山东大学
SHANDONG UNIVERSITY

网络与大数据安全

5 – Blockchain

李琨
Email: kunli@sdu.edu.cn

学无止境 气有浩然

目录

CONTENTS

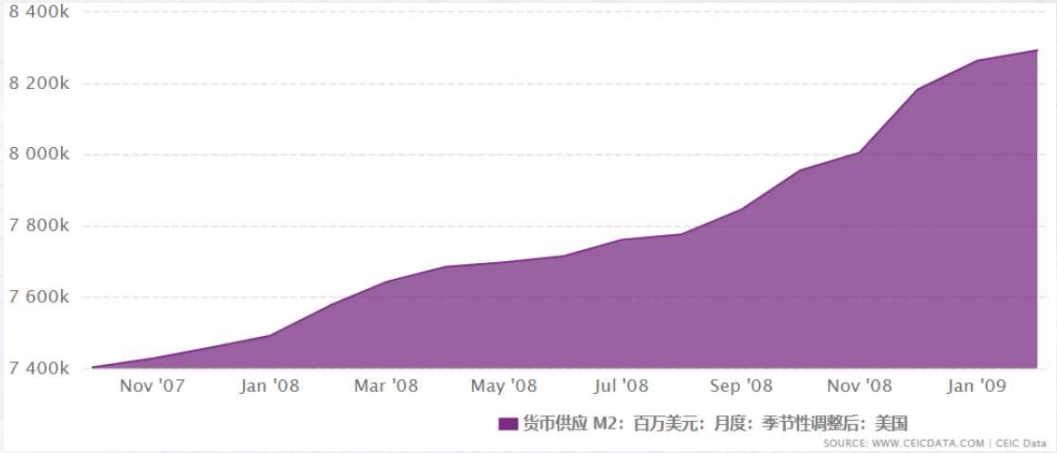
区块链起源

横空出世——比特币与区块链1.0

2008年，美国次贷危机爆发

美国为了避免由第四大投资银行雷曼兄弟的倒闭引发金融机构连锁反应而实行量化宽松政策，即疯狂加印钞票

有没有一种货币可以保障人民财产权不被侵犯、货币可以超越主权，不被第三方机构控制，也不会超发、滥发？



2007年11月-2009年1月美国的货币发行量(M2)

同年，中本聪发布了《比特币：一种点对点的电子现金系统》的论文

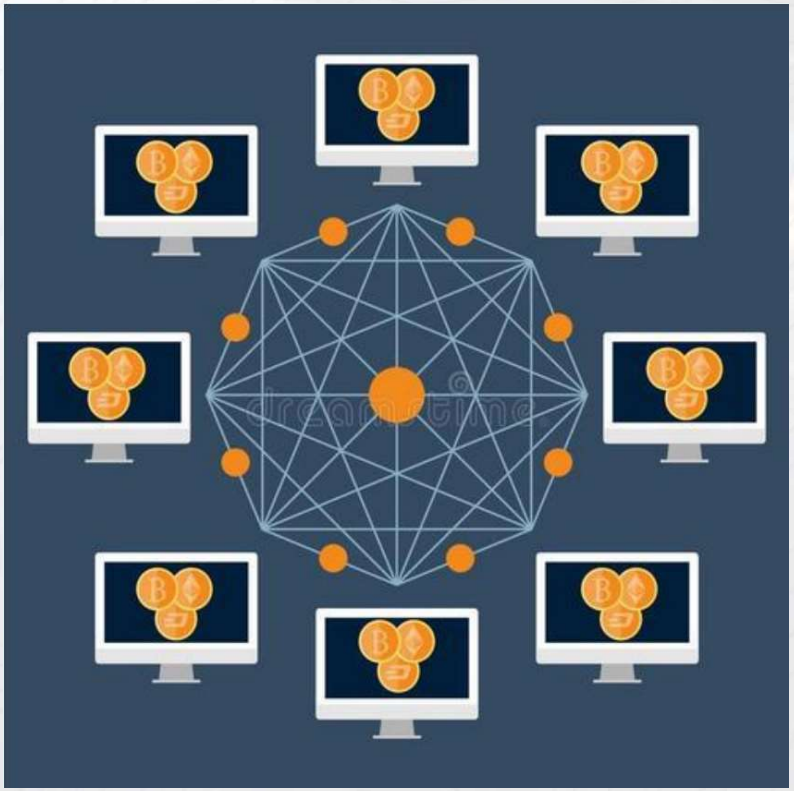
- 提出一种完全通过点对点技术实现电子现金系统
- 信用建立在密码学原理而不基于某个中心
- 买卖双方直接交易，无需第三方金融机构
- 为了防止比特币的超发、滥发，杜绝通货膨胀，在比特币设计上限制了比特币发行上限不超过2100万个

横空出世——比特币与区块链1.0

区块链1.0：以比特币为代表的去中心化虚拟货币

宏伟蓝图

- 希望不依赖于各国央行的发布
- 统一全球化货币



燎原之火——以太坊与区块链2.0

区块链2.0的诞生：以太坊（2014）

以太坊是一个开源的有智能合约功能的公共区块链平台

以太坊的**智能合约技术**使区块链的应用从货币体系发展到了股权，债券登记，转让各种执行手段和防伪应用，大大的扩展了区块链技术的应用

区块链的2.0，可以理解为是一种可编程金融

细水长流——区块链3.0的展望

2018年——区块链元年：

赋能实体经济，加速落地应用

区块链3.0：指被应用到除金融以外的各个领域，不再需要第三方信任认证机构的前提下，实现信息的交换和共享，达到人与人之间的信任，变革生产关系

中共中央政治局第十八次集体学习中，中共中央总书记习近平在主持学习时强调，区块链技术的集成应用在新的技术革新和产业变革中起着重要作用。我们要把区块链作为核心技术自主创新的重要突破口，明确主攻方向，加大投入力度，着力攻克一批关键核心技术，加快推动区块链技术和产业创新发展。


人民日报 海外版
PEOPLE'S DAILY OVERSEAS EDITION
主持中央政治局第十八次集体学习
习近平：把区块链作为核心技术自主创新重要突破口
同巴西总统博索纳罗会谈
习近平：做以诚相交的好朋友、相互支持的好伙伴
习近平会见出席2019年"读懂中国"国际会议的外方嘉宾代表
对中医药工作作出重要指示
习近平：传承精华守正创新
李克强作出批示

比特币大事记

2008年 比特币诞生

美国金融危机爆发，欧洲国家债权危机，全球经济衰退。在这样一个环境下，比特币诞生。比特币创造者中本聪的身份至今成谜。

2009年 第一个比特币

首个比特币客户端发布，中本聪亲手创建了第一个区块——创世区块，并获得了第一笔50枚比特币的奖励，第一个比特币就此问世。

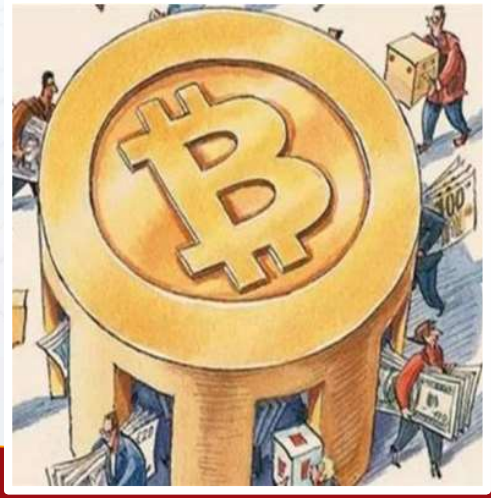
2010年 比特币用于交易

美国程序员拉兹洛用10000个比特币买了2个价值25美元的披萨（史称"最贵的披萨"），比特币产生了自己的价值。

比特币大事记

2010年 比特币进入市场

3月，第一个比特币交易所上线。7月，著名比特币交易所Mt.gox成立，一度成为世界最大的比特币交易所，这标志着比特币真正进入了市场。



2011年 比特币走向大众

美国《连线》杂志刊登了一篇文章，向公众介绍这个开源软件的数字货币，并提到了价格快速上涨的现象。随后各家媒体也先后进行相关报道。

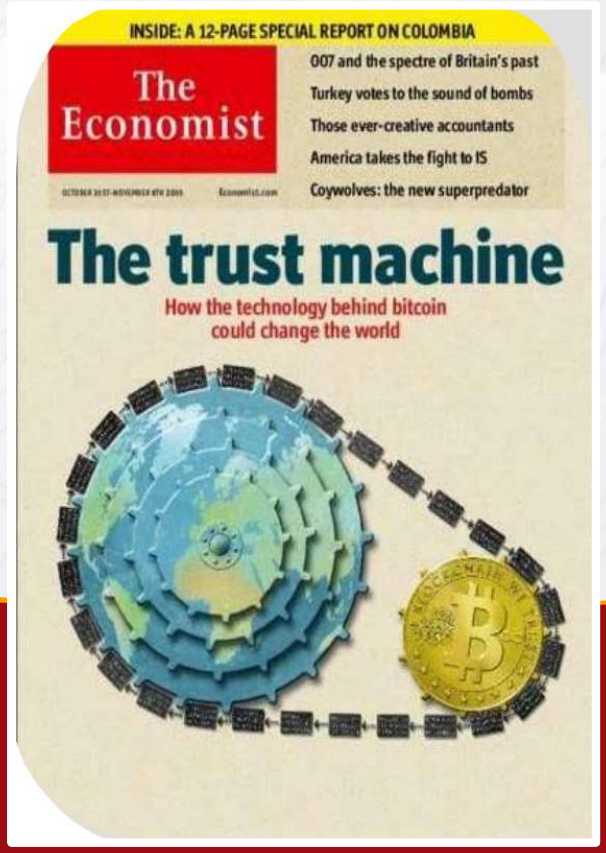
2012年 首次产能减半

陆续多家实体经济供应商宣布接受比特币支付，比特币价格开始回升。11月28日，比特币产出迎来首次"产能减半"，每个区块产生的比特币从50个减至25个。

比特币大事记

2013年 市场总值超10亿

2013年3月，比特币市场总值超过10亿美元，2013年11月底，比特币成交价首次突破1000美元,总市值超100亿美元,市值的10倍增长不到10个月。



2014年-2015年

比特币影响范围、影响能力逐步扩大，引发大量的黑客攻击、盗取比特币等比特币犯罪事件。比特币贪污、犯罪高发。比特币被更多商业公司接纳，许多机构、政府、组织就比特币问题陆续表态。

2015年10月，比特币登上“经济学人”杂志首页。

比特币大事记

2016年 升级与再减半

比特币核心钱包Bitcoin Core进行了诞生以来的最大一次升级，全世界交易量激增。7月9日，区块报酬第二次减半。

2017年 比特币合法支付

2017年4月，日本将比特币宣布为合法的支付方式。同一时期，著名的比特币勒索病毒WannaCry肆虐全球，造成一场全球性互联网灾难。

2017年 比特币“硬分叉”

7月，比特币扩容导致了比特币的“硬分叉”。比特币被“分拆”成比特币（BTC）和比特币现金（BCH）。

比特币大事记

2017年 ICO冲击比特币

9月，ICO监管风暴到来，中国开始关闭所有比特币和加密货币交易所，比特币价格剧烈震荡 。

2017年年底 达到峰值

11月，比特币单价首次突破1万美元。12月，比特币单价甚至达到2万美元，达到比特币的价值顶峰。

2018年至今 比特币震荡

2018年迎来比特币单价大瀑布，在2018年初单价就从2万美元跌至1万美元左右。之后比特币价值持续震荡，19年11月单价在7千美元左右。

小结——区块链技术的发展

区块链1.0

数字货币 去中心化

代表：比特币 、莱特币

具有支付、流通等货币职能

区块链2.0

智能合约 数字资产 金融应用

可编程金融：是对金融领域的使用场景和流程进行梳理、优化的应用

代表：以太坊、瑞波币

区块链3.0

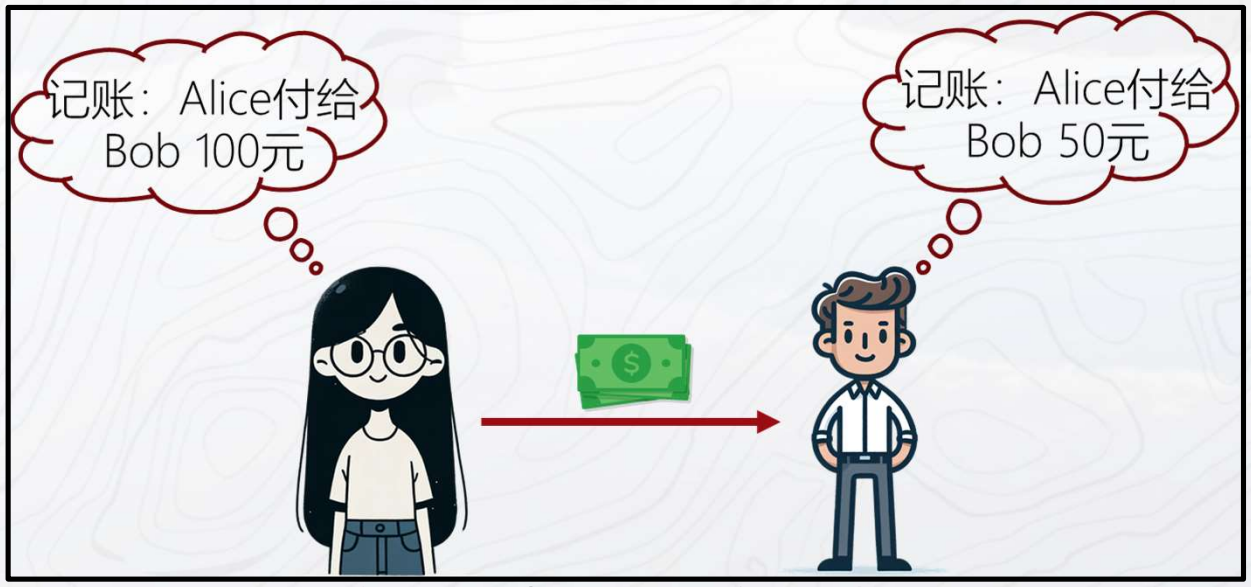
去中心化互信网络
去中心化信任机制

代表：iota、cardano

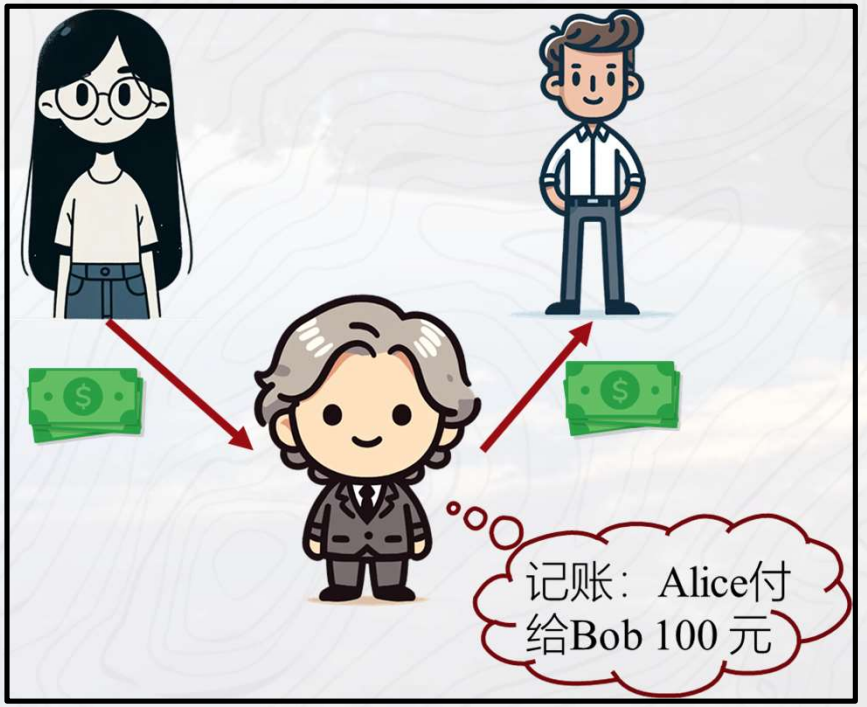
可编程社会：为各种行业提供去中心化解决方案

区块链简介

从交易记账说起——Alice和Bob交易



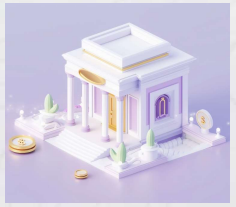
交易账本对不上怎么办?



引入可信第三方

依赖第三方的中心化交易面临问题：

1. 较高的手续费
2. 隐私泄露风险
3. 第三方的不可靠性

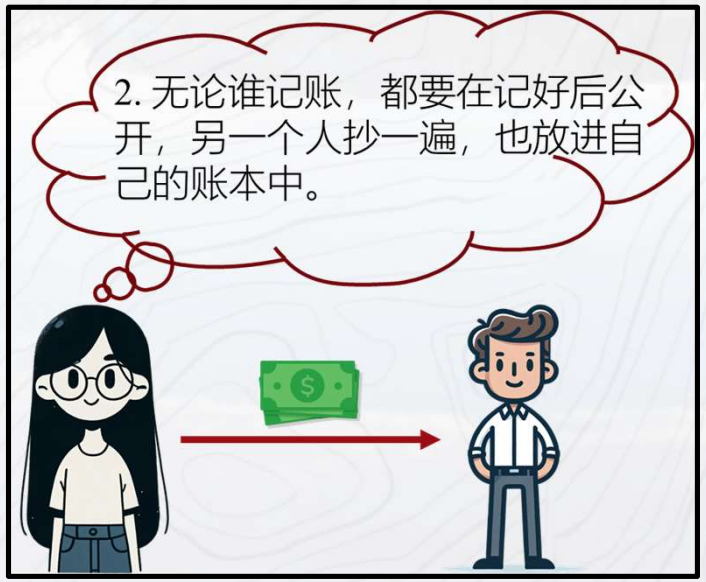


银行

支付宝

微信支付

从交易记账说起——Alice和Bob交易



如果一笔交易两个人都记账，容易记岔；

如果每次都是同一个人记账，这个人很容易做假账；

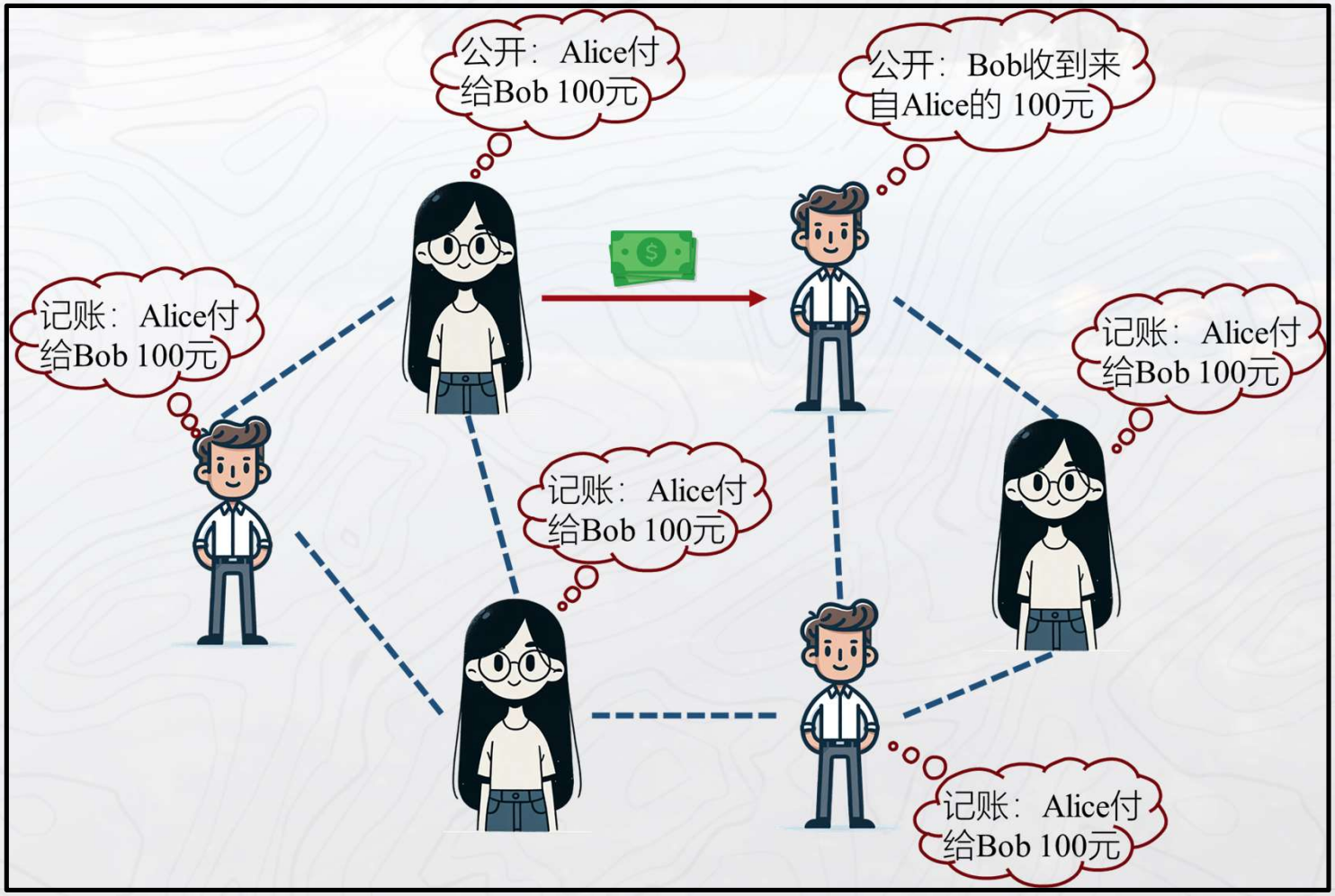
当交易系统中有很多人时，每次记账后所有人都要抄一遍，这样的备份既防丢失，也防篡改；

