区块链与数字经济

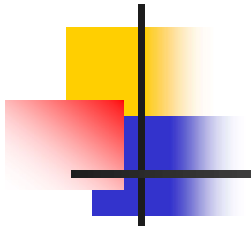
吴 威

电话：82317616， 地址：新主楼1016室

信箱： wuwei@buaa.edu.cn

北京航空航天大学计算机学院

虚拟现实技术与系统国家重点实验室



授课内容

一、数字经济应用

二、区块链安全措施

三、拜占庭容错BFT

四、实用拜占庭容错PBFT

五、知识点

一、区块链在数字经济中的作用

互联网发展历程

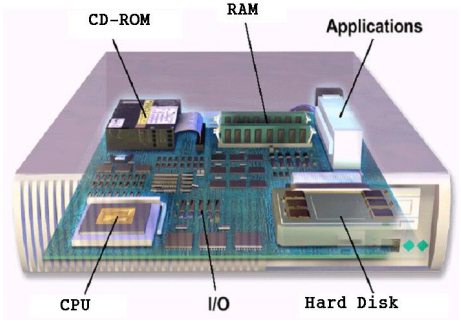
1970-1980

1990-1999

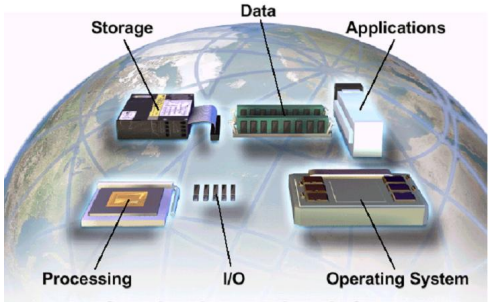
1999-2015

2006-2016

2008-2027



集中式系统

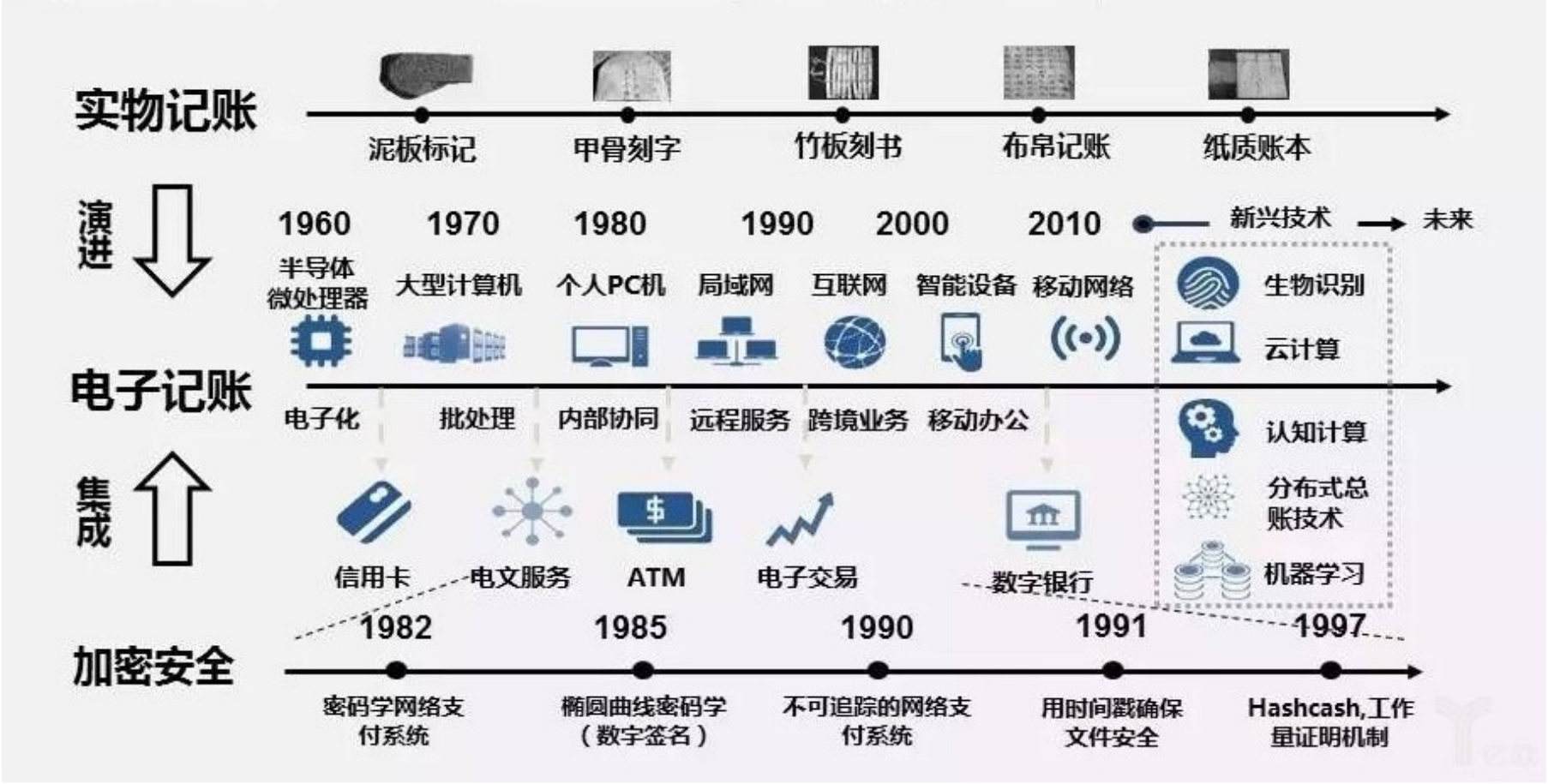


分布式系统

区块链

拜占庭帝国 Byzantine

记账方式的演化


实物记账
泥板标记
甲骨刻字
竹板刻书
布帛记账
纸质账本
演进
1960
1970
1980
1990
2000
2010
新兴技术
未来
半导体
微处理器
大型计算机
个人PC机
局域网
互联网
智能设备
移动网络
生物识别
云计算
电子记账
电子化
批处理
内部协同
远程服务
跨境业务
移动办公
认知计算
分布式总
账技术
集成
信用卡
电文服务
ATM
电子交易
数字银行
机器学习
1982
1985
1990
1991
1997
加密安全
密码学网络支
付系统
椭圆曲线密码学
（数字签名）
不可追踪的网络支
付系统
用时间戳确保
文件安全
Hashcash,工作
量证明机制

