第二章、区块链技术原理

何德彪

武汉大学

国家网络安全学院

目　录

目　录

2.0 引言

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，乱象丛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。

2.0 引言

2.0.1. 国际区块链技术发展现状

美国、英国、俄罗斯、澳大利亚、日本等国纷纷设计国家区块链战略和路线图，促进区块链产业发展.

国外巨头企业谷歌、微软、摩根大通、Facebook、亚马逊、IBM等纷纷布局研究区块链技术，推出了技术解决方案和应用.

以太坊基金会、Hyperledger社区等不断在创新区块链技术，有力促进了区块链技术的迭代发展.

全球区块链迎来了爆发式发展，在金融服务、供应链管理、智能制造、社会公益、医疗健康等领域开展了一系列应用.

美国知名高校包括哈佛、斯坦福等均已开设区块链相关课程，在共识算法、密码学等关键技术方面处于领先水平.

2.0 引言

2.0.2. 中国区块链技术发展现状

2.0 引言

2.0.2. 中国区块链技术发展现状

政府全面布局创新

截止2019年1月，北京、广东、浙江等全国**超过26个省市地区**发布区块链相关政策，福建、云南、重庆、福州等省市将发展区块链技术与产业写入2019年政府工作报告中，**开展区块链产业链布局**

技术应用蓬勃发展

- 国内区块链企业初具规模，**互联网巨头提前布局**区块链
- 我国已具备核心技术的区块链底层平台
- **区块链标准研制**已走在世界前列
- 区块链技术已经在银行、保险、供应链、电子票据等领域**得到了应用验证**

高校重视人才培养

- 北京、上海、深圳等地先后成立了一系列区块链**联盟**，促进区块链的发展
- 我国目前有**62家**区块链研究院，分布在15个城市
- 国内已有**10所**高校开展了区块链课程

目　录

2.1 区块链的概念

工信部指导发布的《区块链技术和应用发展白皮书 2016》的 解释是：

狭义来讲，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。

广义来讲，区块链技术是利用块链式数据结构来验证和存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全性、利用由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。

专业的解释或许有些拗口。顾名思义，区块链（blockchain）是一种数据以区块（block）为单位产生和存储，并按照时间顺序首尾相连形成链式（chain）结构，同时通过密码学保证不可篡改、不可伪造及数据传输访问安全的去中心化分布式账本。区块链中所谓的账本，其作用

2.1 区块链的概念

和现实生活中的账本基本一致，按照一定的格式记录流水等交易信息。特别是在各种数字货币中，交易内容就是各种转账信息。只是随着区块链的发展，记录的交易内容由各种转账记录扩展至各个领域的数据。比如，在供应链溯源应用中，区块中记录了供应链各个环节中物品所处的责任方、位置等信息。

要探寻区块链的本质，什么是区块、什么是链，首先需要了解区块链的数据结构，即这些交易以怎样的结构保存在账本中。

2.1 区块链的概念

区块链形式

数据以交易单的形式存在

交易单记录一笔交易的具体信息，例如付款人比特币地址、收款人比特币地址、付款金额、付款人签名等

许多交易单组成了数据块，每个数据块只记录区块链全世界对应时间内的交易信息

将数据块有序联起来的链表.例如比特币全世界只有唯一一条公共数据链Blockchain

2.1 区块链的概念

数据项	描述	字段长度
Magic no	常数 0xD9B4BEF9	4字节
Blocksize	区块的大小	4字节
Blockheader	区块头	80字节
Transaction counter	区块所包含的交易数量	1~9个节
Transaction	交易列表	Multiple Transaction

数据块

数据项 描述 更新时间 大小

Latest Blocks

Height	Age	Transactions	Mined by	Size
428393	5 minutes ago	2100	AntMiner	998076
428392	14 minutes ago	1445	AntMiner	998096
428391	15 minutes ago	2115	BTCC Pool	998239
428390	36 minutes ago	2139		998157
428389	an hour ago	1942		998169

See all blocks

B 目标	uint32_t
Non	uint32_t

所有的交易过程，包括交易金额、交易金额来源、交易金额去向等细节都以交易单的形式被记录在世界上唯一的数据块

2.1 区块链的概念

区块产生方式

工作量证明（POW）

权益证明（POS）

区块链的数据块中有一个关键的数据项——随机数Nonce这串数字是一个答案且对于每个区块是唯一的；有三大功能：

- ✓ 这个答案很难获得
- ✓ 有效答案有很多，但只需要找到一个答案即可
- ✓ 其他节点对答案的验证很容易

因为问题很难解答，没固定算法，所以唯一方法是不断尝试，寻找这个答案的过程就叫作“挖矿”

挖矿=hash puzzles:

H(Nonce||prev_block||tx||tx||...||tx)

在区块链中的“挖矿”：

一个符合要求的Block Hash由N个前导零构成，零的个数取决于网络的难度值.要得到合理的Block Hash需要经过大量尝试计算，计算时间取决于机器的哈希运算速度.

工作量证明其实是一种算力

应用：

- ✓ 比特币区块链
- ✓ 以太坊区块链

2.1 区块链的概念

区块产生方式

工作量证明（POW）

权益证明（POS）

POS不同于POW之处在于，在POS系统上“挖矿”是以货币的持有数量为基础的.换句话说，在POS的情况下，一个人拥有虚拟货币的5%和在比特币系统上拥有系统5%的算力的效果是一样的.

应用：以太坊区块链

2.1 区块链的概念

交易过程

- 第1步：所有者A利用他的私钥对前一次交易（比特货来源）和下一位所有者B签署一个数字签名，并将这个签名附加在这枚货币的末尾，制作成交易单.

  要点：B以公钥作为接收方地址

- 第2步：A将交易单广播至全网，比特币就发送给了B，每个节点都将收到的交易信息纳入一个区块中.

  要点：对B而言，该枚比特币会即时显示在比特币钱包中，但直到区块确认成功后才可用.目前一笔比特币从支付到最终确认成功，得到6个区块确认之后才能真正确认到帐.

- 第3步：每个节点通过解一道数学难题，从而去获得创建新区块权利，并争取得到比特币的奖励（新比特币会在此过程中产生）

  要点：节点反复尝试寻找一个数值，使得将该数值、区块链中最后一个区块的Hash值以及交易单三部分送入SHA256算法后能计算出散列值X（256位）满足一定条件（比如前20位均为0），即找到数学难题的解.由此可见，答案并不唯一

2.1 区块链的概念

交易过程

- 第4步：当一个节点找到解时，它就向全网广播该区块记录的所有盖时间戳交易，并由全网其他节点核对.

