区块链概念与分类

代炜琦

wqdai@hust.edu.cn
华中科技大学
Huazhong University of Science and Technology

概述

在区块链的发展历程中，从比特币开始，早期的区块链系统都是面向数字货币的，比如比特币、莱特币。这个阶段我们可以认为区块链系统是一个支持数字货币合约的系统。

之后出现了更灵活地，能够支持自定义**智能合约**的系统，其代表作就是**以太坊**，可以认为以太坊就是对比特币这样数字货币系统的扩展，不过以太坊仍然内置了对数字货币的支持，延续了比特币系统的金融特征，也使得以太坊的应用更多的是面向**金融范畴**。

再之后就是代表就是**超级账本**项目，尤其是其中的Fabric子项目，在这个系统中，超越了对金融范畴的应用，支持各个领域的数据定义。

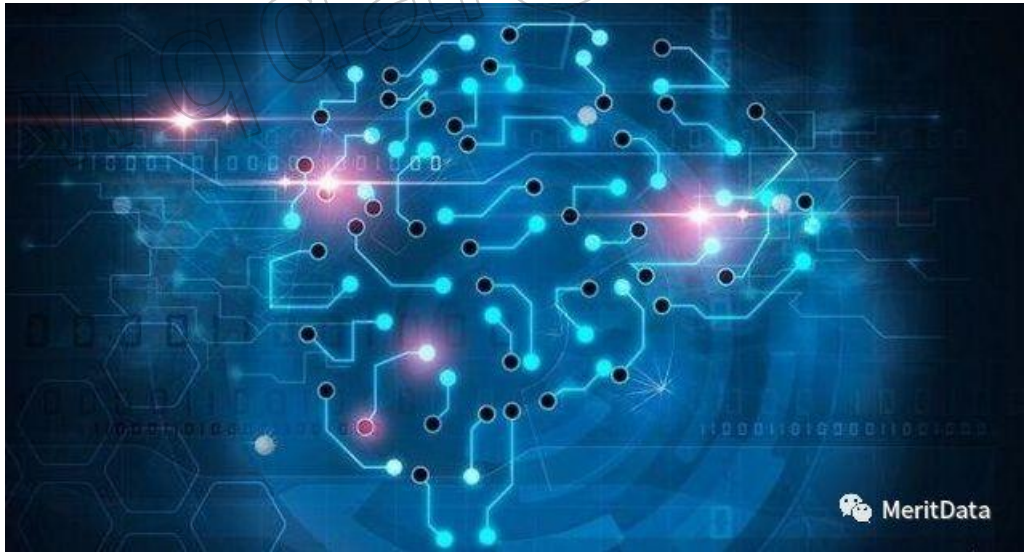
我们分别将这个三个阶段成为区块链系的1.0、2.0、3.0结构时期。为了让大家让大家对发展过程中的区块链系统有一个整体的概念，在本章中，我将描述一下区块链系统的架构，并在不同角度对区块链系统进行分类。

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、利用自动化脚本代码组成的智能合约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。



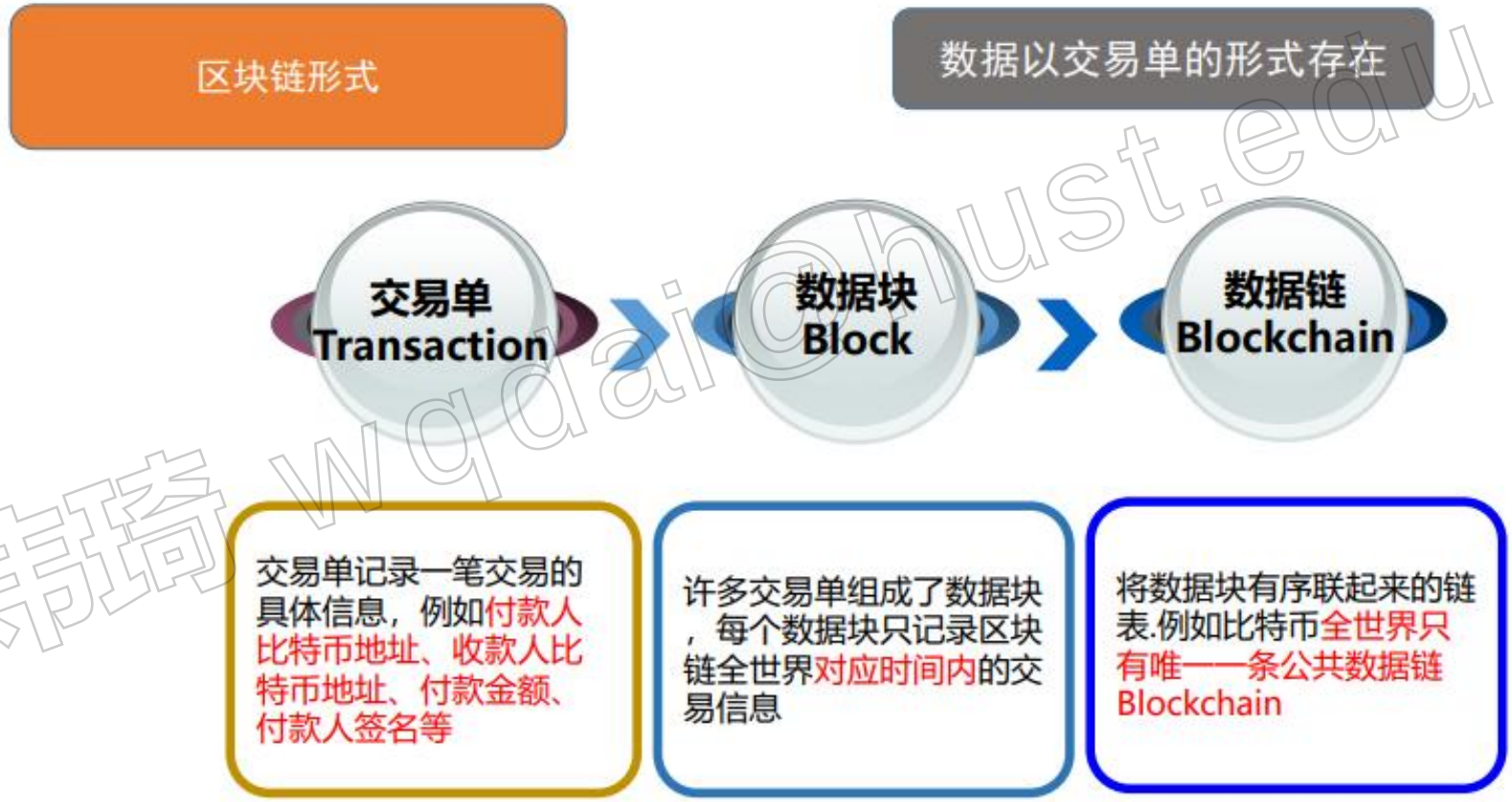
区块链的概念

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，并按照时间顺粗首尾相连形成链式（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。

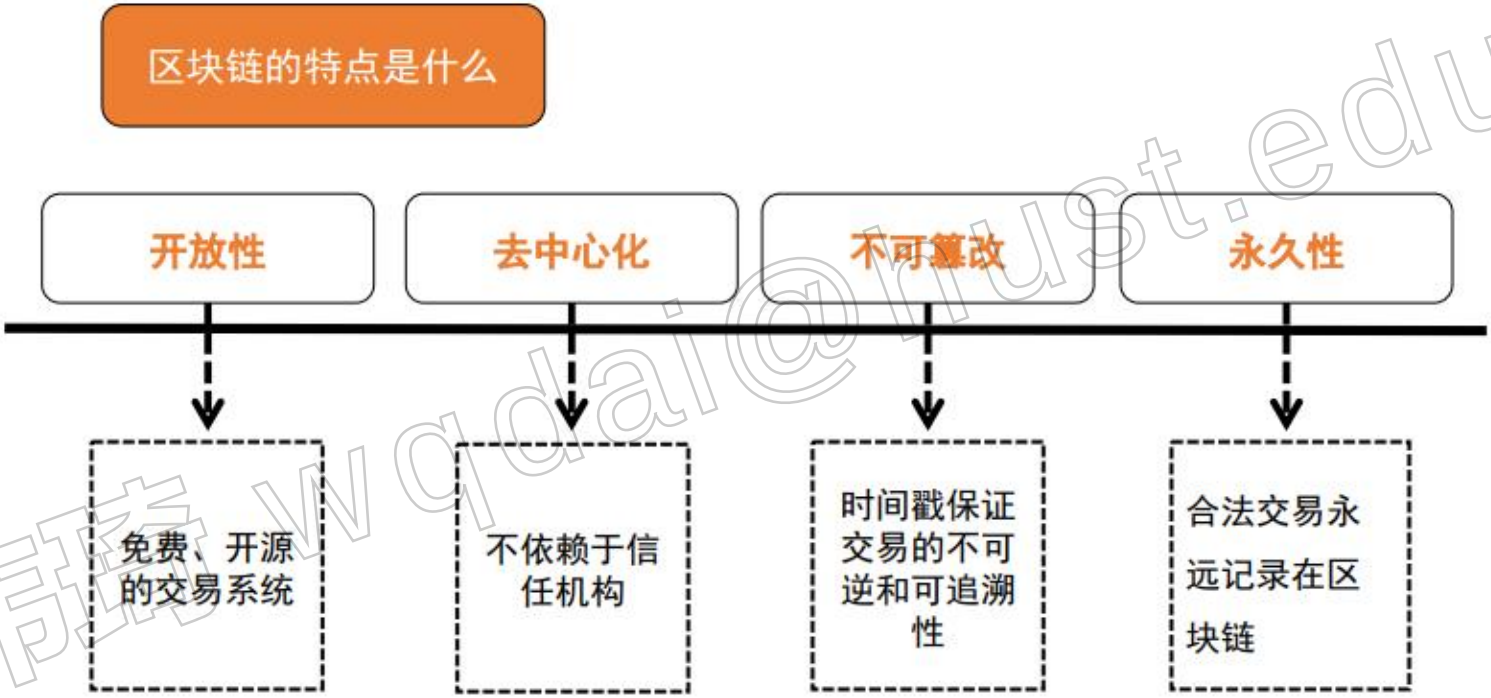
区块链的概念

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。

区块链的概念



区块链的特点



区块链架构

我们知道区块链系统实际上就是一个维护公共数据账本的系统，一切的技术单元的设计都是为了更好地维护好这个公共账本。

通过共识算法达成节点的账本的数据一致；通过密码算法确保账本数据的不可篡改性以及数据发送的安全性；通过脚本系统扩展账本数据的表达范畴。

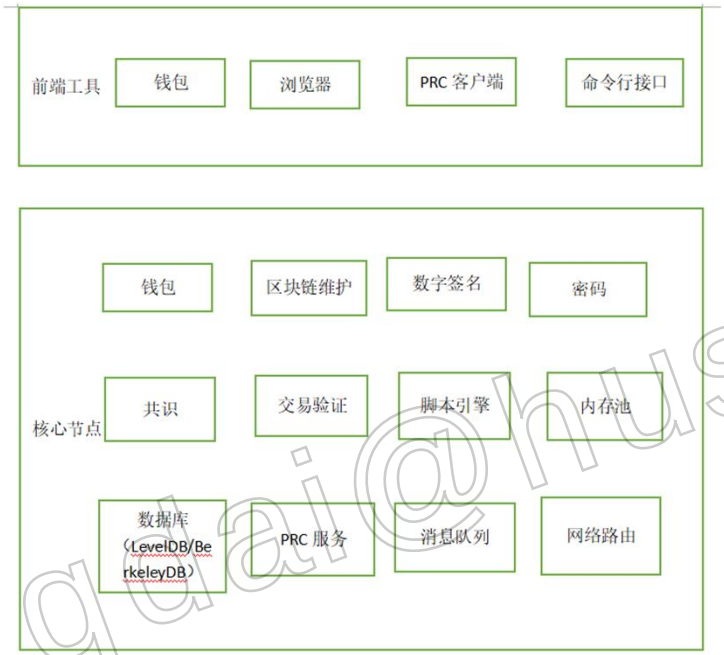
我们甚至可以认为去区块链系统实际上就是特别设计的数据库系统或者分布式数据库系统，在这个数据库可以存储数字货币，也可以存储更复杂的智能合约，以及范围更加广阔的各种业务数据。