金融体制

金融体制：银行等金融机构利用各种信用活动组织、调节货币流通与资金运动的形式和管理制度的总和。

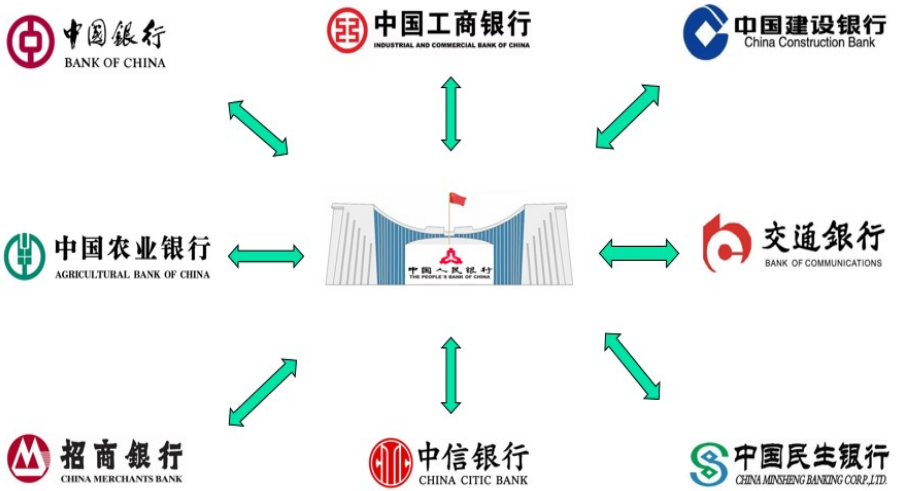
主要有四个方面：

1、银行为主体的多种形式的金融机构并存；

2、中央银行为金融体系的核心机构和宏观调控机构；

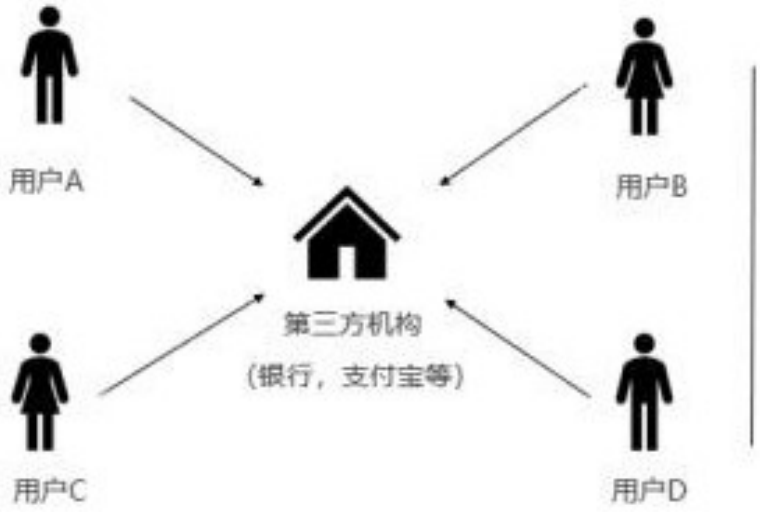
3、中央银行垄断货币发行权；

4、国家对金融机构的设置和金融活动进行严格的管理。

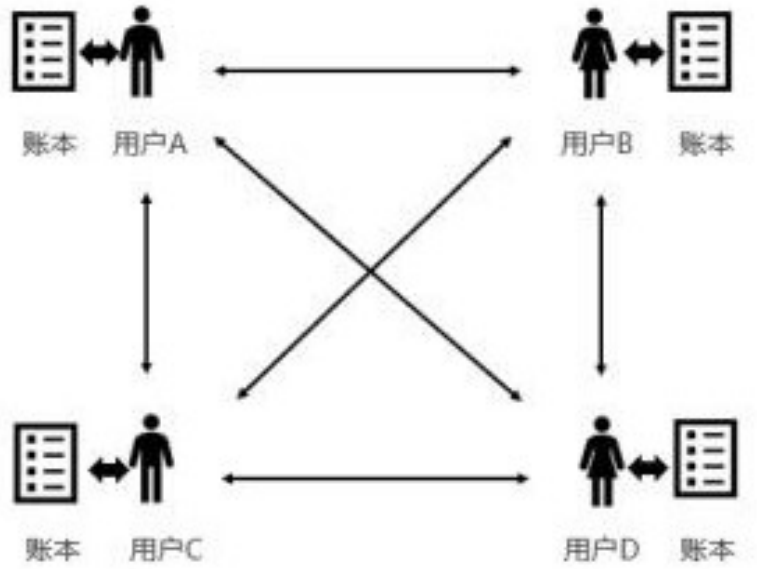


区块链技术释义

- 集体协作共同维护的可靠数据库方案
- 区块链（**Blockchain**）是一个分布式账本

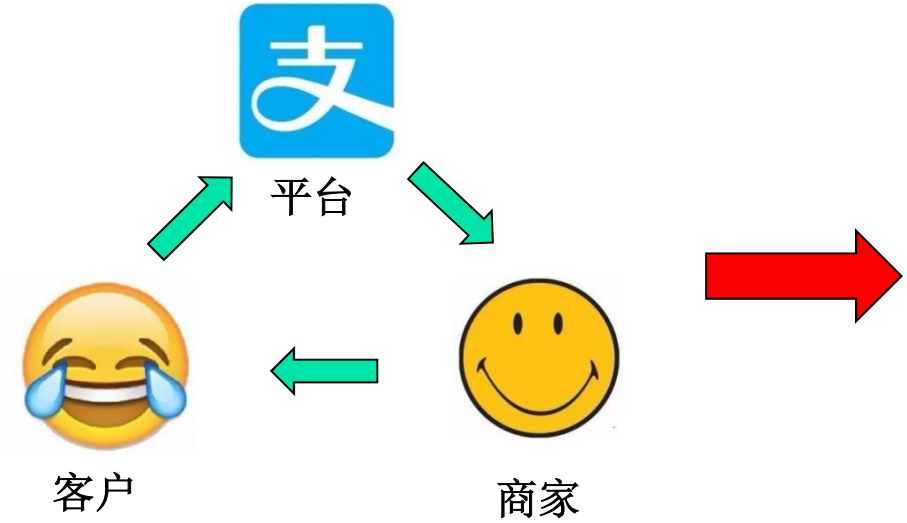


中心化机构运行“账本”并有权记账



以区块链形式存在的“账本”所有人均有记账权

分布式数据库（记账本）


平台
客户
商家


区块链


1. 新交易创建
TX
A
B
2. 交易通过P2P网络传播
TX
3. 交易验证
4. 验证结果通过P2P网络传播
5. 交易写入账本

区块链发展情况

- 区块链 1.0：数字货币（比特币）
- 区块链 2.0：数字资产与智能合约 （以太坊、EOS、股票、证券、期货、保险、募捐）
- 区块链 3.0：DAO/DAC区块链大社会（科学、教育、医疗等）

区块链在数字经济中的作用

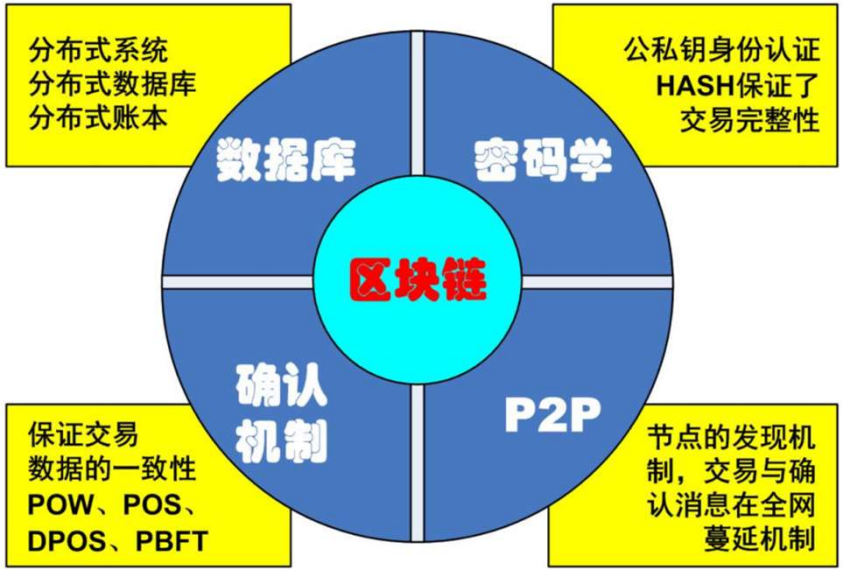
- BTC数量有限
- 跨境支付成本低
- 不受外汇管制限制
- 资产转移快速便捷
- 私密与不可追踪
- 交易媒介
- 军火交易
- 防止在深网、暗网交易

