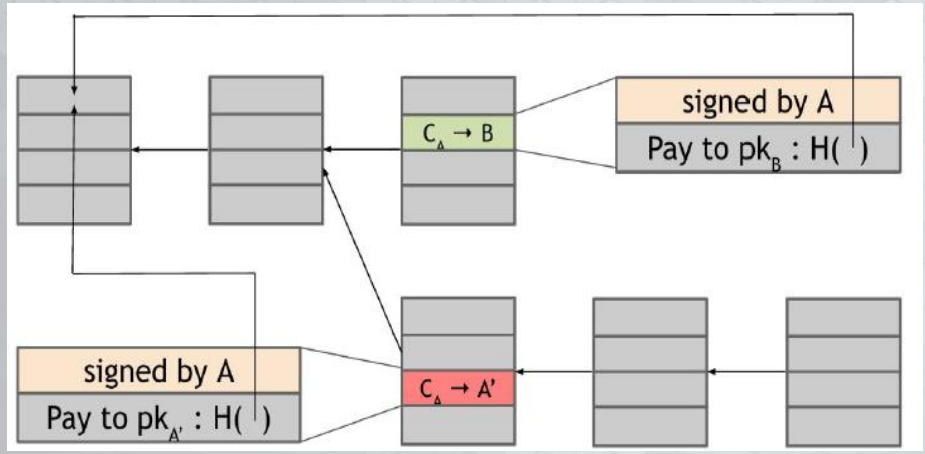
Denial of Service Attack

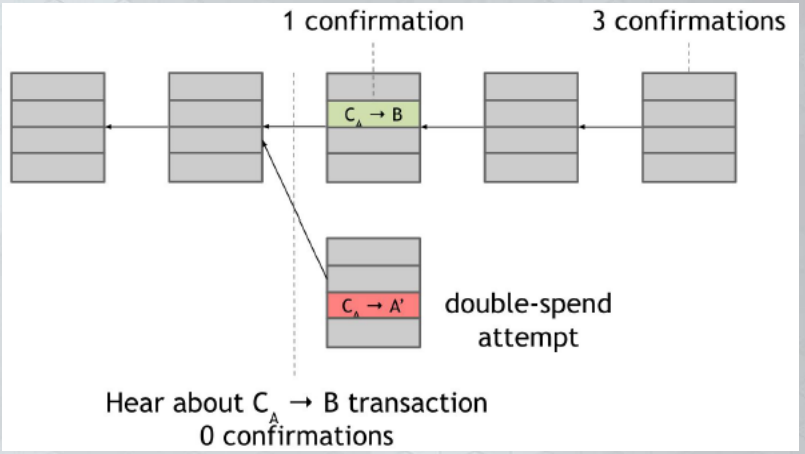
如果Alice收到Bob签名并支付的数字货币而拒绝接受并将认可的数据块写入自己广播出去的区块链中，那Bob只需要稍微等一下，所有诚实的校验过Bob合法签名和支付的节点广播过来接受的数据块就可以确保支付被记录，广播和接受传递。

Double Spending Attack

同一个币被同时花在两笔不同的交易中的时候只有一个交易记录会被合法写入区块链中。比如如果Alice成功的将已经支付给Bob的货币在支付给自己，那她支付给Bob的交易记录就会通不过校验而添加不到再新一轮追加的数据块中，原支付成为孤链而被摒弃。

双花企图 (Double Spending attempt.)





Alice creates two transactions: one in which she sends Bob Bitcoins, and a second in which she double spends those Bitcoins by sending them to a different address that she controls. As they spend the same Bitcoins, only one of these transactions can be included in the block chain. The arrows are pointers from one block to the previous block that it extends including a hash of that previous block within its own contents. CA is used to denote a coin owned by Alice.

This is what Alice's double-spend attempt looks like from Bob the merchant's viewpoint. In order to protect himself from this attack, Bob should wait until the transaction with which Alice pays him is included in the block chain and has several confirmations..