区块链1.0架构

如图所示，在整个结构中，分为核心节点和前端工具

在前端工具中，最明显的就是钱包工具，钱包工具是提供给用户管理自己账户地址以及余额的；浏览器是用来查看区块链网络中发生的数据情况，比如最新的区块高度，内存池的交易数、单位时间的网络处理能力等；PRC客户端和命令行接口都是用来访问节点的功能的，在这个时候，核心节点就相当于一个服务器，通过PRC服务提供功能调用接口。

区块链1.0架构

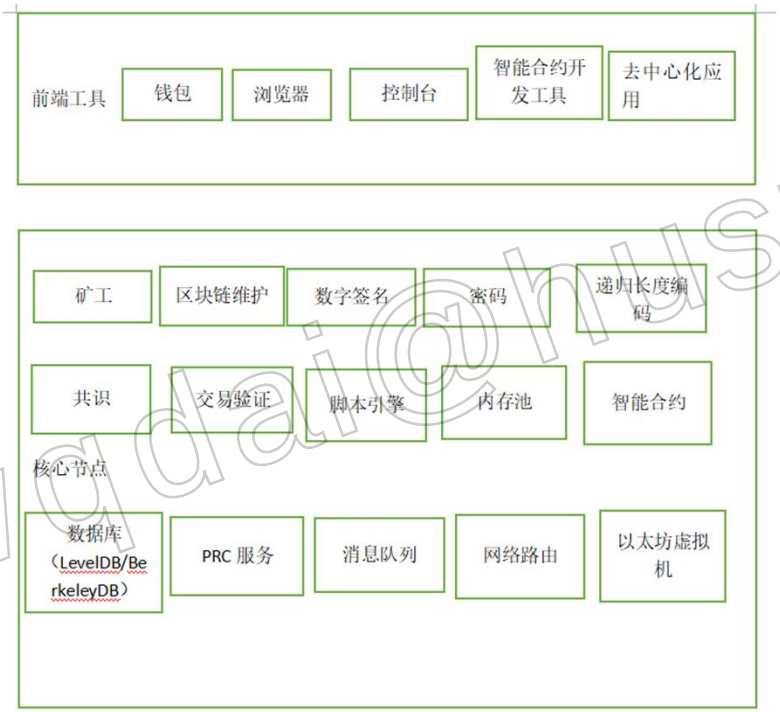


在矿工的1.0系统中，主要承担两个任务：

- 第一个是通过竞争获得区块数据的打包权后将内存池（发送在网络中但是还没有确认进区块的交易数据，属于待确认交易数据）中的交易数据打包进区块，并且广播给其他节点；
- 第二个是接受系统对打包行为的数字货币奖励，从而系统通过这种奖励机制完成新货币的发行。

区块链2.0架构

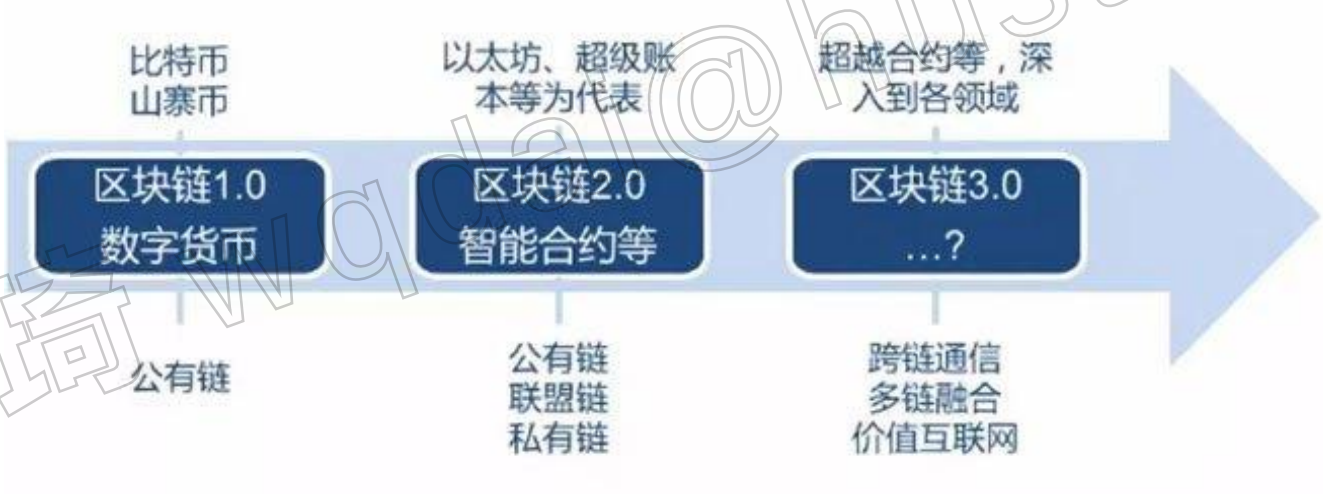
在区块链2.0架构的代表产品是以太坊，因此我们可以套用以太坊的架构来说明，先来看看示意图：



与1.0的架构相比，最大的特点就是支持智能合约，在以太坊中，我们使用智能合约开发工具开发合约程序，并且编译为字节码，最终部署到以太坊的区块链账本中。部署后的智能合约是运行在虚拟机上的，成为“以太坊虚拟机”。正式通过这样的智能合约的实现，扩展了区块链系统的功能，同时我们也看到，在以太坊中还是支持数字货币的，因此在应用工具中还是有钱包工具的。

区块链3.0架构

在3.0的架构中，超越了对数字货币或者金融的应用范畴，而将区块链技术作为一种泛解决方案，可以在其他领域使用，比如行政管理、文化艺术、企业供应链、医疗健康、物联网、产权登记等，可以认为是面向行业应用。

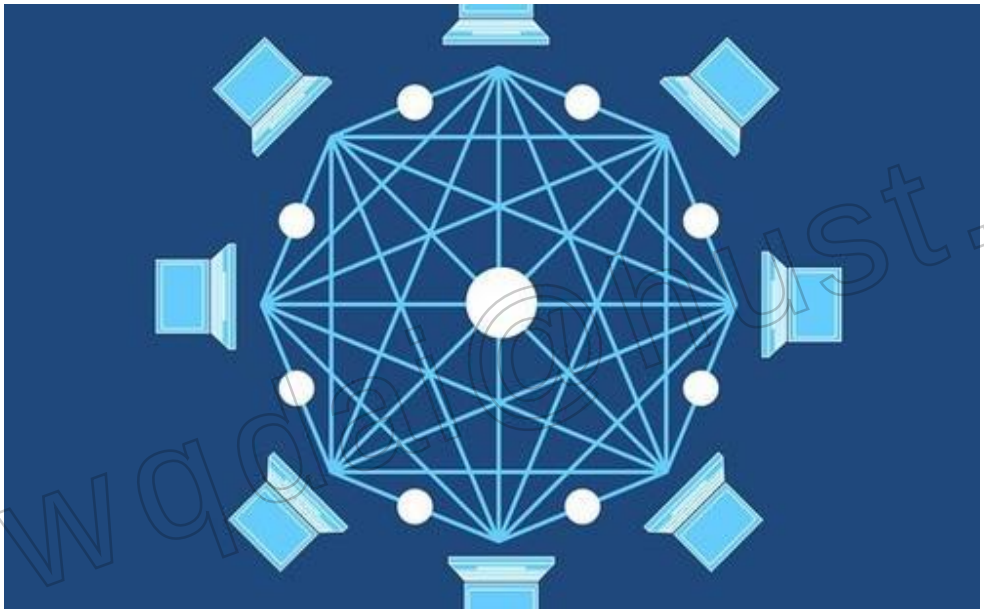


区块链3.0架构

行业应用一般是需要具备企业级属性的，比如身份认证、许可授权、加密传输等，并且对数据的处理性能也会有要求，因此企业级场景下的应用，往往都是联盟链或者私有链。

在上图中，数字货币不再是一个必选的组件了，当然如果需要，我们也可以通过智能合约的方式来实现数字货币的。与之前的架构相比，最大的特点就是增加了一个网管控制，实际上就是增加了对安全保密的需求的支持，并且通过数据审计加强对数据的可靠性管理。

区块链3.0架构

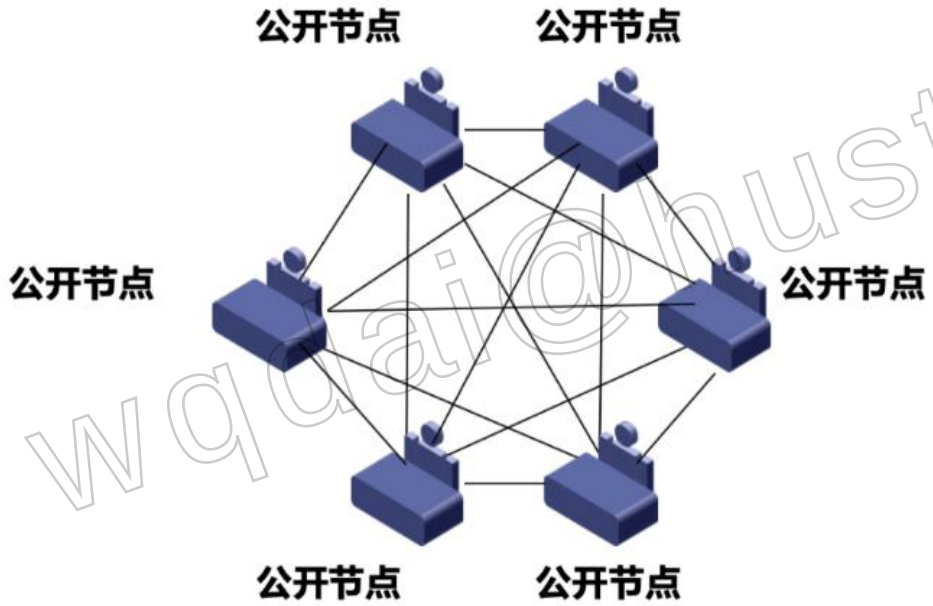


在3.0中，实际上可以看成是一套框架，通过对框架的配置和二次开发可以使用各行业的需求，比如图中的“可插拔共识”，意思就是共识机制不是固定的，而是可以通过用户自己去选用配置。

区块链的分类

公有链

所谓公有就是完全对外开放，任何人都可以任意使用，没有权限的限定，也没有身份认证之类，不但可以任意参与使用，而且发生的所有数据都可以任意查看，完全公开透明。



图：公链

比特币就是一个公有链网络系统，大家在使用比特币系统的时候，只需要下载相应的软件客户端，创建钱包地址、转账交易、挖矿等操作，这些功能都可以自由使用。

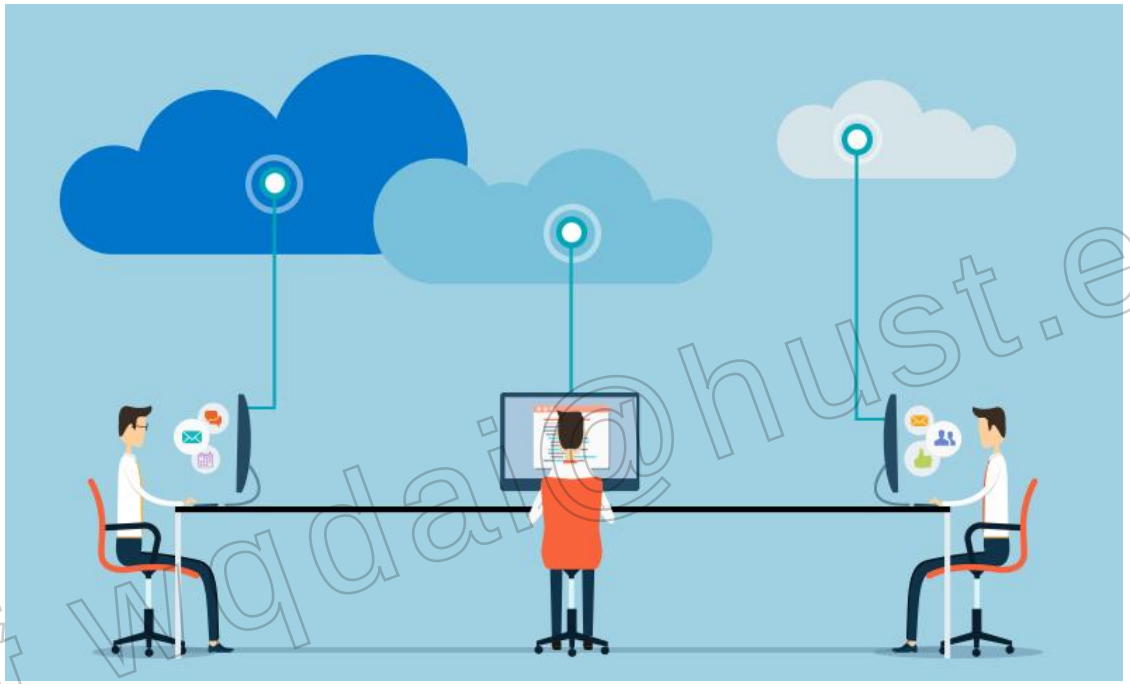
公有链

万向区块链肖风博士曾说：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，不可能没有密码货币，否则无人为区块链工作。

公有链

这里需要注意，在公有链的环境中，节点数量是不固定的，节点的在线与否也是无法控制的，甚至一些节点可能是恶意节点。在介绍区块链工作流程的时候，提到了一个问题，在这种情况下，如何知道数据是被大多数的节点写入确认的呢?