二、区块链安全措施

- 拜占庭将军问题到底是什么问题？
- 区块链技术是如何解决拜占庭将军问题？
- 理解问题比找到解决问题还重要！

区块链相关技术

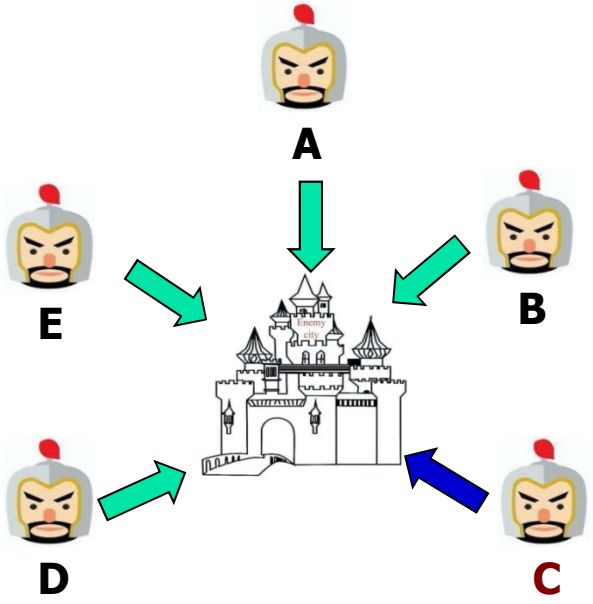
- 分布式系统：分布、选举、替代
- 数据库：分布数据库、事物模型
- 密码学：秘钥公钥、哈希函数
- 共识机制：挖矿、选举、拜占庭容错
- 网络技术：广播、组播、可靠、P2P

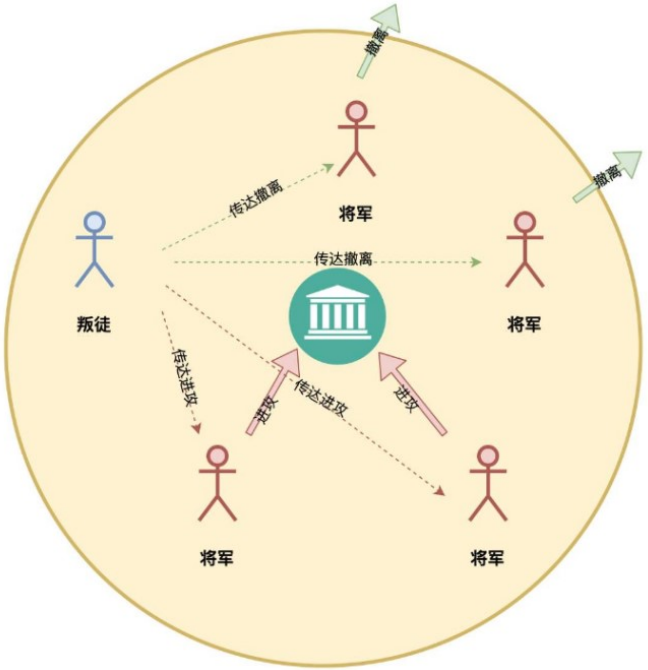


区块链是一个共享数据库，存储于其中的数据或信息，具有“不可伪造”“全程留痕”“可以追溯”“公开透明”“集体维护”等特征，区块链技术奠定了坚实的“信任”安全措施。

拜占庭将军问题

- **Lamport（1982）提出的拜占庭将军问题（Byzantine Generals Problem）；**
- **存在拜占庭将军情况下要达成一致的作战计划；**
- **在不可信任环境下的分布式一致性问题。**