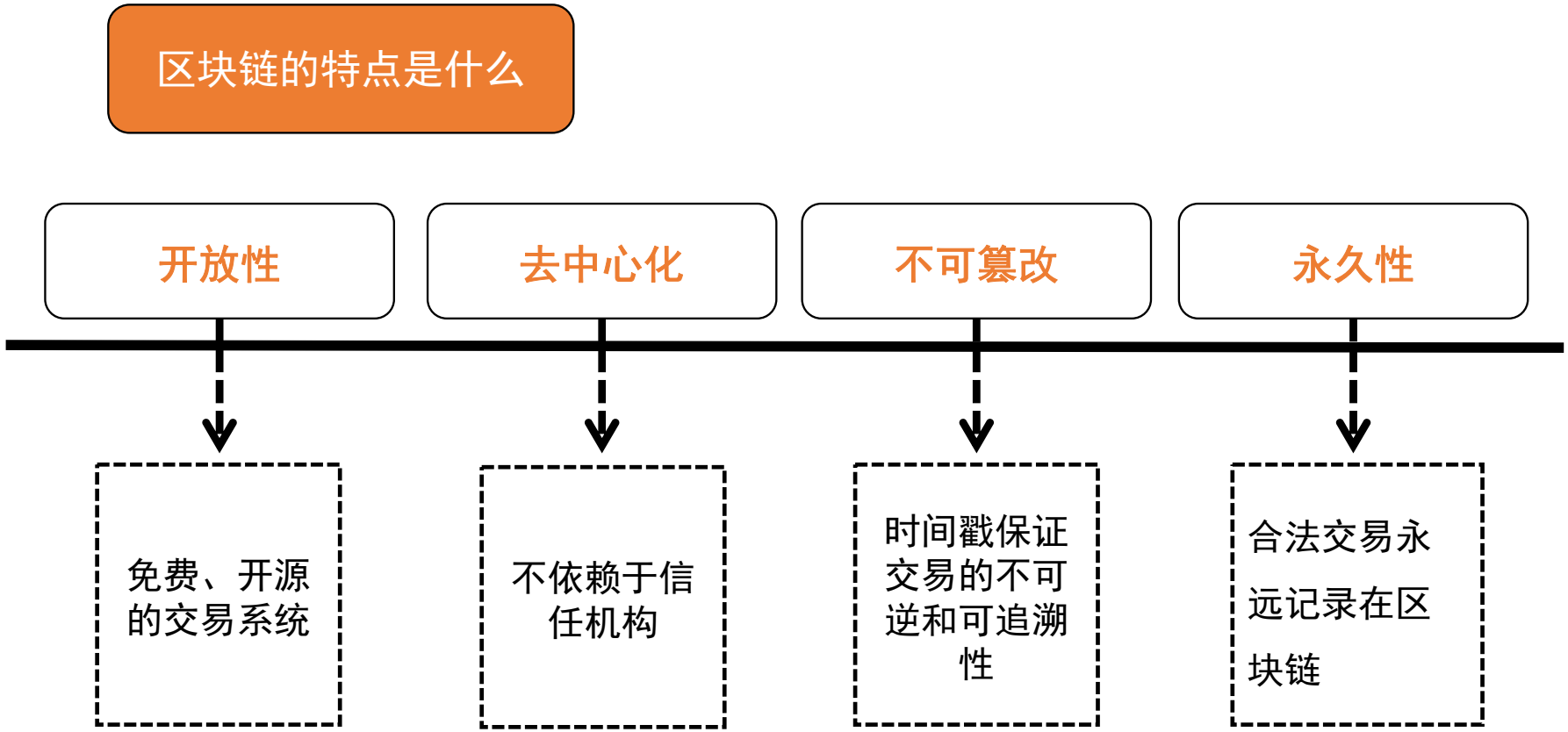
  要点：时间戳用来证实特定区块必然于某特定时间是的确存在的.比特币网络采取从5个以上节点获取时间，然后取中间值的方式作为时间戳.

- 第5步：全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链.

  要点：每个区块的创建时间大约在10分钟.随着全网算力的不断变化，每个区块的产生时间会随算力增强而缩短、随算力减弱而延长.其原理是根据最近产生的2016年区块的时间差（约两周时间），自动调整每个区块的生成难度（比如减少或增加目标值中0的个数），使得每个区块的生成时间是10分钟.

目　录

2.2 区块链的特点


区块链的特点是什么
开放性
去中心化
不可篡改
永久性
免费、开源的交易系统
不依赖于信任机构
时间戳保证交易的不可逆和可追溯性
合法交易永远记录在区块链

2.2 区块链的特点

区块链的特点是什么

自治的—透明：系统节点对等，自由加入和离开；去中心化，无管理机构或第三方仲裁

Autonomous

Distribute

分布式的—共享：只需要连接到最近的节点就可以获取所需要的所有信息

可追溯的—公开：系统的每个节点都有所有附带时间戳的完整拷贝，数据不可篡改

Trackable

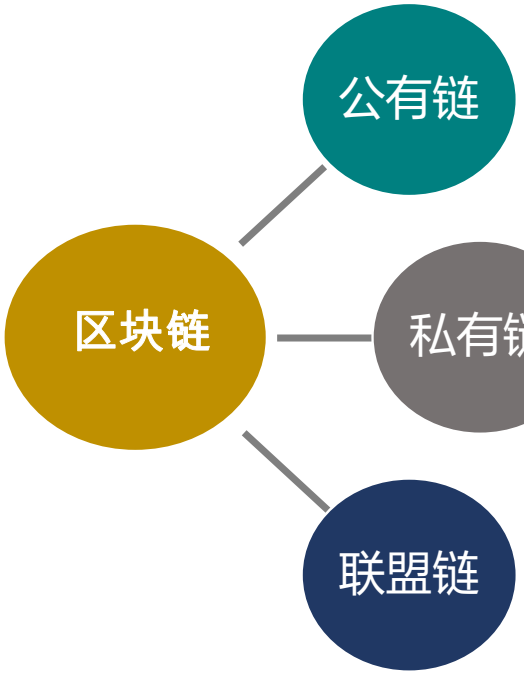
Contractual

按合约执行的—公平：所有的节点都按照一个规则或合约行事并达到共识（智能合约）

互联网的四大特点是“公平、分享、公开、透明”

目　录

2.3 区块链的分类



- **任何节点都是向任何人开放**
- **任何人均可自由参与和退出**

公有区块链是一个完全去中心、去中介的一个自组织，在公有区块链上，不可能没有数字货币，否则无人为区块链工作.

——万向区块链 肖风

- **单机构享有使用权和控制权**
- **权力完全控制在一个组织中**

使用私有链的联盟或公司可以轻松的改变区块链的规则、恢复交易、修改余额信息等等.

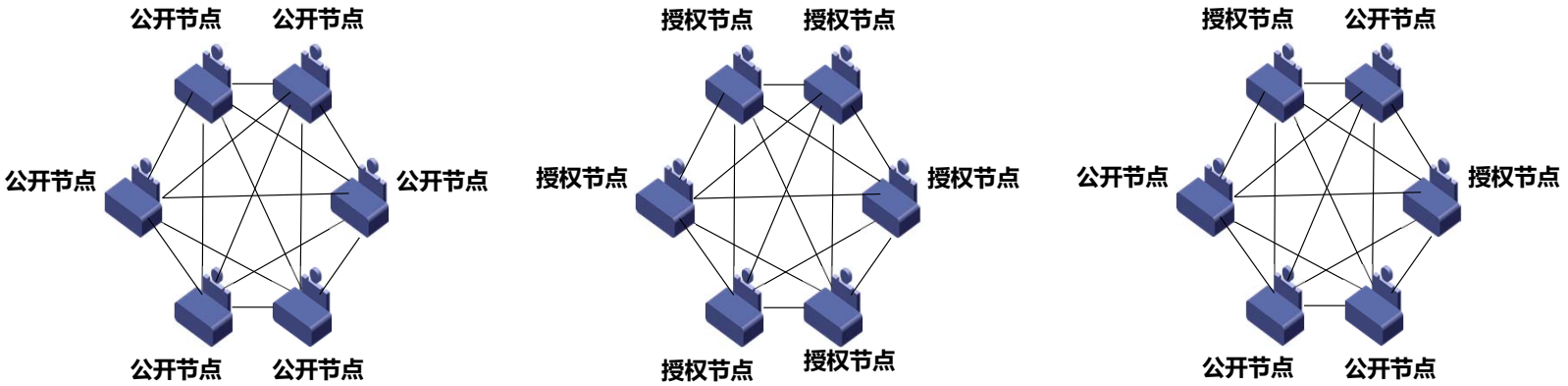
——以太坊创始人Vitalik Buterin

- **介于公有链和私有链之间**
- **加入和退出需经过联盟授权**

这几年区块链技术在私有链、联盟链的应用已经有初步的进展，但不是没有中心的，还是有中心的，只是分布式的.

—— 中行前行长 李林辉

2.3 区块链的分类



(a) 公有链　　(b) 私有链　　(c) 联盟链

图2.1. 公有链、私有链和联盟链结构示意图

2.3 区块链的分类

公链VS私链

优点

优点1：保护用户免受开发者的影响
优点2：公开区块链是开放的，可以应用于多个领域以及产生一定的网络影响.

优点1：较强的灵活性
优点2：私有链节点均已知，不存51%攻击风险.
优点3：交易成本更便宜.
优点4：节点之间可以很好地连接，故障可以迅速通过人工干预来修复，并允许使用共识算法减少区块时间，从而更快地完成交易
优点5：读取权限受到限制，这样私有区块链还可提供更好的隐私保护

缺点

1.在某些特定环境下，如需要保护数据隐私等完成公开则失去隐私.
2.公共区块交易费用较高，确认速度较慢等.
3.公有链的不可更改性降低了一定的灵活性.