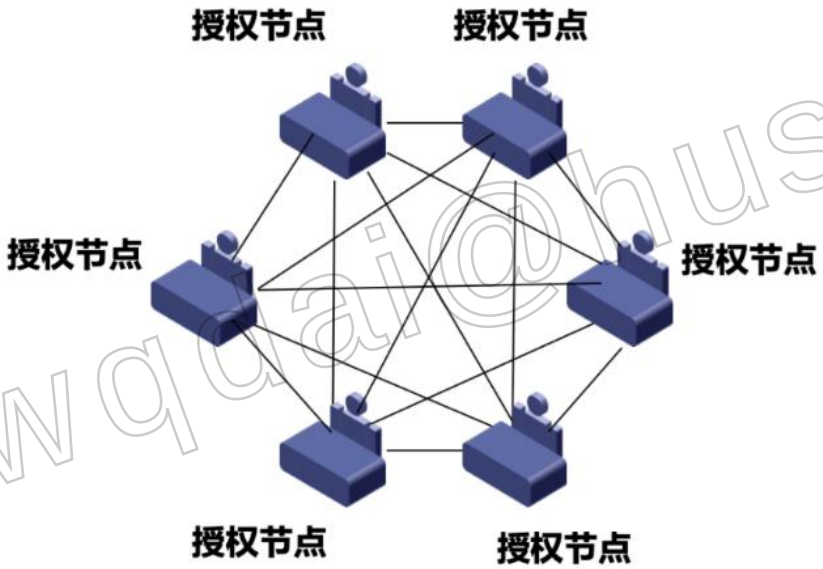
公有链



实际在公有链的环境下，这个问题没有很好的解决，目前最合适的做法就是通过不断地去互相同步，最终网络中大多数节点都同步一致的区块数据所形成的的链就是被承认的主链，这也被称为最终一致性。

私有链

私有链是与公有链相对的一个概念，所谓私有就是指不对外开放，仅仅在组织内部使用的系统。



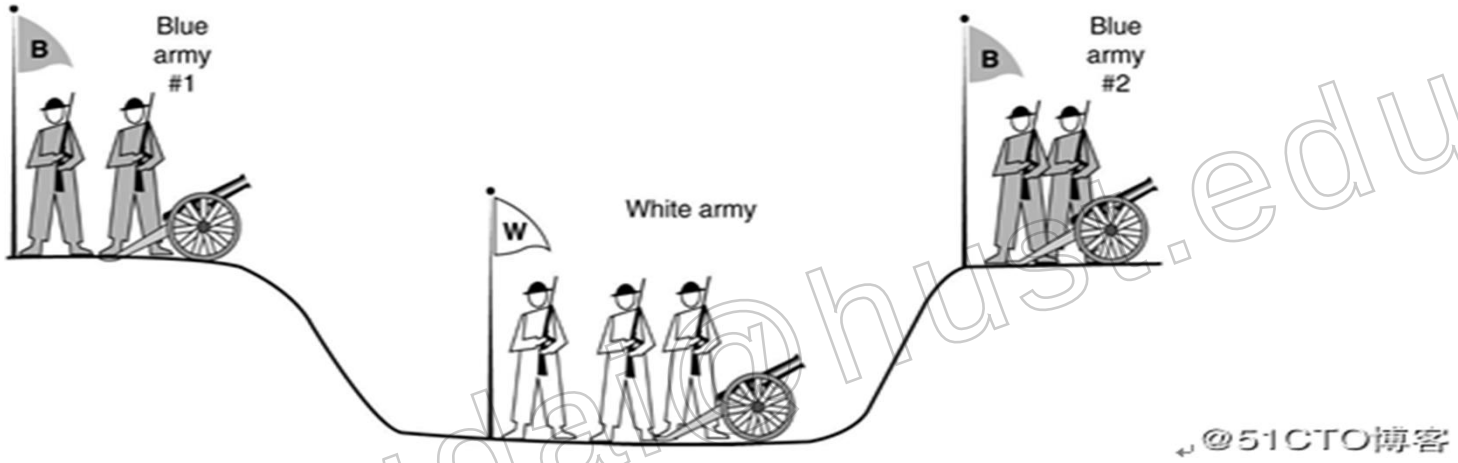
图：私有链

私有链在使用过程中，通常是有注册要求的，即需要提交身份认证，而且具备一套权限管理体系。

私有链的应用

如企业的票据管理、财务审计、供应链管理等，或者一些政务管理系统。私有链在使用过程中，通常是有注册要求的，即需要提交身份认证，而且具备一套权限管理体系。

私有链



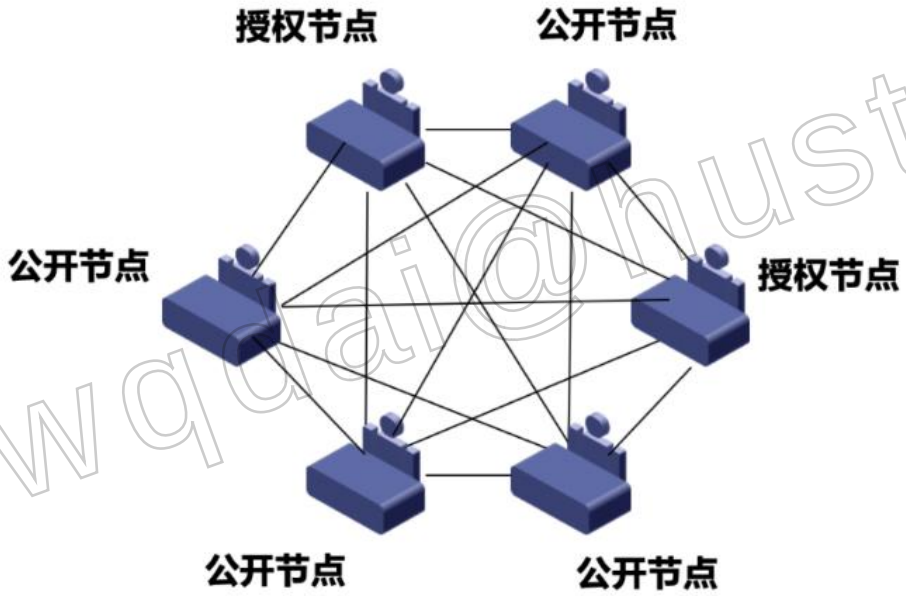
在私有链环境中，节点数量和节点的状态通常是可控的，因此在私有链环境中一般不需要通过竞争的方式来筛选区块数据的打包者，可以采取更加节能环保的方式，比如在上述共识机制介绍中提到的PoS(权限证明)、DPoS(委托权益证明)、PBFT（使用拜占庭容错算法）等。

私有链

以太坊创始人Vitalik Buterin曾说：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。从商业角度来说，私有链适合大公司事业部之间的应用协作。

联盟链

联盟链的网络范围结余共有链和私有链之间，通常是使用在多个成员角色的环境下



图：联盟链

与私有链一样，联盟链系统一般也是具有身份认证和权限设置的，而且节点的数量往往是确定的，对于企业或者机构之间的事务处理和合适。联盟链不一定要完全管控，比如财务系统，有些数据可以对外工卡的，就可以部分放出来。

由于联盟链一般用在明确的机构之间，因此与私有链一样，节点的数量和状态也是可控的，并且通常也是爱用更加节能环保的共识机制。

联盟链的应用

比如银行之间的支付结算、企业之间的物流等，这些场景下往往都是由不同权限的成员参与的。

联盟链

联盟链是目前我国大力发展的方向，虽然联盟链在一定程度上限制了去中心化，但联盟链的概念更加适合实际的商业应用需求。

联盟链

联盟链介于公有链和私有链之间，加入和退出需经过联盟授权，中行前行长李林辉曾说：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。

联盟链虽然“牺牲了”一部分去中心化，但却保留了区块链具有实际应用的特性，更适合开发商业化产品满足客户个性化需求。

公链VS私链

公链

优点

- 保护用户免受开发者的影响。
- 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。

缺点

- 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。
- 公共区块交易费用较高，确认速度较慢等。
- 公有链的不可更改性降低了一定的灵活性。

公链VS私链

私链

优点

- 较强的灵活性。
- 私有链节点均已知，不存51%攻击风险。
- 交易成本更便宜。
- 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。
- 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

- 丧失了一定的去中心化的特性。

公有链、私有链和联盟链比较

	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

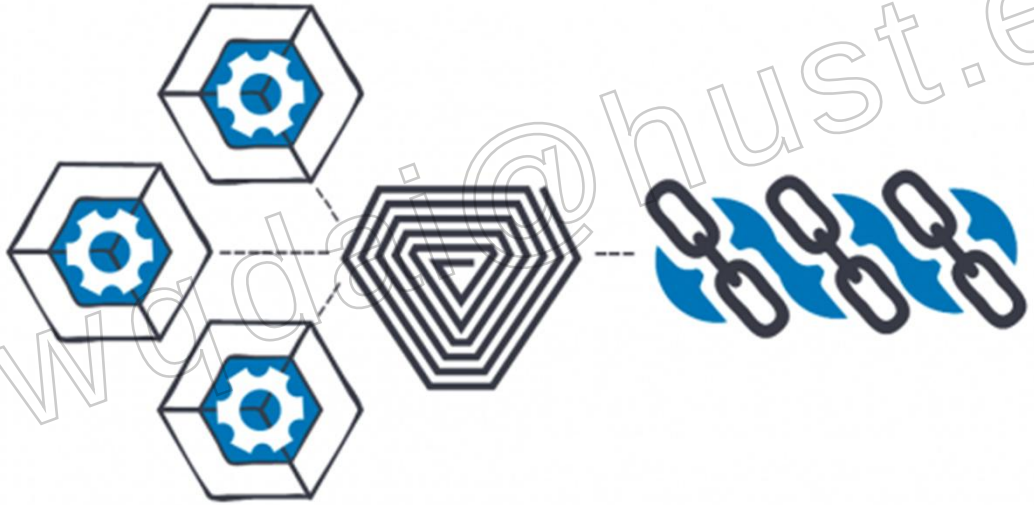
根据部署环境

分为主链和测试链

左边主链钱包，右边是测试链钱包

主链

所谓主链，也就是部署在生产环境中的真正的区块链系统，软件在正式发布前会经过很多的内部测试版本，用于发现一些可能存在的bug，并且用来内部演示以便于查看结果，最后才会正式发布正式版。