希望能找到一个算法，保证在存在叛徒阻挠的情况下，仍然能够达成军事目标！

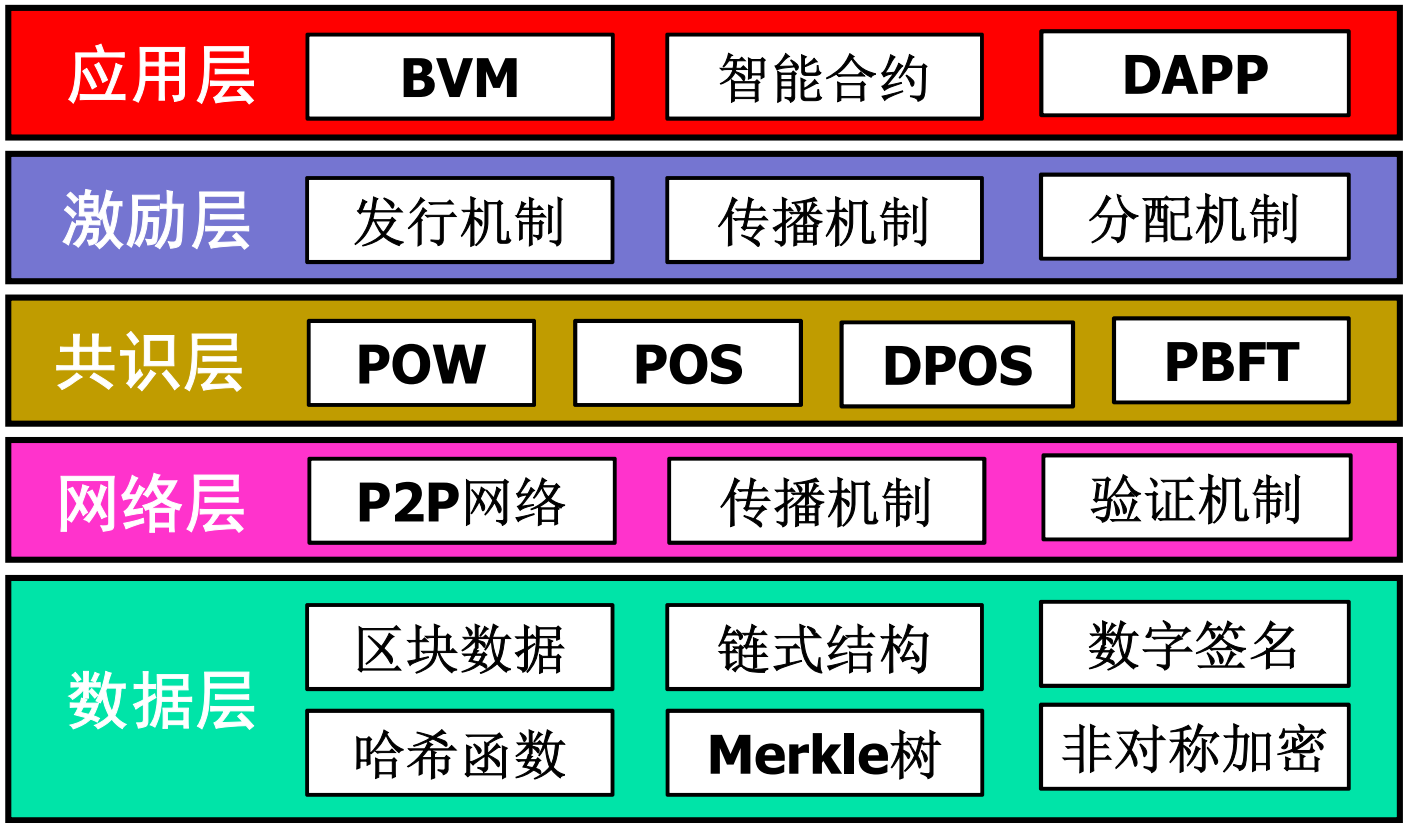
以太坊 Ethereum

智能合约，开发应用

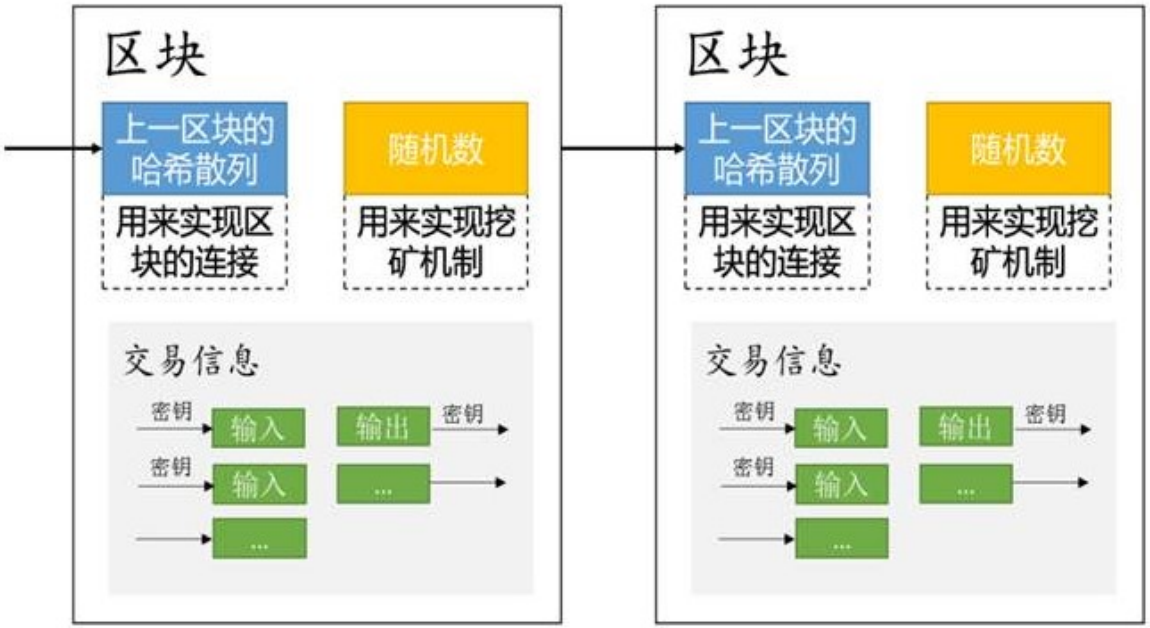
缩短出块时间为16秒

加入POS与DPOS

支持发送数据与变量，采用更加优化的加密算法和Merle树



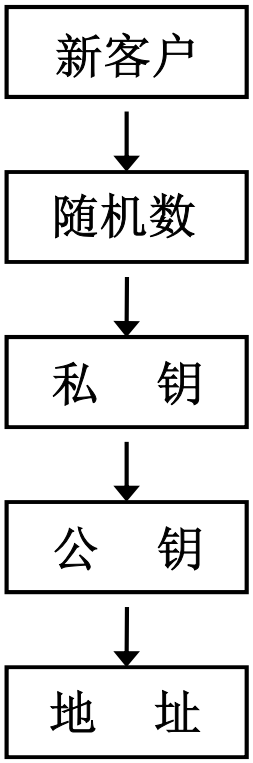
区块数据结构示意图

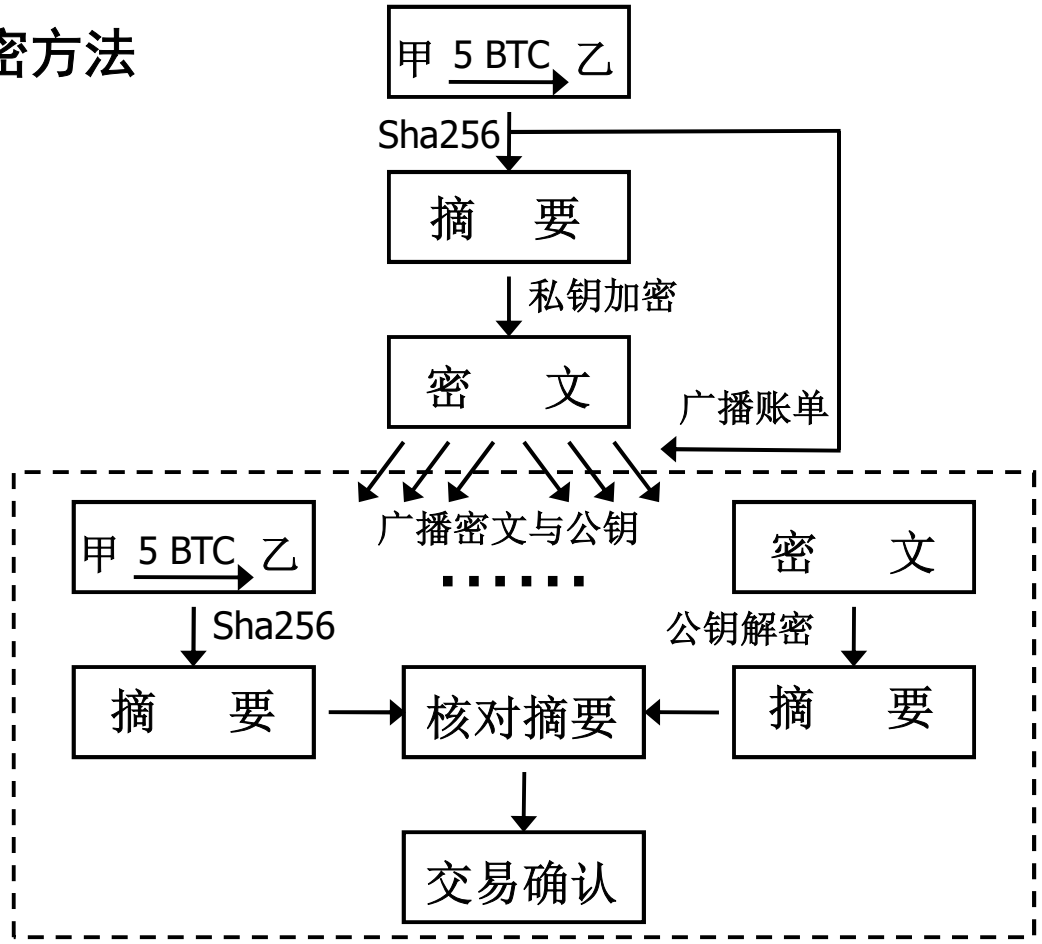

区块
上一区块的哈希散列
随机数
用来实现区块的连接
用来实现挖矿机制
交易信息
密钥
输入
输出
密钥
输入
...
...
区块
上一区块的哈希散列
随机数
用来实现区块的连接
用来实现挖矿机制
交易信息
密钥
输入
输出
密钥
输入
...
...