1.丧失了一定的去中心化的特性

2.3 区块链的分类

	公有链	联盟链	私有链
参与者	任何人自由进出	联盟成员	个体或公司内部
共识机制	PoW/PoS/DPoS 等	分布式一致性算法	分布式一致性算法
记账人	所有参与者	联盟成员协商确定	自定义
激励机制	需要	可选	可选
中心化程度	去中心化	多中心化	(多)中心化
突出特点	信用的自建立	效率和成本优化	透明和可追溯
承载能力	3~20 笔/秒	1 000~1 万笔/秒	1 000~20 万笔/秒
典型场景	加密数字货币、存证	支付、清算、公益	审计、发行

图2.2. 公有链、私有链和联盟链的比较

目　录

2.4 区块链的基础技术

区块链作为一个诞生刚到十年的技术，的确算是一个新兴的概念，但是它所用到的基础技术全是当前非常成熟的技术。区块链的基础技术如哈希运算、数字签名、P2P 网络、共识算法以及智能合约等，在区块链兴起之前，很多技术已经在各种互联网应用中被广泛使用。但这并不意味着区块链就是一个新瓶装旧酒的东西。就好比积木游戏，虽然是一些简单有限的木块，但是组合过后，就能创造出一片新的世界。同时，区块链也并不是简单的重复使用现有技术，例如共识算法、隐私保护在区块链中已经有了很多的革新，智能合约也从一个简单的理念变成了一个现实。区块链“去中心化”或“多中心”这种颠覆性的设计思想，结合其数据不可篡改、透明、可追溯、合约自动执行等强大能力，足以掀起一股新的技术风暴。本小节主要探讨这些技术的原理及在区块链系统中的作用。

2.4 区块链的基础技术

2.4.1. 哈希函数

1. 什么是哈希运算

哈希算法(Hash Algorithm)即散列算法的直接音译。它的基本功能概括来说,就是把任意长度的输入(例如文本等信息)通过一定的计算,生成一个固定长度的字符串,输出的字符串称为该输入的哈希值。在此以常用的 SHA-256 算法分别对一个简短的句子和一段文字求哈希值来说明。

- 输入:This is a hash example!

  哈希值:f7f2cf0bcbfbc11a8ab6b6883b03c721407da5c9745d46a5fc53830d4749504a

2. 哈希运算的特性

一个优秀的哈希算法要具备正向快速、输入敏感、逆向困难、强抗碰撞等特征。

- 正向快速:正向即由输入计算输出的过程,对给定数据,可以在极短时间内快速得到哈希值。如当前常用的 SHA256 算法在普通计算机上一秒钟能做 2 000 万次哈希运算。

2.4 区块链的基础技术

2.4.1. 哈希函数

- 输入敏感：输入信息发生任何微小变化，哪怕仅仅是一个字符的更改，重新生成的哈希值与原哈希值也会有天壤之别。同时完全无法通过对比新旧哈希值的差异推测数据内容发生了什么变化。因此，通过哈希值可以很容易地验证两个文件内容是否相同。该特性广泛应用于错误校验。在网络传输中，发送方在发送数据的同时，发送该内容的哈希值。接收方收到数据后，只需要将数据再次进行哈希运算，对比输出与接收的哈希值，就可以判断数据是否损坏。

- 逆向困难：要求无法在较短时间内根据哈希值计算出原始输入信息。该特性是哈希算法安全性的基础，也因此是现代密码学的重要组成。哈希算法在密码学中的应用很多，此处仅以哈希密码举例进行说明。当前生活离不开各种账户和密码，但并不是每个人都有为每个账户单独设置密码的好习惯，为了记忆方便，很多人的多个账户均采用同一套密码。如果这些密码原封不动地保存在数据库中，一旦数据泄露，则该用

2.4 区块链的基础技术

2.4.1. 哈希函数

户所有其他账户的密码都可能暴露，造成极大风险。所以在后台数据库仅会保存密码的哈希值，每次登录时，计算用户输入的密码的哈希值，并将计算得到的哈希值与数据库中保存的哈希值进行比对。

- 强抗碰撞性：即不同的输入很难可以产生相同的哈希输出。当然，由于哈希算法输出位数是有限的，即哈希输出数量是有限的，而输入却是无限的，所以不存在永远不发生碰撞的哈希算法。但是哈希算法仍然被广泛使用，只要算法保证发生碰撞的概率够小，通过暴力枚举获取哈希值对应输入的概率就更小，代价也相应更大。只要能保证破解的代价足够大，那么破解就没有意义。就像我们购买双色球时，虽然我们可以通过购买所有组合保证一定中奖，但是付出的代价远大于收益。优秀的哈希算法即需要保证找到碰撞输入的代价远大于收益。

2.4 区块链的基础技术

2.4.1. 哈希函数

3. 通过哈希构建区块链的链式结构，实现防篡改

每个区块头包含了上一个区块数据的哈希值，这些哈希层层嵌套，最终将所有区块串联起来，形成区块链。区块链里包含了自该链诞生以来发生的所有交易，因此，要篡改一笔交易，意味着它之后的所有区块的父区块哈希全部要篡改一遍，这需要进行大量的运算。如果想要篡改数据，必须靠伪造交易链实现，即保证在正确的区块产生之前能快速地运算出伪造的区块。同时在以比特币为代表的区块链系统要求连续产生一定数量的区块之后，交易才会得到确认，即需要保证连续伪造多个区块。只要网络中节点足够多，连续伪造的区块运算速度都超过其他节点几乎是不可能实现的。另一种可行的篡改区块链的方式是，某一利益方拥有全网超过 50% 的算力，利用区块链中少数服从多数的特点，篡改历史交易。然而在区块链网络中，只要有足够多的节点参与，控制网络中 50% 的算力也是不可能做到的。即使某一利益方拥有了全网超过 50% 的算力，那已经是既得利益者，肯定会更坚定地维护区块链网络的稳定性。

2.4 区块链的基础技术

2.4.1. 哈希函数

4. 通过哈希构建默克尔树，实现内容改变的快速检测

除上述防篡改特性，基于哈希算法组装出的默克尔树也在区块链中发挥了重要作用。默克尔树本质上是一种哈希树，1979 年瑞夫·默克尔申请了该专利，故此得名。前面已经介绍了哈希算法，在区块链中默克尔树就是当前区块所有交易信息的一个哈希值。但是这个哈希值并不是直接将所有交易内容计算得到的哈希，而是一个哈希二叉树。首先对每笔交易计算哈希值；然后进行两两分组，对这两个哈希值再计算得到一个新的哈希值，两个旧的哈希值就作为新哈希值的叶子节点，如果哈希值数量为单数，则对最后一哈希值再次计算哈希值即可；然后重复上述计算，直至最后只剩一个哈希值，作为默克尔树的根，最终形成一个二叉树的结构。

在区块链中，我们只需要保留对自己有用的交易信息，删除或者在其他设备备份其余交易信息。如果需要验证交易内容，只需验证默克尔树即可。若根哈希验证不通过，则验证两个叶子节点，再验证其中哈希验证不通过的节点的叶子节点，最终可以准确识别被篡改的交易。