测试链

就是开发者为了方面大家学习使用提供的测试用途的区块链系统，比如比特币测试链、以太坊测试链等。

当然，倒也不是树非得是区块链开发者才能提供测试链，用户也可以自行搭建测试网络。测试链中的功能设计与生产环境中的主链是可以有一些差别的，比如主链中使用工作量证明算法进行挖矿，在测试链中可以换成其他算法以便测试使用。

根据对接类型

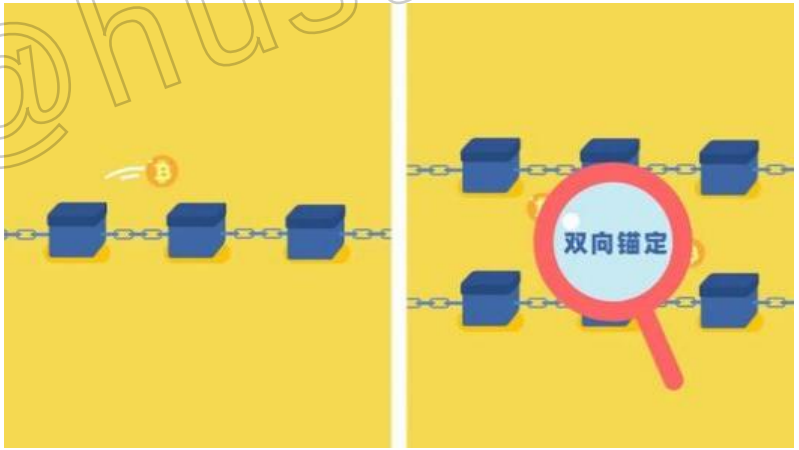
分为单链、侧链和互联链

单链

能够单独运行的区块链系统都可以成为是“单链”，比如比特币主链、测试链，以太坊主链与测试链；超级账本中的Fabric搭建的联盟链等，这些区块链系统拥有完美的组件模块，自成一个体系。

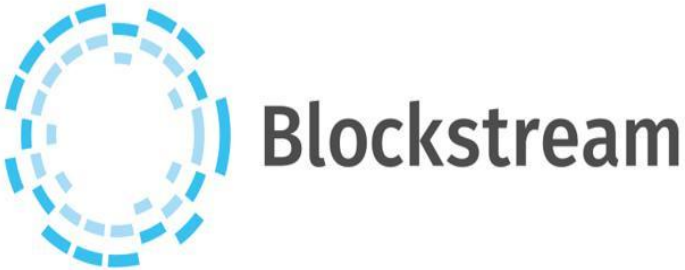
侧链

侧链属于一种区块链系统的跨链技术，这个概念主要是比特币侧链发起的，随着技术的发展，除了比特币，出现了越来越多的区块链系统，每一种系统都有自己的优势特点。如何将不同的链结合起来，打通信息孤岛，彼此互补呢？侧链就是其中的一项技术。



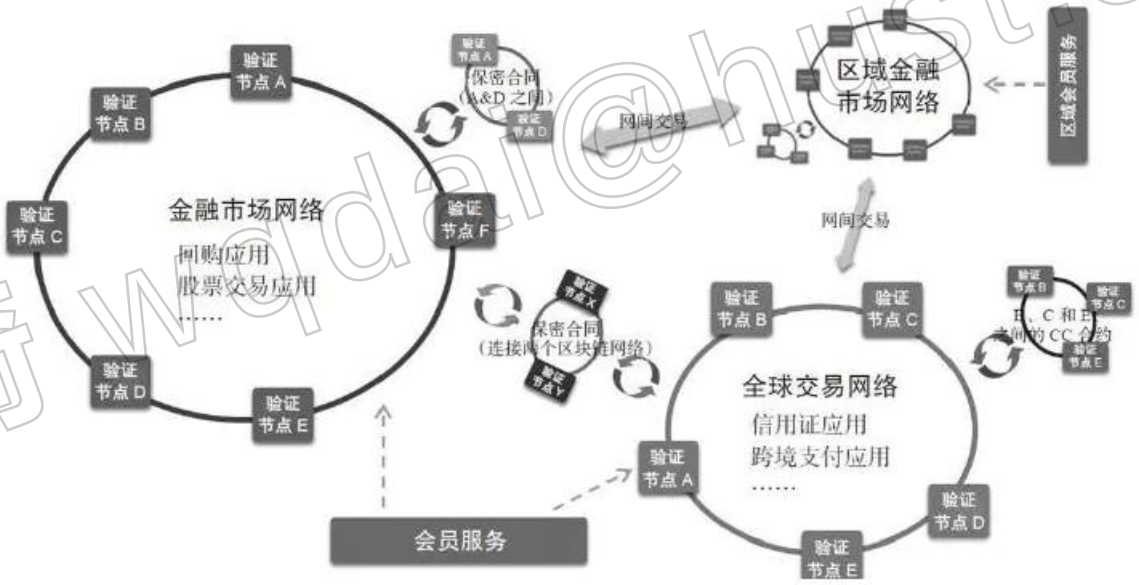
侧链

区块链系统与侧链系统本身都是一个独立的链系统，两者之间可以按照一定的协议进行数据互动，通过这种方式，侧链能起到一个队主链功能扩展的作用，很多在主链中不方便实现的功能可以在侧链中实现，而侧链再通过与主链数据交互增强自己的可靠性。



互联链

互联链就是各种不同的区块链之间的互联互通所形成的一个更大的生态区块链。比如电商平台公有链+物流公有链+物流联盟链+银行联盟链 +.....，它们之间的相互协作、通讯、共识、就是一个典型的互联链。



UTXO和双花问题

代炜琦

wqdai@hust.edu.cn
华中科技大学
Huazhong University of Science and Technology

双花问题

什么是“双花”问题？

双花问题

我们微信钱包里有100块钱，我们先去饭店吃了顿饭，结果微信出了bug，这一笔钱并没有被银行同步，还留在钱包里，于是我们又能拿着同样的100块钱去看场电影，这就属于**双花问题**。

“支付宝”们如何解决双花问题?

我们每天都在淘宝上买买买，也不需要使用现金。支付宝如何解决“双花问题”呢?

“支付宝”们如何解决双花问题?

事实上，支付宝中的钱并不存在于数字世界。相反，它仍存在于现实世界的银行中。

“支付宝”们如何解决双花问题?

当小明在淘宝上下单并付款给卖家时，小明实际上做的是:

- 小明把钱付给支付宝;
- 支付宝将小明的钱存在他们的银行账户中;
- 你确认收货后，支付宝将钱从他们的银行账户中取出，并支付给卖家。

“支付宝”们如何解决双花问题?

实际上支付宝仅仅是一个第三方中介。这类机构对数据进行中心化管理，并通过实施修改账户余额的方法来防止“双花”的出现。

“支付宝”们如何解决双花问题?

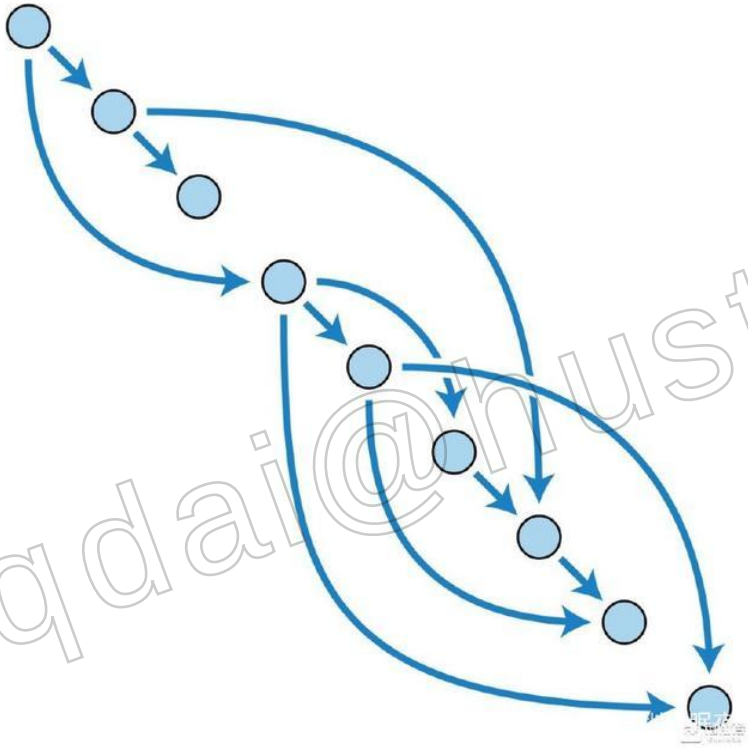
这样有什么问题吗?

虽然每一笔交易的“中介费”并不高，但如果交易数量十分大呢？要知道，全球总共有超过75亿人，每天交易量高达以万亿级别。更值得注意的是，这类第三方机构对数据进行的是中心化管理，它们会不会有意或无意（被黑客攻击）篡改数据呢?

比特币如何解决双花问题?

那我们有没有可能，在不需要信任中心化第三方机构的情况，向某人转移数字资产?

比特币如何解决双花问题



比特币作为一个去中心化的点对点电子现金系统，主要依靠未花费的交易输出（unspend transaction output, UTXO）和时间戳来解决“双花”问题。

UTXO

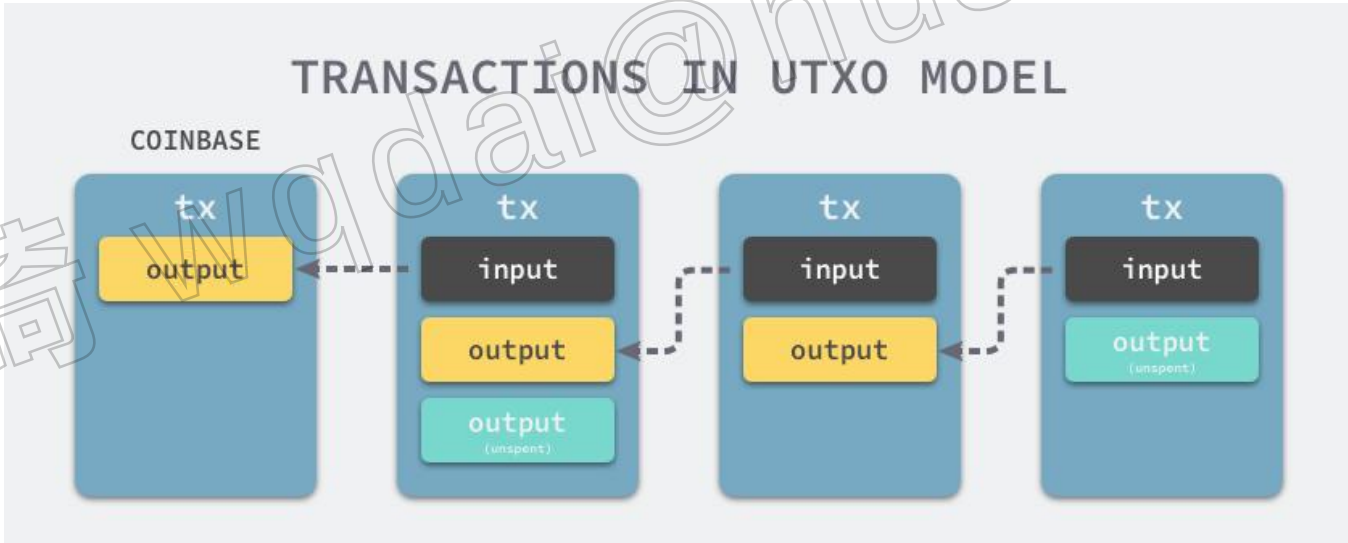
在比特币钱包当中，我们通常能够看到账户余额，然而在中本聪设计的比特币系统中，并没有余额这个概念。“比特币余额”是由比特币钱包应用派生出来的产物。中本聪发明了UTXO交易模型，并将其应用到比特币当中。

账户模式

张三挖到12.5 枚比特币。过了几天，他把其中 2.5 枚支付给李四。又过了几天，他和李四各出资 2.5 比特币凑成 5 比特币付给王五。

什么是UTXO?

