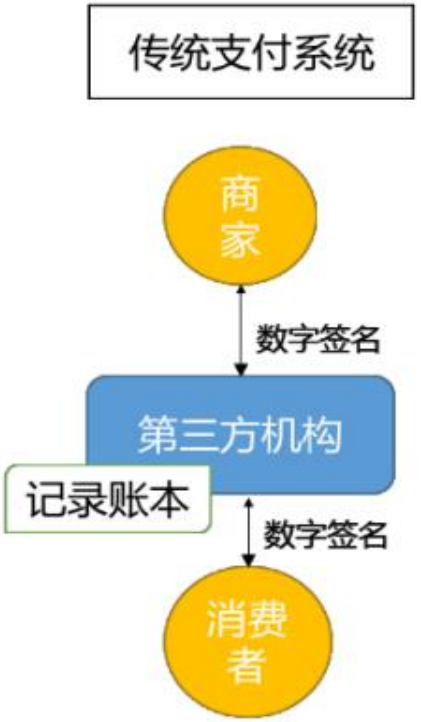
区块链技术原理详解

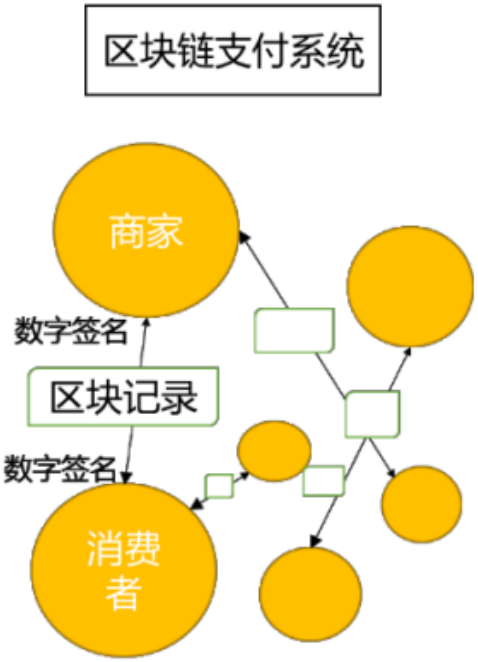
主讲 李少敏
微信&QQ：88977026

目录

背景

互联网上的贸易，几乎都需要借助可资信赖的第三方信用机构来处理电子支付信息。这类系统仍然内生性地受制于“基于信用的模式”。





区块链技术是构建比特币区块链网络与交易信息加密传输的基础技术。它基于密码学原理而不基于信用，使得任何达成一致的双方直接支付，从而不需要第三方中介的参与。

定义

区块链是一个分布式账本，一种通过去中心化、去信任的方式集体维护一个可靠数据库的技术方案。

从数据的角度来看

区块链是一种几乎不可能被更改的分布式数据库。这里的“分布式”不仅体现为数据的分布式存储，也体现为数据的分布式记录（即由系统参与者共同维护）。

从技术的角度来看

区块链并不是一种单一的技术，而是多种技术整合的结果。这些技术以新的结构组合在一起，形成了一种新的数据记录、存储和表达的方式。

动态

国际权威杂志《经济学人》、《哈佛商业周刊》、《福布斯杂志》等相继报道区块链技术将影响世界。

创业公司R3联合全球42家顶级银行成立区块链联盟，包括摩根大通、美国银行、汇丰银行、花旗银行、富国银行、三菱UFJ金融集团、巴克莱银行、高盛、德意志银行等。腾讯2017年4月发布区块链方案白皮书。

目录

特征

开放，共识

任何人都可以参与到区块链网络，每一台设备都能作为一个节点，每个节点都允许获得一份完整的数据库拷贝。节点间基于一套共识机制，通过竞争计算共同维护整个区块链。任一节点失效，其余节点仍能正常工作。

去中心，去信任

区块链由众多节点共同组成一个端到端的网络，不存在中心化的设备和管理机构。节点之间数据交换通过数字签名技术进行验证，无需互相信任，只要按照系统既定的规则进行，节点之间不能也无法欺骗其它节点。