2.4 区块链的基础技术

2.4.1. 哈希函数

5. 其它应用？？（大家想一下）

- **POW**挖矿的数学难题；
- 交易的数字签名；

2.4 区块链的基础技术

2.4.2. 数字签名

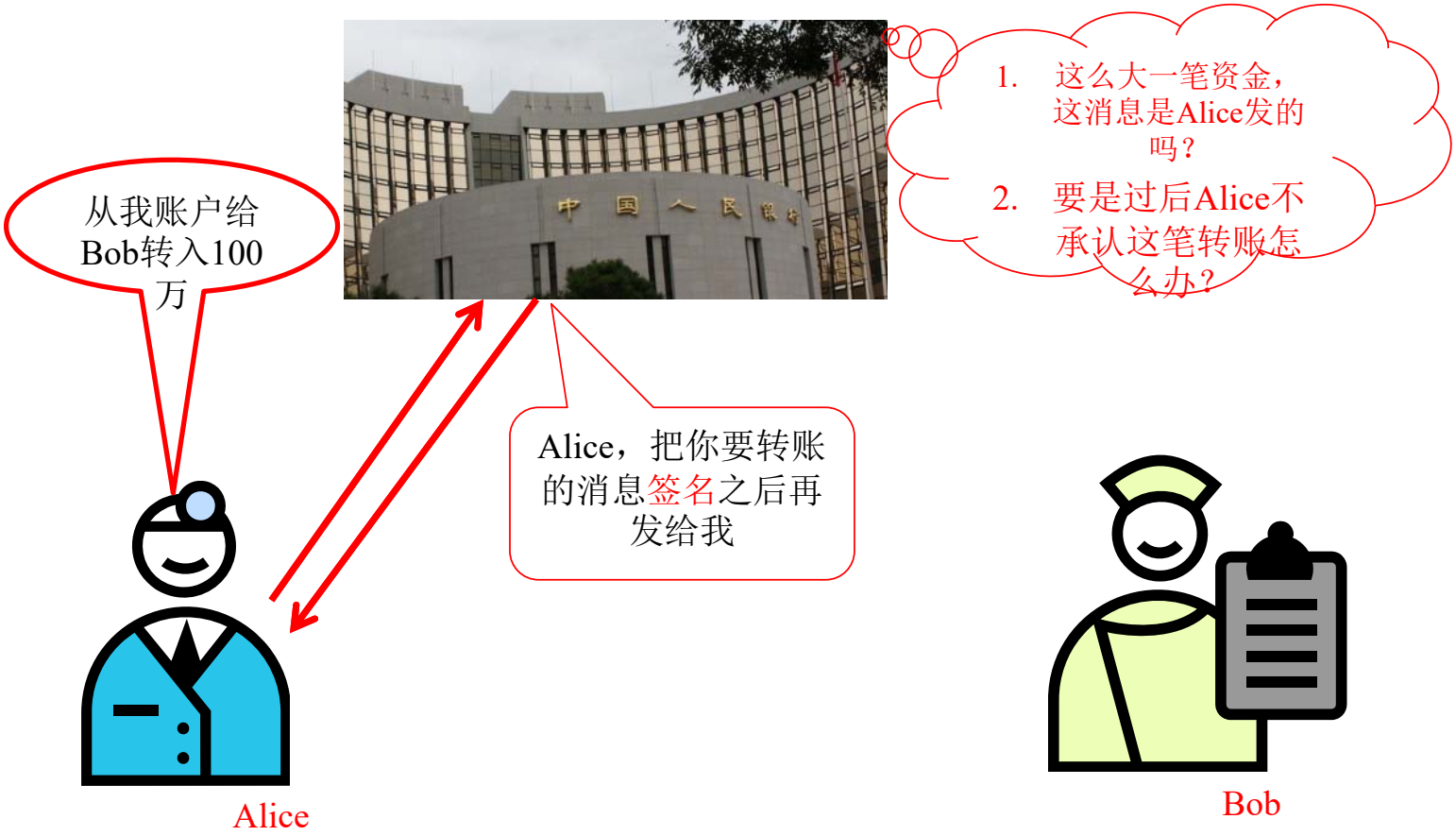
问题的提出

- 手写签名:传统的确认方式，如书信、签约、支付、批复等
- 在网络时代，人们通过网络支付费用、买卖股票，为了保证网上商务活动的安全，需要一个很重要的安全机制——数字签名

图2.3. 传统合同示意图

2.4 区块链的基础技术

2.4.2. 数字签名



2.4 区块链的基础技术

2.4.2. 数字签名

- 数字签名是手写签名数字化的产物，但又有着显著的区
  - **不同消息的签名不同**，甚至相同消息也有不同的签名，否则签名就会被获取并复制到另外的文件中；
  - 数字签名的基础是公钥密码学；

2.4 区块链的基础技术

2.4.2. 数字签名

数字签名的目的和要求

- **数字签名的目的：**保证信息的**完整性和真实性**，即消息没有被篡改，而且签名也没有被篡改，消息只能始发于所声称的一方
- 一个完善的签名方案应满足以下三个条件：
  - ① **不可伪造性：**其他任何人均不能伪造签名，也不能对接收或发送的信息进行篡改、伪造和冒充
  - ② **不可否认性：**签名者事后不能否认或抵赖自己的签名
  - ③ **公正的仲裁：**若当事双方对签名真伪发生争执时，能通过公正的仲裁者验证签名来确定其真伪

2.4 区块链的基础技术

2.4.2. 数字签名

数字签名的过程

➢数字签名方案一般包括三个过程：

① 系统初始化过程：产生数字签名方案中的所有系统和用户参数(公开的+秘密的)

② 签名过程：用户利用给定的签名算法对消息签名，签名过程可以公开也可以不公开，但一定包含仅签名者才拥有的秘密信息（签名密钥）

③ 验证过程：验证者利用公开的验证方法对给定消息的签名进行验证

2.4 区块链的基础技术

2.4.2. 数字签名

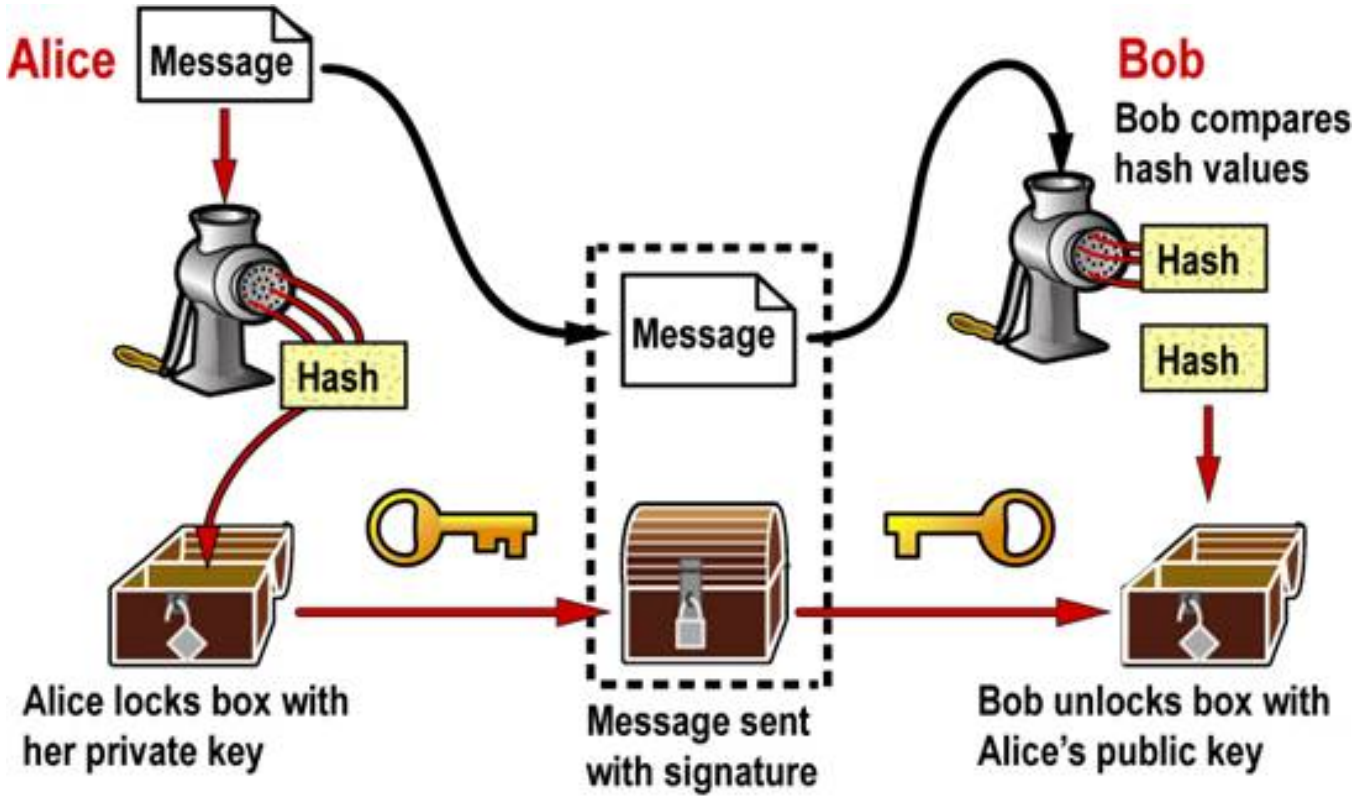


图2.4. 数字签名工作流程示意图

2.4 区块链的基础技术

2.4.2. 数字签名

- 经典的数字签名算法
  - ① RSA数字签名
  - ② DSA数字签名
  - ③ ECDSA数字签名
  - ④ SM2数字签名
  - ⑤ ……
- 其它数字签名算法
  - ① 盲签名
  - ② 群签名
  - ③ 环签名
  - ④ ……

2.4 区块链的基础技术

2.4.3. 共识算法

1. 为什么要共识？

区块链通过全民记账来解决信任问题，但是所有节点都参与记录数据，那么最终以谁的记录为准？或者说，怎么保证所有节点最终都记录一份相同的正确数据，即达成共识？在传统的中心化系统中，因为有权威的中心节点背书，因此可以以中心节点记录的数据为准，其他节点仅简单复制中心节点的数据即可，很容易达成共识。然而在区块链这样的去中心化系统中，并不存在中心权威节点，所有节点对等地参与到共识过程之中。由于参与的各个节点的自身状态和所处网络环境不尽相同，而交易信息的传递又需要时间，并且消息传递本身不可靠，因此，每个节点接收到的需要记录的交易内容和顺序也难以保持一致。更不用说，由于区块链中参与的节点的身份难以控制，还可能会出现恶意节点故意阻碍消息传递或者发送不一致的信息给不同节点，以干扰整个区块链系统的记账一致性，从而从中获利的情况。因此，区块链系统的记账一致性问题，或者说共识问题，是一个十分关键的问题，它关系着整个区块链系统的正确性和安全性。

2.4 区块链的基础技术

2.4.3. 共识算法

2. 有哪些共识算法?