1. 新交易创建
TX
A
B
2. 交易通过P2P网络传播
TX
3. 交易验证
4. 验证结果通过P2P网络传播
5. 交易写入账本

区块链的交易认证

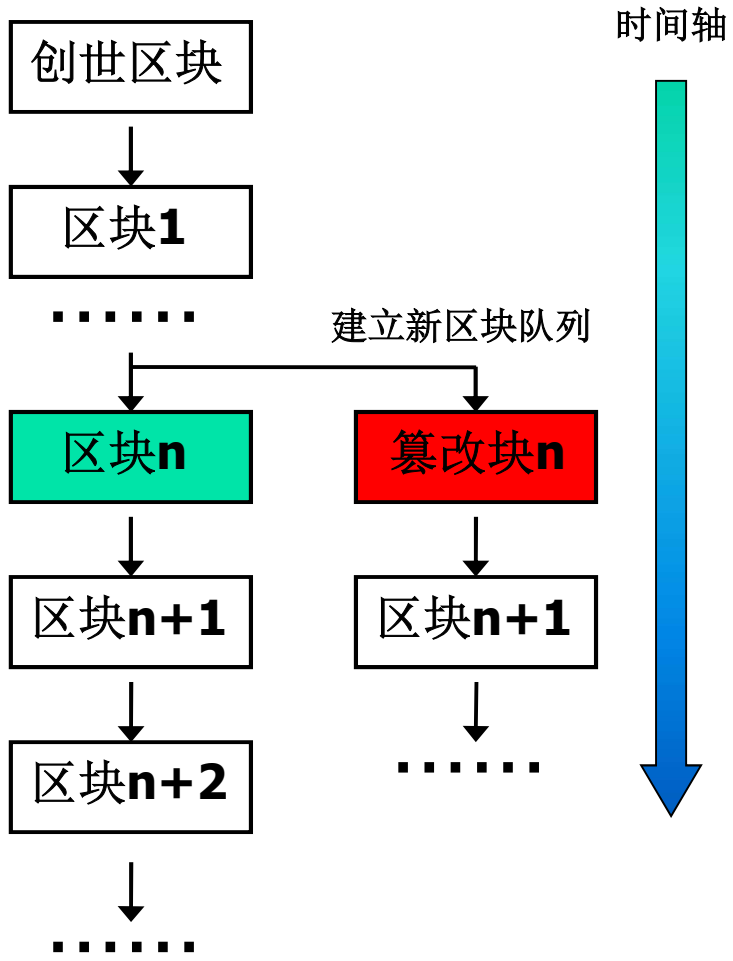
电子签名：非对称加密方法





篡改历史交易的代价

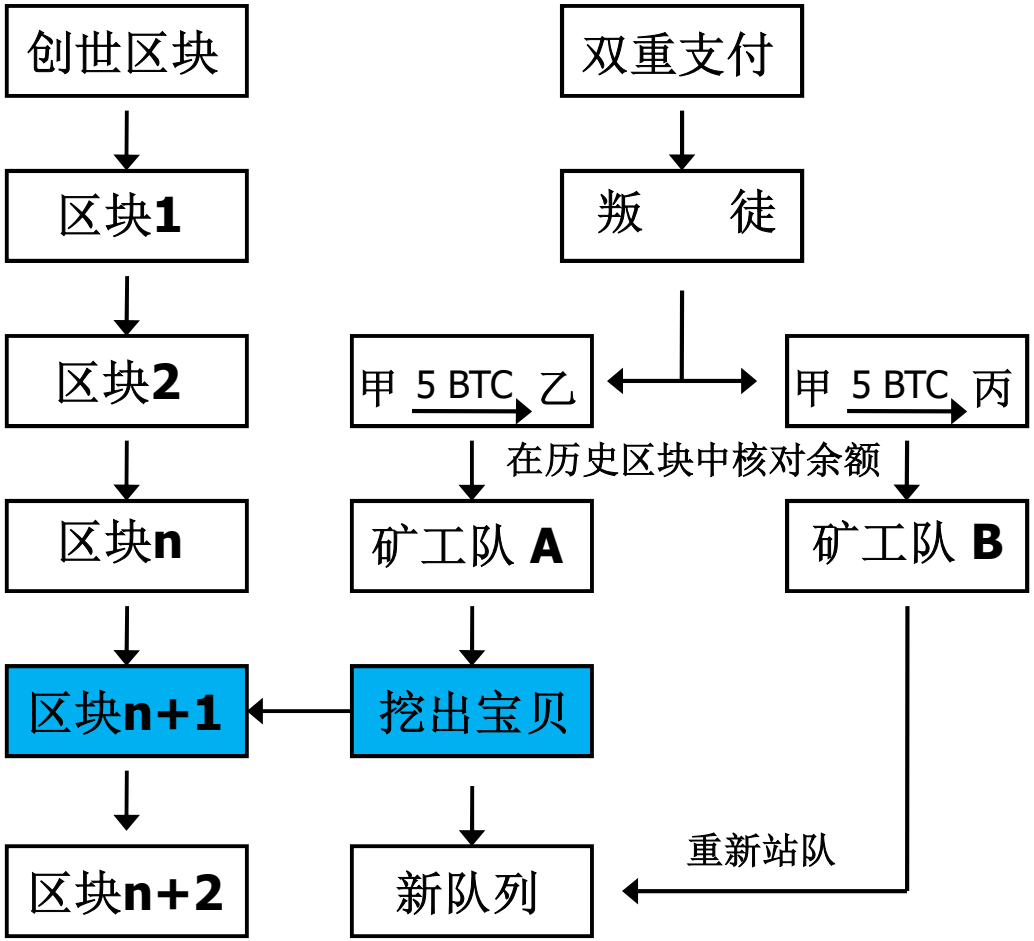
- 非对称加密
- 最长链原则
- 哈希值反算非常困难
- 掌握全网**51%**以上的算力攻击
- 对**BTC**攻击需要**50**亿美元设备
- 每天消耗**1**亿人民币的电费



结论：当你具备作恶能力的时候，你将失去作恶的动机！

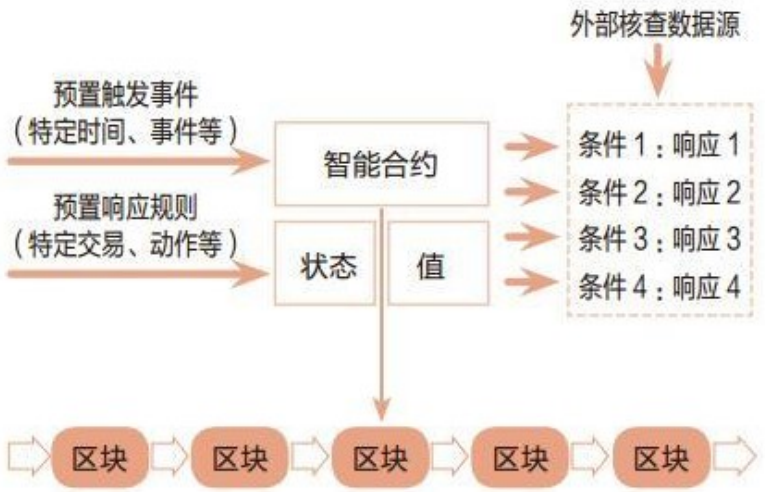
双重支付问题

- 物理货币不存在问题
- 数字世界全网公开
- 历史交易时间戳
- 工作量证明的确认



智能合约 Smart Contract

合　同　　智能合约　　执　行



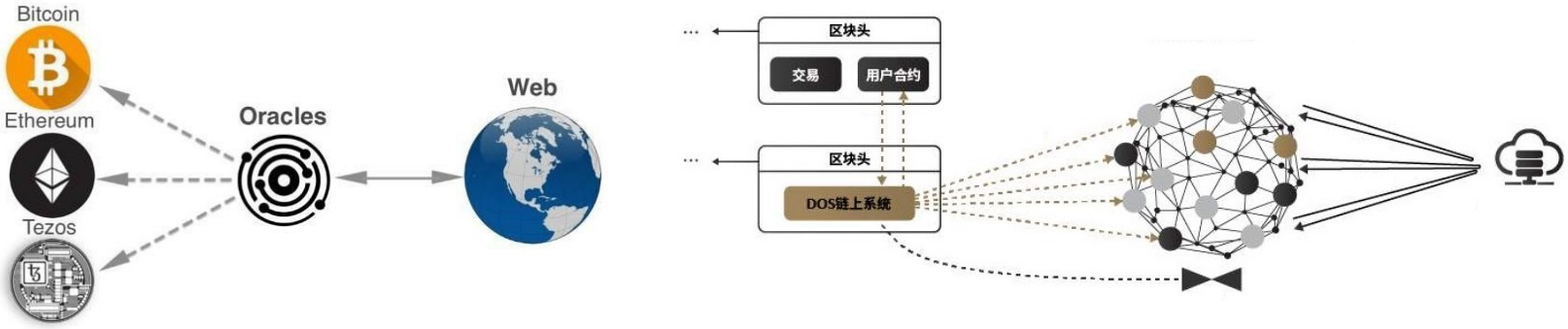
- 智能合约是一种以信息化方式传播、验证或执行合同的计算机一段程序，交易可追踪且不可逆转；
- 智能合约在没有第三方的情况下进行可信交易，在公共监督的情况下去运行一个合约，违反合约的一方将付出事先设定好的代价。