特征

交易透明，双方匿名

区块链的运行规则是公开透明的，所有的数据信息也是公开的，因此每一笔交易都对所有节点可见。由于节点与节点之间是去信任的，因此节点之间无需公开身份，每个参与的节点都是匿名的。

不可篡改，可追溯

单个甚至多个节点对数据库的修改无法影响其他节点的数据库，除非能控制整个网络中超过51%的节点同时修改，这几乎不可能发生。区块链中的每一笔交易都通过密码学方法与相邻两个区块串联，因此可以追溯到任何一笔交易的前世今生。

分类

公有链

无官方组织及管理机构，无中心服务器，参与的节点按照系统规则自由接入网络、不受控制，节点间基于共识机制开展工作。

私有链

建立在某个企业内部，系统的运作规则根据企业要求进行设定，修改甚至是读取权限仅限于少数节点，同时仍保留着区块链的真实性和部分去中心化的特性。

联盟链

由若干机构联合发起，介于公有链和私有链之间，兼具部分去中心化的特性。

目录

科普

数字签名

数字签名涉及到一个哈希函数、发送者的公钥、发送者的私钥。数字签名有两个作用，一是能确定消息确实是由发送方签名并发出来的。二是数字签名能确定消息的完整性。

工作原理

发送报文时，发送方用一个哈希函数从报文文本中生成报文摘要，然后用自己的私钥对摘要进行加密，加密后的摘要将作为报文的数字签名和报文一起发送给接收方，接收方首先用与发送方一样的哈希函数从接收到的原始报文中计算出报文摘要，接着再用发送方的公钥来对报文附加的数字签名进行解密，如果这两个摘要相同、那么接收方就能确认该数字签名是发送方的。

科普

SHA256

一种求Hash值的加密算法。

工作原理

将任何一串数据输入到SHA256将得到一个256位的Hash值（散列值）。

其特点：相同的数据输入将得到相同的结果。输入数据只要稍有变化（比如一个1变成了0）则将得到一个千差万别的结果，且结果无法事先预知。

正向计算（由数据计算其对应的Hash值）十分容易。逆向计算（俗称“破解”，即由Hash值计算出其对应的数据）极其困难，在当前科技条件下被视作不可能。

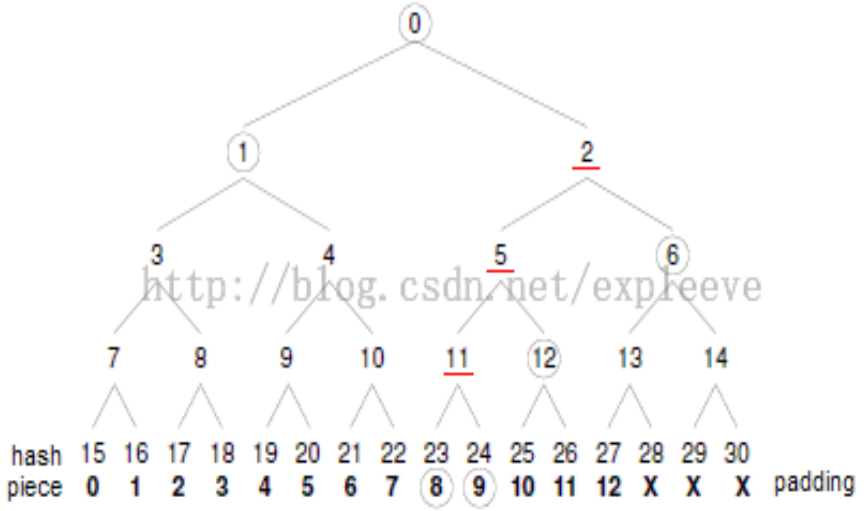
科普

Merkle Tree

一种哈希二叉树，使用它可以快速校验大规模数据的完整性。在比特币网络中，Merkle 树被用来归纳一个区块中的所有交易信息，最终生成这个区块所有交易信息的一个统一的哈希值，区块中任何一笔交易信息的改变都会使得使得 Merkle 树改变。