当前区块链系统的共识算法有许多种,主要可以归类为如下四大类:(1)工作量证明(Proof of Work,PoW)类的共识算法;(2)Po * 的凭证类共识算法;(3)拜占庭容错(Byzantine Fault Tolerance,BFT)类算法;(4)结合可信执行环境的共识算法。接下来本节将分别对这四类算法进行简要的介绍。

- PoW 类的共识算法

PoW 类的共识算法主要包括区块链鼻祖比特币所采用的 PoW 共识及一些类似项目(如莱特币等)的变种 PoW,即为大家所熟知的"挖矿"类算法。这类共识算法的核心思想实际是所有节点竞争记账权,而对于每一批次的记账(或者说,挖出一个区块)都赋予一个"难题",要求只有能够解出这个难题的节点挖出的区块才是有效的。同时,所有节点都不断地通过试图解决难题来产生自己的区块并将自己的区块追加在现有的区块链之后,但全网络中只有最长的链才被认为是合法且正确的。

2.4 区块链的基础技术

2.4.3. 共识算法-PoW

- 比特币系统设计了以每个节点的计算能力即“算力”来竞争记账权的机制.在比特币系统中，大约每10分钟进行一轮算力竞赛，竞赛的胜利者，就获得一次记账的权力，并向其他节点同步新增账本信息.
- 在一个去中心化的系统中，谁有权判定竞争的结果呢?比特币系统是通过一个称为“工作量证明”(Proof of Work, PoW)的机制完成的.
- 简单地说，PoW就是一份确认工作端做过一定量 工作的证明.PoW系统的主要特征是计算的不对称性.工作端需要做一定难度的工作得出一个结果，验证方却很容易通过结果来检查工作端是不是做了相应的工作.

2.4 区块链的基础技术

2.4.3. 共识算法-PoW

- 举个例子，给定字符串“bockchain”,我们给出的工作量要求是，可以在这个字符串后面连接一个称为nonce的整数值串，对连接后的字符串进行SHA256哈希运算，如果得到的哈希结果(以十六进制的形式表示)是以若干个0开头的，则验证通过，为了达到这个工作量证明的目标，我们需要不停地递增nonce值，对得到的新字符串进行SHA256哈希运算.
- 有没有其它的难题？

2.4 区块链的基础技术

2.4.3. 共识算法-PoW

- PoW背后的基本概念很简单:工程端提交已知难于计算但易于验证的计算结果，而其他任何人都能通过验证这个答案就确信工作端为了求的结果已经完成了量相当大的计算工作. **但PoW机制存在明显的弊端**.
- 一方面，PoW的前提是节点和算力是均匀分布的，但随着人们将CPU挖矿逐渐升级到GPU，FPGA，ASIC矿机挖矿，算力越来越集中.
- 另一方面， PoW太浪费资源了.比特币网络每秒可完成数百万亿次SHA256计算，但这些计算除了使恶意攻击者不能轻易地伪装成几百万个节点和打垮比特币网络，并没有任何实际或科学价值.

2.4 区块链的基础技术

2.4.3. 共识算法-Po*

- 有鉴于此，人们引入“凭证”的概念，提出Po*类算法，其中*表示算法使用凭证的类比，权益证明(Proof of Stake, PoS)就是其中的一种方法.
- **权益证明要求用户证明拥有某些数量的货币(即对货币的权益),**点点币(Peercoin)是首先采用权益证明的货币，尽管它依然使用工作量证明挖矿.
- 点点币在SHA256的哈希运算的难度方面引入了币龄的概念，**使得难度与交易输入的币龄成反比**.在点点币中，币龄被定义为**币的数量与币所拥有的天数的乘积**，使得币龄能够反映交易时刻用户所拥有的货币数量.

2.4 区块链的基础技术

2.4.3. 共识算法-Po*

- 点点币的权益证明机制结合了随机化与币龄的概念，未使用至少30天的币可以参与竞争下一区块，越久和越大的币集有更大的可能去签名下一区块.（币一直不使用，币龄越来越大？？）
  - ① 一旦币的权益被用于签名一个区块，则币龄将清为零，这样必须等待至少30日才能签署另一区块.
  - ② 为防止非常老或非常大的权益控制区块链，寻找下一区块的概率在90天后达到最大值.
- 其它算法：Algorand、Quroboros等都是目前热门的PoS类共识算法.
- Po*类算法缺点
  - ① 提高了算法的中心化程度，违背了区块链“去中心化”的思想
  - ② 旷工激励不够明确，节点缺乏参与动力

2.4 区块链的基础技术

2.4.3. 共识算法-BFT类算法

无论是 PoW 类算法还是 Po * 类算法，其中心思想都是将所有节点视作竞争对手，每个节点都需要进行一些计算或提供一些凭证来竞争出块的权利（以获取相应的出块好处）。BFT 类算法则采取了不同的思路，它希望所有节点协同工作，通过协商的方式来产生能被所有（诚实）节点认可的区块。

拜占庭容错问题最早由 Leslie Lamport 等学者于 1982 年在论文 *The Byzantine Generals Problem* 中正式提出，主要描述分布式网络节点通信的容错问题。从 20 世纪 80 年代起，提出了很多解决该问题的算法，这类算法被统称为 BFT 算法。实用拜占庭容错（Practical BFT，PBFT）算法是最经典的 BFT 算法，由 Miguel Castro 和 Barbara Liskov 于 1999 年提出。PBFT 算法解决了之前 BFT 算法容错率较低的问题，且降低了算法复杂度，使 BFT 算法可以实际应用于分布式系统。

2.4 区块链的基础技术

2.4.3. 共识算法-BFT类算法

拜占庭问题起源

拜占廷帝国(即东罗马帝国)国土辽阔，军队之间分隔很远，军队之间只能靠信差传消息.然而，当发生战争时，必须所有的拜占庭军队达成一致共识，才能决定是否去攻打敌人，任意部分军队攻打敌军，都无法取胜.如果军队中出现叛徒或间谍，左右各军队将军的决定，达成的共识可能不代表大多数人意见.这时，在已知有间谍的情况下，其余忠诚的将军在不受叛徒的影响下如何达成一致的协议，就是“拜占庭将军问题”.

2.4 区块链的基础技术

2.4.3. 共识算法-BFT类算法

拜占庭问题

拜占庭问题是一个协议问题，拜占庭军队必须全体一致决定是否攻击敌军.问题是：

1．军队之间分割远，无法同时一起商议，只能通过信使.

2．信使或将军有可能存在叛徒，干扰共识过程.

叛徒可以任意行动达到以下目标：

1．迷惑部分将军，使他们无法做出决定.

2．欺骗将军，采取相反决定，如将军们不希望进攻，但叛徒促成进攻行动.