区块链核心技术 – 以太坊，超级账本与智能合约

以太坊Ethereum和超级账本Hyperledger是一个开源的区块链底层系统，提供各种API和接口快速开发区块链应用，另外还有R3(Corda)，Ripple等

以太坊Ethereum和超级账本Hyperledger都是是一个开源的区块链底层系统技术构架，就像安卓一样，提供了非常丰富的API和接口，让许多人在上面能够快速开发出各种区块链应用，而以太坊和超级账本很大的特色就是能够实现智能合约。另外还有银行联盟R3(Corda)，跨境资产转移Ripple。

智能合约

区块链为智能合约提供可信执行环境，智能合约为区块链扩展应用。智能合约一旦设立指定后，能够无需中介的参与自动执行，并且没有人可以阻止它的运行。而在以太坊和超级账本上的智能合约，能够控制区块链上各种数字资产进行复杂的操作

区块链核心技术 – 智能合约

智能合约是一种可自动执行的合约。买卖双方达成合约，并以程序代码的形式固定下来。代码和达成的协议就存在于一个分布式的，去中心化的区块链网络

区块链发展以及展望

区块链发展阶段

洪荒时代

1. 2008年金融危机后

蛮荒时代

1. 2012年始
2. 基于原始的链

拓荒时代

1. 2015年
2. 以太坊

觉醒时代

1. 2017年
2. ICO

区块链元年

1. 底层链
2. 杀手级应用

区块链展望

底层链

- TPS不足
- 块的大小不足

应用

- 社交
- 游戏
- 金融
- 供应链
- 存证/取证
- …

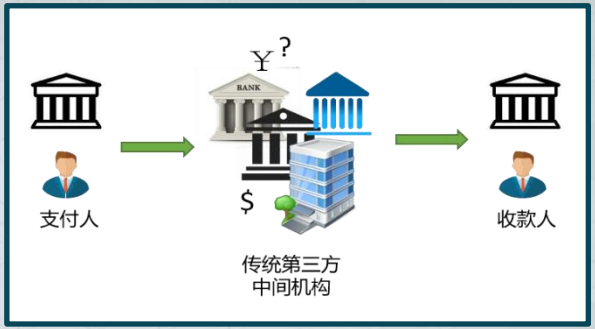
周围相关

- 交易平台
- 矿机/矿池
- 钱包

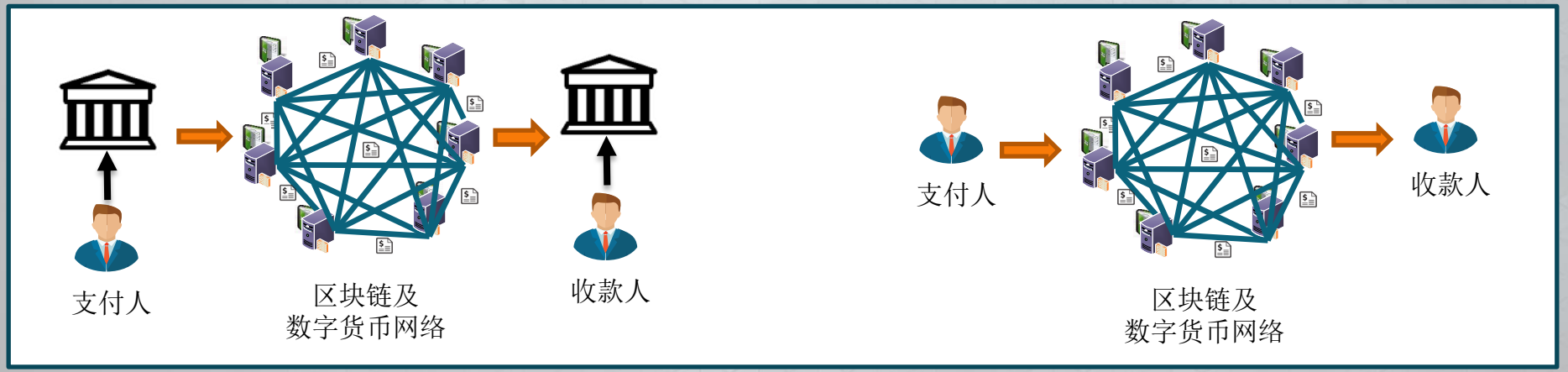
区块链技术的应用

区块链金融服务 – 跨境支付

基于区块链技术的支付通过数字货币（数字资产）完成资产转移，终极情况甚至可以不需要通过传统金融机构



机构内部或远程分支机构可以通过高度安全和信任的联盟链及私有链完成资产转移。



区块链技术在金融服务的应用

私人证券/私募基金

- NASDAQ利用Chain.com技术开办什么基金交易所用于管理pre-IPO和私募基金和证券交易
- 香港也在出现用区块链技术做的交易所尝试

保险行业

- Tradle提供了解你的客户应用简化并加快入职流程2016/08
- SafeShare设立了基于区块链技术的平台记录英国的按需式保险产品2016/03
- 安联宣布一项可以自动完成巨灾互换交易的原型测试成功2016/06
- Blem，一家在保险解决方案提供商与Z/Yen集团合作在区块链上记录索赔事件，能够准确的在保险公司和再保险公司之间分解成本2016/05
- Everledger将钻石交易记录上区块链并提供保险业务