工作原理

非叶子节点value的计算方法是将该节点的所有子节点进行组合，然后对组合结果进行hash计算所得出的hash value。

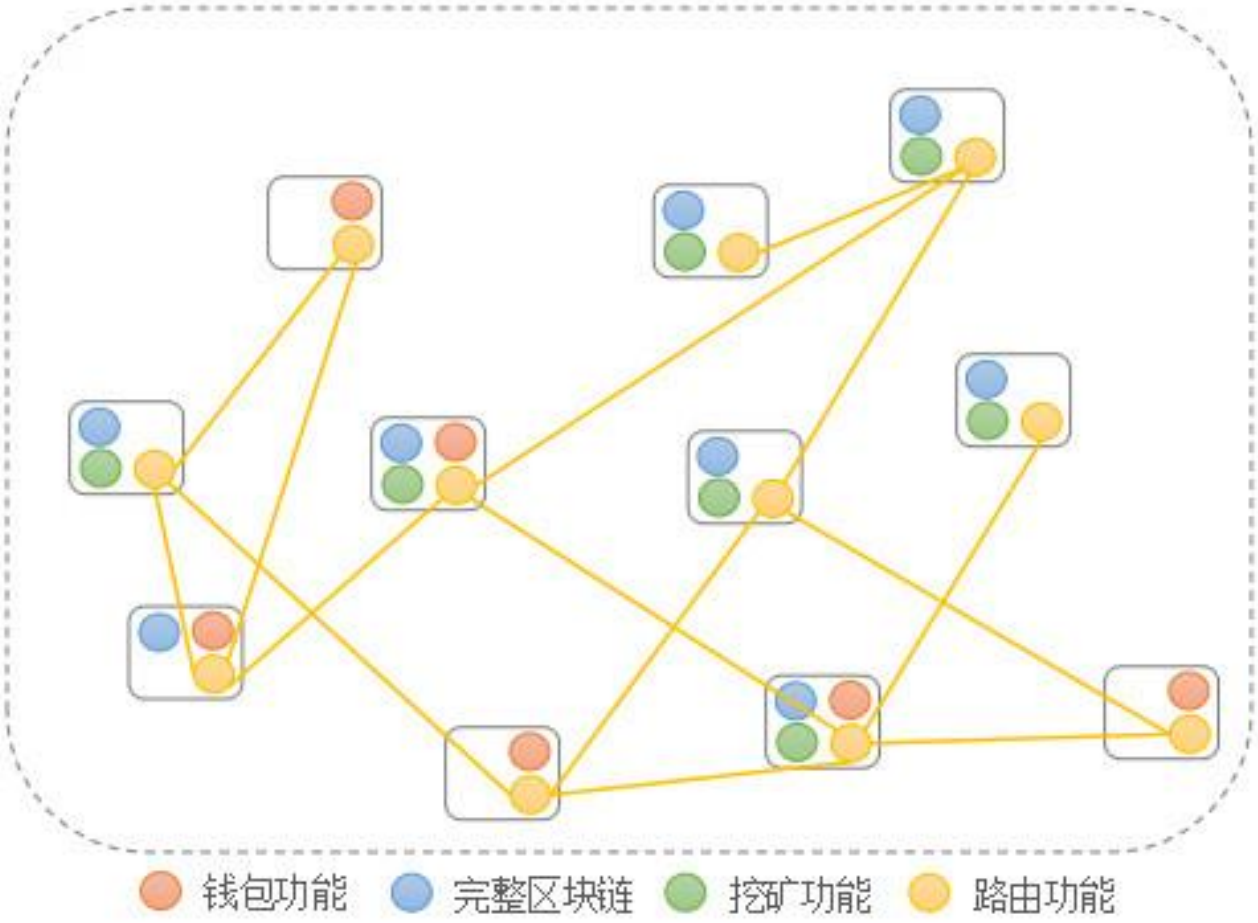


科普

时间戳服务器

大多用来进行比对以及验证处理，时间戳服务器是一款基于PKI（公钥密码基础设施）技术的时间戳权威系统，对外提供精确可信的时间戳服务。它采用精确的时间源、高强度高标准的安全机制，以确认系统处理数据在某一时间的存在性和相关操作的相对时间顺序，为信息系统中的时间防抵赖提供基础服务。