账目一旦记好盖章，就不能再修改了。

*实际上在区块链系统中，并不是剪刀石头布这样简单的方式决定记账人，但同样具有随机性。

*区块链交易系统中的交易内容是可以加密的，尽管密文全网同步存储，但只有具备密钥才能解密。

区块链交易记账方式


公开：Alice付给Bob 100元
公开：Bob收到来自Alice的 100元
记账：Alice付给Bob 100元
记账：Alice付给Bob 100元
记账：Alice付给Bob 100元
记账：Alice付给Bob 100元

什么是区块链

区块链本质上是一个去中心化的分布式账本数据库，目的是解决交易信任问题。

- 广义来看，区块链技术是利用块链式数据结构验证与存储数据、利用分布式节点共识算法生成和更新数据、利用密码学方式保证数据传输和访问的安全、利用自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。
- 狭义来看，区块链是一种按照时间顺序将数据区块以顺序相连的方式组合成的一种链式数据结构，并以密码学方式保证的不可篡改和不可伪造的分布式账本。

区块链分类

类型		特性
公有链		世界上任何个体或团体都能发送交易，且交易能获得该区块链的有效确认 任何人均可参与其共识过程。 最早出现、目前应用最广泛的区块链。 现阶段每秒3~20 次数据写入。
许可链	联盟链	某个群体内部指定多个记账节点， 每个区块的生成由所有预选节点共同决定。 预选节点参与共识过程 其他接入节点可以参与交易 但不过问记账过程 ， 可满足监管(AML, Anti Money Laundering, 反洗钱/KYC, Know Your Customer, 客户识别） 。 现阶段每秒1000 次以上数据写入。
	私有链	仅使用区块链记账技术进行记账，某一组织或个人独享写入权限改善可审计性，不解决信任问题。

什么是区块链

从2009年比特币问世至今,区块链已经走过了第一个十年。十年间,区块链逐步进入大众视野,尤其是在单枚比特币的价格被炒作到近2万美元以后，整个社会对于比特币的关注度急剧上升。

一方面，乱象从生的自媒体流传着各种“币圈”暴富神话，各种鱼龙混杂的区块链项目浮出水面，其中不乏打着区块链技术创新名号，实则通过ICO融资圈钱的低质量项目。

另一方面，区块链技术本身吸引了越来越多的人对其进行深入研究并探索其宽广的应用空间：各地政府对区块链积极扶持，国内外科技及金融巨头纷纷涉足区块链行业。

背后隐患　　新华社发 朱慧卿 作

专家提醒　　新华社发 朱慧卿 作

区块链技术详解

中心化交易vs分布式交易

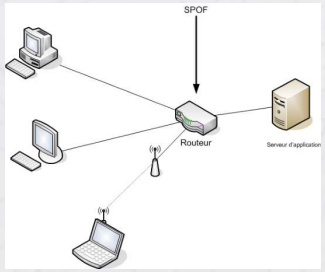
① 买家下单并把钱打给淘宝；
② 淘宝收款后通知卖家可以发货了；
③ 卖家收到淘宝通知之后给买家发货；
④ 买家收到书之后，觉得满意，在淘宝上选择确认收货；
⑤ 淘宝收到通知，把款项打给卖家。

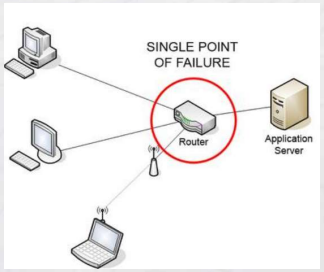
中心信任问题

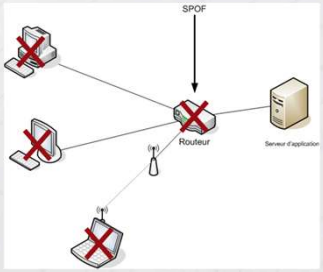
中心化系统由资金雄厚和技术实力强大的机构、企业做信任背书，只能完全信任中心节点。

单点故障问题

全部交易记录和账本都存储在支付宝服务器上，一旦所有相关的服务器被攻击，交易记录、余额宝的钱就会消失。

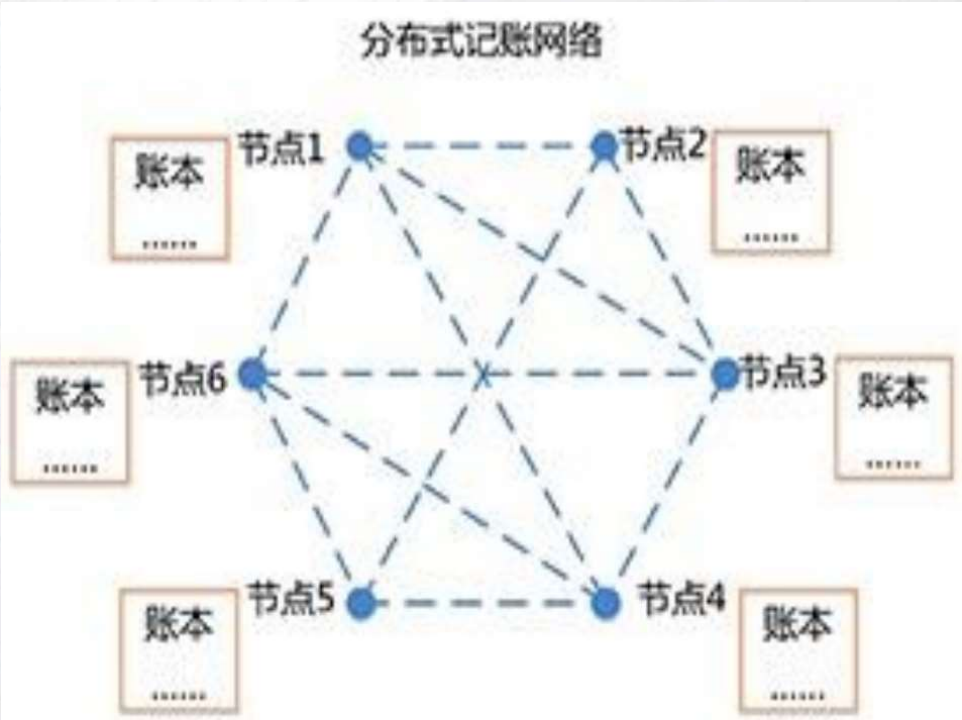






中心化交易vs分布式交易

① 买家下单并把钱打给卖家；
② 买家将这条转账信息记录在自己账本上；
③ 将这条转账信息广播出去；
④ 卖家和其他人在收到买家的转账信息之后，在他们自己的账本上分别记录；
⑤ 卖家发货，同时将发货的事实记录在自己的账本上；
⑥ 卖家把这条事实记录广播出去；
⑦ 买家和其他人收到这条事实记录，在自己的账本上分别记录；
⑧ 买家收到书籍。



分布式交易系统面临的问题

- **为什么人们愿意做记账的志愿者?**

我是A，其他X、Y、Z的交易记录跟我无关我为什么还要去记录呢?

- **这些交易记录以谁为准?**

比如因为网络延迟，有的账单先记录交易1，再记录交易2，再记录3...；有的账单先记录交易2，再记录交易3，再记录1...。每个人的记的账本都不一样。

- **怎么进行交易记录的防伪?**

比如B给了A 10个比特币，A如果记录成B给了A 1个比特币，怎么防止篡改?

- **如何防止双重支付?**

比如A有5个比特币，他同时把这5个比特币寄给了B又给了C，怎么办?

分布式交易系统面临的问题

- 为什么人们愿意做记账的志愿者？

答：因为记账有奖励：

① 手续费收益：由交易方给

② 打包（记账）奖励：由区块链系统给

一开始每打一个包奖励50个比特币，过4年之后每打一个包奖励25个比特币，再过4年，每打一个包奖励12.5个比特币。

每过4年，奖励减半，这样算下来，到2140年时，将不再有新的比特币产生，最终流通中的比特币将总是略低于2100万个。

分布式交易系统面临的问题

- 这些交易记录以谁为准?

如果人人都负责记账，需要的记账奖励就非常高

比特币的方法：让想记账的人解一道数学题

- 这个数学题非常难，用人脑是算不出的，必须要用计算机才能算出
- 这个数学题不看脑子的聪明程度，而完全是看解题的工作量和勤奋程度
- 每个数学题的答案需要用计算机不断去解题试错，试的次数越多，解出来的可能性越大 （这就是为什么有些人拼命买矿机，因为矿机越多解出来的概率越大。）
- 这个数学题的求解需要不断试错才能得到，而验证这个解的正确性只需要进行非常简单的运算。→哈希

分布式交易系统面临的问题

- 这些交易记录以谁为准?

如果人人都负责记账，需要的记账奖励就非常高

比特币的方法：让想记账的人解一道数学题→哈希

- 给出两个骰子，要求掷出的结果之和小于等于12。概率为1
- 给出两个骰子，要求掷出的结果之和小于等于8。概率为0.72
- 给出两个骰子，要求掷出的结果之和小于等于4。概率为0.11

分布式交易系统面临的问题

这些交易记录以谁为准?

如果人人都负责记账，需要的记账奖励就非常高

比特币的方法：让想记账的人解一道数学题→哈希

- 给定一个哈希值（区块内所有交易数据的哈希），要求记账人在该哈希值后面添加一个随机数字(一般是从零开始递增)，然后再去计算这个结果的哈希值，直到求出来的哈希值小于某一个目标数字。
- 比特币系统会通过限制目标数字来动态调节难度，使得两个区块之间的间隔时间相对稳定。

分布式交易系统面临的问题

这些交易记录以谁为准?

如果人人都负责记账，需要的记账奖励就非常高

比特币的方法：让想记账的人解一道数学题→哈希

- 如果你试出了答案，那么你就有机会将收到的交易记录打包成一个区块放到区块链网络上。
- 可能有多个节点在同一个时间段内都解出了这个数学题，区块链系统就会比较打包时在区块上加盖的时间戳，选出最快的那一个作为有效区块，这就是区块链中的共识机制。交易记录就以有效区块的记录为准。
- 共识机制：全网节点对谁最终获得记账权达成共识的机制。
- 如果你第一个试出了答案，完成了打包，获得大家的认可，所有人都会以你打的这个包的交易记录为准，那么手续费和打包的比特币奖励就会归到你的名下。这个过程就叫做挖矿。

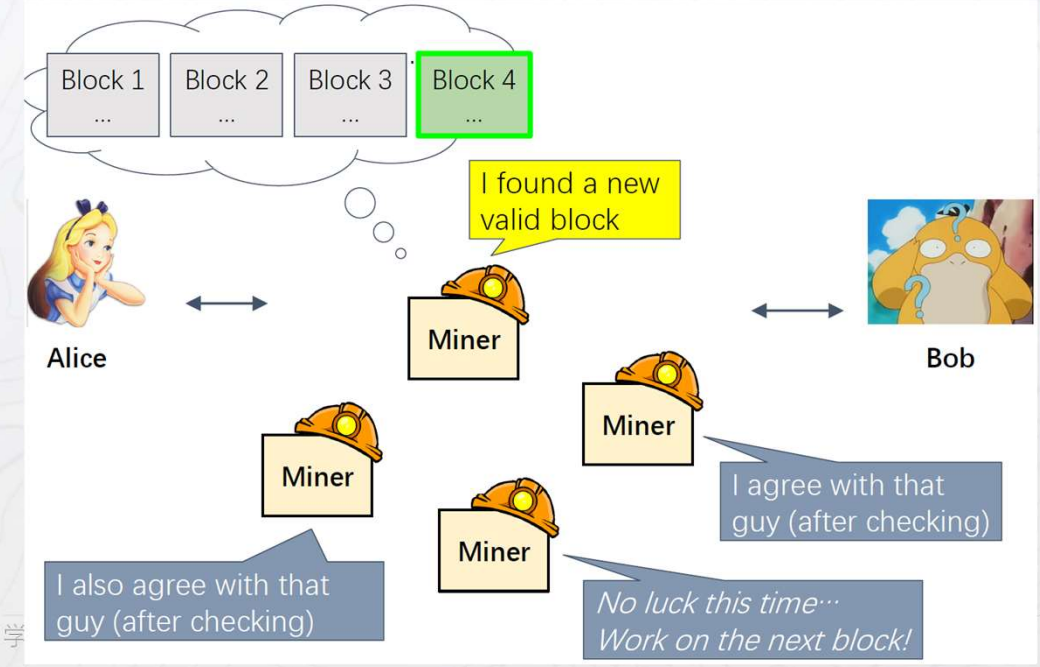
区块链共识

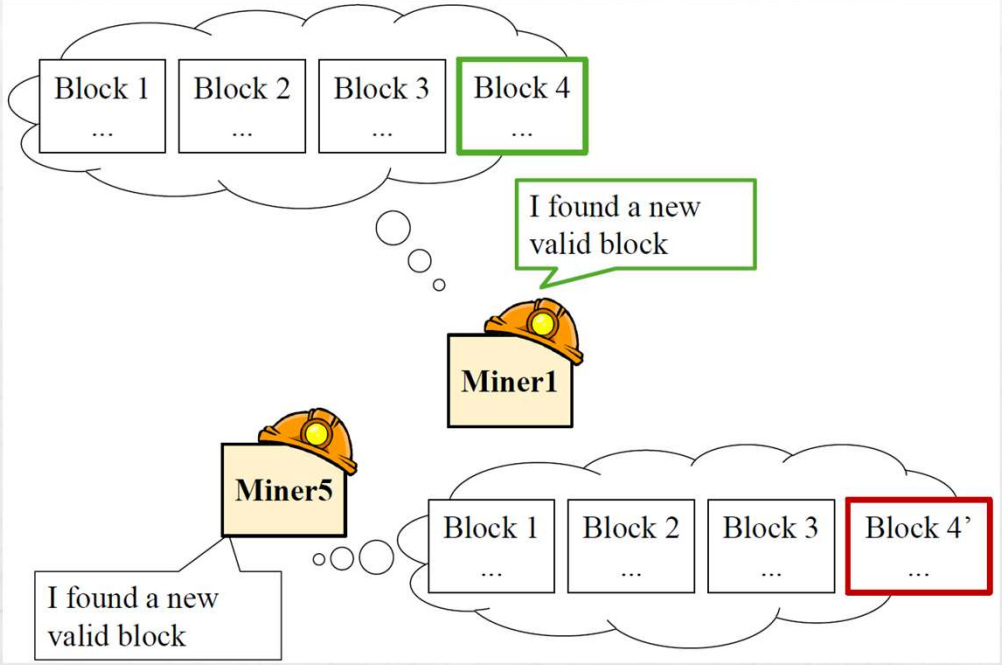
- 这些交易记录以谁为准?

  →共识机制：全网节点对谁最终获得记账权达成共识的机制。

比特币的方法：让想记账的人解一道数学题→工作量证明机制 (PoW, Proof of Work)

如果两个矿工同时成功怎么办?





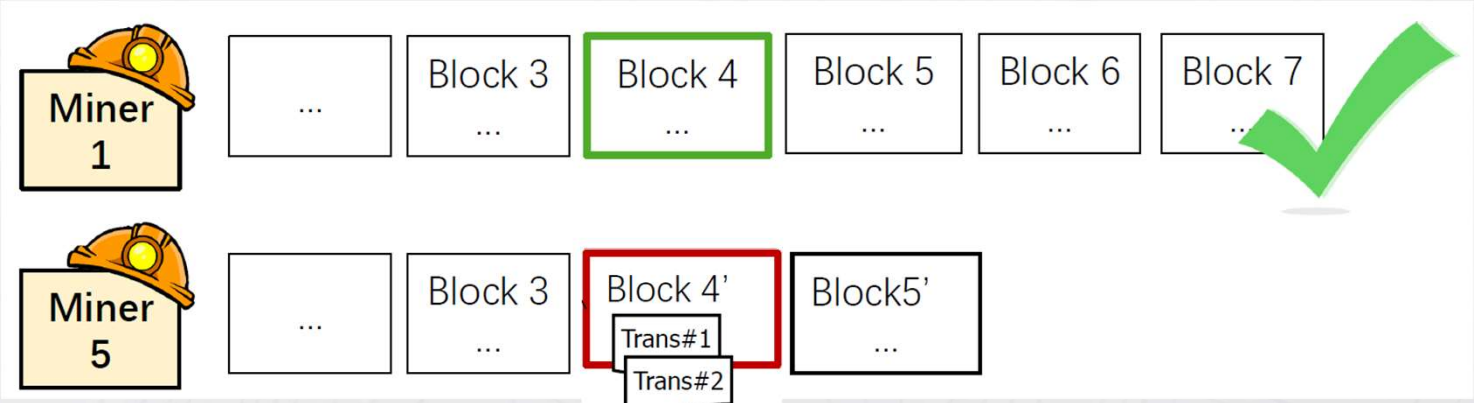
区块链共识

两个或更多节点可能同时找到正确的区块

- 节点收到2个以上的正确区块（区块链分叉）

最长链原则

- 沿着最长链继续"挖掘"
- 6个区块以确认交易（上链后约1小时确认交易）
- 支链中的交易被放回到交易池中



区块链共识

- 这些交易记录以谁为准?