UTXO（Unspent Transaction Outputs）是未花费的交易输出，它是比特币交易生成及验证的一个核心概念。交易构成了一组链式结构，所有合法的比特币交易都可以追溯到前向一个或多个交易的输出，这些链条的源头都是挖矿奖励，末尾则是当前未花费的交易输出。



基于账户的交易

我们先看下传统的交易是如何进行的：我们设计一个支付系统，给张三一个账户，里面有余额100 元，李四有一个账户，里面有余额50元。当张三要付给李四20元时，做以下操作：

1. 检查张三账户余额是否充足，如果不足20元就终止交易，向张三报“余额不足”
2. 在张三账户里减去20元（假设零手续费）
3. 在李四账户里增加20元

基于账户的交易

现在的银行也好、信用卡也好、证券交易系统也好，互联网第三方支付系统也好，其核心都是基于账户（account based）的设计，由关系数据库支撑。

基于UTXO的交易

要理解UTXO，最简单的办法就是把一枚比特币从诞生到在商海中沉浮的经历描述一下。
我们假设一个这样的场景：张三挖到12.5 枚比特币。过了几天，他把其中 2.5 枚支付给李四。又过了几天，他和李四各出资 2.5 比特币凑成 5 比特币付给王五。

每笔交易都有若干交易输入，也就是资金来源，也都有若干笔交易输出，也就是资金去向。一般来说，每一笔交易都要花费（spend）一笔输入，产生一笔输出，而其所产生的输出，就是“未花费过的交易输出”，也就是 UTXO。

比特币的区块链账本里记录的是一笔又一笔的交易。

基于UTXO的交易

比特币交易遵守几个规则:

第一，除了Coinbase交易之外，所有的资金来源都必须来自前面某一个或者几个交易的UTXO，就像接水管一样，一个接一个，此入彼出，生生不息，钱就在交易之间流动起来了。

第二，任何一笔交易的交易输入总量必须等于交易输出总量，等式两边必须配平。

基于UTXO的交易

*Coinbase **字面意思是“币根基”***

可以理解为系统最初生成的比特币，在比特币区块链上的每个区块之中都会包含一个或者多个交易，其中第一个交易就叫做 Coinbase 交易。 Coinbase 交易中包含一个 input 和 output，input 由 coinbase 提供，output 指向矿工的地址，总余额等于区块奖励和手续费之和。

基于UTXO的交易流程（1）

右图第一个交易#1001 号交易是 coinbase 交易。
比特币是矿工挖出来的，当一个矿机找到一个合格的区块之后，它就获得一个特权，能够创造一个coinbase交易，在其中放入一笔新钱，并且在交易输出的收款人地址一栏写上自己的地址。

假设这笔比特币的数额为12.5 枚，这个coinbase 交易随着张三挖出来的区块被各个节点接受，经过六个确认以后永远的烙印在历史中。

基于UTXO的交易流程（2）

过了几天，张三打算付 2.5 个比特币给李四，张三就发起#2001号交易，这个交易的资金来源项写着“#1001(1)”，也就是 #1001 号交易——张三挖出矿的那个 coinbase 交易——的第一项 UTXO。然后在本交易的交易输出 UTXO 项中，把2.5个比特币的收款人地址设为李四的地址。

请注意，这一笔交易必须将前面产生那一项 12.5 个比特币的输出项全部消耗，而由于张三只打算付给李四 2.5 个比特币，为了要消耗剩下的10比特币，他只好把剩余的那 10 个比特币支付给自己，这样才能符合输入与输出配平的规则。

基于UTXO的交易流程（3）

再过几天，张三和李四打算AA制合起来给王五付 5 枚比特币。那么张三或李四发起 #3001 号交易，在交易输入部分，有两个资金来源，分别是#2001(1) 和 #2001(2)，代表第 #2001 号交易的第 (1) 和第 (2) 项 UTXO。

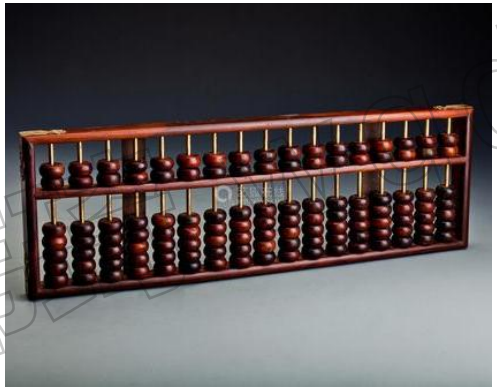
然后在这个交易的输出部分里如法炮制，给王五5比特币，把张三剩下的 7.5 比特币发还给自己。以后王五若要再花他这5比特币，就必须在他的交易里注明资金的来源是 #3001(1)。

UTXO

所以，其实并没有什么比特币，只有UTXO。当我们说张三拥有 10 枚比特币的时候，我实际上是说，当前区块链账本中，有若干笔交易的 UTXO 项收款人写的是张三的地址，而这些 UTXO 项的数额总和是 10。而**我们在比特币钱包中所看到的账户余额，实际上是钱包通过扫描区块链并聚合所有属于该用户的UTXO计算得来的。**

两种交易方式对比

- UTXO只需要看最后一次交易，而账户系统要看历史全数据后所有的增减操作全部加起来才能获得正确的余额，两者效率差异随着时间推移会越来越大；
- UTXO未来可以裁剪历史老数据，而账户系统则不能丢弃老数据，前者区块链可以控制住整体大小，而后者只能持续膨胀。



51%攻击和分叉

代炜琦

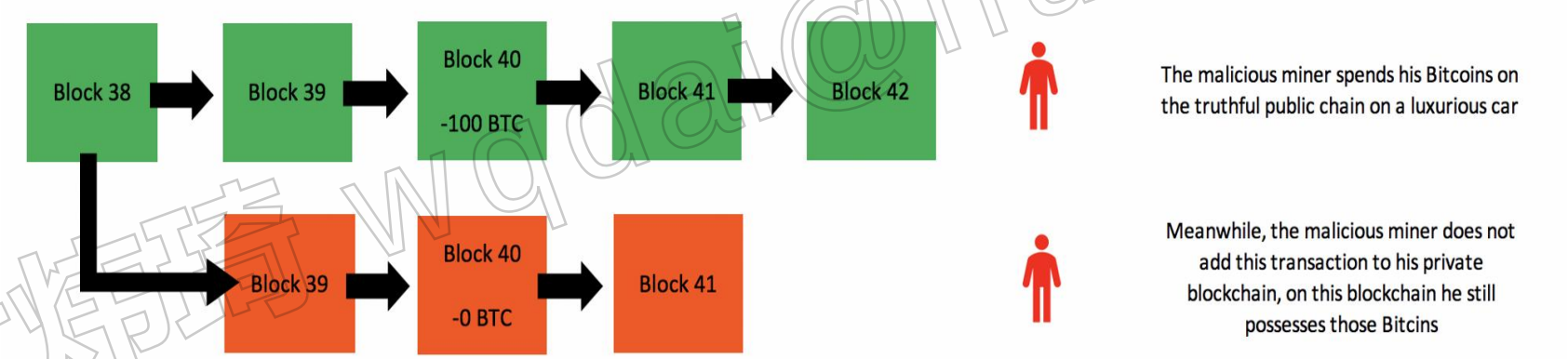
wqdai@hust.edu.cn
华中科技大学
Huazhong University of Science and Technology

双花问题的例外-51%攻击

双花问题还是存在例外的

双花问题的例外-51%攻击

如果小明能掌握比特币网络中50%以上的节点，即使他落后最长的区块链（记录“小明在12点34分56秒转给李雷1个比特币”）也没关系，他可以一直在另一条区块链（记录“小明在12点34分57秒转给韩梅梅1个比特币”）上构建区块，直到追上并成为新的最长链，这就是比特币的“51%攻击”。



什么是51%攻击

比特币：一种点对点的电子现金系统

Bitcoin: A Peer-to-Peer Electronic Cash System

作者：中本聪（Satoshi Nakamoto） satoshin@gmx.com www.bitcoin.org 2008.10.31

事实上，比特币白皮书全文中并没有出现“51%攻击”这个词，不过倒是有过相关的描述，算是最接近对51%攻击的定义了：*The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.* **只要诚实的计算节点在总体上比任何一个攻击群控制更多的计算能力，那么系统就是安全的。**

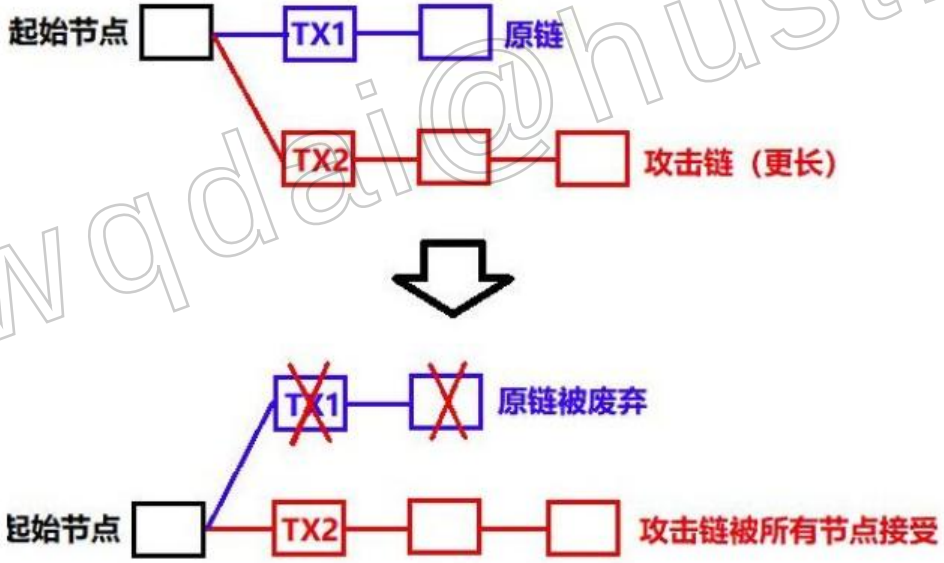
了解51%攻击

The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.

从这句话可以推论一下，要想一方的计算能力超过另外一方，最好是一方的算力超过50%，比如达到51%时，那它就肯定比另一方多。如果诚实节点拥有51%算力，那系统就是安全的；如果作恶节点拥有51%算力，那它就能对另一方发动51%攻击，那系统就是不安全的，在我看51%攻击就是从这里来的。

了解51%攻击

莱特币矿池创始人江卓尔在《天下大义，当混为一——算力战》中有专门提到他的定义：大家都知道“51%算力攻击”： 1、攻击者通过优势算力，挖掘一条比原链更长的攻击链。 2、攻击链向全网广播后，节点按规则，将接受更长的链，丢弃原链。 下图中的直线链（上面的蓝色链和下面的红色链），表示被中立节点接受的主链。



51%攻击

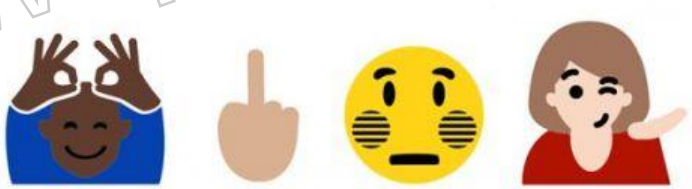
下面，我将把51%攻击拆成“51%”与“攻击”这两个词来分别讲解。

一、51%的算力不是绝对的

1、即使没有51%的算力，比如只有30%，40%的算力，也能发动“51%攻击”； 并不是超过了51%的算力，就一定会发动51%攻击，只是存在这种可能性。

事实上，即使你只有30%的算力，你也有可能连续出5-6个块，也已经可以开始发动很有威胁的“51攻击”了； 即使你有51%的算力，你也有可能半天出不了一个块，而攻击失败，只不过长久看来，你出块的概率等于你算力的权重。