节点网络



本章节后续内容，均以比特币网络特性展开阐述

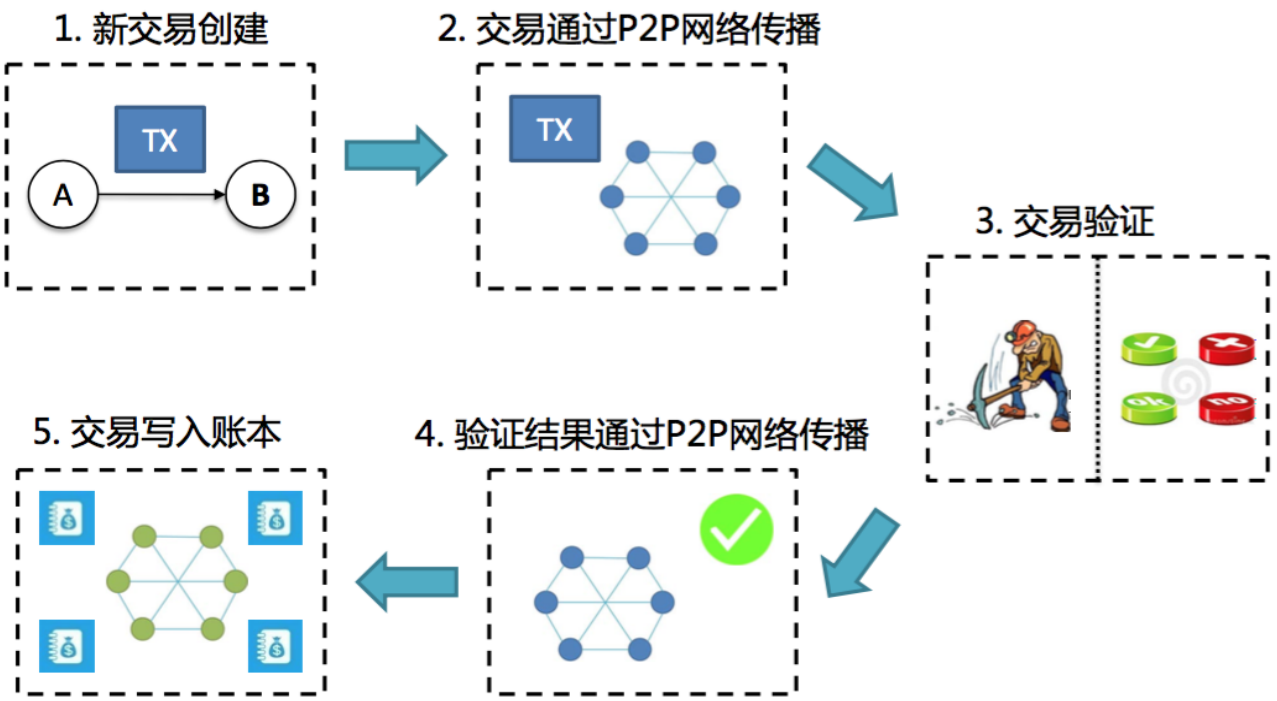
节点网络

任何机器都可以运行一个完整的比特币节点，一个完整的比特币节点包括如下功能：

1. 钱包，允许用户在区块链网络上进行交易
2. 完整区块链，记录了所有交易历史，通过特殊的结构保证历史交易的安全性，并且用来验证新交易的合法性
3. 矿工，通过记录交易及解密数学题来生成新区块，如果成功可以赚取奖励
4. 路由功能，把其它节点传送过来的交易数据等信息再传送给更多的节点