→共识机制：全网节点对谁最终获得记账权达成共识的机制。

以太坊的方法：最有话语权的那个人记账→权益证明机制 (PoS, Proof of Stake)

话语权依据什么确定？ →抵押资金和投票选举

1. 验证者押下一定比例的他们拥有的以太币作为保证金。
2. 然后，开始验证每一个区块高度上的每一个候选块（由缴纳了保证金的验证人提交的块）。也就是说，当他们发现一个可以他们认为可以被加到链上的区块的时候，他们将以通过押下赌注来验证它。
3. 通过多位验证人的下注，对于每个高度最终会选出唯一一个胜出块。
4. 如果该区块被加到链上，然后验证者们将得到一个跟他们的赌注成比例的奖励。
5. 但是，如果一个验证者采用一种恶意的方式行动、试图做"无利害关系"的事（如多次下注，反复下注），他们将立即遭到惩罚。

区块链共识总结

共识机制：全网节点对谁最终获得记账权达成共识的机制。

共识机制	特点	优点	缺点
工作量证明 (PoW)	节点通过解决数学难题来证明工作量	安全性高；难以修改链	能源消耗巨大；交易速度慢；易受51%攻击
权益证明 (PoS)	节点根据持币量和持币时间获得创建区块的权利	能源消耗低；提高交易速度	可能导致富者更富；安全性较低
委托权益证明 (DPoS)	持币者投票选出节点代表，由代表验证和创建区块	交易速度快；效率高	中心化倾向强；依赖选出的代表
实用拜占庭容错 (PBFT)	通过消息传递和投票过程容忍一定比例的恶意节点	能在部分节点恶意的情况下维持运行	网络规模增大时，消息复杂度和开销增大
权威证明 (PoA)	在预选的可信节点中进行区块验证，常用于私有链	交易速度快；效率高	高度中心化；安全性依赖于预选节点的可信度
容量证明 (PoSpace)	使用存储空间作为验证的资源，节点必须分配一定的存储空间来参与区块的创建	能源消耗较低，尤其与PoW相比	初始硬盘空间需求较大；可能导致存储空间的无效使用

分布式交易系统面临的问题

◘ 怎么进行交易记录的防伪?

如果A 要给 B10 个比特币，怎么保证 A有充足的余额?

通过追溯整个区块链来完成。

比如，A 通过挖矿获得了 50 个比特币，记录在了区块链的块 1 里，一段时间后， A 给了 C 20 个比特币，记录在了块 2 里，后来 A 又给了 D 15 个比特币，记录在了块 3 里。

现在A 要给 B 10 个比特币，系统就会追溯 A 的所有交易，发现 A 的余额是够的，就会认可 A 给 B 10 个比特币的这个交易记录。

分布式交易系统面临的问题

◘ 如何避免双重支付?

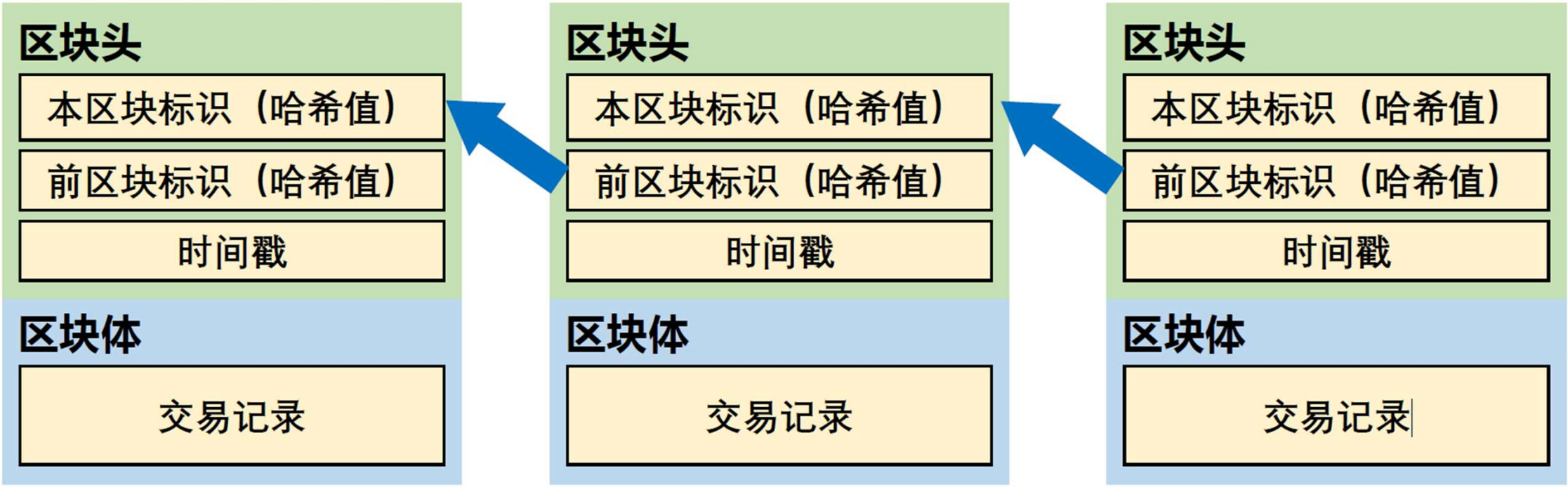
假设A 一共只有 10 个比特币，他同时把这 10 个比特币分别给了 B 和 C 。因为网络延迟的关系，有的人先接收到 A 给 B 10 个比特币，那么再接收到 A 给 C 10 个比特币就会拒绝；有的人先接收到 A 给 C 10 个比特币，那么再接收到 A 给 B 10个比特币就会拒绝。

这就造成每个人打包的A 的交易记录是不一样的。这时某个幸运儿解出了数学题，完成了这个打包，那么他所打包的交易记录将作为最终记录，形成一个块，这个块里记录的是 A 给 B 那么就是成功的给了 B，拒绝了 A 给 C的交易，反之亦然。

当我们做比特币交易的时候，不能当时就认为钱到账了，一定要等着，等到这个块形成了，这条记录已经被确认链在区块链上了，才能认为这个钱真的打给我们了。

区块链结构

区块链技术是一种分布式数据库，是一串使用密码学方法相关联产生的数据块，每个数据块都包含了一次网络交易信息，用于验证其他信息的有效性和生成下一个区块。



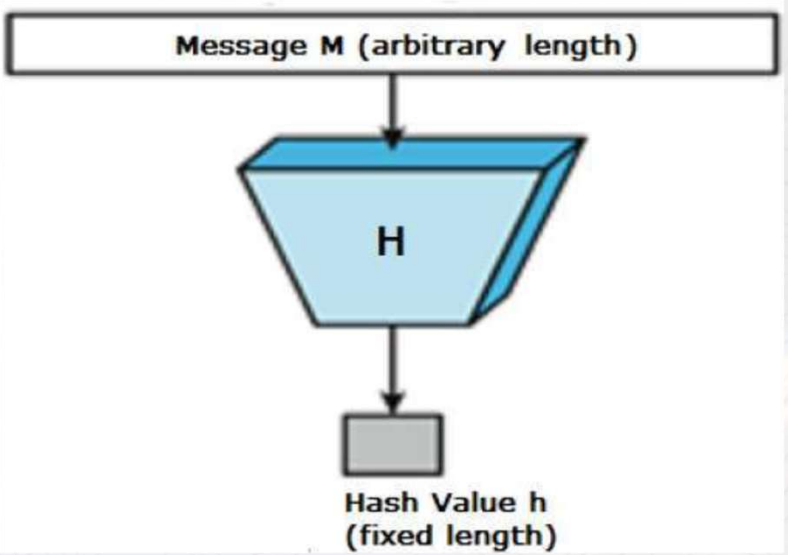
区块链结构——哈希

确定性映射算法，可以将任意长度的输入数据编码为固定长度的输出，该输出就是哈希值。

- 例如：SHA-256 输出256bits

哈希函数特性

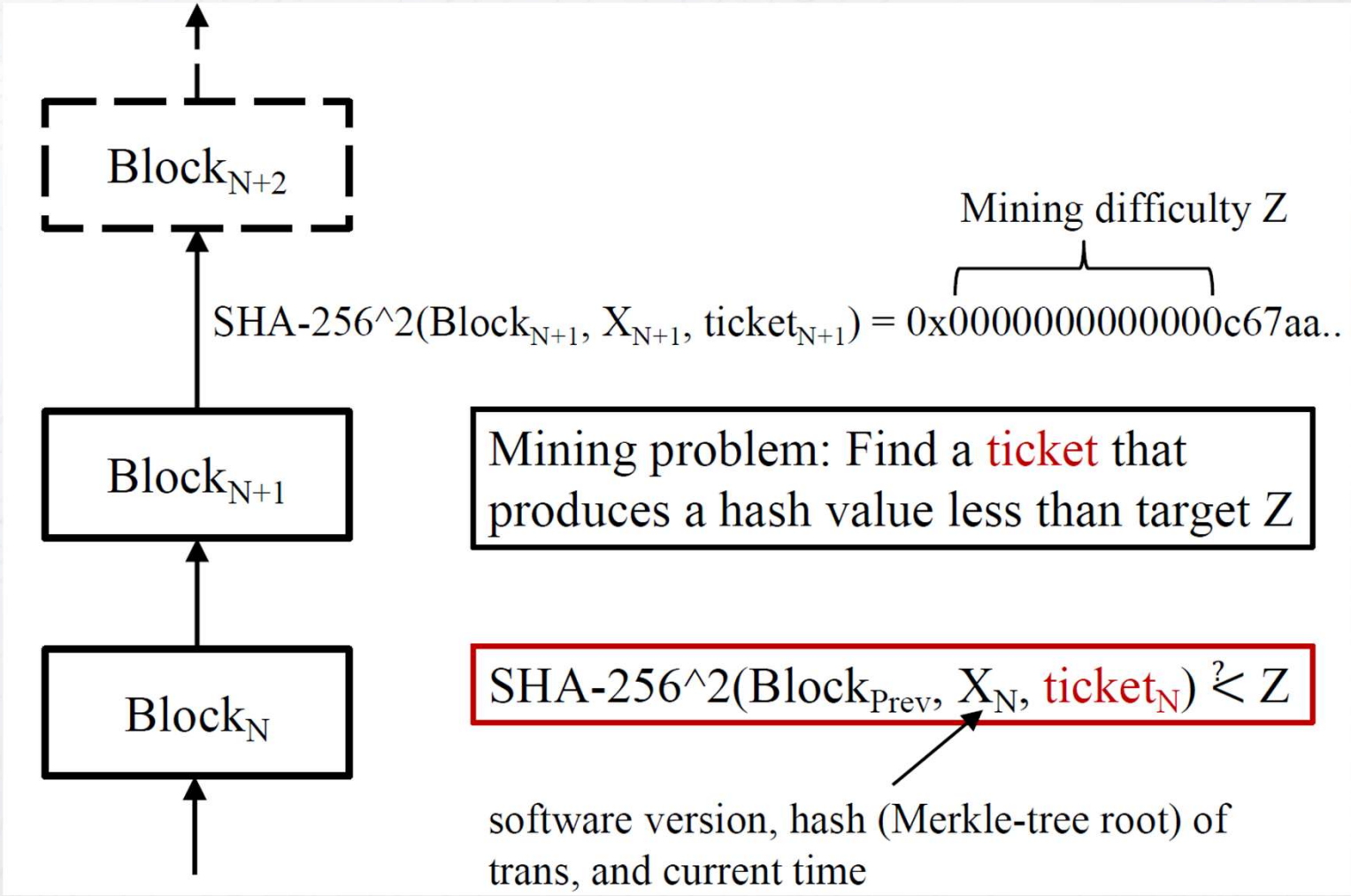
- 防碰撞性（Collision-resistance）
- 隐秘性（Hiding）
- 支持迷惑（Puzzle-friendliness）



对于每一个可能的n-bit 位输出y，如果k是随机性很强的值，那么找到一个合适的x使得$H(x||k) = y$是不可能显著地低于2^n的时间复杂度。这意味着，不存在比随机尝试x好很多的解决策略来找到解，即$H(x||k) = y$。

区块链结构——哈希

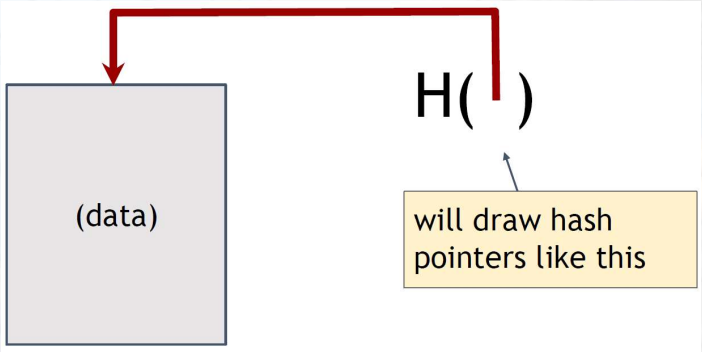
挖矿：给定一个“谜题ID”k，和一个目标集合Y，尝试找到一个“解x”，使得：$H(x||k) = y$。



区块链结构——哈希指针

哈希指针

- 包含了一段数据的位置（pointer to where some info is stored）
- 这段数据原始的哈希值（hash of the info）

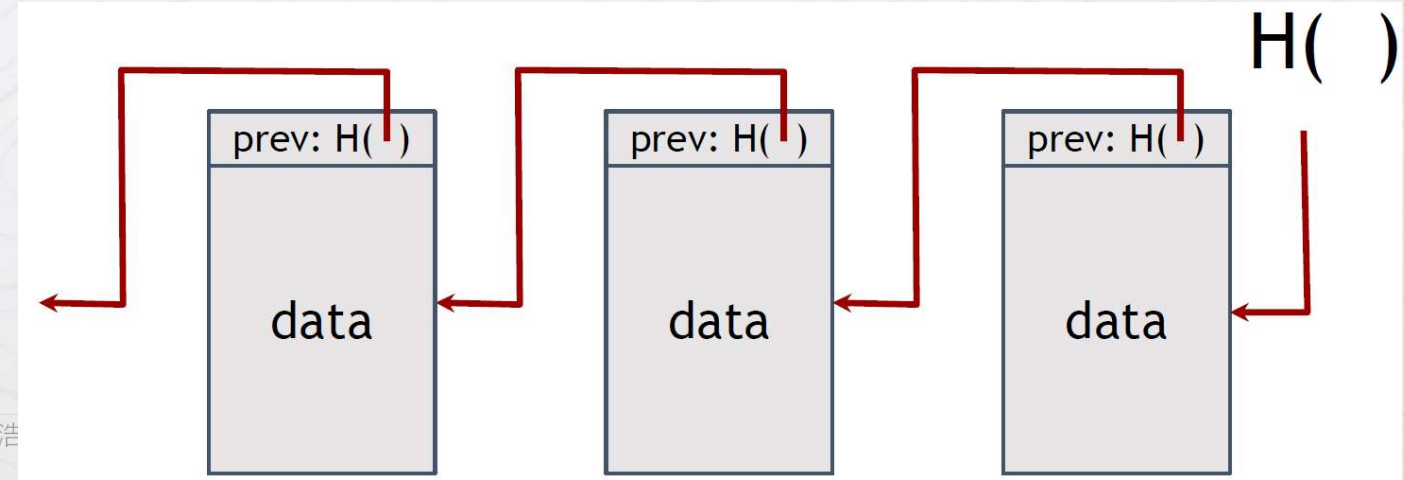


给定一个哈希指针，我们可以

- 获取指针指定的原始数据
- 验证数据是否被篡改过

区块链核心构造思路：

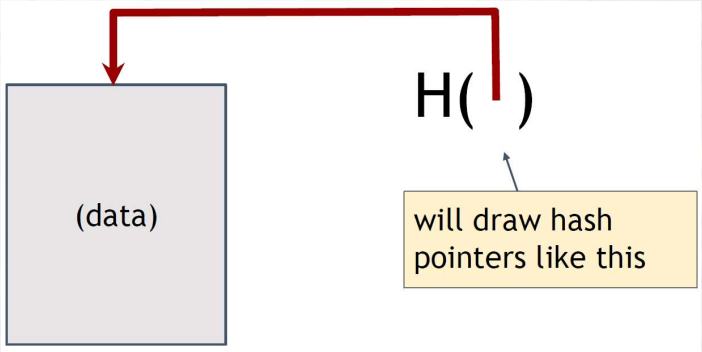
- 用哈希指针为存储数据的区块（Block）建立一个链表（chain）



区块链结构——哈希指针

哈希指针

- 包含了一段数据的位置（pointer to where some info is stored）
- 这段数据原始的哈希值（hash of the info）



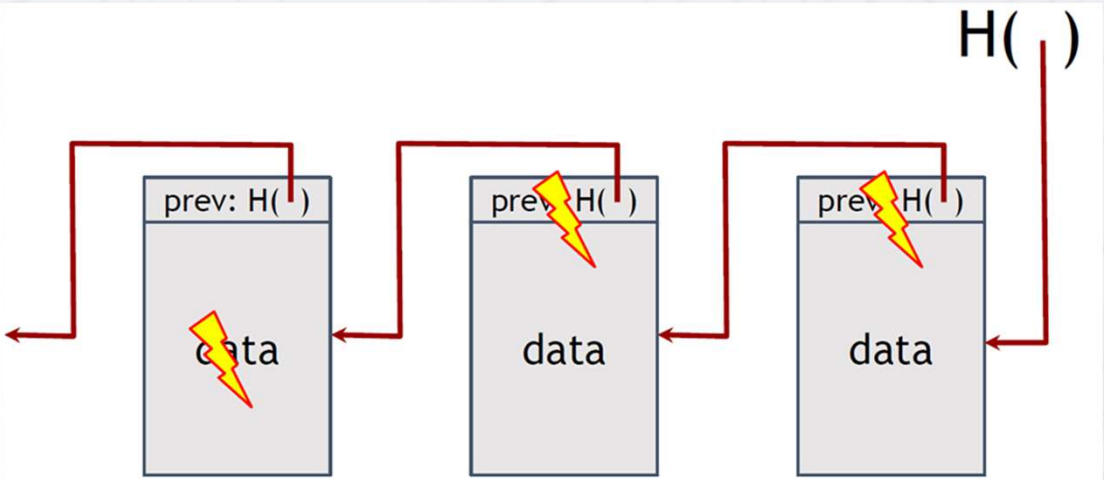
给定一个哈希指针，我们可以

- 获取指针指定的原始数据
- 验证数据是否被篡改过

区块链核心构造思路：

- 用哈希指针为存储数据的区块（Block）建立一个链表（chain）

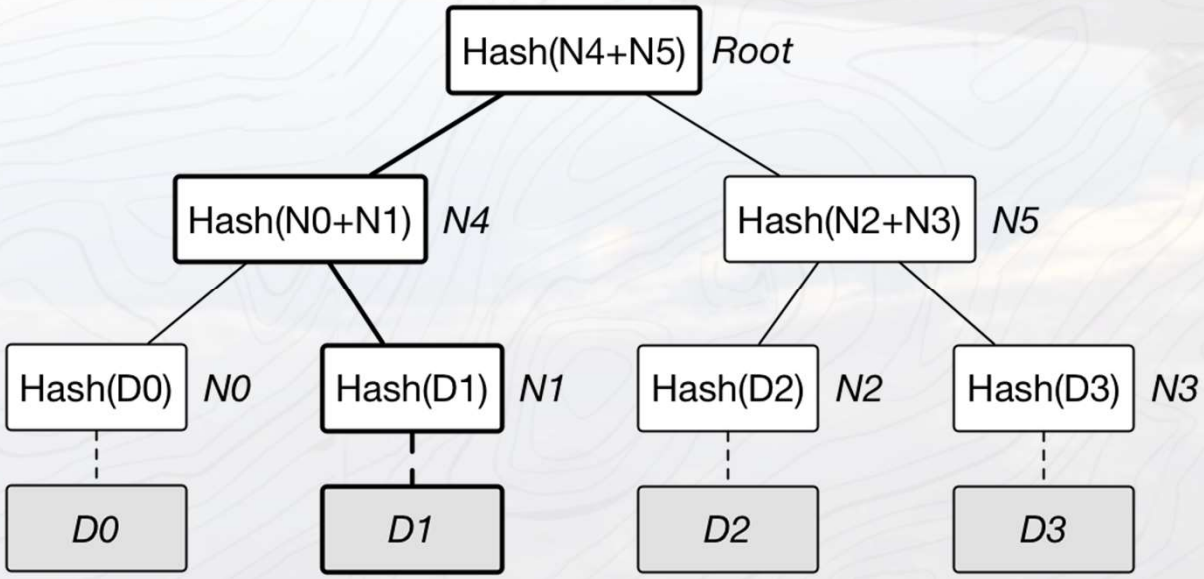
检测
篡改



区块链结构——默克尔树

哈希树（hash tree；Merkle tree）在密码学及计算机科学中是一种树形数据结构，每个叶节点均以数据块的哈希作为标签，而除了叶节点以外的节点则以其子节点标签的加密哈希作为标签 。哈希树能够高效、安全地验证大型数据结构的内容，是哈希链的推广形式。