如果把节点分为诚实节点、中立节点、作恶节点的话，那么你只需要比诚实节点的算力多即可，而不必一定需要51%的算力。



51%攻击

2、算力只是这场竞赛的一个方面，还有网络传播等方面因素。

在出块有先后的情况下，基本上谁先出块谁就有很大概率成为最长链。
在同时出块的情况下，谁能更快的传播到51%的网络节点并被接受，并在此基础上进行进一步的扩展和记账，谁就是最长链。
从这个角度说，51%指的不仅是算力，更是指网络节点的接受度。 从这个角度说，更重要的不仅是51%算力，而是利用优势算力抢先出块后的“最长链法则”。

51%攻击

二、算力竞争本身并不是攻击

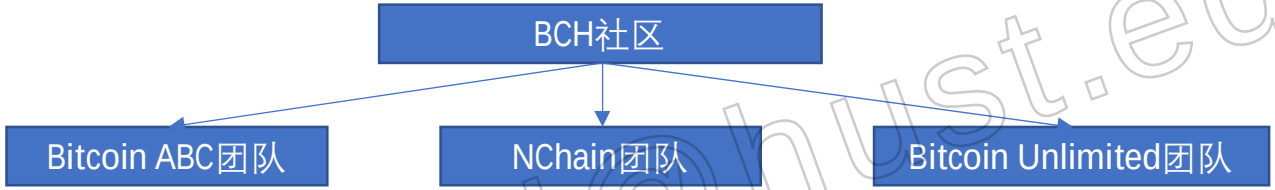
这里说的是“51%攻击”，而不是说的“51%竞争”，“51%争夺”。这两者有什么区别呢？

案例-ABC和BSV之争

2018年8月，Bitcoin ABC提出了一种新的共识变更，以提高BCH节点的速度，并引入外链。该变更将在2018年11月15日上线。但Craig Wright拒绝这种变更，称其为垃圾，宣称应当坚持中本聪最初的设计（Satoshi's Vision），否定了ABC开发组，并在当前客户端版本上发布了自己的版本SV。由于ABC的共识变更会和原有共识不兼容，因此这将是一次硬分叉，而双方都拒绝增加防重放，这次和以往硬分叉生"仔"不同之处在于，以往更多是新的算力来维持一个新链。

案例-ABC和BSV之争

背景故事



Bitcoin ABC团队和NChain团队都是BCH社区比较重要的技术开发团队，NChain在2018年8月16日发布了Bitcoin SV (Satoshi's Vision)客户端，这就是当前一直提到的BCH的ABC和BSV；其实还有一个大的开发组Bitcoin Unlimited，这位则保持中立。

案例-ABC和BSV之争

分歧点

战争爆发于ABC在BCH官网 https://www.bitcoincash.org 发布0.18版升级之后，CSW提出强烈批评，并且发布BSV版本，提出取消ABC的0.18版本升级，全网采纳BSV版本。此举遭到ABC团队和比特大陆等方面的反对，并对BSV版本提出反对。这次事件的主要矛盾点在于客户端采用的共识机制不同，两个版本的主要差别在于：

*Bitcoin ABC**方案***

1.对区块内交易使用CTOR（顺序交易排序）交易排序规则替代了原有的TTOR（拓扑交易排序）交易排序规则。
2.设置了最小的交易大小（100bytes）防止对SPV的攻击。
3.增加了两个操作码OP_CHECKDATASIG和OP_CHECKDATASIGVERIFY，以便引入外链。
4.push-only规则。

*Bitcoin SV**方则十分简单：***

1.区块大小上限从32M扩展到128M
2.启用加减乘除的操作码以便在未来支持链上智能合约
3.恢复中本聪早期版本设计了但被禁用的4个操作码

案例-ABC和BSV之争

而Bitcoin ABC反对BSV的主要是将区块大小上限扩展到128M，主要理由为：

目前BCH每块实际容量在200k左右，现有32M区块上限是实际容量的160倍，没有扩容的市场需求。对此，CSW一方强调他们向大的银行和百货公司推荐使用BCH时，这些大公司强调BCH容量限制太小，无法满足它们的需求。因此，先升级128M然后取消区块容量上限是吸引大公司应用BCH的先决条件。

案例-ABC和BSV之争

这次事件的结局如何

2018年11月16日凌晨2点16分，BCH硬分叉算力战落下帷幕，以BCH ABC的算力胜利告终。在SVpool挖出分叉前最后一个区块后，BCH就此分裂成BCH ABC和BSV两条链，随后吴忌寒便转发了一条Twitter称：“祝贺！在这个新的区块之后，BCH社区中将不会再有捣乱分子了！”澳本聪则放话表示游戏仍在继续。

图为**吴忌寒**，比特大陆联合创始人。

2019年8月，获2019福布斯全球亿万富豪榜第1511名。

2019年胡润百富榜排名第214位。10月28日，胡润研究院发布《2019胡润80后白手起家富豪榜》，吴忌寒以170亿元排名第7。2019福布斯中国400富豪榜排名第200位，财富值127.3亿元人民币。

51%攻击

竞争是为了从中获益，而攻击是为了摧毁这条链。

竞争是合理的，即使你拥有超过51%的算力，只要你在规则允许的范围下，正常出块，正常挖矿，那么这就是正常的竞争，仍然是以谁先出块，谁的链最长为判断标准，不能算攻击。

但是，像在ABC与BSV的算力大战中发生的事，比如BSV最初的宣传就是要“用算力摧毁BCHABC”，“让BCH上两年没有任何交易”（虽然最终都没有达成），这种行为就是明确的攻击，而不是单纯的竞争。

51%攻击--结果

大型加密货币更安全

到目前为止，我们已经利用比特币来说明51%的攻击是如何发生的。然而，虽然在技术层面上比特币易受攻击，但在更实际的层面上，由于三个原因，它不太可能成为这个受害者：

成本　　矿池　　Nice Hash

1、成本

比特币网络规模巨大，想要获得足够用于攻击的哈希算力，需要相当大量的资金投入。

据Crypto51称，对比特币进行长达一小时的黑客攻击需要花费237,941美元。 对以太坊进行攻击的成本同样令人望而却步 ——将花费74,837美元。

51%攻击--结果

大型加密货币更安全

3、NiceHash

NiceHash是世界上最大的加密货币挖矿算力市场。
据Crypto51估计，NiceHash可以产生的总功率不到比特币网络总功率的百分之一。 以太坊是5%，比特币现金是2%。 所有主流币的百分比都保持相似的低百分比。

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$108.47 B	SHA-256	53,813 PH/s	*$528,105*	1%
Ethereum	ETH	$20.46 B	Ethash	231 TH/s	*$149,929*	5%
Bitcoin Cash	BCH	$7.80 B	SHA-256	3,795 PH/s	*$37,247*	13%
Litecoin	LTC	$3.04 B	Scrypt	249 TH/s	*$33,817*	6%
Monero	XMR	$1.69 B	CryptoNightV7	576 MH/s	*$11,616*	13%
Dash	DASH	$1.37 B	X11	2 PH/s	*$11,881*	25%
Ethereum Classic	ETC	$1.04 B	Ethash	15 TH/s	*$9,668*	73%

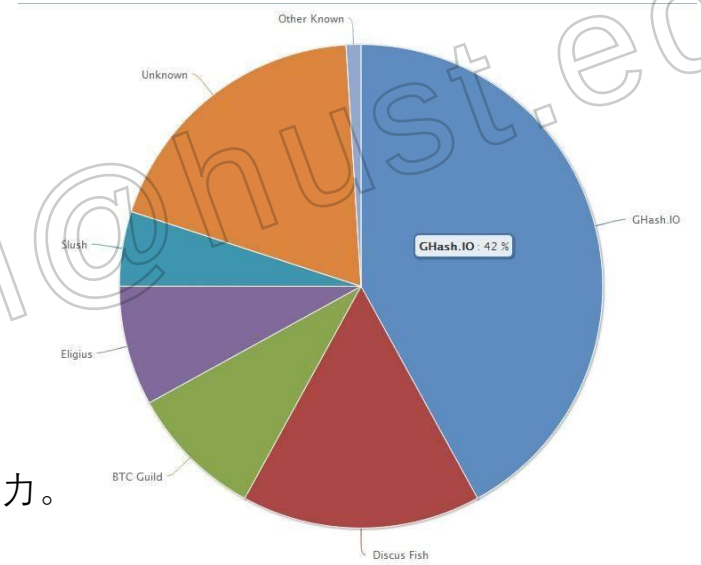
因此，即使是武器化的NiceHash也没有足够的力量对主流币进行51％的攻击。

51%攻击--结果

大型加密货币更安全

2、矿池

如今，最大的加密货币的矿池分布广泛。



2014年，Ghash.io大概掌握量51％的比特币哈希算力。

51%攻击--结果

小币种面临风险

就像市值排名前十的币种，对其发动攻击基本都是天价，而排名再往后就不好说了。其对应的NiceHash百分比也开始增加。 也有一些较大币种的百分比令人担忧。 以太坊经典为82%，门罗币79%.....

PoW 51% Attack Cost

This is a collection of coins and the theoretical cost of a 51% attack on each network.

Learn More

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	$108.47 B	SHA-256	53,813 PH/s	*$528,105*	1%
Ethereum	ETH	$20.46 B	Ethash	231 TH/s	*$149,929*	5%
Bitcoin Cash	BCH	$7.80 B	SHA-256	3,795 PH/s	*$37,247*	13%
Litecoin	LTC	$3.04 B	Scrypt	249 TH/s	*$33,817*	6%
Monero	XMR	$1.69 B	CryptoNightV7	576 MH/s	*$11,616*	13%
Dash	DASH	$1.37 B	X11	2 PH/s	*$11,881*	25%
Ethereum Classic	ETC	$1.04 B	Ethash	15 TH/s	*$9,668*	73%

51%攻击--结果

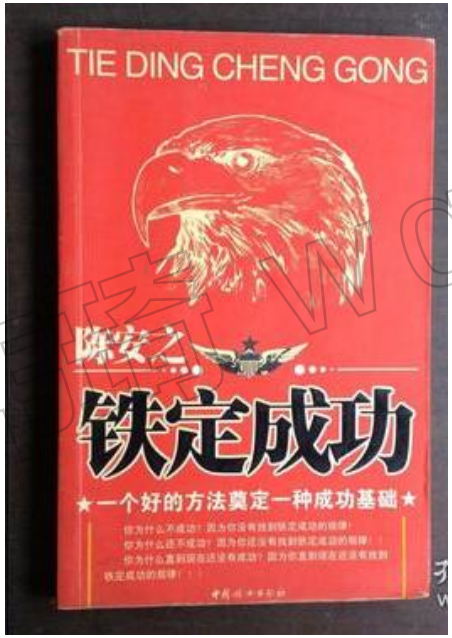
比特黄金遭受攻击

2018年5月比特币黄金遭遇51%的攻击时，小币种的脆弱性成为焦点。***比特黄金 ——来自2017年比特币的硬分叉 - 当时甚至出现不到六个月。***

以至于该项目的发言人爱德华·伊斯克拉尔必须告知所有可以交易比特黄金的交易所，将确认数从5个增加到50个，并手动审查大额交易是否存在可疑活动。

矿池会联手攻击比特币系统吗？

51%算力是铁定成功，而研究指出，只要算力达到全网30%就有机会成功，那么，会不会出现大的矿池联手呢?



算力大佬们发现老老实实挖矿收益更高，因此不会主动成为作恶节点。同时出现这样一个事件，当某矿池算力达到40%，矿工会自动切换到其他矿池，并不是良心或者信仰维护算力均衡，而是怕自己手里的币贬值。

一定是51%吗？--分叉概念

当出块频率过高，就会出现分叉过多的情况，导致算力分散，即便没有51%的算力，20%或者30%都有可能控制最长链的产生，比特币大约每10分钟出一次快，碰撞分叉概率较小，因此，出块速度慢不见得是劣势。

区块链核心技术——分布式结构

GLOBAL BITCOIN NODES DISTRIBUTION

Reachable nodes as of Wed May 11 2016 17:39:05 GMT+0800 (CST).