麦肯锡公司报告

麦肯锡公司调查了200家公司企业，发现了64种不同的使用案例。该报告声称**保险行业**是最大的比特币区块链解决方案—22%。之后是支付行业—13%。金融服务总体上占据了50%的使用案例。就美元价值而言，最大的创收领域就是跨境企业对企业支付，收入高达500—600亿美元，排在之后的是贸易金融，140-170亿美元。

- 供应链金融：区块链能够降低成本和提高周转速度，可增加**140-170**亿美元的收入。
- 跨境**B2B**支付：区块链可以带来更低的成本和手续费，同时加快支付服务速度，将节约大约**500-600**亿美元。
- 跨境**P2P**支付：与**B2B**支付一样，区块链也可以降低该领域的成本同时加快速度，不过对于个人汇款，预计可以节约**30-50**以美元。
- 回购协议交易：区块链可以降低这种交易的成和系统性风险，预计价值大约**20-50**亿美元。
- **OTC**衍生品市场：区块链可简化结算流程，从而降低运营成本以及对资本的需要，预计可节约大约**40-70**亿美元。
- **KYC/AML**管理：区块链可减少重复工作以及疏通介入流程，预计可带来**40-80**亿美元收入。
- 身份欺诈：区块链带来更高的安全性，让消费者少受损失，预计可以节约**70-90**亿美元。

区块链技术建立开放，信任可溯源的产品供应链管理

WHAT 1

消费者要求获得真实透明关于产品的原产地，生产流程细节及物流信息。政府也需要了解企业的供应链细节信息，惩罚违规行为。提供商品供应链全周期管理建立信任关系来系统性的确保产品质量，安全，合规。