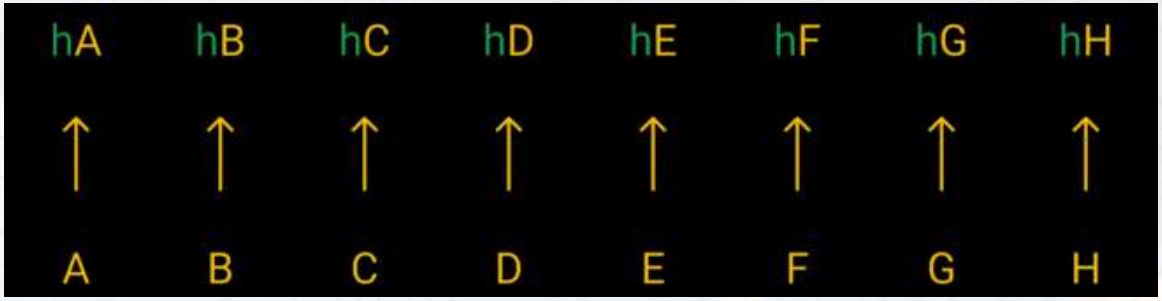
优势：方便快速地校验大数据块

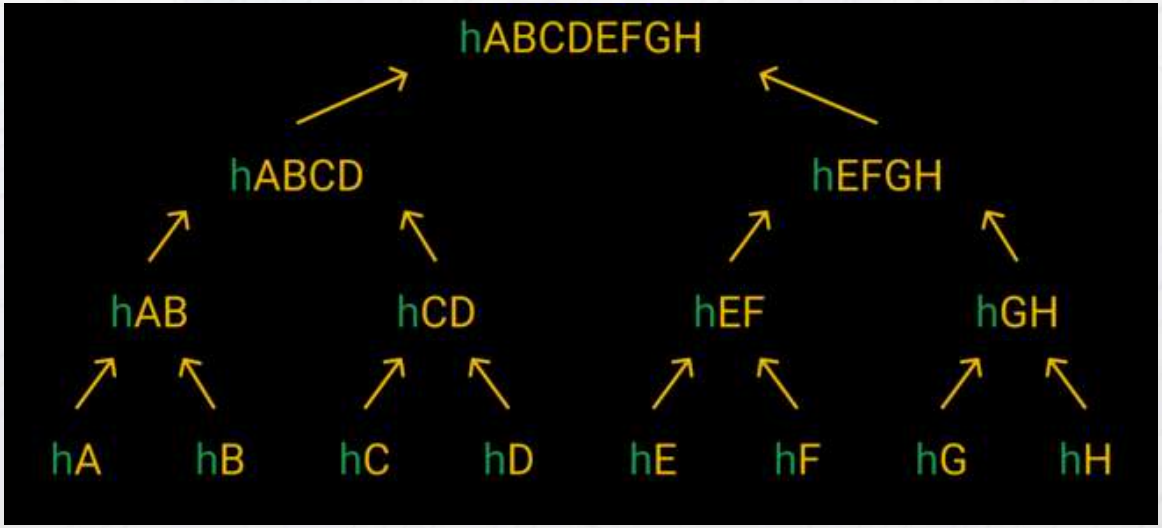


区块链结构——默克尔树

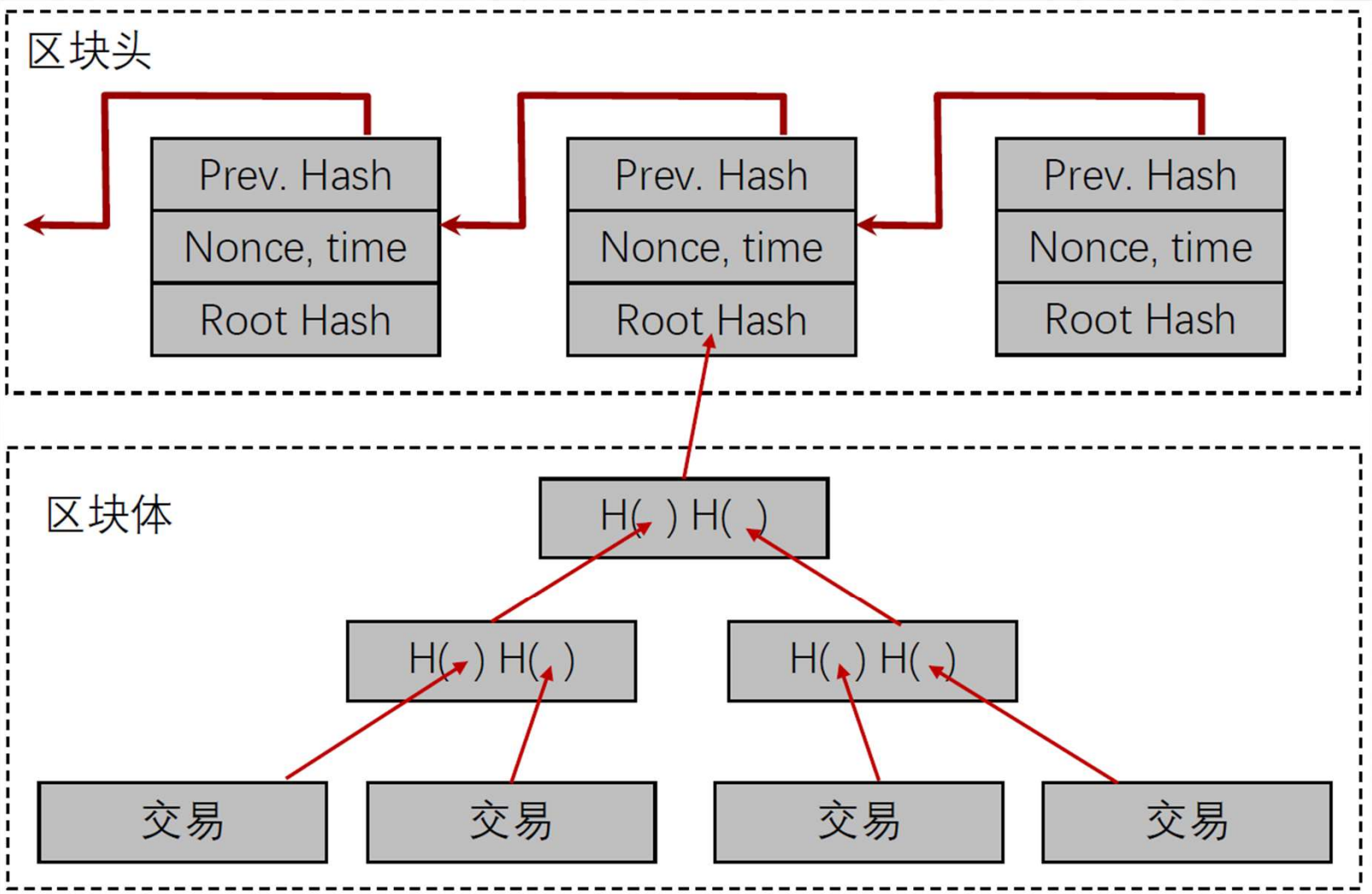
例：文件校验过程

1. 将一个8GB的文件分为八份，每个片段分别以*A*到*H*命名。随后，每个片段代入哈希函数，得出八个不同的哈希值。
2. 接下来两两组合，对两个哈希值再计算一次哈希，得到四个哈希，再两两组合，依此类推直到得到最终的一个哈希值，称为主哈希值，也就是默克尔根（亦称为根哈希值）。
3. 校验时，若根哈希不一致，就往下查生成默克尔根的两个哈希值（hABCD和hEFGH）是否和原记录一致，若hABCD一致而hEFGH 不一致，说明左边子树对应的数据片段无误，需要继续查右边子树。由此可以最终找到出错的片段。





区块链结构——默克尔树

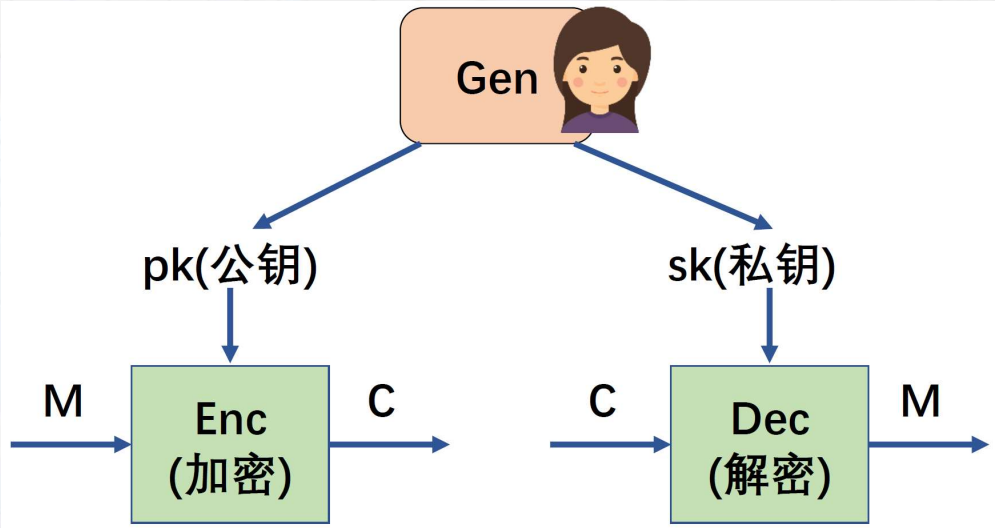

区块头
Prev. Hash
Nonce, time
Root Hash
Prev. Hash
Nonce, time
Root Hash
Prev. Hash
Nonce, time
Root Hash
区块体
H( ) H( )
H( ) H( )
H( ) H( )
交易
交易
交易
交易

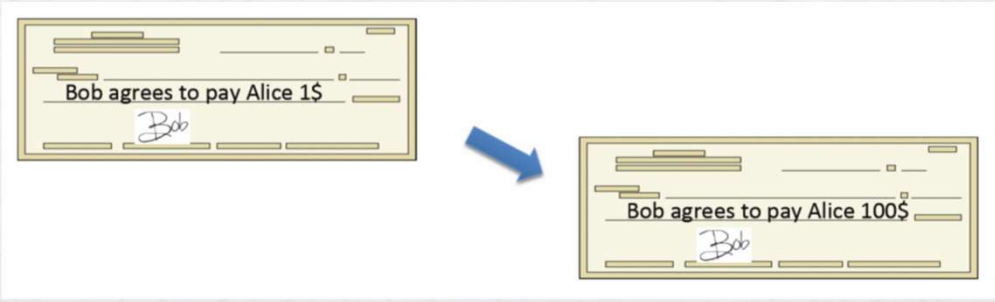
区块链数据安全验证——公钥密码学

生成一对密钥：公钥+私钥
公钥加密的数据只能用私钥解密
私钥加密的数据只能用公钥解密

数字签名：

1. Alice生成公钥pk_a和私钥sk_a，并公开公钥pk_a。
2. Alice对一段数据msg用私钥sk_a加密得到密文sig，公开msg和sig。
3. 他人收到加密数据后，用Alice的公钥pk_a解密sig，比对msg和sig，若一致，说明该数据是经过Alice认证并未篡改的。



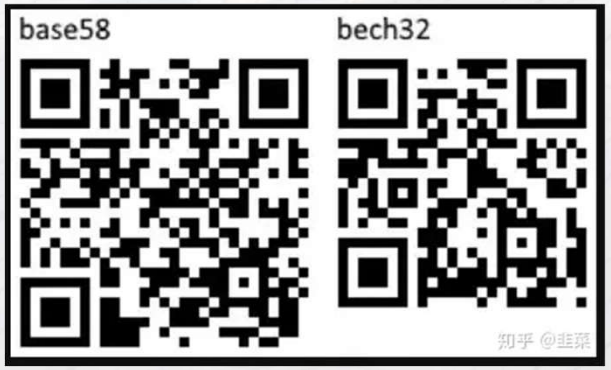


区块链数据安全验证——公钥密码学

区块链系统中某账户的公钥：该账户地址（ID）——随机生成
使用公钥（pk）的区块链地址必定是私钥（sk）的持有者

比特币地址是一个标识符（帐号），包含27-34个字母数字拉丁字符（0，O，I除外）。地址可以以二维码形式表示，是匿名的，不包含关于所有者的信息。

地址示例：14qViLJfdGaP4EeHnDyJbEGQysnCpwn1gd



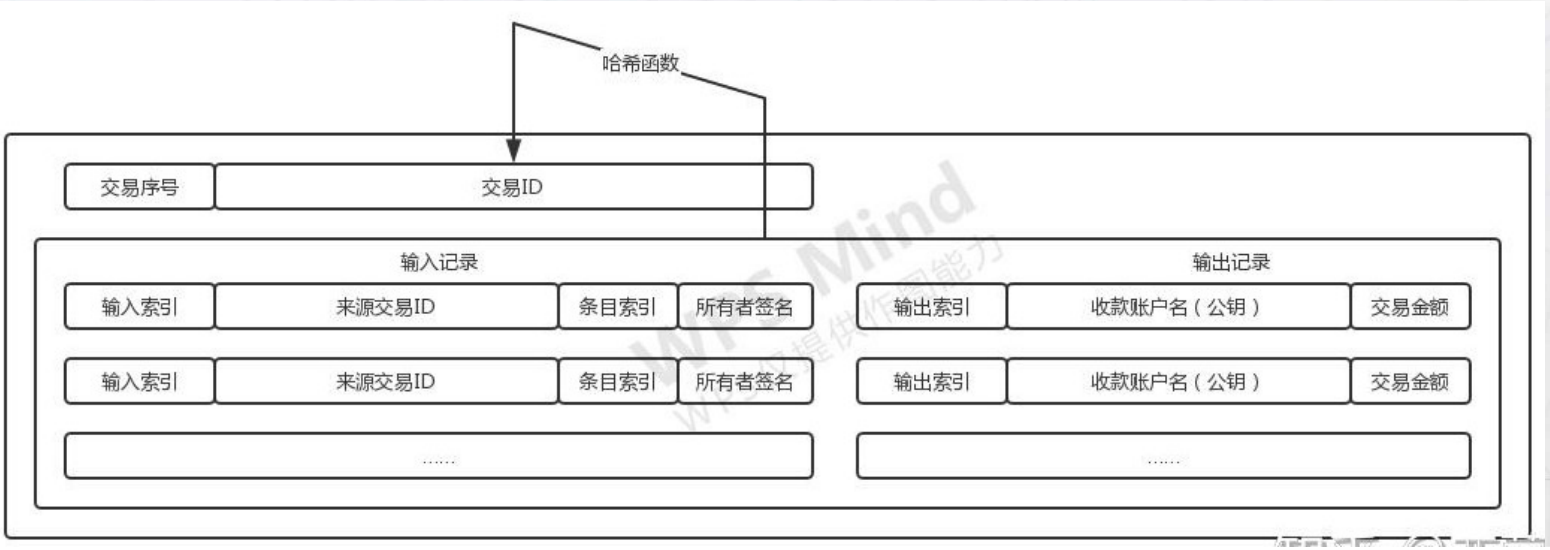
用户发出交易和矿工挖矿：用自己的私钥签名后广播，他人可用公钥验证

签名的意义：

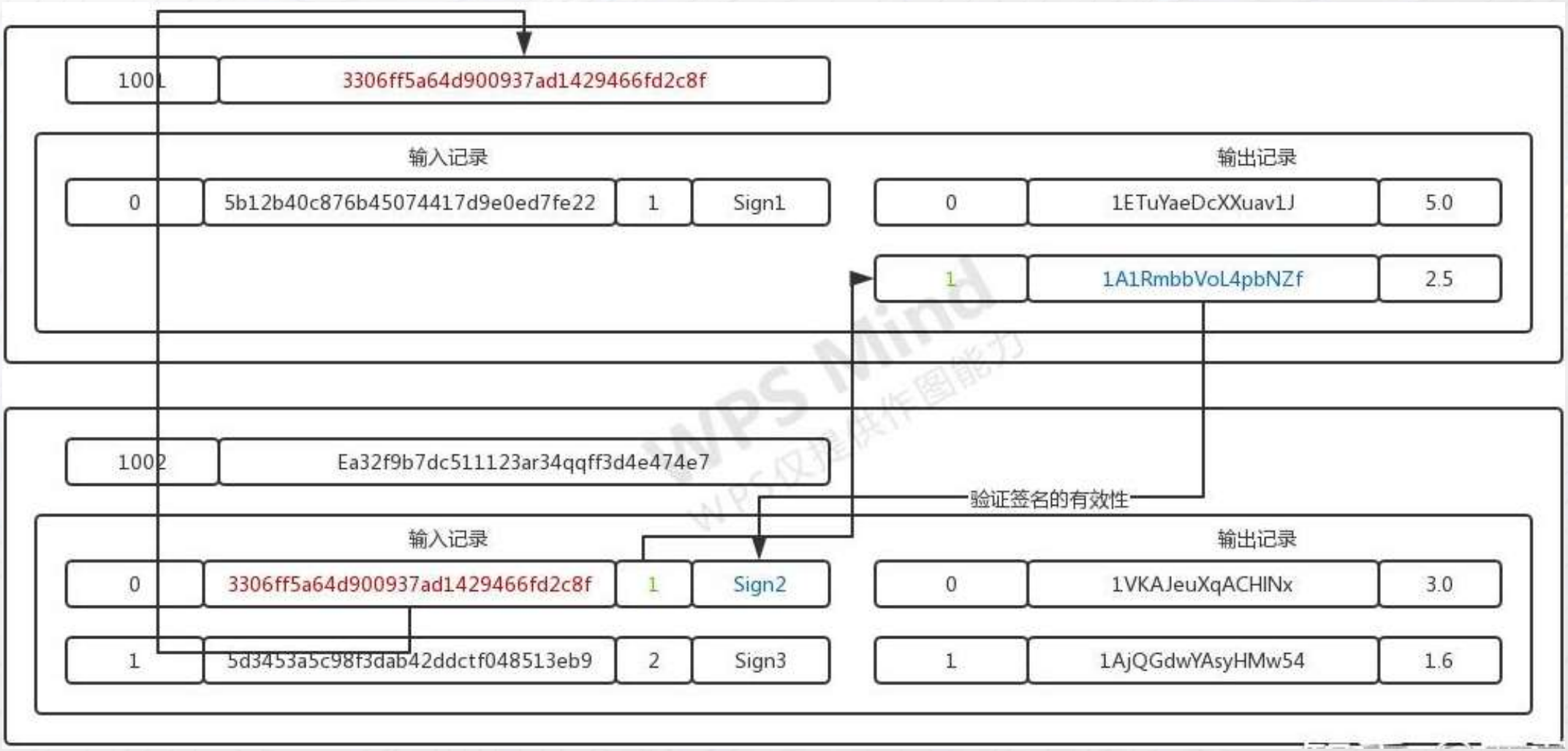
1. 签名证明私钥的所有者，即资金所有者，有权花费这些资金。
2. 授权证明是不可拒绝的（不可否认性）。
3. 签名证明交易（或交易的具体部分）在签字之后没有也不能被任何人修改。