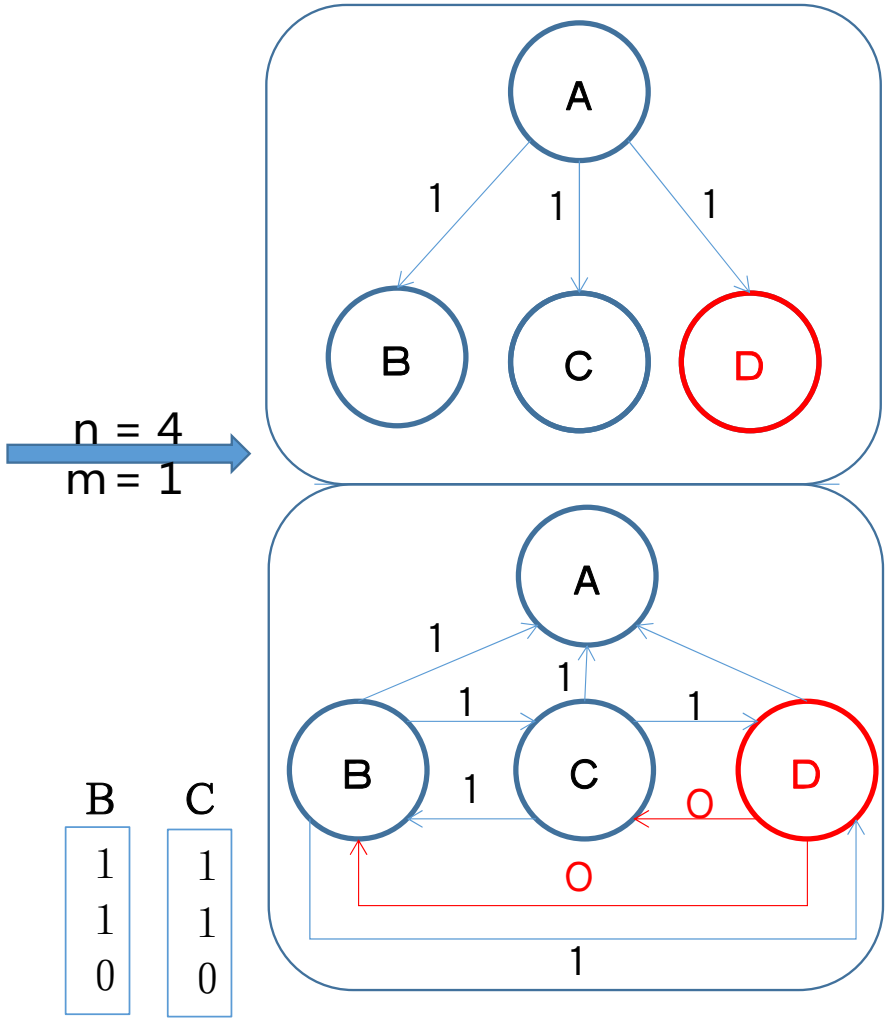
叛徒只要完成任意目标，都代表攻击行动的结果失败.

2.4 区块链的基础技术

2.4.3. 共识算法-BFT类算法

拜占庭解决

Lamport 证明了在将军总数 n 大于3m ， 背叛者为m 或者更少时，忠诚的将军可以达成命令上的一致.



2.4 区块链的基础技术

2.4.3. 共识算法-BFT类算法

BFT 类算法一般都有完备的安全性证明，能在算法流程上保证在群体中恶意节点数量不超过三分之一时，诚实节点的账本保持一致。然而，这类算法的协商轮次也很多，协商的通信开销也比较大，导致这类算法普遍不适用于节点数目较大的系统。业界普遍认为，BFT 算法所能承受的最大节点数目不超过 100。

- BFT类共识算法能否用于比特币等公链项目？

2.4 区块链的基础技术

2.4.3. 共识算法-结合可信执行环境的公示算法

- 可信计算是在计算和通信系统中广泛使用基于硬件安全模块支持下的可信计算平台，以提高系统整体的安全性.
- 早期可信计算的研究主要以国际可信计算工作组TCG (Trusted Computing Group)为主.可信计算最核心的就是TPM硬件芯片，其TPM (Trusted Platform Module) 1.2规范是比较经典的，大多数厂家的芯片都以TPM 1.2为标准，该规范已经升级到TPM 2.0.
- 国内对应的是TCM(Trusted Computing Module)芯片，可以参考“可信计算密码支撑平台功能与接口规范”，而且已经成为国家标准，即GB/T 29829-2013.

2.4 区块链的基础技术

2.4.3. 共识算法-结合可信执行环境的共识算法

- 随着可信计算的发展，可信平台模块不一定再是硬件芯片的形式，特别是在资源比较受限的移动和嵌入式环境中，**可信执行环境（TEE，Trusted Execution Environment）**的研究比较热，如基于ARM TrustZone、智能卡等可以实现可信计算环境；

- 2013年, Intel推出SGX(Software Guard Extensions)指令集扩展，旨在以硬件安全为强制性保障,不依赖于固件和软件的安全状态，提供用户空间的可信执行环境，通过一组新的指令集扩展与访问控制机制，**实现不同程序间的隔离运行**，保障用户关键代码和数据的机密性与完整性不受恶意软件的破坏.具体介绍参考：

https://blog.csdn.net/kouryoushine/article/details/89966837

2.4 区块链的基础技术

2.4.3. 共识算法-结合可信执行环境的共识算法

可信执行环境是一类能够保证在该类环境中执行的操作绝对安全可信、无法被外界干预修改的运行环境，它与设备上的普通操作系统（Rich OS）并存，并且能给 Rich OS 提供安全服务。可信执行环境所能够访问的软硬件资源是与 Rich OS 完全分离的，从而保证了可信执行环境的安全性。

利用可信执行环境，可以对区块链系统中参与共识的节点进行限制，很大程度上可以消除恶意节点的不规范或恶意操作，从而能够减少共识算法在设计时需要考虑的异常场景，一般来说能够大幅提升共识算法的性能。

- 结合可信执行环境的共识算法能否用于比特币等公链项目？

2.4 区块链的基础技术

2.4.4. 智能合约

1. 智能合约是什么？

其实，智能合约并不是区块链独有的概念。早在 1995 年，跨领域学者 Nick Szabo 就提出了智能合约的概念，他对智能合约的定义为："一个智能合约是一套以数字形式定义的承诺，包括合约参与方可以在上面执行这些承诺的协议。"简单来说，智能合约是一种在满足一定条件时，就自动执行的计算机程序。例如自动售货机，就可以视为一个智能合约系统。客户需要选择商品，并完成支付，这两个条件都满足后售货机就会自动吐出货物。

合约在生活中处处可见：租赁合同、借条等。传统合约依靠法律进行背书，当产生违约及纠纷时，往往需要借助法院等政府机构的力量进行裁决。智能合约，不仅仅是将传统的合约电子化，它的真正意义在革命性地将传统合约的背书执行由法律替换成了代码。俗话说，"规则是死的，人是活的"，程序作为一种运行在计算机上的规则，同样是"死的"。但是"死的"也不总是贬义词，因为它意味着会严格执行。

- 严格执行有什么价值？传统环境能否实现？

2.4 区块链的基础技术

2.4.4. 智能合约

2. 为什么区块链的出现使智能合约受到了广泛的关注?

尽管智能合约这个如此前卫的理念早在 1995 年就被提出,但是一直没有引起广泛的关注。虽然这个理念很美好,但是缺少一个良好的运行智能合约的平台,确保智能合约一定会被执行,执行的逻辑没有被中途修改。区块链这种去中心化、防篡改的平台,完美地解决了这些问题。智能合约一旦在区块链上部署,所有参与节点都会严格按照既定逻辑执行。基于区块链上大部分节点都是诚实的基本原则,如果某个节点修改了智能合约逻辑,那么执行结果就无法通过其他节点的校验而不会被承认,即修改无效。

3. 智能合约的原理

一个基于区块链的智能合约需要包括事务处理机制、数据存储机制以及完备的状态机,用于接收和处理各种条件。并且事务的触发、处理及数据保存都必须在链上进行。当满足触发条件后,智能合约即会根据预设逻辑,读取相应数据并进行计算,最后将计算结果永久保存在链式结构中。