除了路由功能以外，其它的功能都不是必须的。

交易过程


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

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。

交易过程

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

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。

交易过程

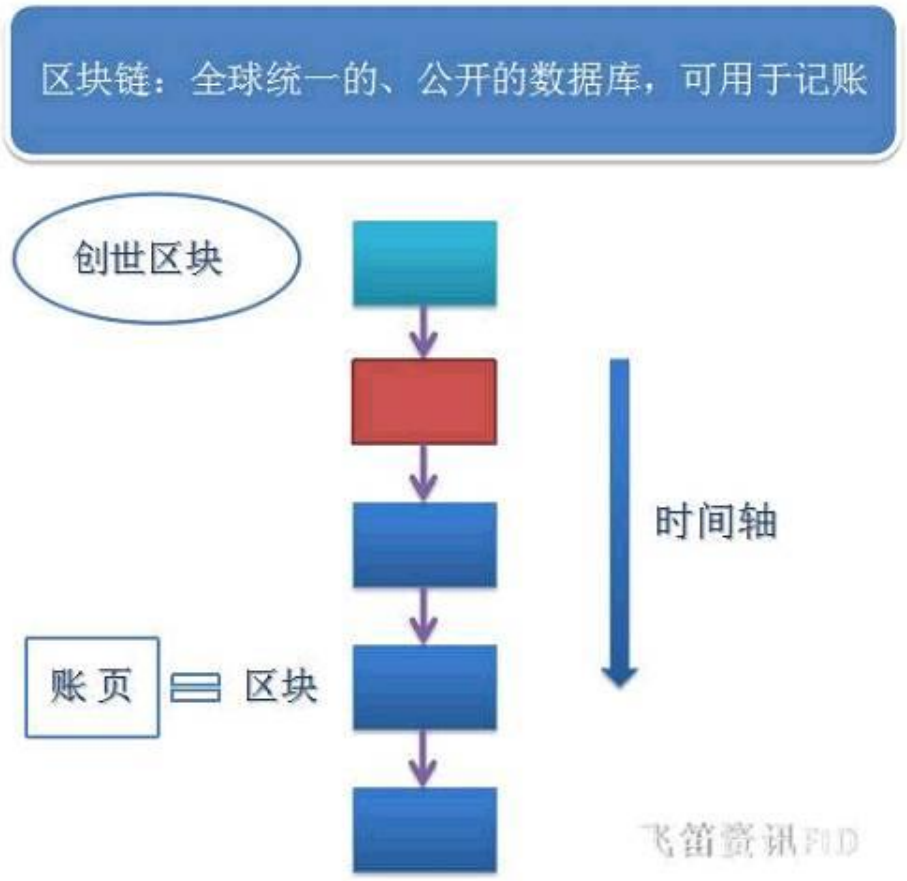
第5步：全网其他节点核对该区块记账的正确性，没有错误后他们将在该合法区块之后竞争下一个区块，这样就形成了一个合法记账的区块链。