区块链数据安全验证——交易索引与验证

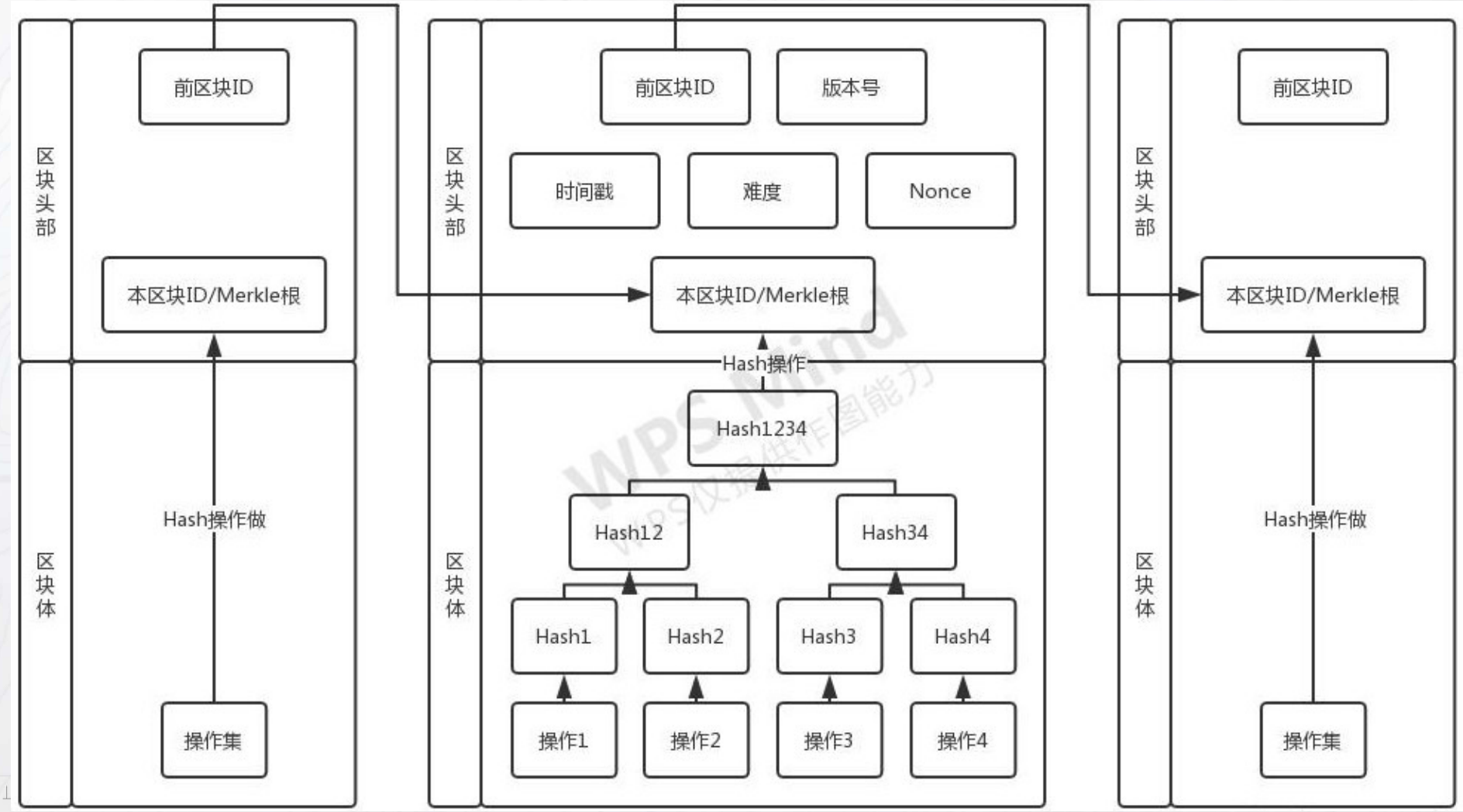
- 输入记录记载了此次交易涉及资金的来源问题。
- 输出记录记载了资金的去向问题，输出索引将会和整个交易的ID配合以便于与该交易有关的后续交易找到该笔交易信息；收款账户名即为账户对应的公钥，可用其对后续交易的所有者签名进行解密，以验证签名的合法性。
- 将输入记录和输出记录打包后进行哈希计算就得到本次交易的总ID，交易的索引在交易被打包成区块的过程中决定，交易ID会和索引、输入记录和输出记录的包再打包，最后与其他交易记录和区块头一起打包成一个区块。



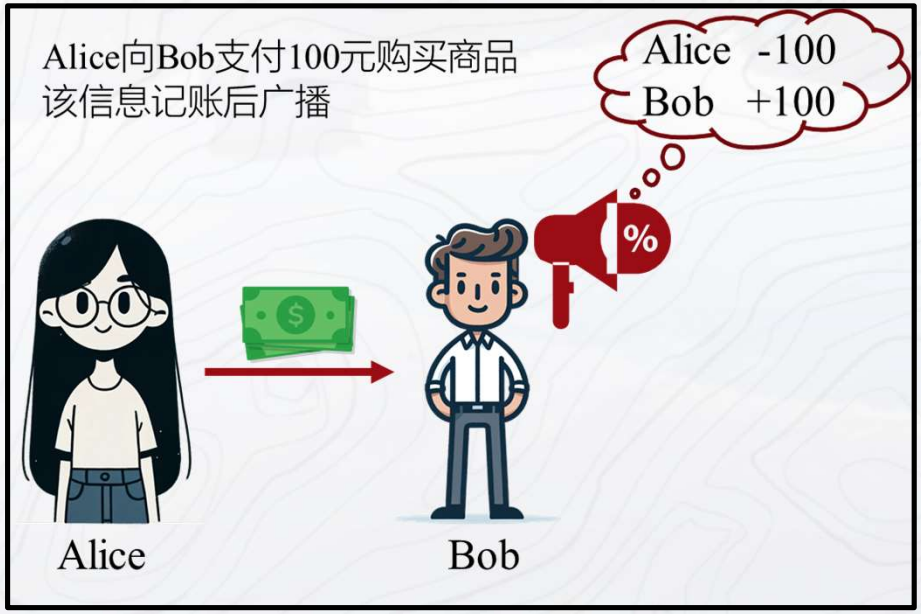
区块链数据安全验证——交易索引与验证

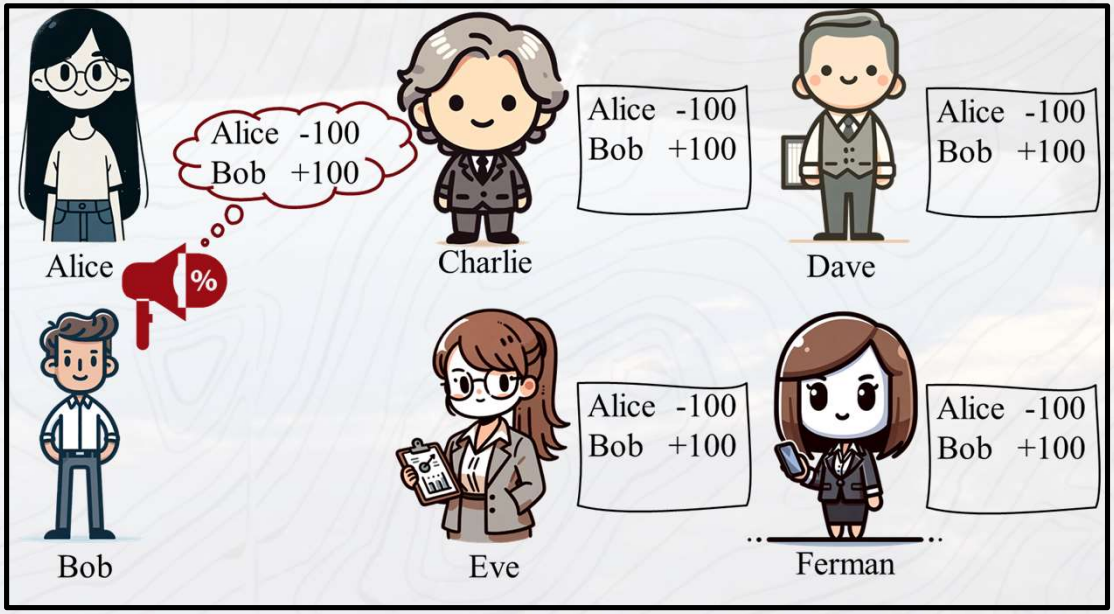


区块链结构总结


区块头部
前区块ID
本区块ID/Merkle根
区块体
Hash操作做
操作集
区块头部
前区块ID
版本号
时间戳
难度
Nonce
本区块ID/Merkle根
Hash操作
Hash1234
Hash12
Hash34
区块体
Hash1
Hash2
Hash3
Hash4
操作1
操作2
操作3
操作4
区块头部
前区块ID
本区块ID/Merkle根
区块体
Hash操作做
操作集

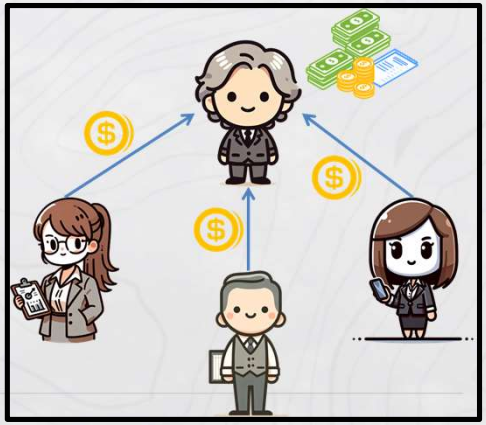
区块链结构总结


Alice向Bob支付100元购买商品
该信息记账后广播
Alice -100
Bob +100
Alice
Bob

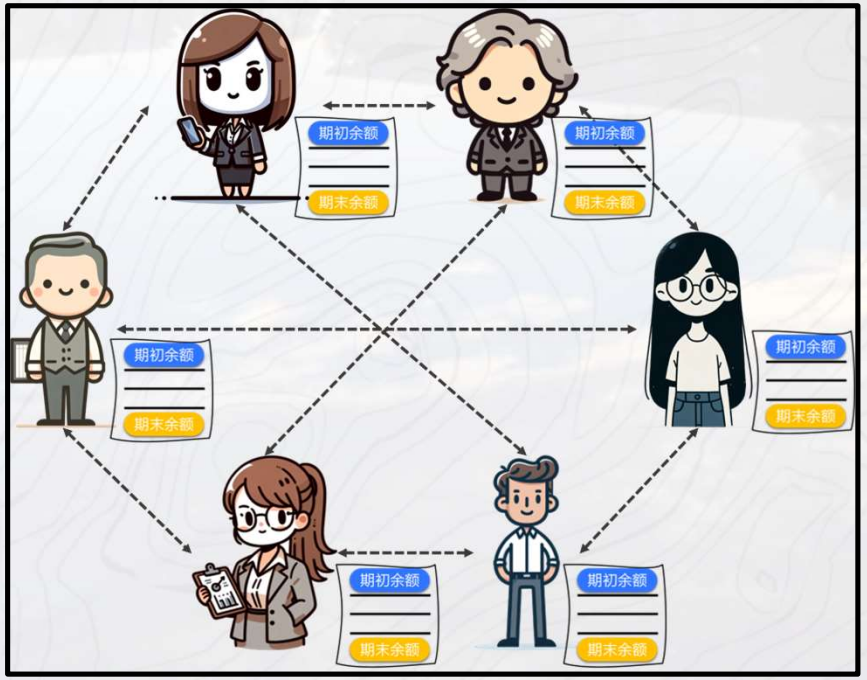

Alice -100
Bob +100
Alice
Charlie
Dave
Bob
Eve
Ferman


公告板
Alice -100
Bob +100
4月28日账本
4月29日账本
4月30日账本
Charlie


Alice -100
Bob +100
区块一
区块二
区块三
期初余额
期末余额
期初余额1000
买书-50
买衣服-100
工资+200
期末余额1050
期初余额
期末余额



区块链结构总结



区块链特征

分布式账本　点对点传输　防篡改　可追溯

技术支撑

哈希算法　默克尔树　公钥密码学　共识机制

分布式共识PBFT

分布式共识

给定n个节点（包含某些恶意节点），每个节点都有其自身的输入值。达成分布式共识需满足以下两点：

- 一致性：It must terminate with all honest nodes in agreement on the value；
- 准确性：This value must have been generated by an honest node；

拜占庭将军问题

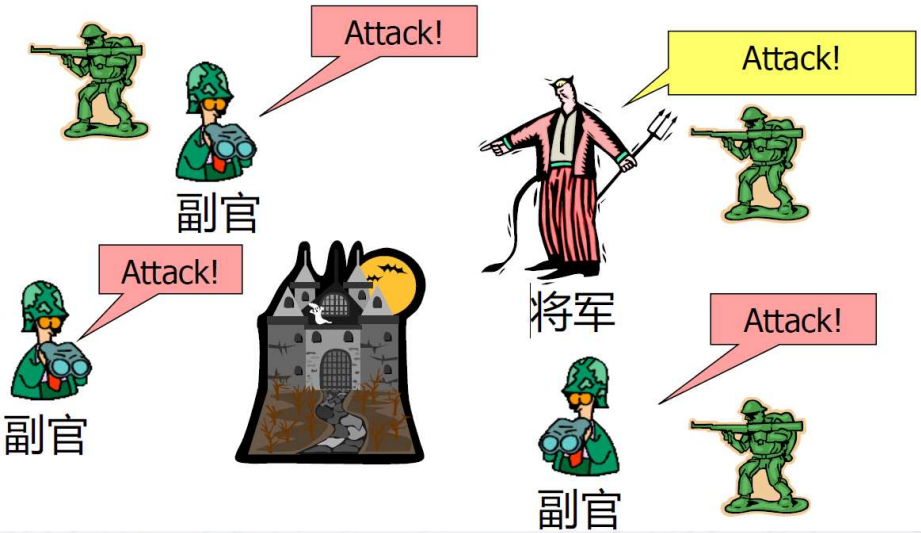
拜占庭军队包围了一个城市，并决定占领该城市

- 副官之间仅可以通过信使与将军进行沟通；

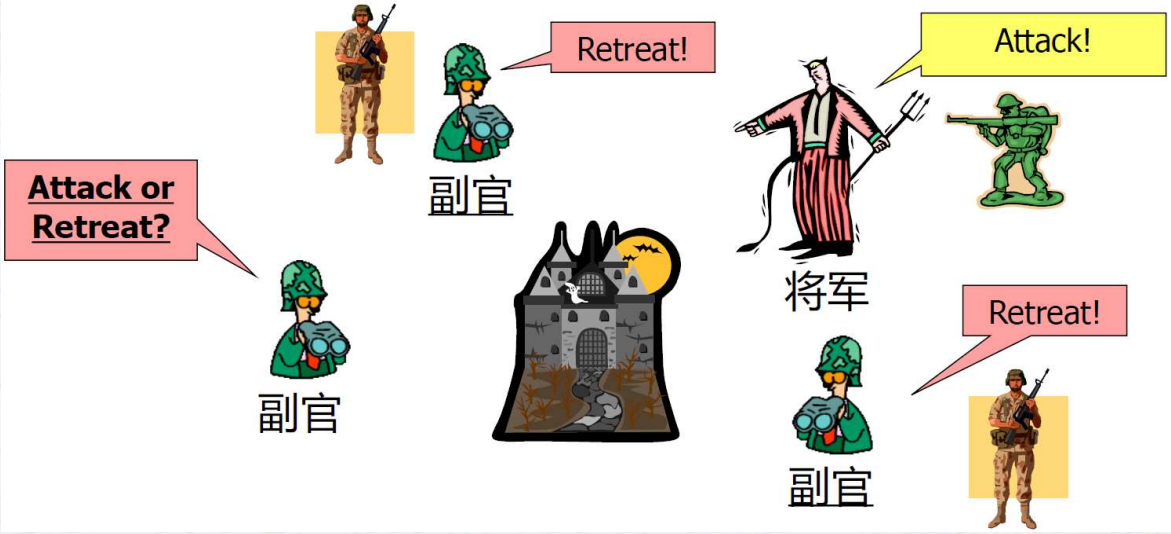
他们必须商定以下两个行动计划：

- 一次进攻的准确时间
- 如果遇到猛烈抵抗，一次性撤退的准确时间

拜占庭将军问题



如果将军与副官都是诚实的



如果某些副官/将军是叛徒，不遵循命令或传递不正确的消息

□ Problem Formalization

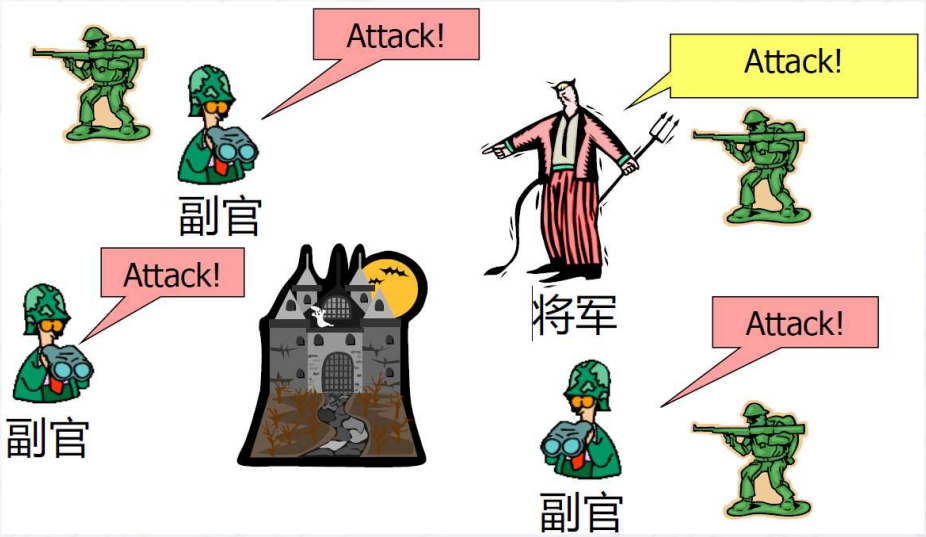
一个将军将命令发送给$n-1$个副官，其中:

a) 所有忠诚的副官都遵守相同的命令

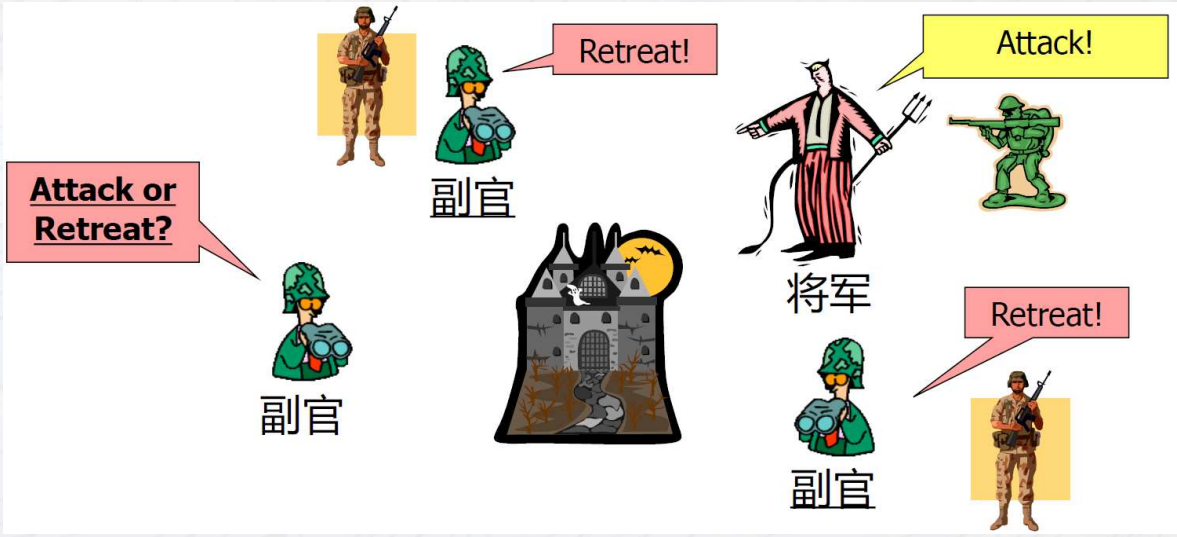
b) 如果将军是诚实的，那么每个忠诚的副官都遵守他发送的命令

注意：将军和副官都可能是不诚实的

拜占庭将军问题



如果将军与副官都是诚实的



如果某些副官/将军是叛徒，不遵循命令或传递不正确的消息

□ Problem Demonstration

一个将军和两个副官，其中一个是叛徒，那么其他诚实的副官可以达成一致的命令么？

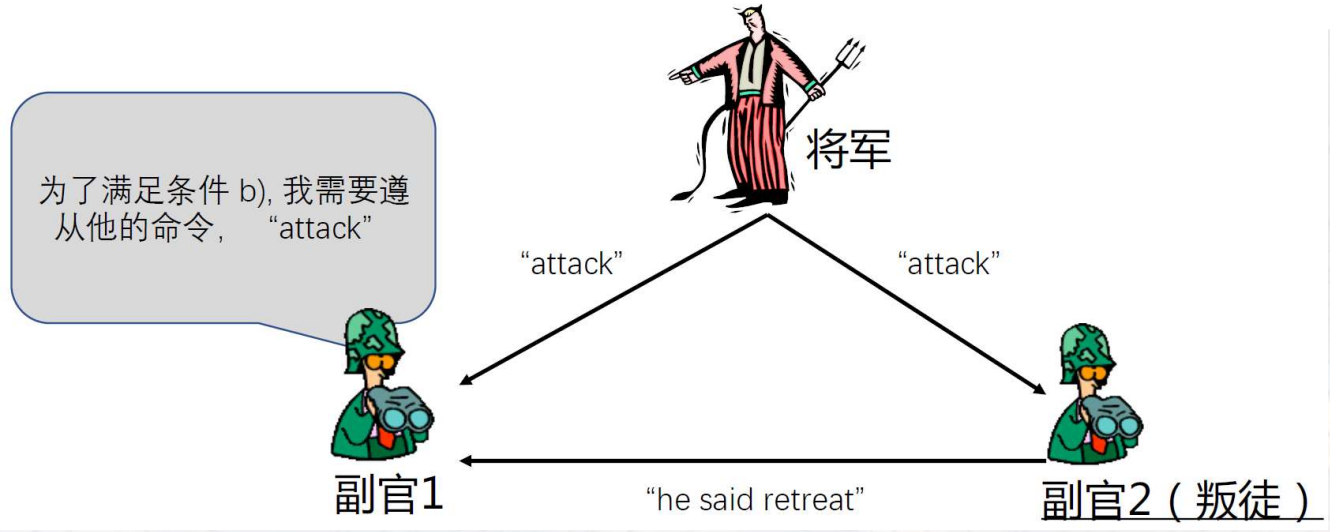
拜占庭将军问题

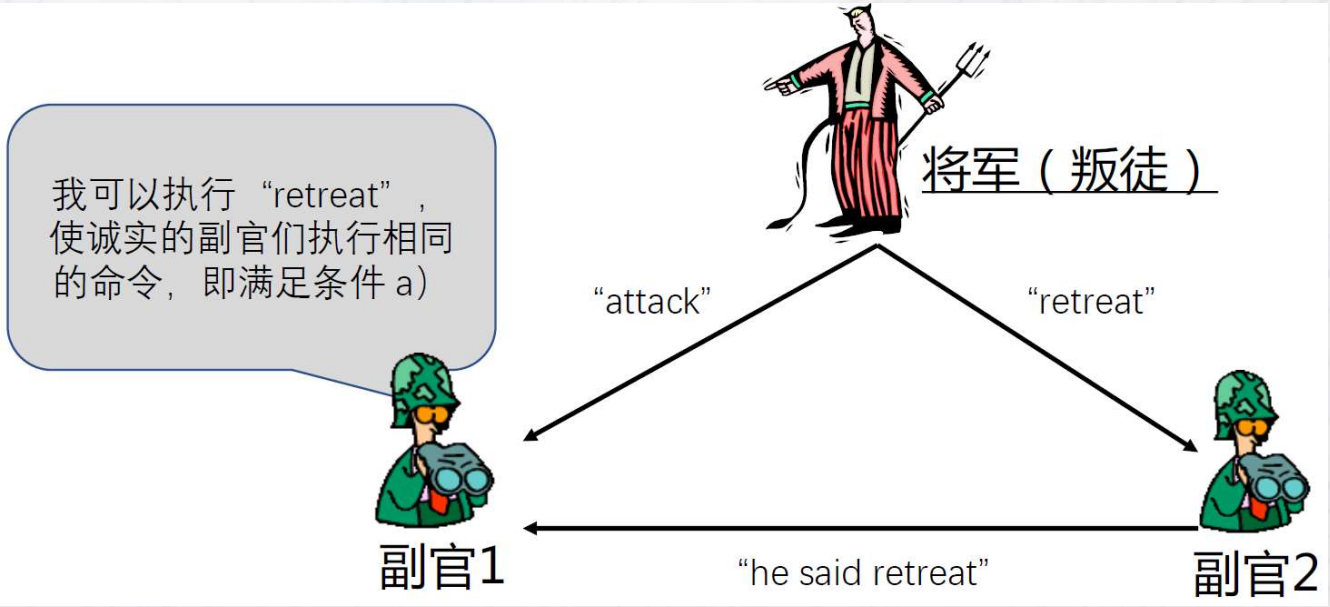
- 假设场景一

将军是诚实的，副官2是叛徒

- 假设场景二

将军是叛徒，副官2是诚实的



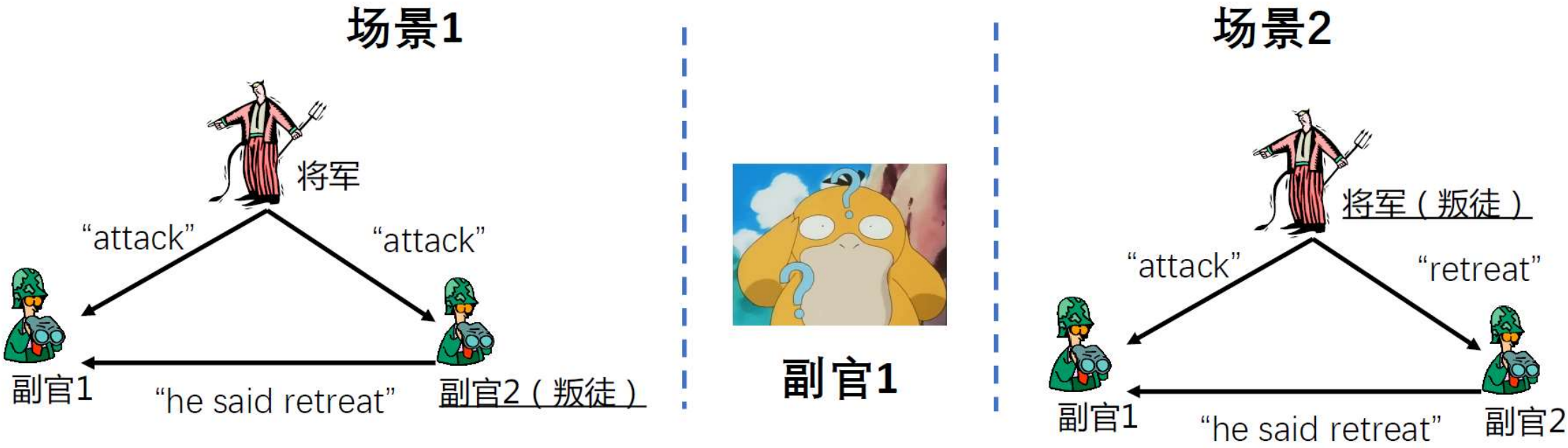


拜占庭将军问题

◘ 实际问题

无法预先知道谁是叛徒，无法知道将军给另一个人的命令是什么

拜占庭将军问题



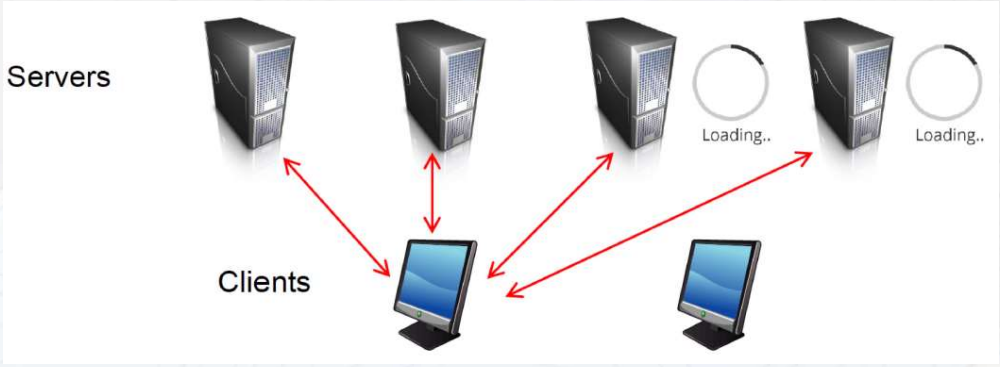
实际问题

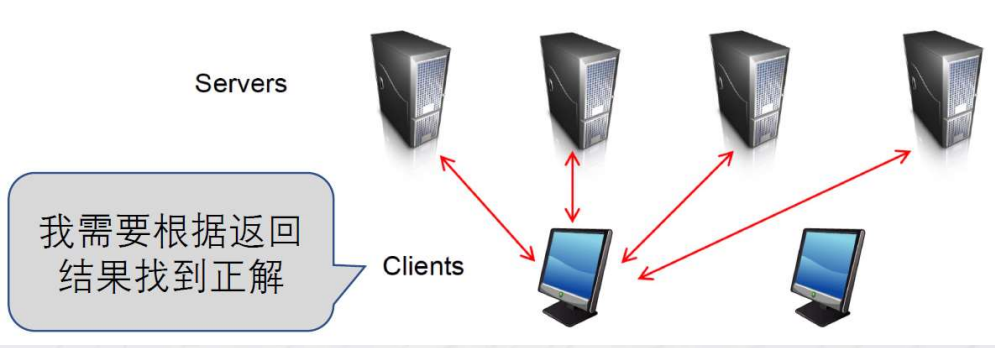
当命令发生冲突，副官1永远无法区分这两种场景，拜占庭问题无解。

一个叛徒使三个参与方的拜占庭问题无解
当有f 个节点可以任意表现时，2f+1 个节点不足以容忍它

拜占庭将军问题

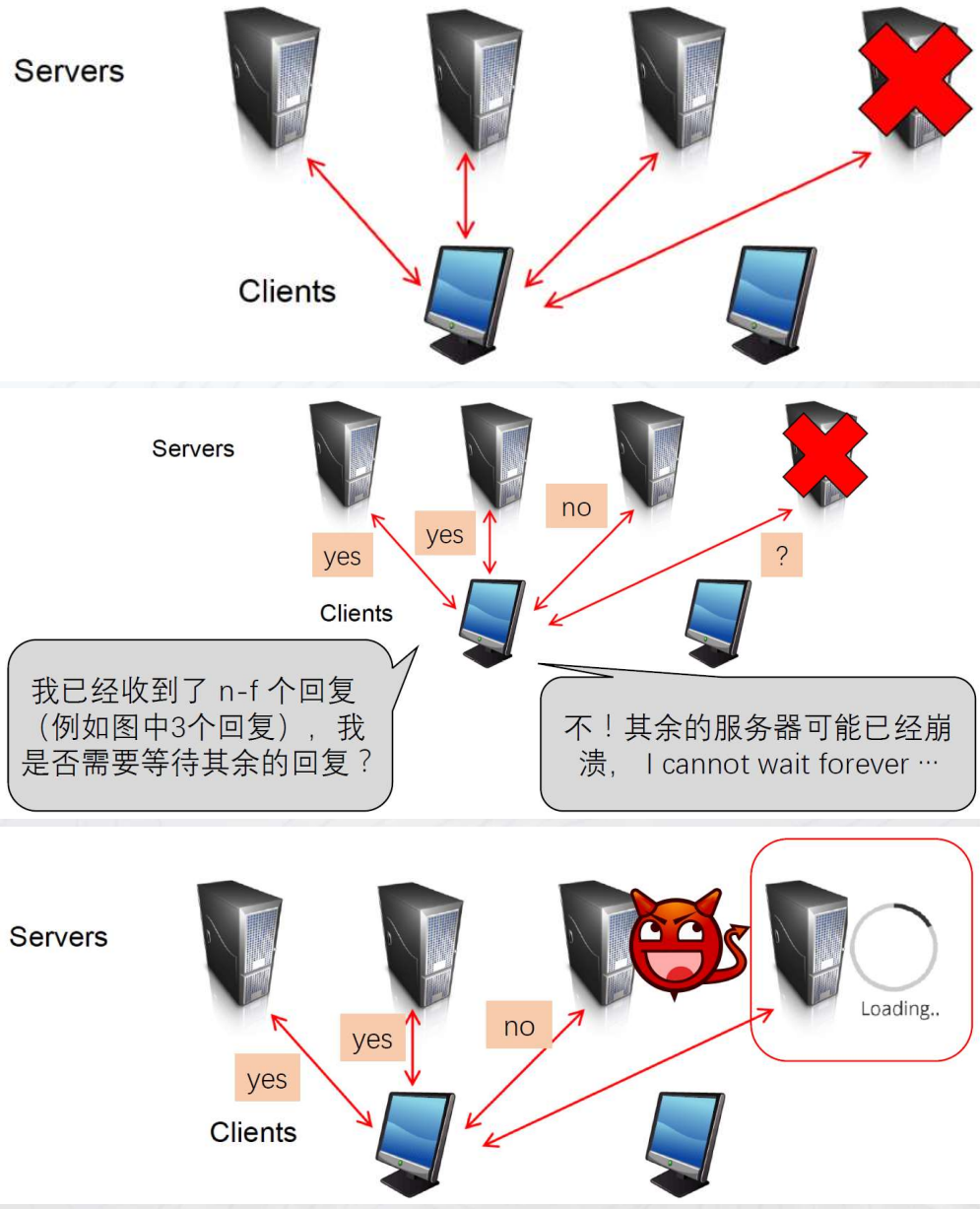
- **同步vs异步**
  在真实的系统中（例如复制的Web服务器），一些服务器可能会很慢。
- **新的场景**
  一个客户端提问，多个服务器回答（yes or no），客户端根据回复决定正确答案。
- **发生错误的原因有很多种**
  进程崩溃，消息丢失，恶意行为等
  客户端无法区分错误是属于哪种情况
- **拜占庭容错问题**
  给定恶意节点数量f，系统需要预设多少个服务器才可以容忍拜占庭错误?
  - 恶意服务器可以说谎（例如yes 返回no；no返回yes）





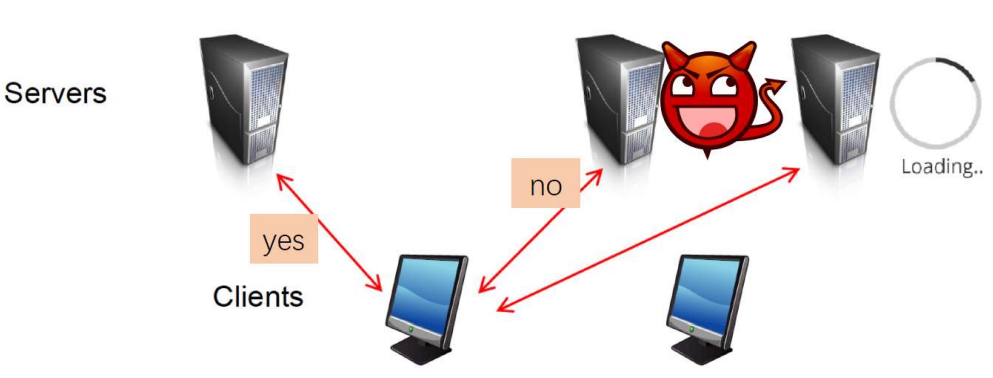
拜占庭将军问题

- **拜占庭容错问题**
  给定恶意节点数量f，系统需要预设多少个服务器才可以容忍拜占庭错误?
  - 恶意服务器可以说谎（例如yes 返回no；no返回yes），也可以假装故障。
  - 假设有n个服务器
- 客户端至少能收到多少个回复？$n-f$
- 客户端收到多少个回复后需要做出决定?
- 客户端收到的回复中（最多）会有多少个谎言信息呢？f
- 能够让客户端确定正确答案的最小n是多少?



拜占庭将军问题

- 能够让客户端确定正确答案的最小n是多少?



$$n = 2f + 1$$

如果$n - f$个回复中正确节点的回复数量比拜占庭节点的多，则系统可以有效容忍拜占庭错误!