2.4 区块链的基础技术

2.4.4. 智能合约

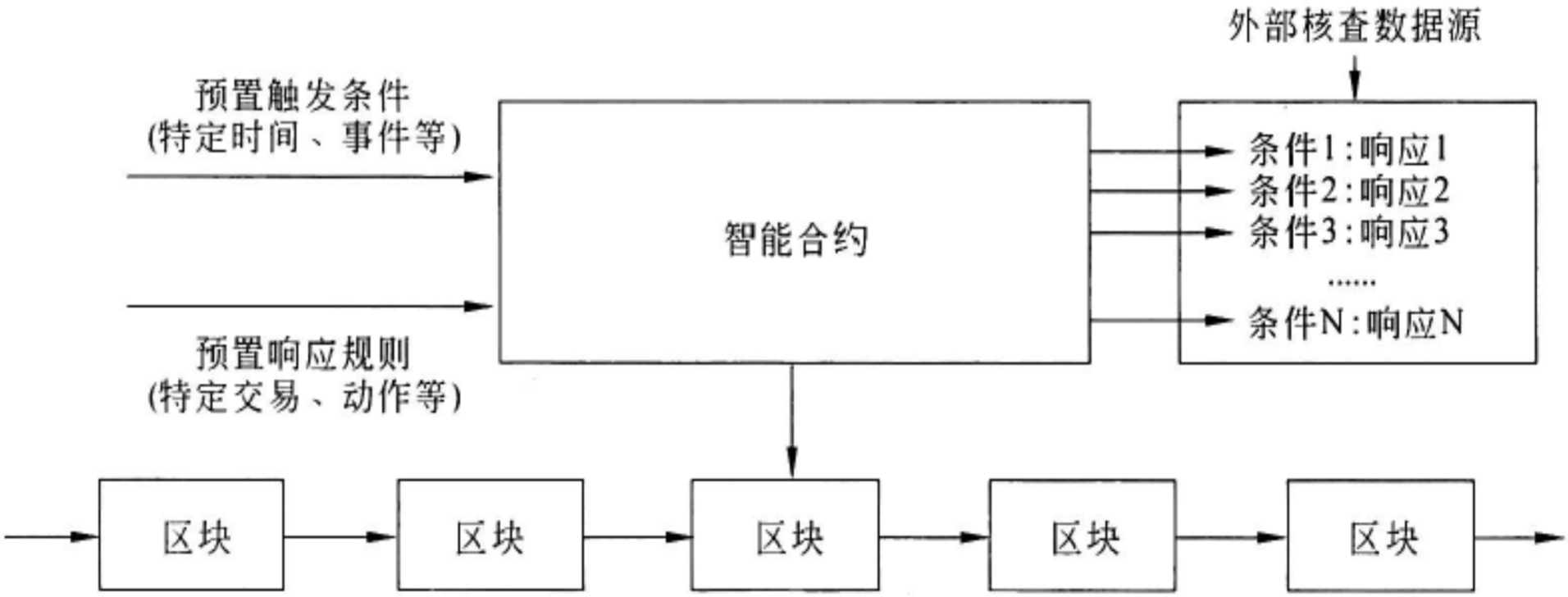


图2.5. 智能合约在区块链中的运行逻辑

2.4 区块链的基础技术

2.4.4. 智能合约

图2.6. 传统合约与智能合约的比较

链接：https://www.sohu.com/a/328796235_100217376

2.4 区块链的基础技术

2.4.4. 智能合约

详情见：智能合约安全事故回顾分析
https://www.cnblogs.com/gzhlt/p/10218447.html

4. 智能合约的安全性需要关注

因为合约是严肃的事情，传统的合约往往需要专业的律师团队来撰写。古语有云："术业有专攻。"当前智能合约的开发工作主要由软件从业者来完成，其所编写的智能合约在完备性上可能有所欠缺，因此相比传统合约，更容易产生逻辑上的漏洞。另外，由于现有的部分支持智能合约的区块链平台提供了利用如 Go 语言、Java 语言等高级语言编写智能合约的功能，而这类高级语言不乏一些具有"不确定性"的指令，可能会造成执行智能合约节点的某些内部状态发生分歧，从而影响整体系统的一致性。

2016 年著名的 The DAO 事件，就是因为智能合约漏洞导致大约几千万美元的直接损失。The DAO 是当时以太坊平台最大的众筹项目，上线不到一个月就筹集了超过 1 000 万个以太币，当时价值一亿多美元。但是该智能合约的转账函数存在漏洞，攻击者利用该漏洞，盗取了 360 万个以太币。由于此事件影响过大，以太坊最后选择进行回滚硬分叉挽回损失。

2.4 区块链的基础技术

2.4.4. 智能合约

预防策略：

1. 充分测试

① 测试用例设计：对业务进行全方位分析，通过等价类划分法、边界值分析法、正交实验法等方法设计出尽可能全面的测试用例，编写成测试代码，做自动化回归测试.

② 多人交叉测试：一个人的思维是局限的，我们需要通过多人的跳跃性思维，将尽可能多的情况覆盖在内.

③ 回归测试：每一次修改都必须做整套回归测试.

2.4 区块链的基础技术

2.4.4. 智能合约

预防策略：

2. 工具监控

以太坊的所有交易都是公开透明可查的.我们可以通过工具将某一个智能合约交易数据实时爬取出来，并对可能的异常交易做短信和邮件告警.这样我们能第一时间发现问题，并采取措施.

3. 第三方审计

可以找一些专业的智能合约开发工程师做审计.审计可以从另一个角度去发现智能合约可能存在的潜在问题.可能做审计的人的专业能力没有开发者的专业能力强大.

链接：**https://www.jianshu.com/p/b400ca9926a8**

2.4 区块链的基础技术

2.4.5. P2P网络

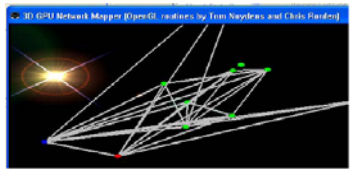
大家接触过P2P吗？

- 文件共享：

- 媒体播放：

- 数据存储：

- 分布计算：



2.4 区块链的基础技术

2.4.5. P2P网络

- P2P(Peer to Peer)：即对等网络，计算机之间通过直接交换来实现计算机资源和服务的共享.

- P2P网络环境中每个结点既充当服务器，为其他结点提供服务，同时也享用其他结点提供的服务，弱化了服务器的作用，甚至取消服务器.

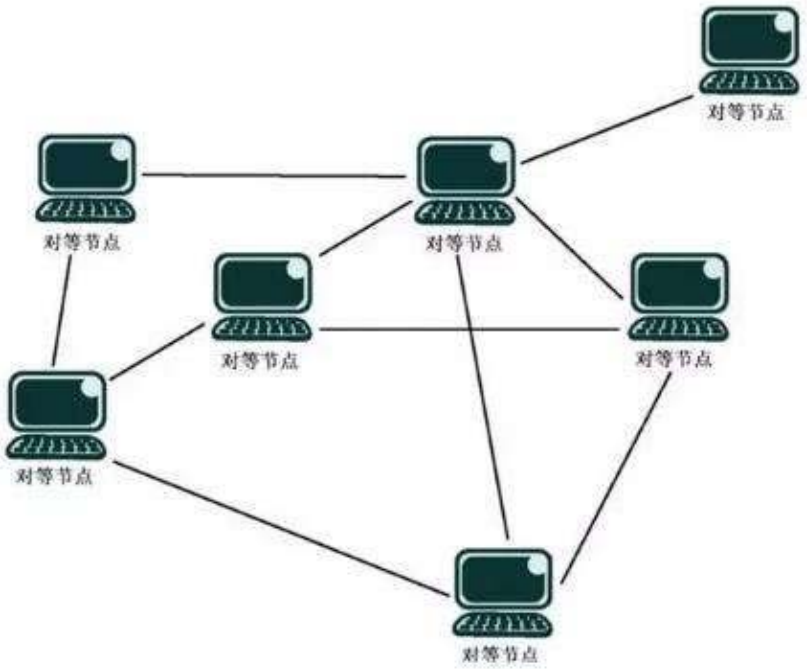
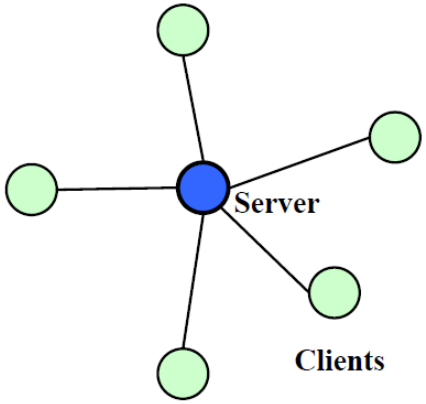


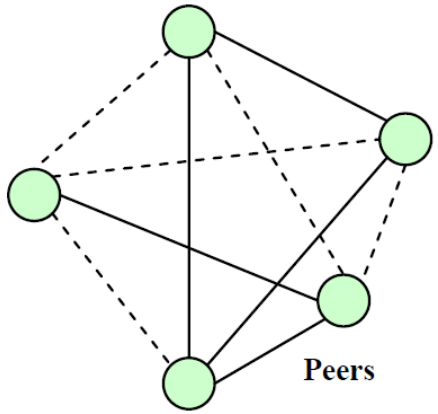
图2.7. P2P网络示意图

2.4 区块链的基础技术

2.4.5. P2P网络

C/S和P2P模式比较





自由
平等
互联

图2.8. C/S网络与P2P网络的比较

2.4 区块链的基础技术

2.4.5. P2P网络

C/S 模式的优点

- 信息存贮与管理比较集中规范.互联网上可以公开访问的信息基本上都保存在服务器上，信息的储存管理功能较为透明，用户提出访问请求后，无须再过问其他，服务器则根据一定的规则应答访问请求.
- 安全性较好.