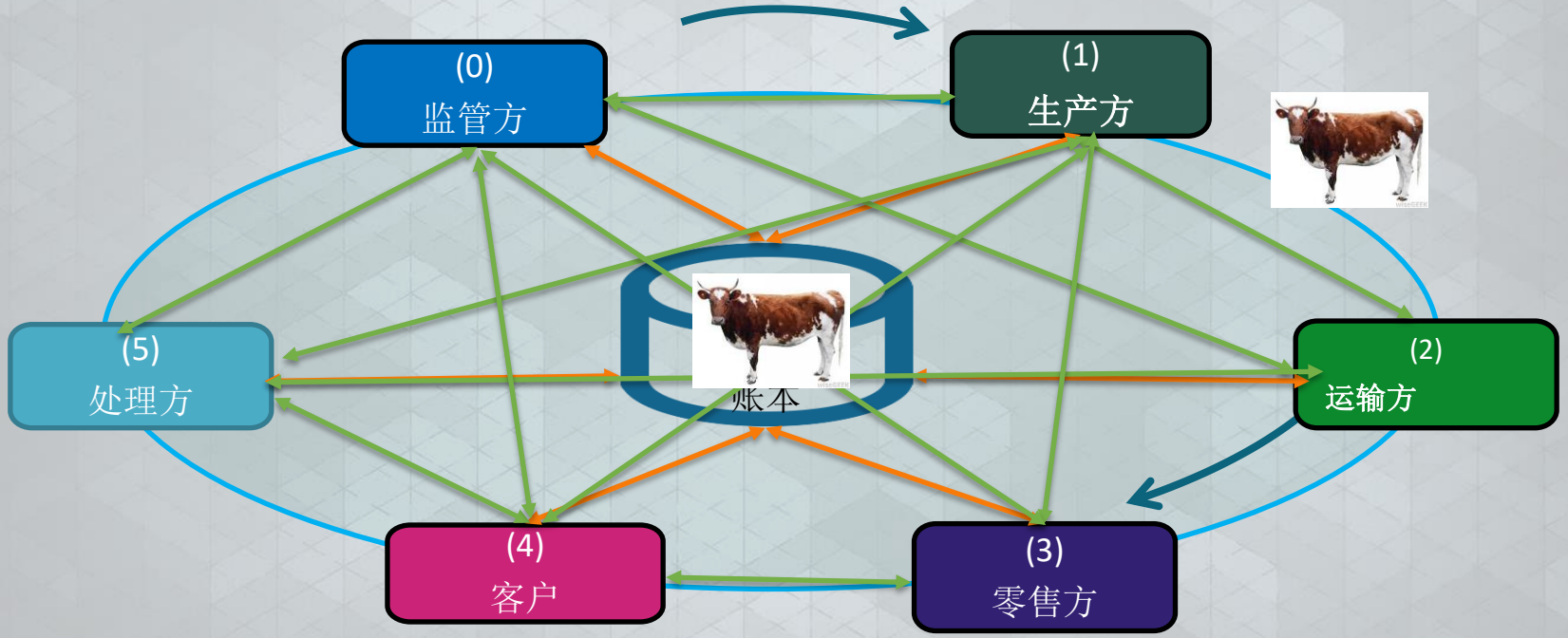
HOW 2

区块链技术确保产品安全完整不被篡改的在产品供应链中端到端的安全传递。

BENEFIT 3

- 可校验，防止任何单位和个人在全球供应链和物流过程中篡改信息挑战产品的合法性
- 允许消费者更明智清晰的做出购买选择
- 政府可快速便捷的从产品供应链各个节点获取可信赖的信息用于监管