- 错误节点回复数f，节点回复数$n - f$
- $n - f - f > f \rightarrow n > 3f$

实用拜占庭容错算法Practical Byzantine Fault Tolerance (PBFT)

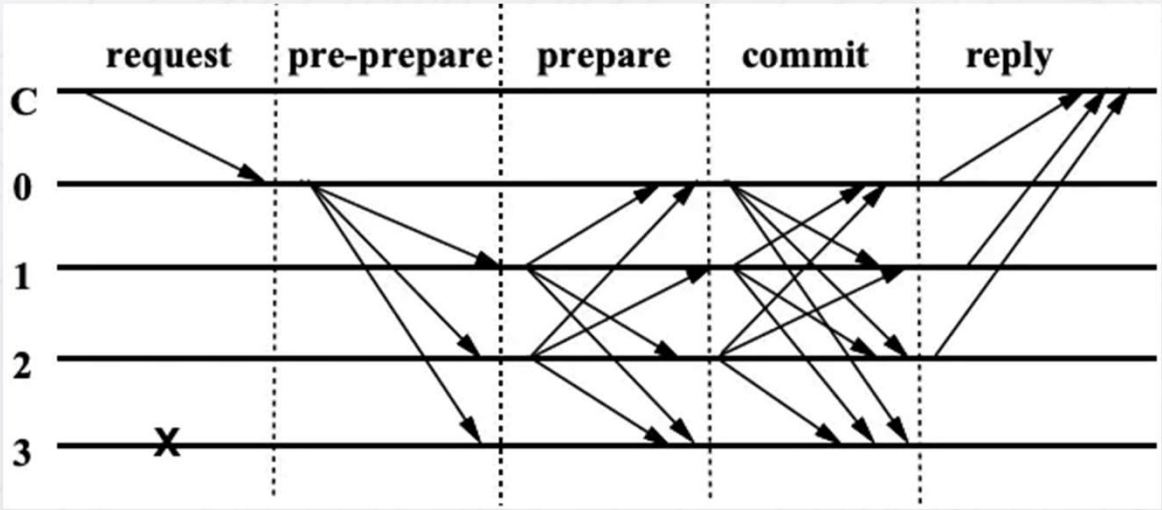
- 概述
  - 专为复制状态机设计
    - 通过操作访问任意服务
    - 例如，文件系统中的读写操作
  - 在异步模型中，可通过至少$3f+1$个副本容忍f个故障节点
- 复制状态机中的正确性论证
  - 假设：
    - 操作是确定的
    - 复制以相同的状态开始
  - 那么，如果复制以相同的顺序执行相同的请求
    - 正确的副本将产生相同的结果

实用拜占庭容错算法Practical Byzantine Fault Tolerance (PBFT)

流程

客户端发送消息m给主节点0，主节点开始PBFT三阶段协议：预准备，准备，提交。

- Pre-prepare阶段：副本验证主节点发出的消息，决定是否接收开始共识
- Prepare阶段：节点同意预准备请求后会向其它节点发送prepare消息，每个节点会验证来自其他节点的prepare消息，在一定时间范围内，如果收到超过 $2f$个其他节点的prepare 消息，就代表 prepare 阶段已经完成。最后共识节点发送commit消息并进入Commit阶段。
- Commit阶段：当节点接收到并验证了$2f$个来自其他共识节点的commit消息后，节点确定消息m已经在整个系统中得到至少$2f+1$个节点的共识，而这保证了至少有$f+1$个非故障节点已经对消息m达成共识。于是节点就会执行请求，写入数据。



实用拜占庭容错算法Practical Byzantine Fault Tolerance (PBFT)

- PBFT的应用实例
  - 波音777信息管理系统，以及波音777和787飞行控制系统
  - The SpaceX Dragon 飞行系统
- 缺点
  - 仅仅适用于permissioned systems (联盟链/私有链)。
  - 通信复杂度过高，可拓展性比较低，一般的系统在达到100左右的节点个数时，性能下降非常快。
  - PBFT在网络不稳定的情况下延迟很高。

区块链与安全

区块链系统的安全特性

1. 信任和透明度

区块链技术通过去中心化和不可篡改性的特性建立了信任和透明度。所有的交易都被记录在一个公开的账本上，并且可以被网络中的任何一个节点验证，这消除了传统交易中的信任问题，并提高了数据的透明度和可信度。

2. 安全和防篡改

区块链技术的密码学特性使得数据在传输和存储过程中更加安全。数据被加密和链接在一起，使得任何的篡改都会被立即检测到。这种安全性极大地降低了数据被盗窃或篡改的风险，尤其对于金融、医疗等领域的应用具有重要意义。

3. 去中介化和降低成本

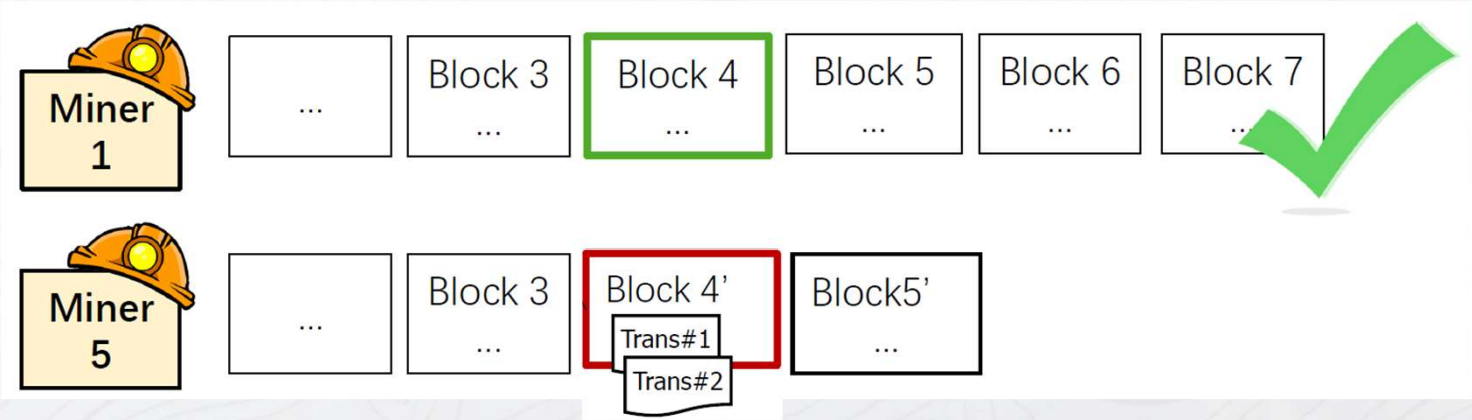
区块链技术的去中心化特性消除了许多中间人，从而降低了交易的成本和时间。传统金融交易和跨境支付往往需要经过多个中间人的处理，而区块链技术使得直接点对点的交易成为可能，极大地提高了效率并降低了费用。

区块链系统的安全特性

区块链类型	特点	安全性优势	安全性劣势
公有链	完全去中心化，任何人都可以参与交易和验证过程。	高透明度增加了安全性 更广泛的节点分布可能增加抗攻击能力	可能面临更多的恶意攻击 交易验证时间可能较长
联盟链	部分去中心化，只有授权的节点可以进行交易验证。	控制的节点入网增强了交易的安全和隐私 适合合规要求高的应用场景	节点较少，可能影响抗拒绝服务攻击的能力 联盟成员间需要较高的信任
私有链	中心化，一个组织或少数几个组织控制整个网络。	快速验证交易 可以完全控制和调整安全设置	安全性高度依赖于中心节点的保护 抗攻击能力较弱

51%攻击

定义：当系统中有合作关系的恶意节点所控制的算力，超过诚实节点所控制的算力，系统就是有被攻击的风险。 这种由恶意节点控制超过50%算力所发起的攻击，称为51%算力攻击。



能实现：

- 修改/撤销过去的区块/交易：以更高的算力构建新的最长链
- 双重支付：通过切换最长链实现向两个人转同一笔钱（实际上只会有一个人收到）
- 限制某地址发送/接收数字货币：通过构建新的最长链排除掉与该地址相关的交易

日蚀攻击

日蚀，同日食，是指月球运动到地球和太阳的中间，如果三者正好在一条直线上，月球就会挡住太阳射向地球的光，月球身后的黑影正好落到地球上，这时发生日食现象。月球就切断了地球和太阳之间的（太阳光）联系。

日蚀攻击：攻击者针对特定的某个节点，通过一些方法，控制了这个节点进出网络的信息，切断它与其他节点的所有入站/出站通信，造成被攻击节点被“伪隔离”的现象。

日蚀攻击

原理：

比特币作为一个采用点对点网络的区块链应用，网络中的所有节点相互是平等的，相互之间也能无障碍地进行沟通链接，当然这只是理论情况。

实际上，由于网络带宽限制和算力分布限制，比特币限制了**单个节点可接收信息和主动链接其他节点的上限**。

- 对于**接受信息**，单个节点最多只能接收117个节点的信息
- 对于主动链接其他节点，单个节点只能主动联系其他8个节点

如果一个节点所接收信息的117个节点和对外链接的8个节点全部都是由恶意节点操控的话，相当于该节点被恶意者所孤立，其所有接受的信息都受到攻击者控制，这种情况我们便称该节点遭受了“日蚀攻击”。

日蚀攻击

日蚀攻击会导致：

- 阻止受害节点查看真实的区块链信息

  受害节点被恶意节点包围之后，恶意节点可以选择性的给受害节点发包或者篡改真实的数据包，本质上就是让这个节点误以为自己还在这个网络中挖矿，然而真实情况是它已经从网络中隔离开来了。

- 隔离网络中多个节点，以达到分裂网络的可能

  如果受害节点很多的情况，从整个网络全局来看就是被隔离成多个部分，网络实际上已经被分裂了。

- 用少于 51% 的算力发起 51% 攻击

  用比原来 51%攻击更少的算力可以很容易对分裂后的网络发起51%攻击。

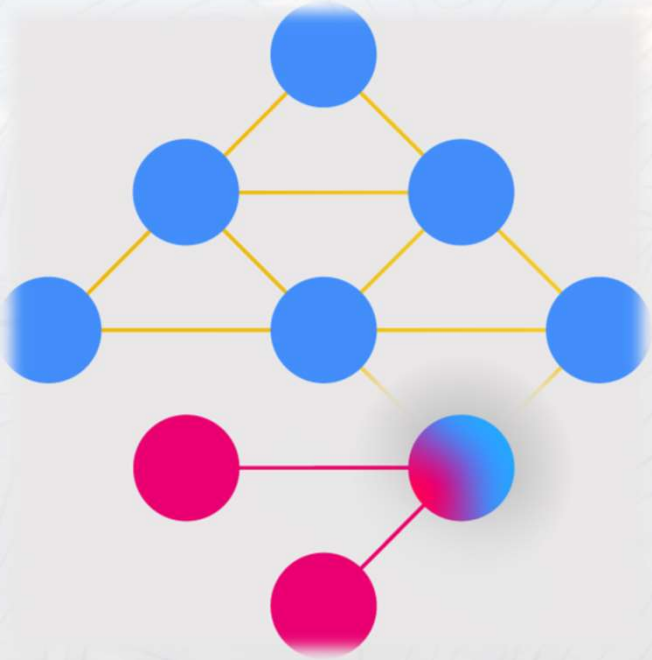
日蚀攻击

如何防御日蚀攻击

- 提高节点进入网络的准入门槛

  有效防止大批量伪造节点进入网络，从而从源头上避免日蚀攻击。

- 针对同一个 IP 段的节点做连接限制
- 对节点主动建立连接和被动建立连接的数量做一定的均衡
- NodeID 重启之后变化
- 其他辅助措施



Sybil攻击

女巫攻击(Sybil Attack), 是一种在线网路安全系统威胁，是指个人试图通过创建多个帐户身份，多个节点或电脑坐标从而控制网络。

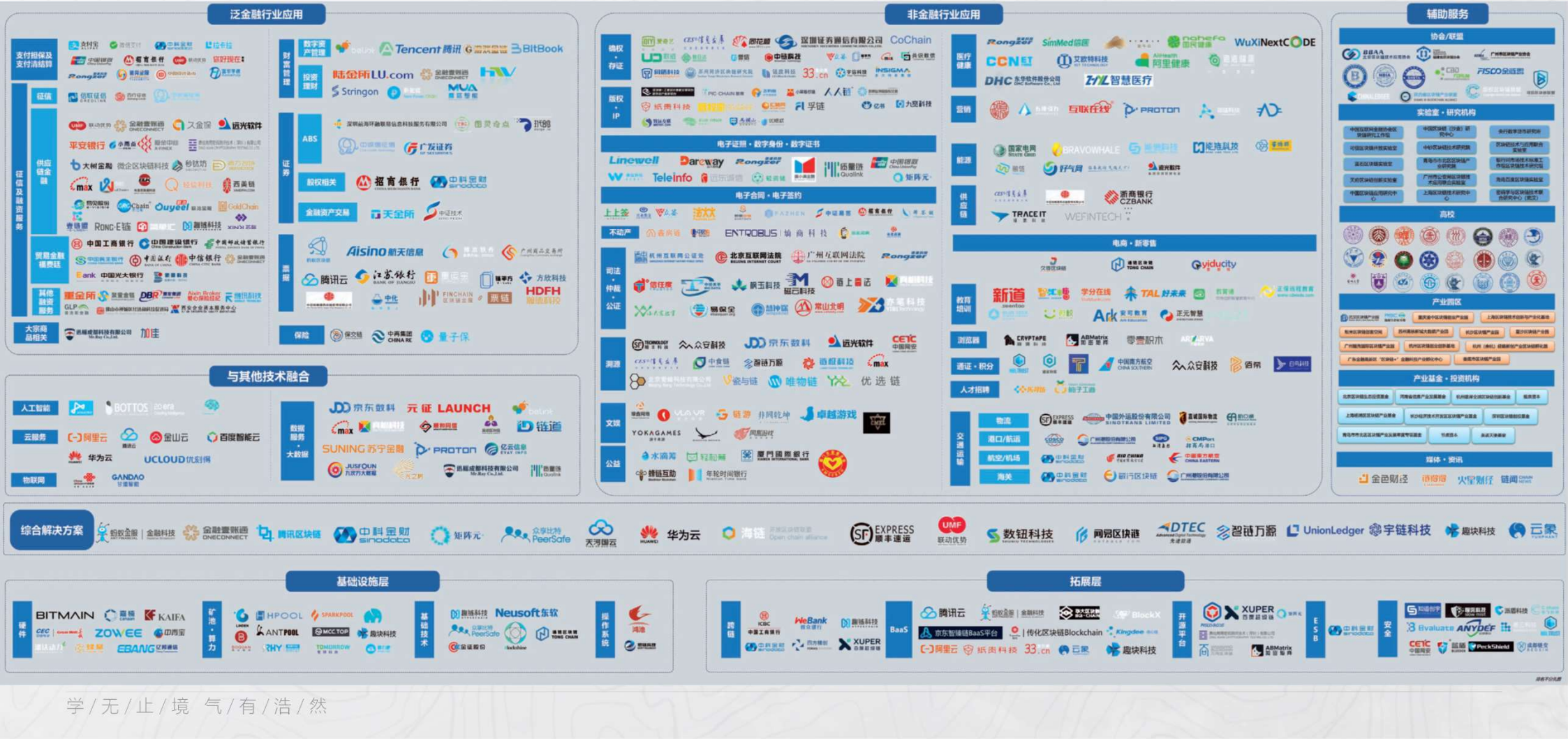
恶意攻击者在区块链网络中创建多个虚假身份或节点，以获得不当的影响和控制力。攻击者可以使用这些众多的虚假身份来操纵网络、破坏其功能或进行其他恶意活动。

- 攻击者可以拒绝传输或接收区块，有效地阻止用户访问网络。
- 可以促使随后的 51% 攻击，从而可以操纵交易和双重支付。

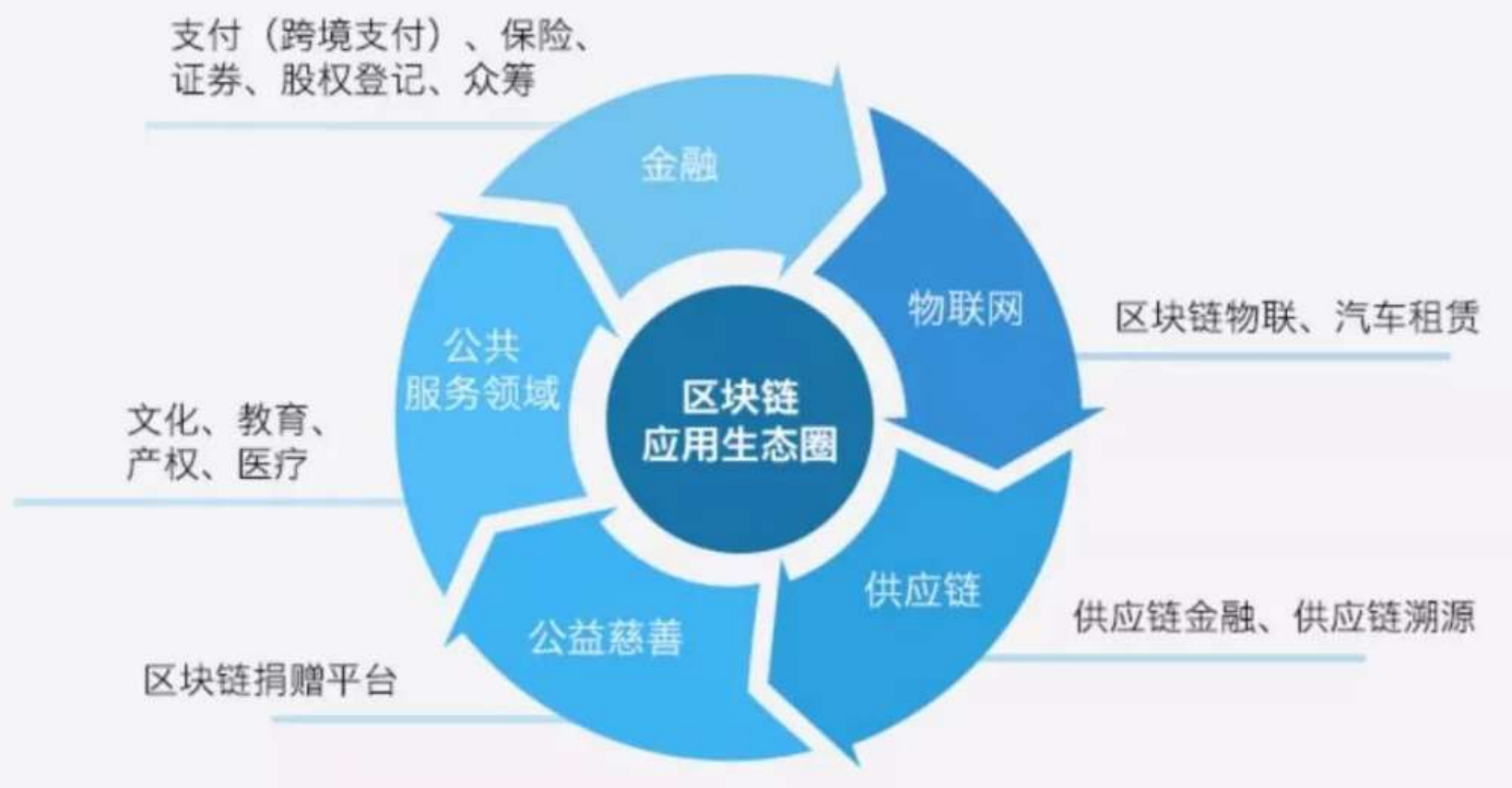
防御方式：类似日蚀攻击，改进共识机制

区块链的应用

区块链行业地图



区块链应用生态圈


支付（跨境支付）、保险、
证券、股权登记、众筹
金融
物联网
区块链物联、汽车租赁
公共
服务领域
文化、教育、
产权、医疗
区块链
应用生态圈
供应链
供应链金融、供应链溯源
公益慈善
区块链捐赠平台