例如：A向B借钱不还，欠条等于合约，而将这张欠条公布于天下让所有人都知道的合约这就是智能合约，解决要脸与不要脸的借款关系；

智能合约应用示例

区块链在国际贸易中的作用

预言机 Oracles



- 预言机是智能合约与链外进行数据交互的唯一途径；
- 预言机为智能合约的触发和运行提供一定的链外数据；
- 提供智能合约在合约条款得到满足时运行的链外条件。

共识机制 Consensus

- 工作量证明：**POW**算法适合应用在公有链，**POW**算法的出块时间较长，导致共识效率较低；

- 股份授权证明：**DPOS**在网络中拥有数字货币也就是拥有股份的节点，可以进行投票来选择共识代表，按照约定的记账时间轮流生成区块，但其依赖于数字货币才能完成共识的机制；
- 实用拜占庭容错：**PBFT**共识算法是适用于联盟链，是解决存在一定数量的各种错误节点情况下仍然可以达成共识。

目前主要的共识机制

区块链主要共识机制：

- 工作量证明 **POW**
- 权益证明 **POS**
- 股份授权证明 **DPOS**
- **EOS在DPOS基础上，融合了拜占庭容错PBFT，构建了实用的PBFT-DPOS共识机制。**

制度与成本的约束力

- 采用工作量证明相当于提高了做叛徒的成本，极大降低了叛徒超过半数的可能性，由此可以认为叛徒不至于太多；
- 在计算机网络中，如果没有类似工作量证明的机制，那么成为叛徒矿工的成本就是非常低的，这就很有可能使得叛徒比忠诚的矿工还要更多；
- 从经济学的角度看，在需要工作量证明的前提下，成为叛徒矿工也是不明智的，如果拥有比较强的算力，通过挖矿赚取收益更为稳妥。

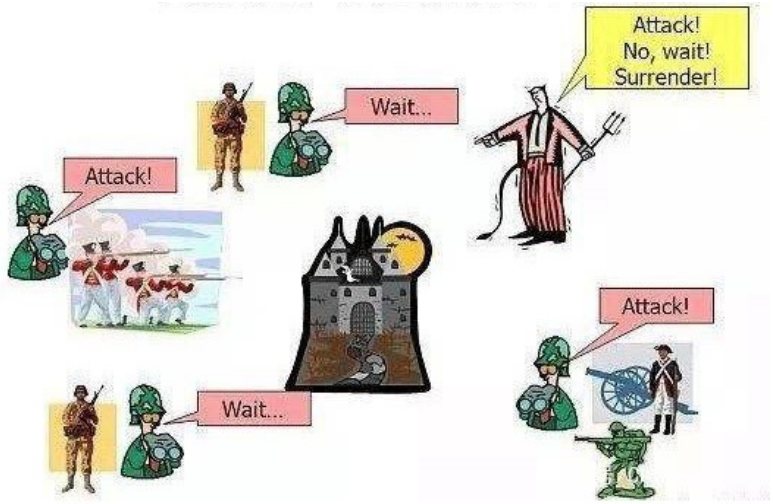
三、拜占庭容错BFT

- Lamport（1982）提出拜占庭将军问题BFT（Byzantine Fault Tolerance）
- BFT共识算法的目的是在不信任网络中的节点间建立信任关系
- BFT在计算领域发展成了一种容错理论

拜占庭将军问题BFT

拜占庭将军问题：

- 忠实的将军们听从大多数将军们的方案；
- 坏的将军的数目小于1/3；
- 忠实的将军们就可以达成正确的共识；
- 当存在叛徒情况下，仍然能达成军事目标！

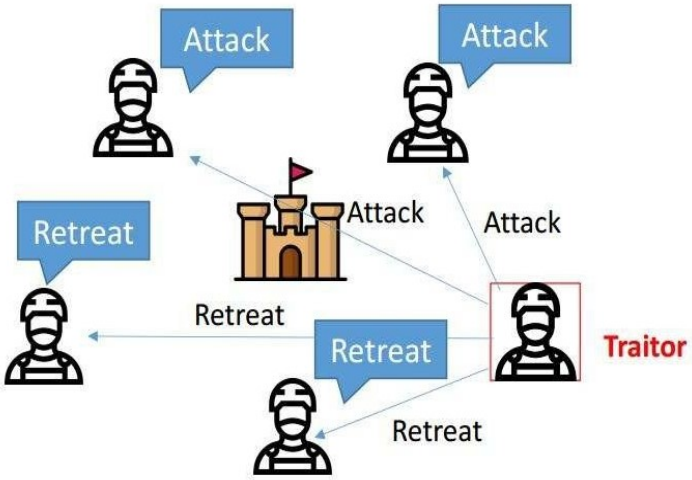


区块链问题：

- 区块链中也存在出错的节点或者恶意节点；
- 节点可能因为种种原因伪造签名、恶意破坏系统的一致性；
- 要求区块链网络的共识机制有容错设计；
- 部分节点作恶或者失效之时仍然能达成整体的一致性。

协同一致的界定条件

- 节点可信任，达成共识的条件是收到可信任节点回复的消息>n/2，即要收到大多数节点的反馈才能表示共识完成；
- 不可信节点m个，可信任节点是n-m个，收到的可信任节点数回复信息必须>(n-m)/2才表示绝大多数可信任节点已经收到消息了；
- 可能收到m个不信任节点回复，当（n-m)/2 > m 的时候，根据多数原则，得出 n> 3m，即总数n>= 3m+1。



“拜占庭将军问题”的解法应该是最强的一类分布式一致性算法，它理论上能够处理任何错误，通常把能够处理拜占庭错误的这种容错性称为BFT。

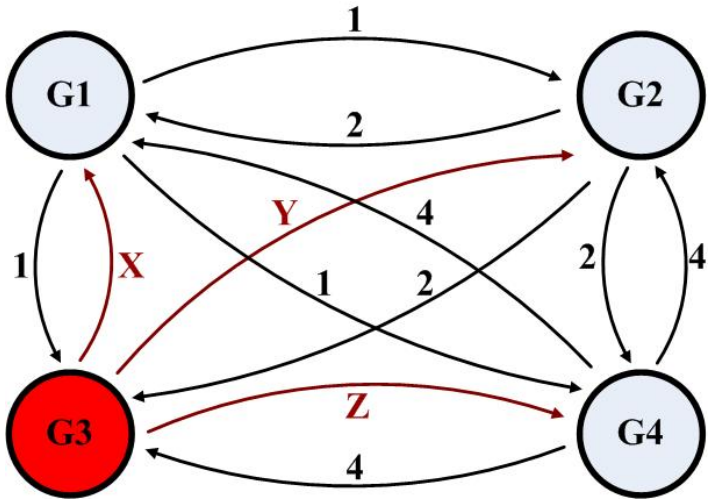
口头协议与书面协议

- 如果使用口头消息，至少需要多于2/3的将军是忠诚的，如果使用签名消息，对忠诚将军的数量是没有要求的；
- 如果将军之间使用口头消息，消息被转述的时候是可能被篡改的，那么要对付m个叛徒，需要至少有3m+1个将军；

- 如果将军之间使用签名消息，即消息被发出来之后是无法伪造的，只要被篡改就会被发现，那么对付m个叛徒，只需要至少m+2个将军，即至少2个忠诚的将军；
- 如果只有 1个忠诚的将军，显然这个问题没有意义，这种情况实际相当于对忠诚将军的数目没有限制；
- 如果忠诚的将军数目太少，不管最终确定的作战计划是什么，还是会失败，因为叛徒可能不执行这个作战计划。