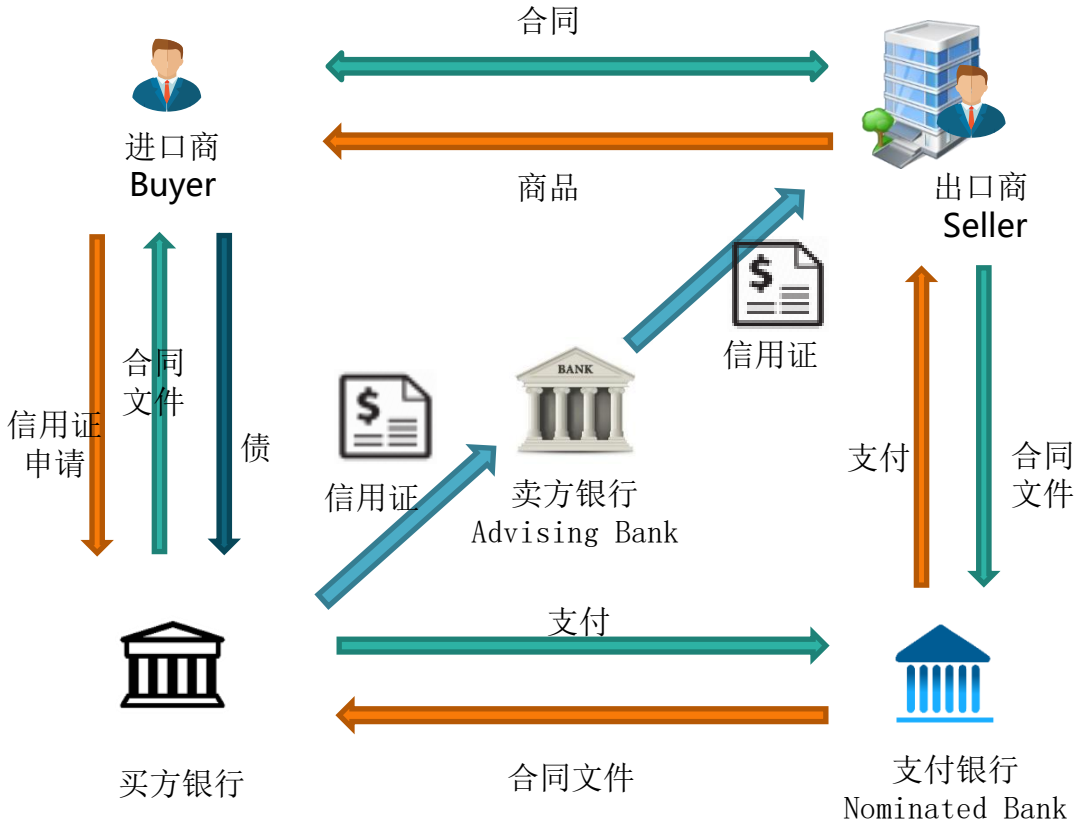
产品端对端全生命周期流程供应链管理



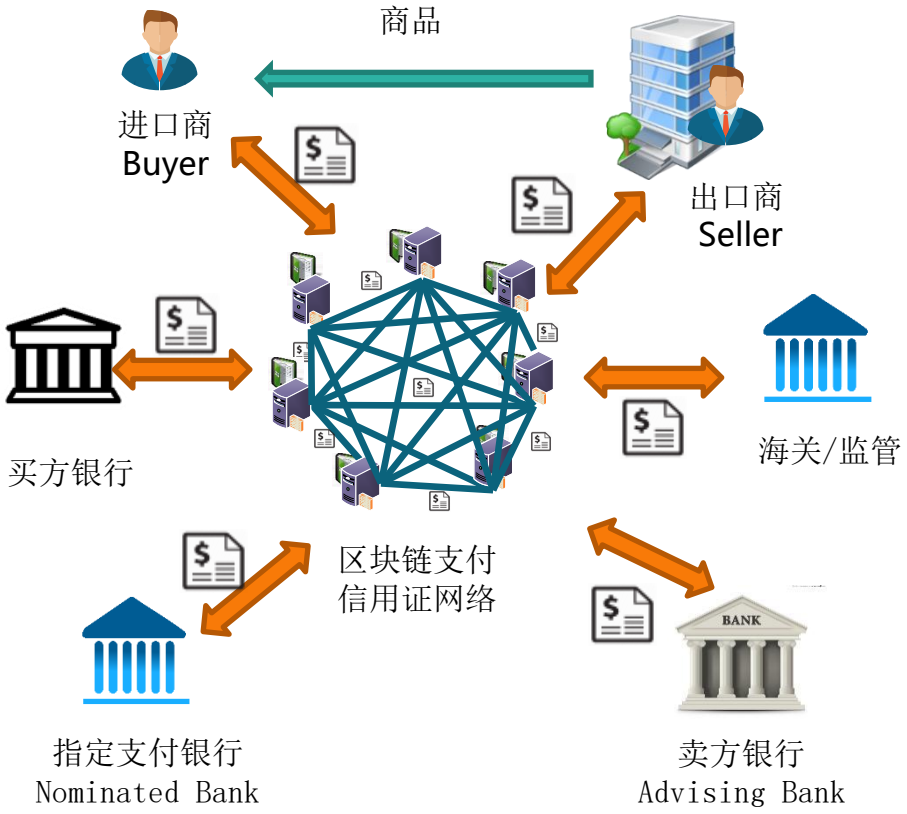
区块链技术用于政府与供应链管理

- 沃尔玛联合IBM和清华大学使用超级账本技术打造区块链试行项目，保障中国猪肉市场供应链
- 美国国土安全局测试使用区块链跟踪跨境人口和商品，防止黑客攻击物联网设备。区块链分布式账本可以永久地存储交易详细信息，通过加密来确保这些数据的安全，这样这些数据就无法被篡改。通过存储到区块链上，设备数据，如在美国边境来回的旅客和商品的视频和其他类型信息，就会很安全。区块链技术未来可能还会被用于维护数据完整性，从而在之后作为起诉的证据。
- 澳大利亚邮政已计划将区块链技术用于选举投票。这一系统将做到防篡改、可追溯、匿名和安全。
- 新加坡政府正寻求用区块链技术保护进出口货运公司免受诈骗银行之害。交易的装货清单将被记录在电子分类账上，一旦重复录入，所有银行都将收到提醒。
- 瑞典正在土地注册系统中使用区块链技术。只要交易双方同意，土地交易将被记录在区块链上，所有相关方面都能够对土地交易进行实施监控，确保没有诈骗行为。该系统还允许所有交易相关方面监控交易进展，包括卖家、买家、不动产中介、银行以及土地注册局自身。
- 六月，英国政府进行了区块链试点，跟踪福利基金的分配以及使用情况。这一计划能够提供金融参与度的深度信息，并为财政预算提供支持。

区块链技术 – 传统信用证


合同
进口商
Buyer
商品
出口商
Seller
信用证
申请
合同
文件
债
信用证
BANK
卖方银行
Advising Bank
信用证
支付
合同
文件
支付
买方银行
合同文件
支付银行
Nominated Bank

区块链技术 – 区块链信用证



- 区块链类型：私有链，联盟链，公有链，许可链，混合链？
- 共识机制是什么，谁来制定或牵头？
- 什么样的监管机制和法规？
- 银行保险等金融机构间数据保密性
- 商业秘密如何保护，（区块链交易数据隐私）
- 什么样的信用证智能合约？
- 用户联盟 vs. 技术构架联盟