区块链的应用——金融领域

资产支付

支付、交易清结算

资产数字化、信贷

证券市场

供应链金融、智能证券

场外市场、票据、股权

金融业务

机构间对接、旅游金融

征信、反洗钱、债务金融

区块链的应用——金融领域

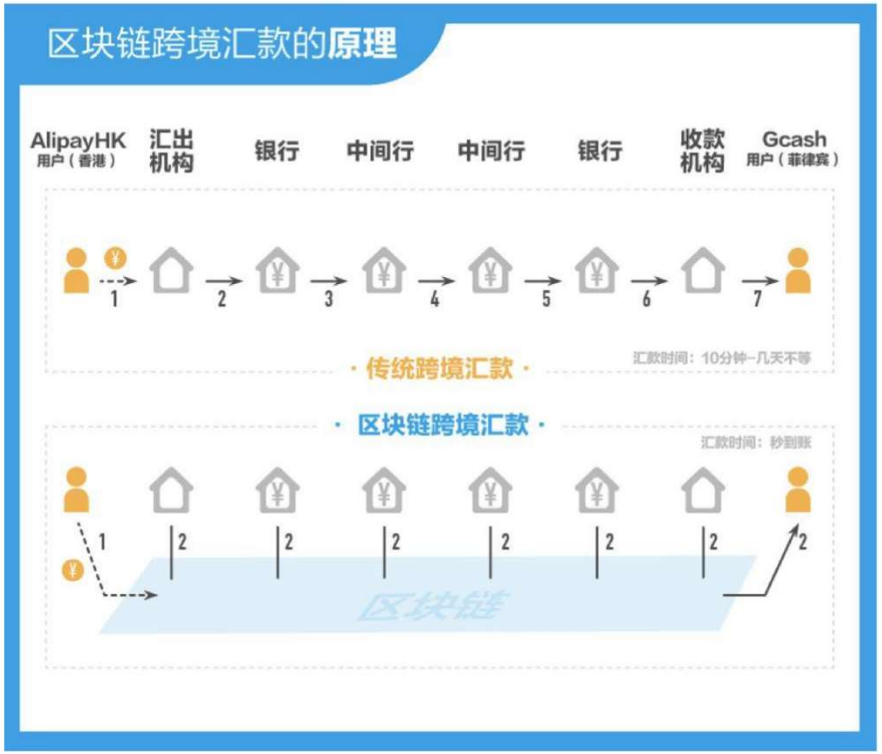
区块链解决方案——跨境支付

■ 行业现状与痛点

- 过程复杂
- 等待时间长
- 有转丢风险

■ 实施案例-基于区块链的电子钱包跨境汇款服务

■ 解决方案与优势



区块链的应用——社会管理

司法服务
电子合同存证链
可信电子固证平台
电子借据平台

政务服务
代理投票、工商管理
档案管理、遗产继承
政务诚信管理

社会服务
自然资源登记、鉴证证明
身份认证、智慧社区
人才招聘、区块链发票
家政服务征信平台

区块链的应用——社会管理

区块链解决方案——司法区块链

■ 行业现状与痛点

- 证据分散，不完整、易丢失
- 电子数据易被篡改、伪造
- 电子证据的法律效力

■ 解决方案与优势

■ 实施案例-杭州互联网法院

2018年09月18日，杭州互联网法院宣布司法区块链正式上线运行，成为全国首家应用区块链技术定纷止争的法院。司法区块链让电子数据的生成、存储、传播、和使用的全流程可信。

区块链的应用——社会管理

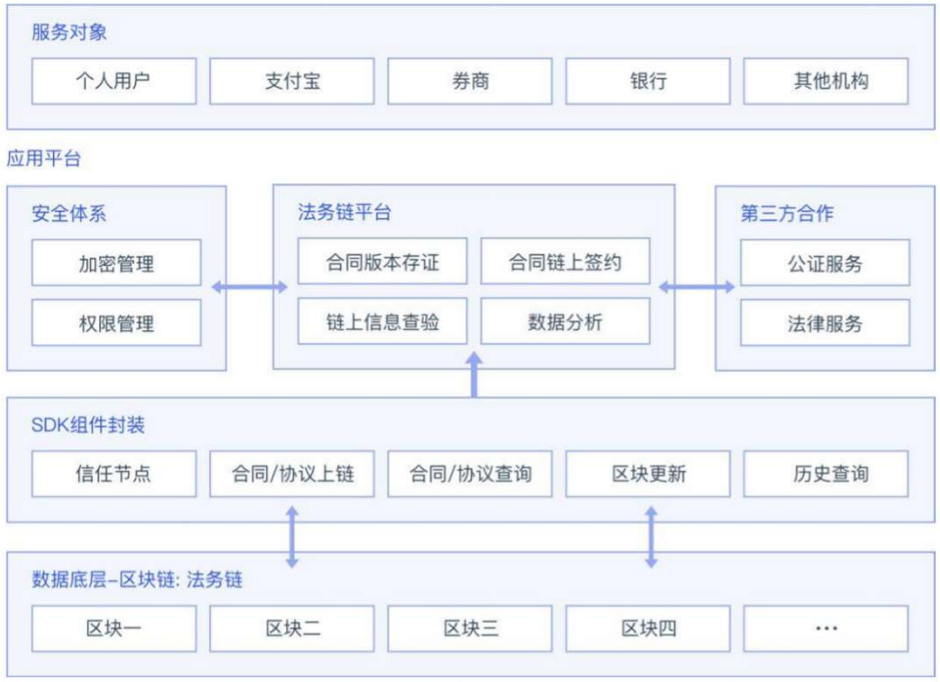
区块链解决方案——合同存证

■ 行业现状与痛点

- 行为不可追溯，数据易被篡改
- 信息数据过于集中
- 举证难度大
- 实施监管难

■ 实施案例-法大大

■ 解决方案与优势



区块链的应用——社会管理

区块链解决方案——商保快赔

■ 行业现状与痛点

- 纸质单据难保管，易丢失
- 存在骗保可能性
- 效率低下
- 保险理赔过程不透明
- 监管活动大量依赖纸质证据

■ 实施案例-信息美人寿相互保

■ 解决方案与优势

区块链的应用——慈善公益和医疗健康

慈善公益

善款公益、公益审计

互助急救联盟链、公益寻人链

医疗健康

数字病例、健康管理、

区块链+人工智能医疗服务体系

区块链的应用——慈善公益和医疗健康

区块链解决方案——电子票据区块链

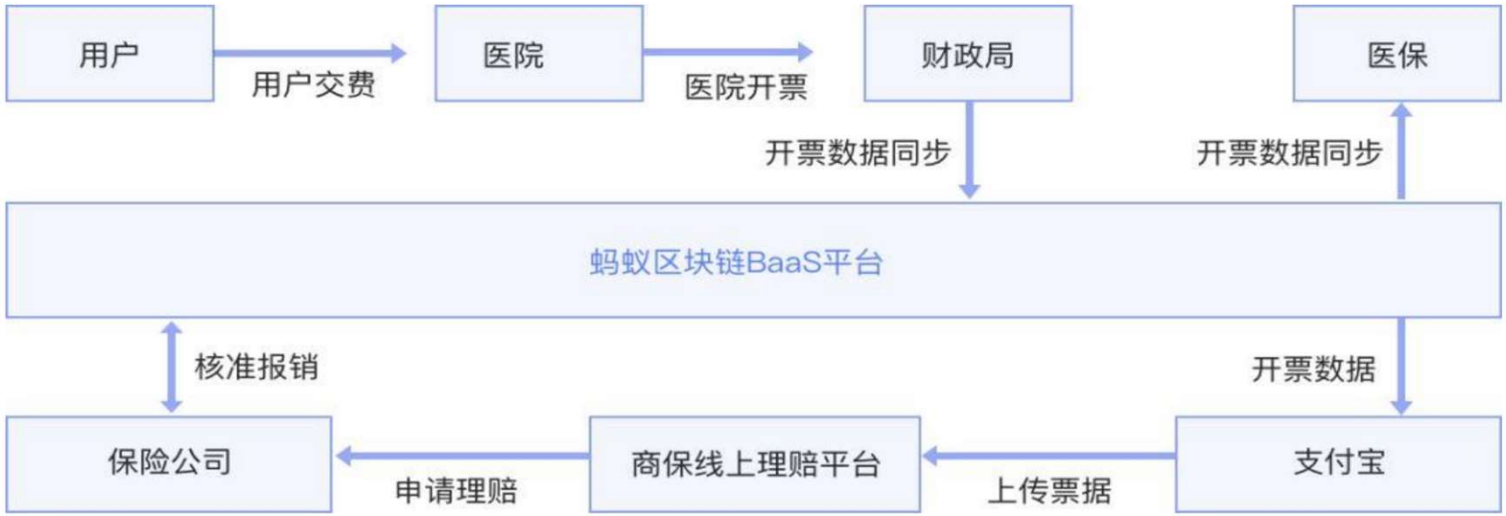
■ 行业现状与痛点

- 用户排队难
- 医院管理难
- 财政局监管难

■ 实施案例-杭州、台州和金华医院

从2018年8月2日开始，杭州、台州和金华三地医院的患者只要使用支付宝缴纳挂号费、门诊费用和住院费后，与此相关的电子票据就会即时发送到支付宝“发票管家”里。这些电子票据是区块链电子票据。

■ 解决方案与优势



区块链的应用——慈善公益和医疗健康

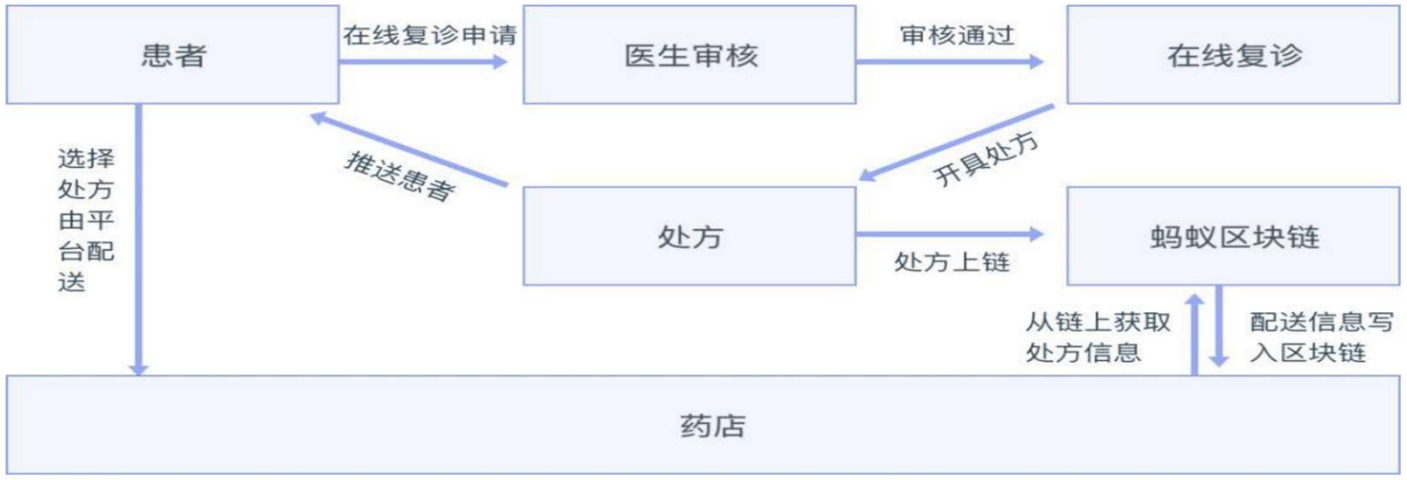
区块链解决方案——处方流转

■ 行业现状与痛点

- 信息的隐私保护
- 全程可被追溯
- 流转过程中防止被篡改

■ 实施案例-
华山医院电子处方

■ 解决方案与优势



区块链的应用——文化与版权保护和网络应用

版权存证流程图

文化与版权保护

专利保护、书籍许可证、数字内容保护

文学音乐视频游戏的版权保证

（人民版权平台、版权存证交易平台）

网络应用

区块链游戏、云计算

社交应用、文件存储

区块链的应用——物联网

智能制造
仓储管理
零件生命周期监控

共享经济
智能电网
汽车房屋租赁

供应链管理
物流链溯源、防伪认证
物流追溯、责任认定

智能家居
智能家电
（门锁、冰箱）

区块链的应用——物联网

区块链解决方案——供应链金融

■ 行业现状与痛点

- □ 小微企业融资难融资贵问题突出
- □ 金融机构操作风险与成本较高
- □ 核心企业参与意愿不足

■ 实施案例-德志星

蚂蚁金服区块链发布 “双链通”：
融资到付账期 3 个月变 1 秒

■ 解决方案与优势

区块链的应用——物联网

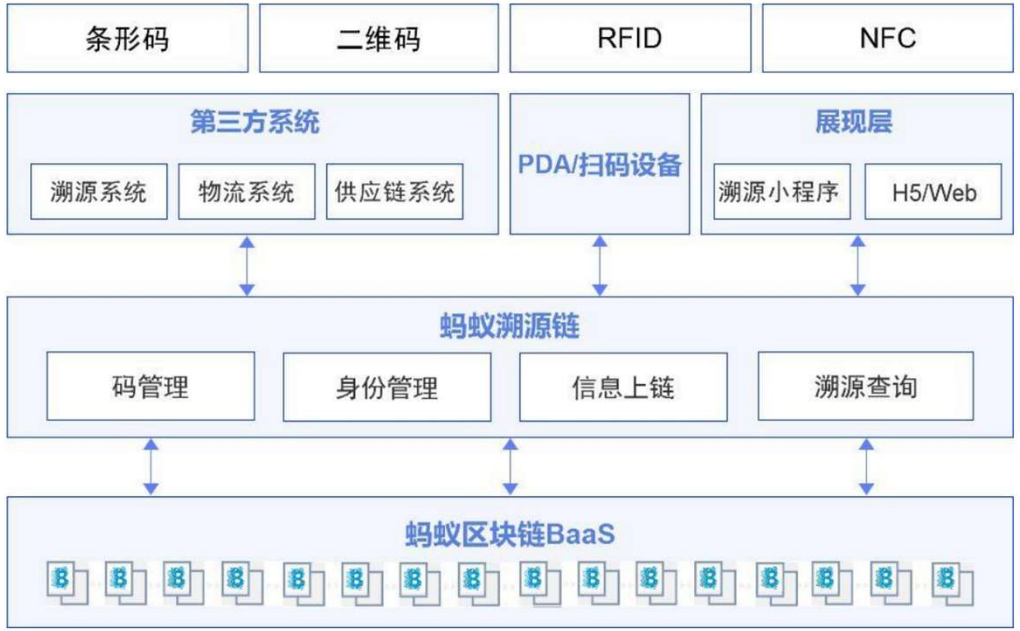
区块链解决方案——通用溯源

■ 行业现状与痛点

- 信息不对等以次充好
- 纠纷无法处理
- 供应链效率低

■ 实施案例-五常大米

■ 解决方案与优势



区块链的应用——物联网

区块链解决方案——智慧租房

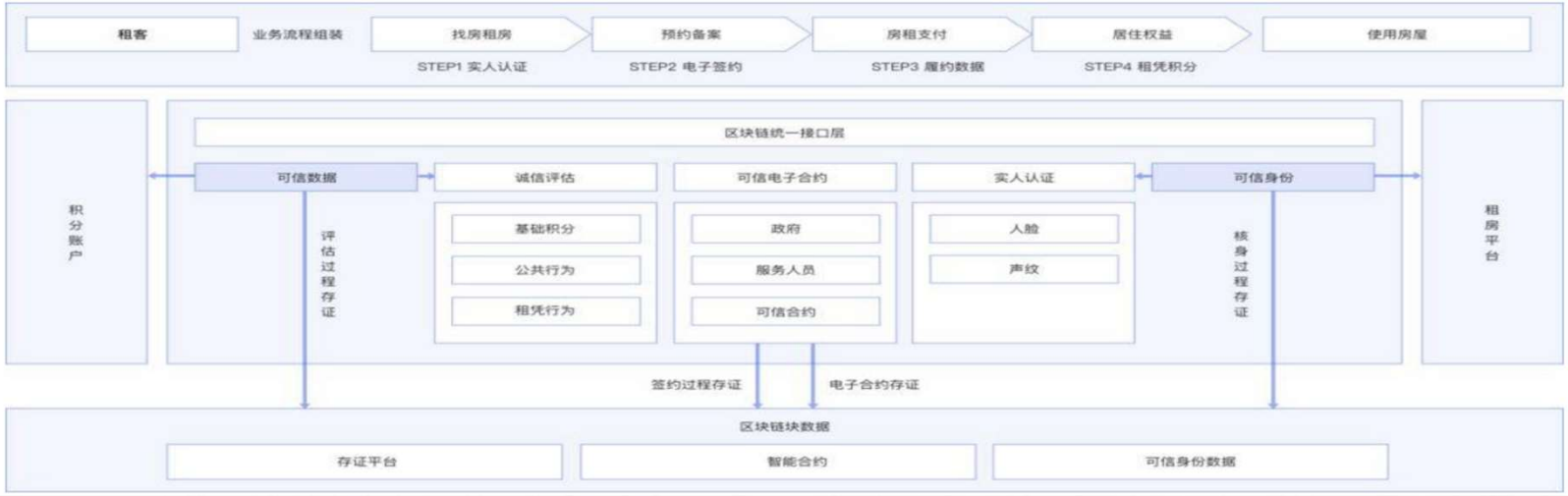
■ 行业现状与痛点

- 运营规范难
- 风险把控难
- 政府监管难
- 享受权益难

■ 实施案例-雄安上线区块链租房应用平台

雄安已在2018年4月4日建成区块链租房应用平台，这是国内首例把区块链技术运用到租房领域。此举有望解决租房场景最核心的“真人、真房、真住”的问题。

■ 解决方案与优势

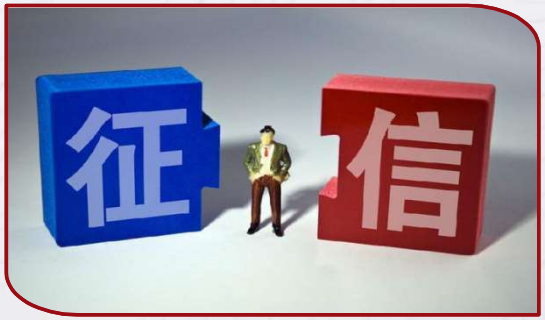


区块链的应用——教育方面

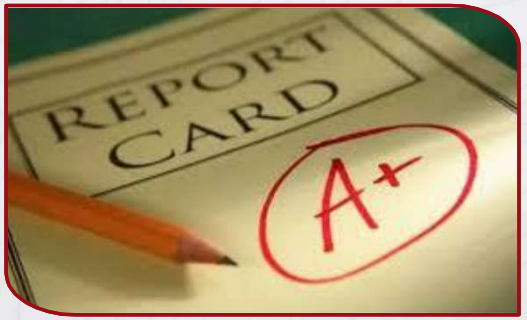
档案管理

学历证明

产学合作



学生征信



成绩证明


Any Questions?