拜占庭将军问题算法BFT

- 假设通讯正常，而处理机出错
- 3个忠诚将军，1个叛变将军
- 交换人数，交换情报
- 结果：1、2、4可协同一致



1 Got（1，2，x，4）
2 Got（1，2，y，4）
3 Got（1，2，3，4）
4 Got（1，2，z，4）

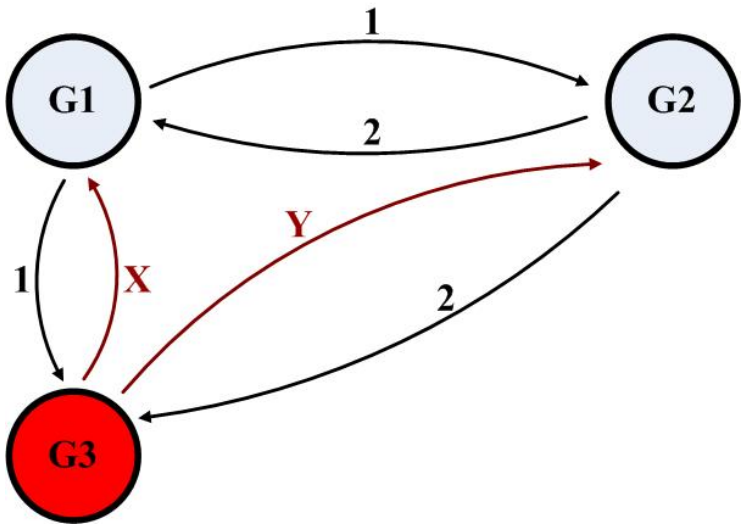
1 Got（1，2，y，4）
（a，b，c，d）
（1，2，z，4）

2 Got（1，2，x，4）
（e，f，g，h）
（1，2，z，4）

4 Got（1，2，x，4）
（1，2，y，4）
（i，j，k，l）

拜占庭将军问题算法BFT

- 若三个将军中，两个忠诚，一个叛变，则不能判断出哪个将军叛变
- 若要有m个处理机出错的系统实现协同一致，最少要有2m＋1个正常处理机，处理机总数为3m+1，大于2/3即可？

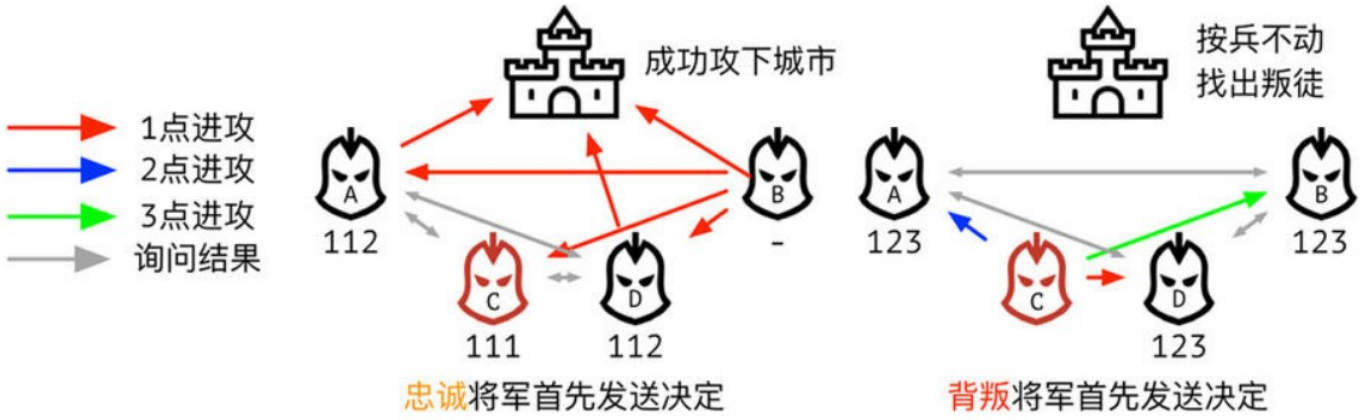


1 Got（1，2，x）
2 Got（1，2，y）
3 Got（1，2，3）

1 Got（1，2，y）
（a，b，c）

2 Got（1，2，x）
（d，e，f）

BFT存在的问题



- **Fischer（1985）证明难以区别特别慢的处理机与失效的处理机，当传输有延时，当仅一台处理机出现问题（fail-silent），协同几乎是不可能；**
- **Lamport只在同步环境中（所有的消息总是及时到达）采用算法的理论可行性。但在现实世界中，不能真正地相信互联网能及时交付任何东西；**
- **假设区块链分布式网络中存在出错的节点或者恶意节点，这些节点可能因为种种原因伪造签名、恶意破坏系统的一致性；**
- **要求区块链网络的共识机制有容错设计，在部分节点作恶或者失效之时仍然能达成整体的一致性。**

四、实用拜占庭容错PBFT

- Castro和 Liskov（1999）提出实用拜占庭容错算法PBFT；
- PBFT的改进使得拜占庭将军问题的实际应用成为可能；
- PBFT将算法复杂度从指数级降低到多项式级；
- PBFT可以在传输有延时或不可靠的情况下，保证系统的正确性。

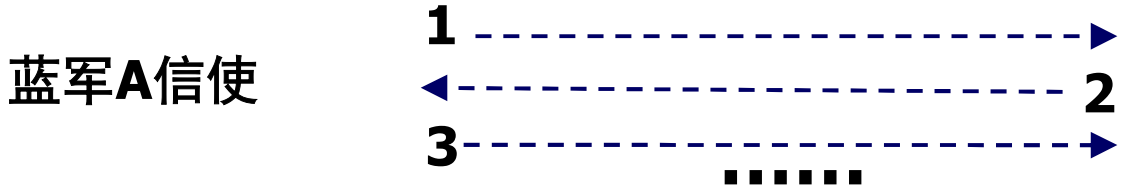
协同一致与共识

- 通讯：假设处理机正常，通信不可靠，可能会时延及丢包；
- 问题：最后消息发送者不能确定其信是否安全到达；
- 结论：两个进程达成协同一致可能吗？讨论最小协议问题。

蓝军A（3000人）

红军A（5000人）

蓝军B（3000人）



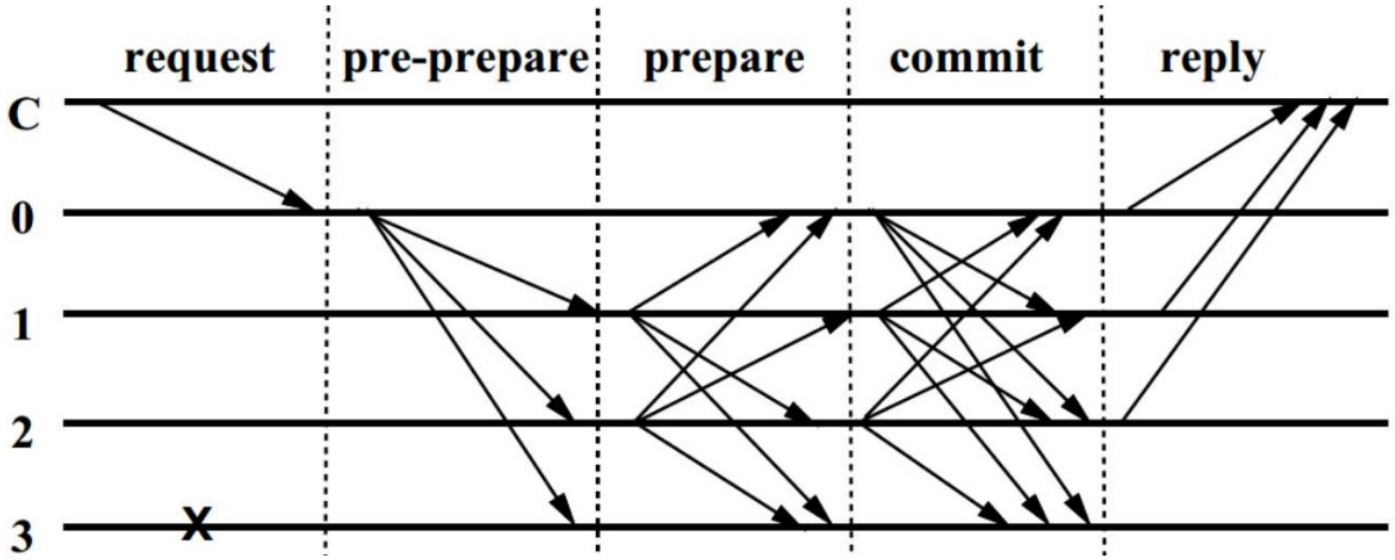
实用拜占庭容错PBFT

PBFT实现的三个协议

- 一致性协议：一致性协议用来保证全网所有的节点保存数据的一致性，其通过三阶段节点间的互相通信来实现；
- 视图更换协议：主节点出现故障时，立即触发视图更换协议来更换主节点；
- 检查点协议：该协议则定时触发，用来清理一致性协议执行过程中各个节点存储的通信消息，并同步各个节点的状态。