区块链社交

区块链社交的技术需求

技术需求

并发

社区/群组活动经常有抢红包，秒杀，或者抢答等场景，随着登录用户数的提高，对于区块链的并发性能，吞吐率提出了更高的要求

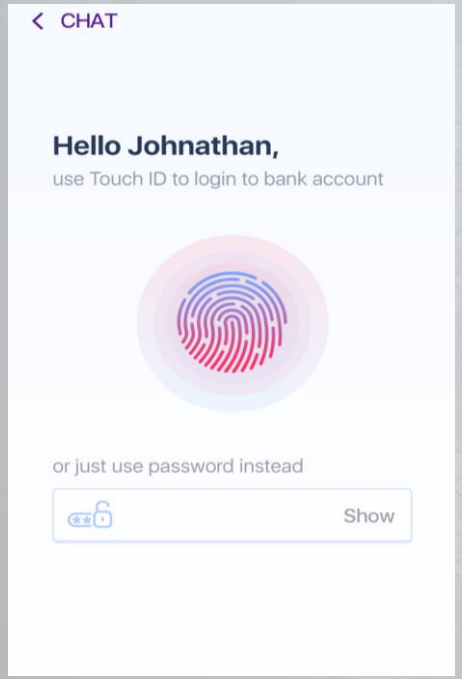
私密安全性

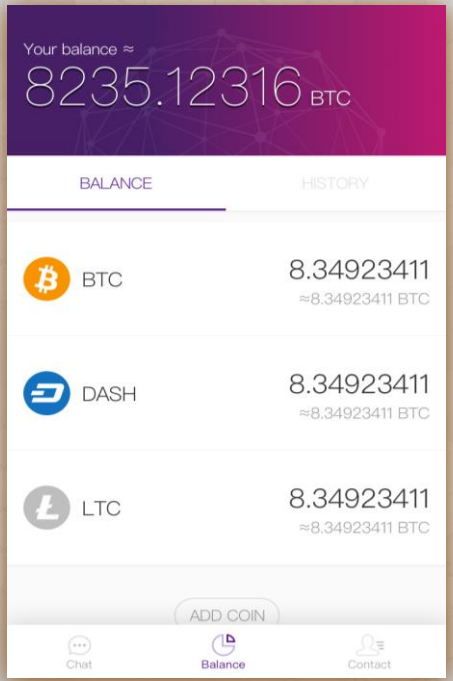
聊天，会话需要安全性的保证，同时，信息在区块链上的传输必须有唯一标识，不会泄露，让用户放心使用

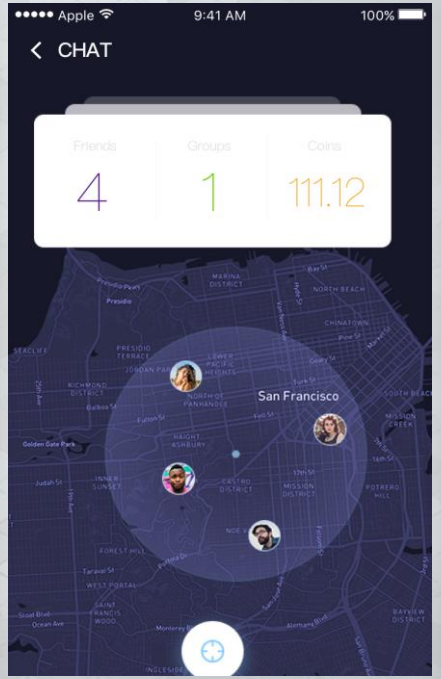
即时/实时性

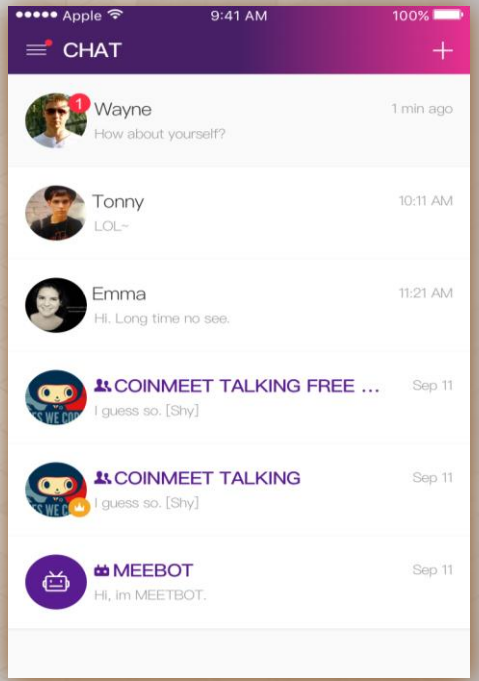
社交活动主要特点在于交互性，互动性。活动信息必须能及时的传递，显示。而传输速度是P2P网络的一大软肋