2.4 区块链的基础技术

2.4.5. P2P网络

C / S模式的缺点

- 成本高：服务器投资大且维护成本高昂.
- 服务器及带宽决定了网络的性能：每台服务器的自身存储空间决定了所能提供的信息量，而且客户端访问数量过多，超过了服务器所能容纳的量，服务器会负荷过大而造成系统的瘫痪.
- 服务器容错性不高：一旦服务器出现问题，整个系统将会瘫痪.

2.4 区块链的基础技术

2.4.5. P2P网络

P2P模式下，没有提供信息的服务器和接受信息的客户端之分，每台电脑既是信息提供者又是索取者，结点之间通过直接互连实现信息资源的共享，而无需依赖集中式服务器的支持.它具有以下优点：

- 资源的高利用率：每一个结点可以贡献自己的资源，也可以利用网络上其他结点的信息资源，使闲散资源有机会得到利用.
- 无sever瓶颈：对等点越多，网络的性能越好.
- 负载均衡：对等网中由于资源分布在多个结点上，更好的实现了整个网络中数据流量和处理能力的负载均衡.
- 成本低：信息在网络设备间直接流动，高速及时，降低中转服务成本.

2.4 区块链的基础技术

2.4.5. P2P网络

- 中本聪在白皮书中提过，在电子现金系统中，第三方系统是多余的，没有价值，意思就是整个系统不要依赖任何特殊的第三方来完成自身系统的运转.
- 区块链系统之所以选择P2P作为其组网模型，就是因为两者的出发点都是去中心化，可以说具有高度的契合性.
- P2P网络的优势就是全网平等、无特殊节点，两者的思想高度契合，P2P技术也已发展成熟，所以对于区块链来说是一大利器.

目　录

2.5 区块链与密码货币的关系

2.5.1. “链”与“币”的关系

提起区块链，我们首先想到的就是加密货币，甚至很多人将区块链技术等同于比特币.实际上，二者不能混为一谈，它们有本质区别：

① 数字货币的概念是个很大的概念：它不仅包括区块链技术产生的数字货币，还包括了一切数字化的其它种类数字货币.比如我们即将看到的国家法定数字货币，就极可能使用区块链以外的其它技术.

② 区块链的概念也是很大的：数字货币只是区块链的一个成功应用场景，它的应用场景，不仅包括数字货币，而且包括诸如“产品溯源”“数字身份认证”"司法存证”等.

③ 很多区块链系统没有数字货币：区块链分为公链、私链和联盟链，只有公链有数字货币，私链和联盟链里面并没有数字货币.

2.5 区块链与密码货币的关系

2.5.1. “链”与“币”的关系

2013 年底，Vitalik Buterin 发表以太坊(Ethereum)白皮书，将“智能合约”的概念引入区块链技术中，这标志着区块链技术应用场景已不再局限于加密数字货币领域。智能合约使得区块链实现了图灵完备(Turing Complete)——可基于区块链开发适用于任何场景的应用程序。包含智能合约等技术的区块链被称为第二代区块链。目前区块链的应用场景已扩展至金融、供应链、政务服务、物联网、社交、共享经济等领域，由此可见，加密数字货币只是区块链的应用场景之一，区块链应用场景不仅局限于加密数字货币，二者属于包含关系。

公有链离开“币”的概念难以存活，这是由于公有链的开发、维护和节点的建设、运行，都需要社会大众的参与和付出，如果没有“币”作为激励，他们参加的动力从哪里来？另外，公有链对“币”的依赖也部分源自于其共识算法。通常，公有链共识算法的核心思想都是通过经济激励来鼓励节点对系统的贡献和付出，通过经济惩罚来阻止节点作恶，这种激励和惩罚的载体便是“币”。

2.5 区块链与密码货币的关系

2.5.1. “链”与“币”的关系

联盟链和私有链则与此完全不同。联盟链或私有链的参与节点的投资和收益都是较为特殊的，参与者希望从链上获得可信数据或共同完成某种业务，所以他们更有义务和责任去维护区块链系统的稳定运行。因此，PBFT 及其变种算法成为这种场景下的共识算法首选，这样，系统中一般也就不会出现“币”的概念。

资本市场对于加密数字货币的青睐为区块链的发展提供了资源和机会，而区块链的不断发展又为加密数字货币类应用提供了更加可靠的保障，这也加固了资本市场的投资信心，二者成了相辅相成的关系。

2.5 区块链与密码货币的关系

2.5.2. “链圈”与“币圈”的关系

虽然区块链和加密数字货币并不等同，但由于其关系密切，当大家谈论其中一个时，必然会提到另一个。有些人认为区块链技术更有价值，而有些人则热衷于投资加密数字货币，由此形成了两个不同的圈子，分别被称为“链圈”和“币圈”。

“链圈”的人关注区块链技术本身，包括大量企业创新人员、技术人员、非技术出身而对其感兴趣的人等人群，他们或研究算法以提高区块链的性能，或研究区块链的应用场景以加快其落地。对他们而言，加密数字货币只是区块链最原始的应用，区块链的潜力远不止于加密数字货币。“链圈”相信区块链技术是一场革命，能够重塑未来社会的生产关系。

“币圈”的人则主要关心加密货数字币的价值，并期望能够从中牟利。“币圈”的人包括一些投资人和投资机构，也包括一些对区块链技术丝毫不了解的投机散户。“币圈”的人也有两类，一类坚信区块链的价值，并愿意对一些币种进行长期投资，这些人可能也是“链圈”的人；另一类人并不关心区块链的长期价值，只想通过交易这些加密数字货币来获取利润。

2.5 区块链与密码货币的关系

2.5.2. “链圈”与“币圈”的关系

由于智能合约可以生成代币，所以任何人或机构都可以在一个支持智能合约的公有链（如以太坊）上面发行自己的代币。 机构也因此可以募集大量的比特币或以太币。这个过程非常类似于大公司上市时的首次公开募股 IPO，因此，这种融资方式被称为首次代币发行（Initial Coin Offering，ICO）。

传统的融资方式通常需要很严格的资质审批，门槛较高，而区块链技术使得融资门槛大幅度降低，小型机构也能够在全球范围内大量的融资。表面看起来这好像是传统金融业的进步，但实际上有时候会被一些人用来做非法集资。2017 年，ICO 出现了爆炸式增长，有许多 ICO 获得了非常高额的收益，这造成了巨大的泡沫，也使得区块链技术名声在一些不明内情的人心中变坏，很多人甚至直接将区块链与诈骗相关联。

2.5 区块链与密码货币的关系

2.5.2. “链圈”与“币圈”的关系

挖链网 首页 链视听 闪讯 挖链号 行情 活动 人物

挖链独家 | 新研究表明：2017年80%的ICO是诈骗案

麦麦 | 07-13 17:27 22824

挖链网7月13日报道 ICO曾被认为是未来的融资方式，然而目前看来，ICO充满了黑幕。近日，ICO咨询公司Statis Group最近的研究显示，2017年进行ICO中有超过80%被认定为骗局。该研究从ICO最初发行到交易成熟的进程，分析了2017年ICO运行的生命周期。

该研究表明，到目前为止，超80%的ICO项目被认定为骗局。分析师发现，4% ICO失败，3%“已经死了”。研究认为，ICO死亡是因为“未在交易所上市交易，并且从那个时间点开始，没有在Github上贡献代码三个月。”

根据该研究，2017年硬币和代币的总资金达到119亿美元。13.3亿美元（11%）的ICO资金用于诈骗，绝大多数用于三个大型骗局项目：Pincoin（6.6亿美元），Arisebank（6亿美元）和Savedroid（5000万美元），总计13.1亿美元。这表明虽然大量ICO是骗局，但与整个行业相比，他们获得的资金并不多。

本月早些时候，TechCrunch 发布了一份基于Coinopsy和DeadCoins数据的报告。该报告发现：截至2018年6月30日，已有超过一千个加密项目“死亡”。根据Coinopsy的名单，有247个“死亡”硬币，而DeadCoins列出了一个包含830个“死亡”项目的加密货币清单。

图2.9. 关于ICO的报到新闻

2.5 区块链与密码货币的关系

2.5.2. “链圈”与“币圈”的关系

“链圈”和“币圈”也并非泾渭分明。有许多“链圈”的人对某些加密数字货币的前景持看好态度，也会对其进行投资。而“币圈”的人为了识别出更好的项目，也会对区块链技术进行深入的研究。本书重点讲述区块链技术本身，对于加密数字货币的投资不作任何评述。可以预见的是，随着时间的推移，人们对于区块链和加密数字货币的理解不断加深，“链圈”与“币圈”之争也将慢慢消失。

谢谢！