6318 NODES

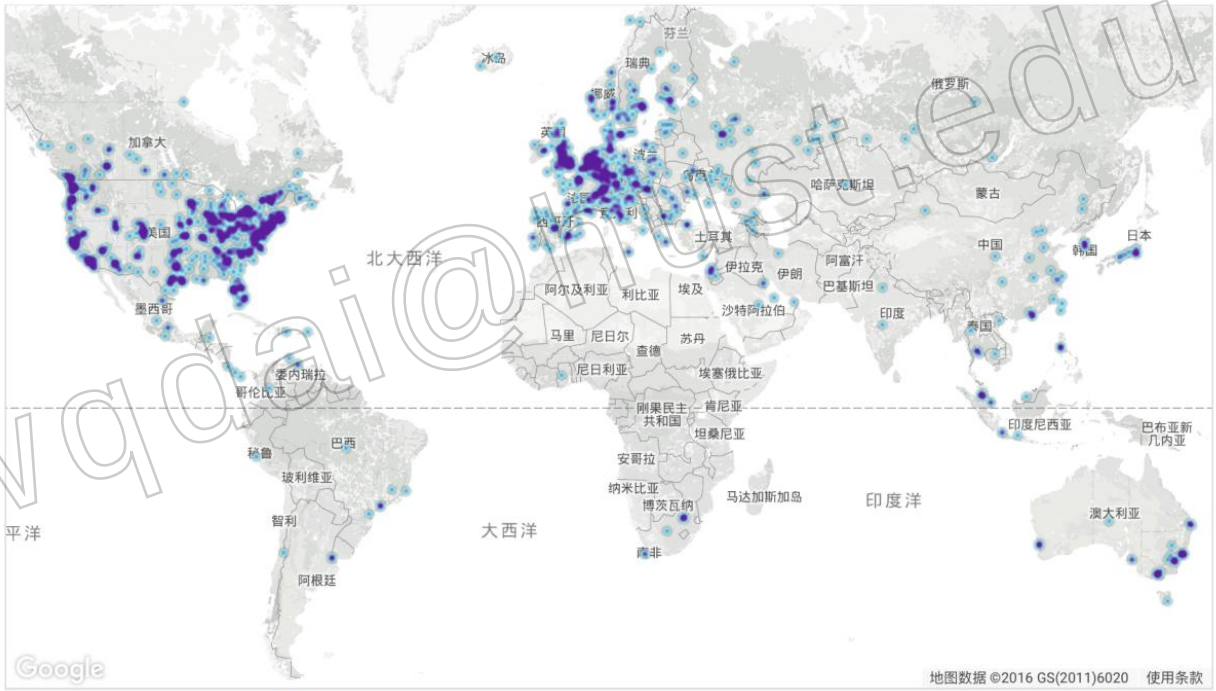
24-hour charts »

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	United States	2177 (34.46%)
2	Germany	798 (12.63%)
3	France	455 (7.20%)
4	Netherlands	306 (4.84%)
5	Canada	274 (4.34%)
6	United Kingdom	252 (3.99%)
7	Japan	206 (3.26%)
8	Ireland	178 (2.82%)
9	Russian Federation	153 (2.42%)
10	n/a	126 (1.99%)

More (85) »

全球比特币区块链节点分布



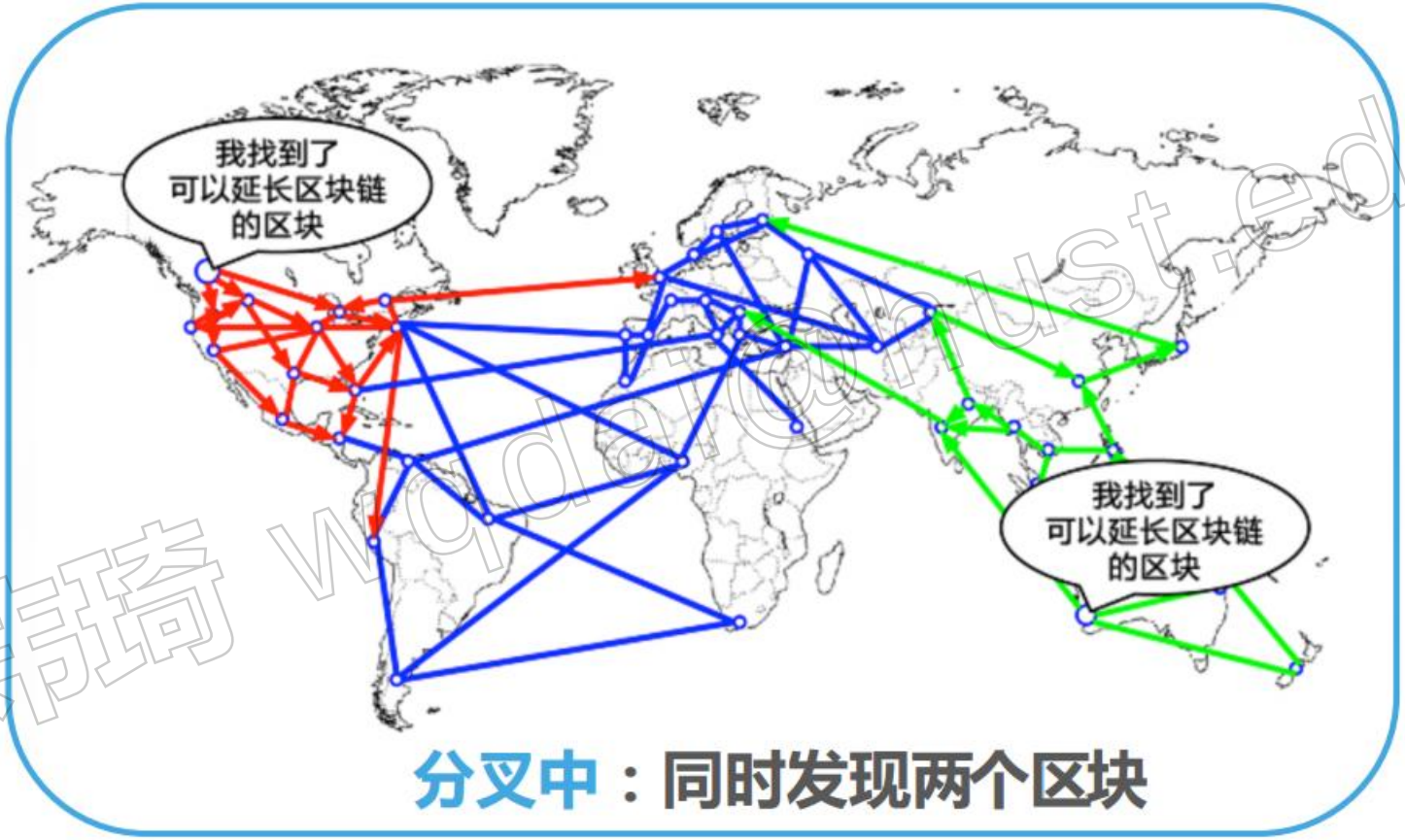
Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

注释：数据截至2016年5月11日

分叉处理

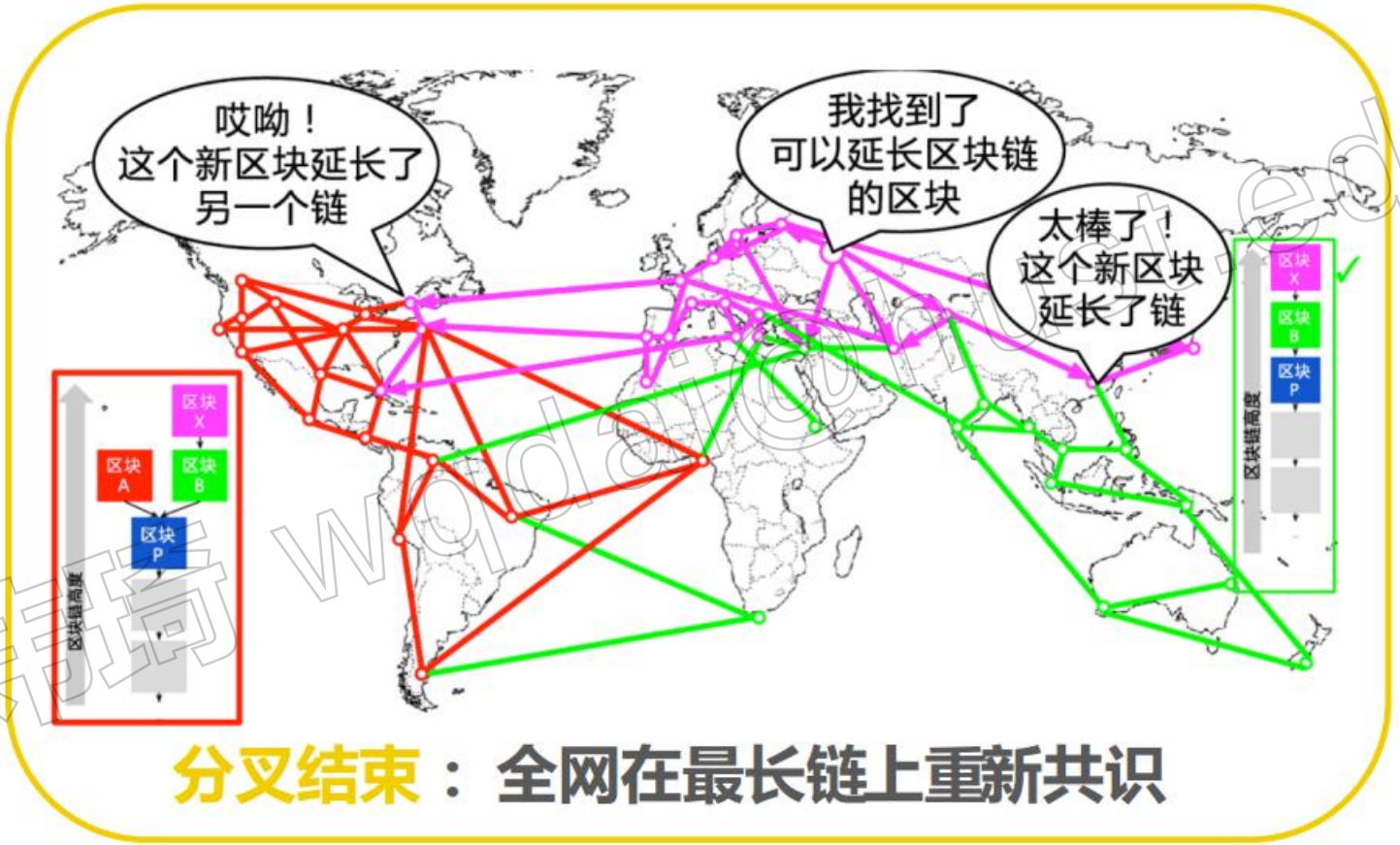
分叉处理



分叉处理

分叉处理

分叉处理



工作机制分析

- **其他问题**
  - 比特币会一直增加下去，岂不是会严重通货膨胀？
    - 随着账簿的增加，奖励逐渐减少，总的比特币数量有限
  - 没有奖励后，就没人做矿工了，岂不是没人帮忙确认交易了
    - 矿工的收益会由挖矿所得变为收取手续费
  - 矿工如果越来越多，比特币生成速度会变快吗
    - 矿工数量越多，编码器效率越低，保证比特币产出效率一定
  - 如果泄露了某个人的代号，账簿又是公开的，岂不是他的所有账目都查出来了？
    - 每个人可以有多个保密印章，建议交易一次换一个保密印章。

比特币的分叉

我们日常在用的手机APP，系统更新犹如家常便饭，偶尔还会上几个新功能。而这看似简单的更新在比特币系统中却是难上加难，为什么呢?