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

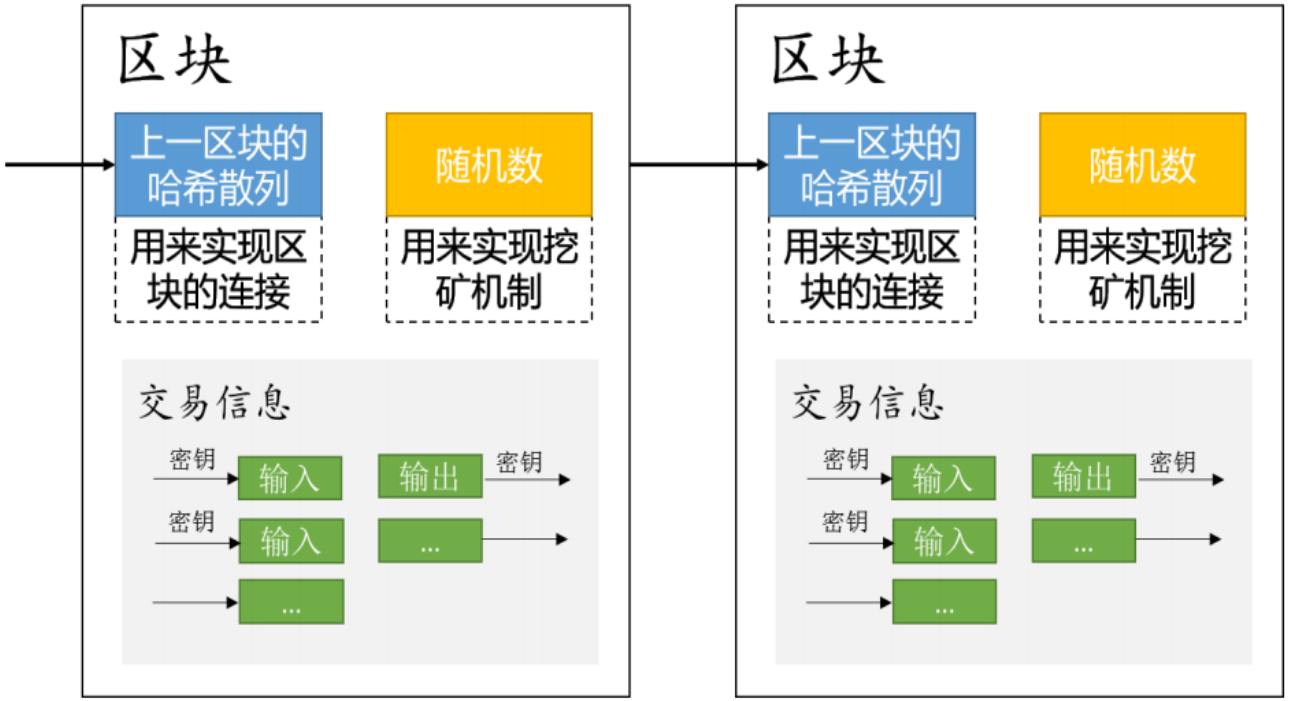
区块链

区块链以区块为单位组织数据。全网所有的交易记录都以交易单的形式存储在全网唯一的区块链中。



区块

区块是一种记录交易的数据结构。每个区块由区块头和区块主体组成，区块主体只负责记录前一段时间内的所有交易信息，区块链的大部分功能都由区块头实现。



区块头

1. 版本号，标示软件及协议的相关版本信息
2. 父区块哈希值，引用的区块链中父区块头的哈希值，通过这个值每个区块才首尾相连组成了区块链，并且这个值对区块链的安全性起到了至关重要的作用
3. Merkle 根，这个值是由区块主体中所有交易的哈希值再逐级两两哈希计算出来的一个数值，主要用于检验一笔交易是否在这个区块中存在
4. 时间戳，记录该区块产生的时间，精确到秒
5. 难度值，该区块相关数学题的难度目标
6. 随机数(Nonce)，记录解密该区块相关数学题的答案的值

区块形成过程

在当前区块加入区块链后，所有矿工就立即开始下一个区块的生成工作。

1. 把在本地内存中的交易信息记录到区块主体中
2. 在区块主体中生成此区块中所有交易信息的 Merkle 树，把 Merkle 树根的值保存在区块头中
3. 把上一个刚刚生成的区块的区块头的数据通过 SHA256 算法生成一个哈希值填入到当前区块的父哈希值中
4. 把当前时间保存在时间戳字段中
5. 难度值字段会根据之前一段时间区块的平均生成时间进行调整以应对整个网络不断变化的整体计算总量，如果计算总量增长了，则系统会调高数学题的难度值，使得预期完成下一个区块的时间依然在一定时间内