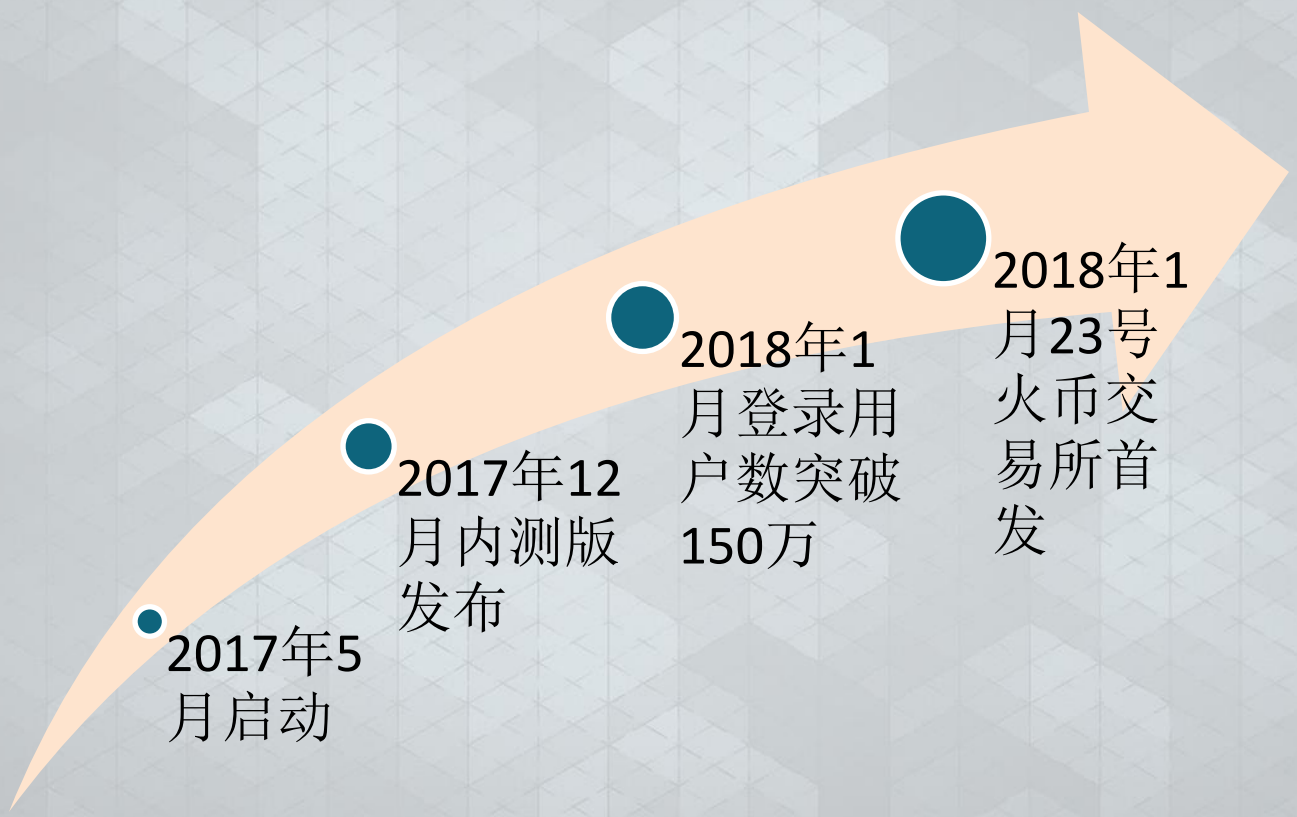
Coinmeet 覆盖了从通讯社交，身份认证，交易支付到娱乐游戏的全方位功能










2017年5月启动
2017年12月内测版发布
2018年1月登录用户数突破150万
2018年1月23号火币交易所首发

谢谢聆听

Q&A

By 郑嘉文

- 2018/02 -