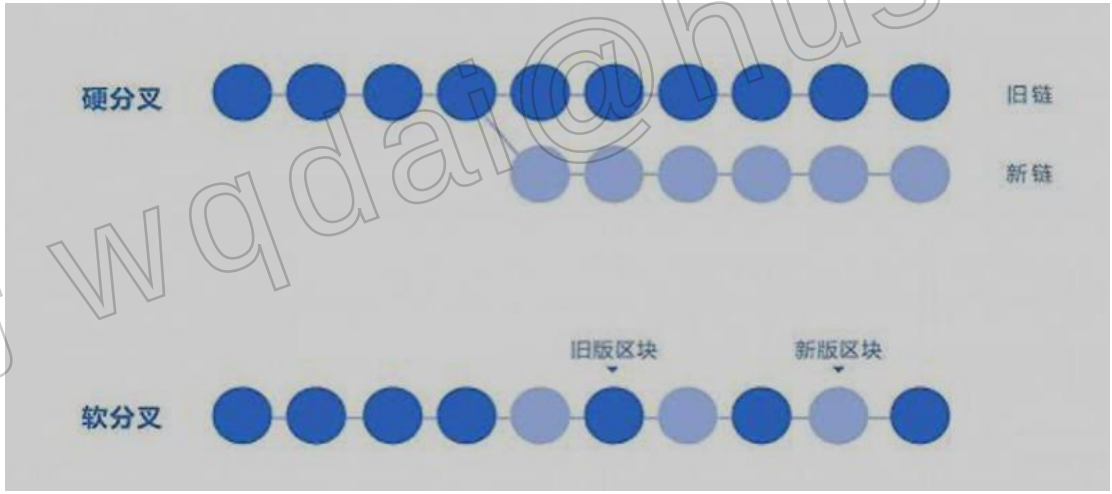
比特币的分叉

软件由于方案优化、BUG修复等原因进行升级是一种非常常见的现象。如手机应用等传统软件，升级非常简单，只需厂商发布，用户接受升级即可。

但是对于比特币这种去中心化的系统，升级是非常困难的，需要协调网络中每个参与者。软件升级意味着运行逻辑的改变，但是在比特币中，升级必然会导致不同节点在一定时间内运行不同的版本，于是就会产生分叉。

软分叉和硬分叉

分叉主要包含软分叉和硬分叉两种。如果比特币升级后，新的代码逻辑向前兼容，即新规则产生的区块仍然会被旧节点接受，则为软分叉；如果新的代码逻辑无法向前兼容，即新产生的规则产生的区块无法被旧节点接受，则为硬分叉。



软分叉

软分叉由于向前兼容，新旧节点仍然运行在同一条区块链上，并不会产生两条链，对整个系统影响相对较小。到目前为止，比特币发生过多次软分叉，BIP-34，BIP-65，BIP-66，BIP-9。

软分叉过程

以BIP-34为例，简单说明软分叉的过程。
在旧版本中，存在一个无意义的字段＂coinbase data＂，矿工不会去验证该字段的内容。BIP-34升级的新版本则要求该字段必须包含区块高度，同时将版本信息由“1”修改为“2”。该升级共包含三个阶段。

软分叉过程-第一阶段

第一阶段：矿工将版本号修改为“ 2 ”，此时所有矿工验证区块时，按照旧的规则验证，即不关心“ coinbase data ”字段内容，所有矿工不论以新规则还是旧规则打包区块，均可以被整个网络接受。

第二阶段：如果最新产生的1000个区块中，版本号为“ 2 ”的区块个数超过75%时，则要求版本号为“ 2 ”的矿工必须按照新的规则打包区块，升级的矿工收到版本号为“ 2 ”的区块时，只会接受“ coinbase data ”字段包含区块高度的区块，对于版本号为“ 1 ”的区块，仍然不校验该字段并接受。

第三阶段：如果最新产生的1000个区块中，版本号为“ 2 ”的区块个数超过95%,则升级的矿工只接受版本号为“ 2 ”的区块，并会对“ coinbase data ”字段进行校验，版本号为“ 1 ”的区块则不被接受，以此来逼迫剩余少量矿工进行升级。

比特币科普-“第一次”分叉

凡是都有第一次，让我们看看比特币第一次分叉是怎么回事儿呢?

第一次软分叉

比特币的第一个软分叉协议升级后禁用了协议特性的OP_RETURN。从技术上讲，这是一个UASF，但在早期，实际上只是中本聪在制定协议规则。升级没有导致区块链分叉。

第一次硬分叉

比特币的第一次硬叉协议升级增加了一个新功能OP_NOP，而且也是由中本聪指定的。然而，并不是所有人都认为这次升级实际上是一个硬分叉。从结果来看，它没有导致区块链分叉。

硬分叉

硬分叉就像议会表决一样，会出现“吵翻天”的情况。

硬分叉修改余地很大，方案设计比较简单，但是如果整个网络中有两种不同的意见，就会导致整个生态的分裂。

硬分叉

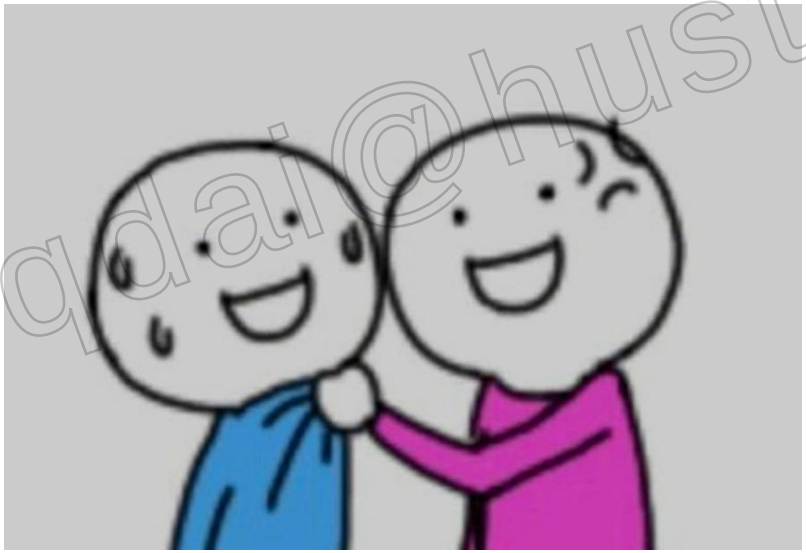
如果最新产生的1000个区块中，版本号为“ 2 ”的区块个数超过95%,则升级的矿工只接受版本号为“ 2 ”的区块，并会对“ coinbase data ”字段进行校验，版本号为“ 1 ”的区块则不被接受，以此来逼迫剩余少量矿工进行升级。

硬分叉

硬分叉相比软分叉则会“暴力”很多，由于不向前兼容，旧版本矿工无法验证新版本的区块而拒绝接受，仍然按照旧的逻辑只接受旧版本矿工打包的区块。而新版本产生的区块则会被新版本矿工接受，因此新版本矿工保存的区块会和旧版本矿工保存的区块产生差别，即会形成两条链。

硬分叉--案例

当前比特币影响最广泛的硬分叉事件即为2017年8月1日的硬分叉，比特币由一条链分叉产生一条新的链“比特现金（*Bitcoin Cash,BCH*）”。这是一场开发者与矿工之间没有硝烟的战争！



下面我们就来还原这次事件的原委。

硬分叉--案例

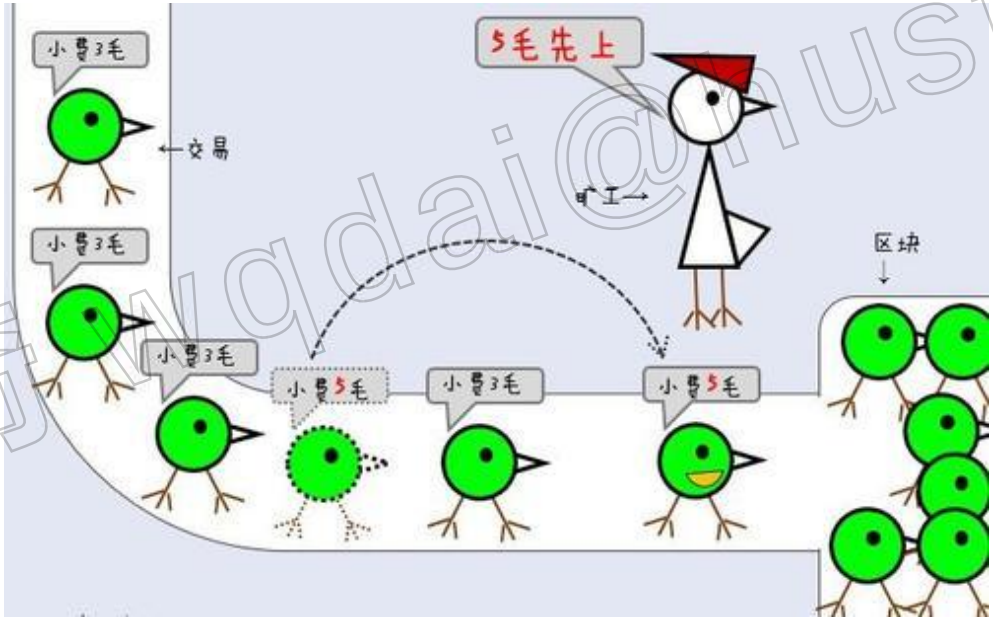
这次硬分叉的起因是开发者与矿工在比特币扩容方案上的分歧。比特币区块大小为1MB,按照每10分钟一个区块的速度，全球每秒只能完成大约7笔交易。比特币发展初期，1MB的区块足够打包出块间隔内产生的所有交易，但是在比特币如此火爆的今天，这种处理速度显然达不到要求。

硬分叉--案例

扩容方案的想法比较直接，既然现在因为区块太小而导致交易处理速度低下，那就直接扩大区块的容量，使其能容纳更多的交易。原来1MB不够用，那么就扩成2MB、8MB，甚至直接扩到32MB.

硬分叉--案例

隔离见证方案的想法是，将交易分为两部分，一部分是交易信息，另一部分是见证信息，这两部分信息分开进行处理。好比一辆车太小，要搭车的人太多，于是让车上所有人将背包和行李放在另一辆跟着的货车上，这样原来的车就可以容纳更多的人了。



硬分叉--案例

支持扩容方案的主要是矿工们。采用扩容方案，矿工可以在每个区块中包含更多的交易，从而获取更多的手续费，然而若使用隔离见证的扩容方案，小额的交易将不通过区块确认，矿工的手续费收益会大幅降低，因此矿工更倾向于支持扩容方案。

硬分叉--案例

隔离见证方案的支持者主要是比特币开发团队的部分核心成员。他们认为，扩容方案是一个“扬汤止沸”的方案，毕竟不可能无限制地对区块的容量进行扩大。同时，区块的变大会使得挖矿的门槛提高，从而降低普通矿工的参与度，导致比特币系统的去中心化程度减弱。

硬分叉--案例

2016年2月和2017年3月，争议双方两次进行商讨，希望双方“握手言和”，接受一个折中的方案。该方案中，区块容量将会被扩大到2MB，同时也对比特币部署隔离见证的方案。**但是，由于期间有参与方反悔或者反对，导致最终没有达成共识，这也给“硬分叉”埋下了导火索。**

在2017年8月1日，比特大陆投资的矿池ViaBTC团队，采用比特大陆提出的UAHF（用户激活的硬分叉）方案，挖出了第一个区块，对比特币区块链进行了硬分叉。自此，与比特币竞争的分叉币比特币现金诞生。比特币现金区块链的区块容量达到了8MB，且没有采用隔离见证方案。可以说这是一次矿工的胜利。

硬分叉--案例

硬分叉后称为比特币现金（*BCH*），随后比特币黄金（*BTG*）、比特币钻石（*BCD*）、超级比特币（*SBTC*）等密码货币出现。

区块链核心技术--分布式结构

传播

区块链中每一笔交易信息由单个节点发送给全网所有节点。因此，信息拦截者无法通过拦截某个信息传播路径而成功拦截信息，因为每个节点均收到了该信息。另外采用非对称加密的数学原理，只有拥有该交易信息私钥才能打开信息读取内容，保证了信息安全性。

记录

区块链构建了一整套协议机制，让全网络的每个几点在参与记录数据的同时，也参与验证其他节点记录结果的正确性。只有当全网大部分节点（甚至所有节点）都确认记录的正确性时，该数据才会被写入区块。

存储

在区块链的分布式结构的网络系统中，参与记录的网络节点会时时更新并存放全网系统中的所有数据。因此，即使部分节点遭到攻击或被破坏，也不会影响这个数据系统的数据更新和存储。