实用拜占庭算法PBFT

- 实用PBFT将复杂度由指数级降低到多项式级，每个节点都可以发布公钥，节点将签名所有通过节点的消息，以验证其准确性，当得到一定数量的签名节点，此交易就被认定为有效；
- 一致性协议是PBFT算法能够完成共识的核心协议，主要分为预准备（pre-prepare）、准备（prepare）和提交（commit ）3个阶段完成。

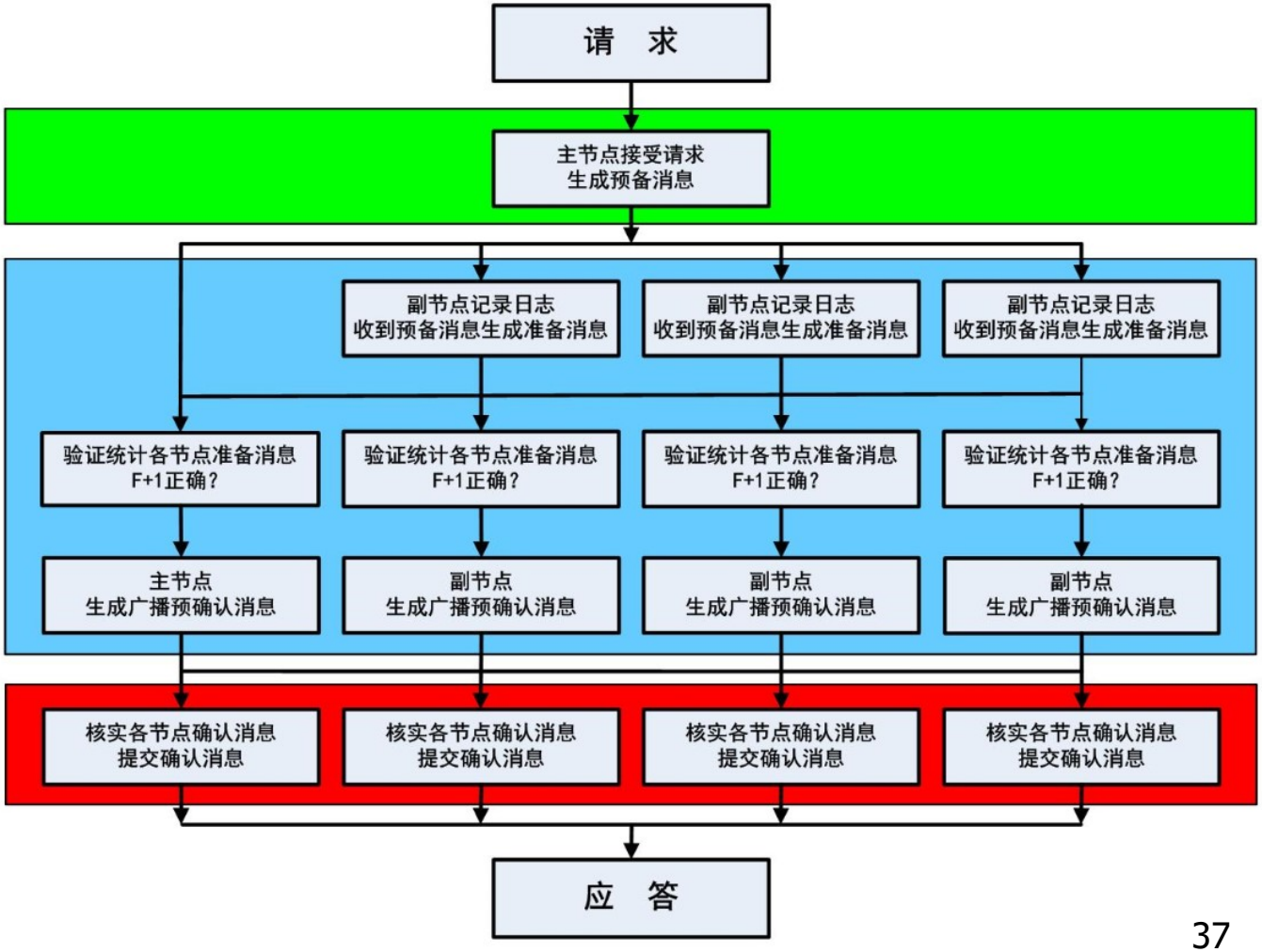


PBFT算法流程

预准备阶段

准 备 阶 段

确 认 阶 段



拜占庭将军问题的模型化

- 中本聪发明的比特币完美地解决了拜占庭将军问题；

- 拜占庭将军问题解决的条件：
  （1）信息发送的身份追溯；
  （2）信息的私密性；
  （3）不可伪造的签名；
  （4）发送信息的规则。
- 拜占庭将军问题是网络世界的模型化，第一个广播信息的将军就是第一个发现有效哈希值的计算机节点。

PBFT算法的问题

- PBFT计算效率依赖于参与协议的节点数量，不适用于节点数量过大的系统，扩展性差；
- PBFT节点是固定的，无法应对开放环境，仅适用于带身份认证的联盟链或私有链系统；
- PBFT失效节点数量必须小于全网节点的三分之一，容错率相对较低；
- PBFT不能很好的存储记录其交易信息，黑客能够截取一些失效的副本，这会让信息外漏；
- PBFT就是少数服从多数，在整个网络中的任意节点都无法信任彼此，创建出共识基础来进行安全的信息交互；
- PBFT的出现大幅推动了分布式领域的共识算法研究。如今区块链的不少共识算法在基础上进化而来。期待更多更好的共识算法的出现。

各种共识机制比较

应　用	zookeeper	edcd	bitcoin	eris	hyperledger
共识机制	Paxos	Raft	Pow	BFT	PBFT
一致性	强一致性	强一致性	弱一致性	弱一致性	弱一致性
网络组织	主从	主从	对等	对等	对等
数据库	适配	自身	LevelDB	LevelDB	RockDB
允许失败节点数	< 1/2	< 1/2	< 1/3	< 1/3	< 1/3
恶意节点	不允许	不允许	允许	允许	允许
虚拟机	无	无	无	有	有
需要代币	无	无	有	有	无

知识点

- 区块链是个无法篡改的超级账本？
- 区块链是个去中心化的交易系统？
- 区块链是构建数字货币的底层工具？
- 区块链构建完备智能合约体系?
- 区块链+智能合约=？
- 区块链是解决了拜占庭将军问题的分布式网络，在完全开放的环境中，实现了数据的一致性和安全性；
- 区块链解决的根本问题是信任，相信非拜占庭将军的人数多，相信大多数非拜占庭将军的决定；
- 区块链的比特币系统，它是分布式系统技术与数字经济应用相结合造就的一次成功的创举，是好莱坞预言再一次被实现。