目录

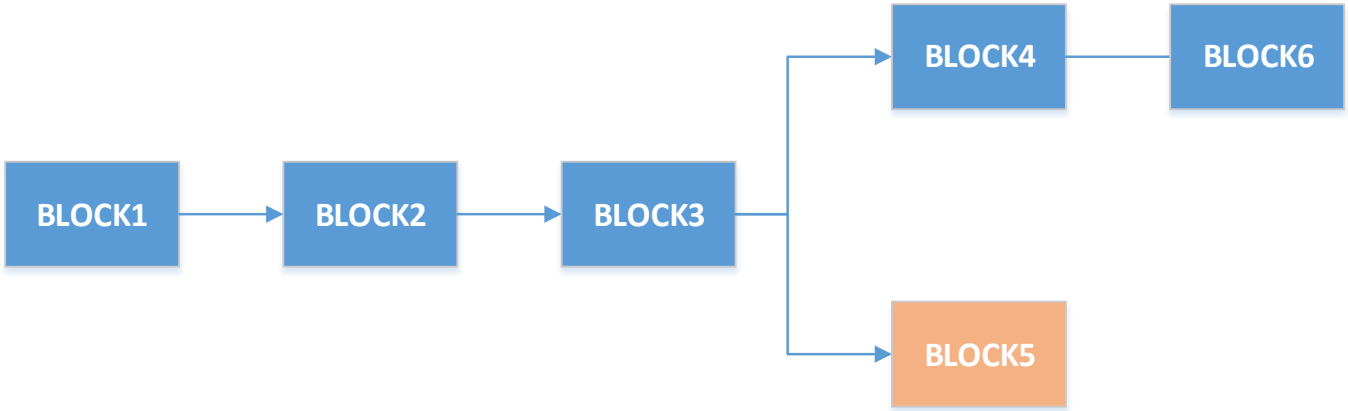
工作量证明

区块头包含一个随机数，使得区块的随机散列值出现了所需的0个数。节点通过反复尝试来找到这个随机数，这样就构建了一个工作量证明机制。

工作量证明机制的本质是一PC一票，“大多数”的决定表达为最长的链，因为最长的链包含了最大的工作 量。如果大多数的PC为诚实的节点控制，那么诚实的链条将以最快的速度延长，并超越其他的竞争链条。如果想要修改已出现的区块，攻击者必须重新完成该区块的工作量外加该区块之后所有区块的工作量，并最终赶上和超越诚实节点的工作量。

分叉

同一时间段内全网不止一个节点能计算出随机数，即会有多个节点在网络中广播它们各自打包好的临时区块（都是合法的）。



某一节点若收到多个针对同一前续区块的后续临时区块，则该节点会在本地区块链上建立分支，多个临时区块对应多个分支。该僵局的打破要等到下一个工作量证明被发现，而其中的一条链条被证实为是较长的一条，那么在另一条分支链条上工作的节点将转换阵营，开始在较长的链条上工作。其他分支将会被网络彻底抛弃。

双花

双花，即双重支付，指攻击者几乎同时将同一笔钱用作不同交易。

每当节点在把新收到的交易单加入区块之前，会顺着交易的发起方的公钥向前遍历检查，检查当前交易所用的币是否确实属于当前交易发起方，此检查可遍历到该币的最初诞生点（即产生它的那块区块源）。虽然多份交易单可以任意序的广播，但是它们最终被加入区块时必定呈现一定的顺序。区块之间以Hash值作为时间戳则区块，这决定了任意一笔交易资金来源都可以被确定的回溯。六度社交理论（6次交易确认）可以在一定程度应用来解决此问题。

5.核心问题

高能耗（主要指挖矿的能耗）

数据库存储空间（如目前比特币的区块数据已接近130G）

处理海量交易的抗压并发能力（如淘宝双11这类交易量）

安全性（目前比特币的安全性比以太坊好，以太坊功能更强。）

目录

6. 前景展望

从2009年的比特币开始，到2014年的以太坊，区块链经历了可编程货币、可编程金融与可编程社会三大应用时代，其应用范围逐步扩展到社会生活的方方面面。

从需求端来看，金融、 医疗、公证、通信、供应链、域名、投票等领域都开始意识到区块链的重要性并开始尝试将技术与现实社会对接。

从投资端来看，区块链的投资资金供给逐步上升， 风投的投资热情也不断高涨，投资密度越来越大，供给端的资金供给有望推动技术的进一步发展。

从市场应用来看，区块链能成为一种市场工具，帮助社会削减平台成本，让中间机构成为过去；区块链将促使公司现有业务模式重心的转移，有望加速公司的发展。

6. 前景展望

从底层技术来看，区块链有望促进数据记录、数据传播及数据存储管理方式的转型；区块链本身更像一种互联网底层的开源 式协议，在不远的将来会触动甚至最后彻底取代现有互联网的底层基础协议。

从社会结构来看，区块链技术有望将法律与经济融为一体，彻底颠覆原有社会的监管模式；组织形态会因其而发生改变，区块链也许最终会带领人们走向分布式自治的社会。