# 公链技术挑战及 GateChain 技术创新研究报告

作者：Gate.io 研究院 Eric、Guin、Caroline、Cherry、Jame、Tlntin、Isla、Jill

## 摘要

作为现今社会最具颠覆性的核心技术之一，区块链将有可能改变人们传输价值的方式，然而其崛起却面临重重技术挑战。区块链公链中，从理论上又受限于“分布式不可能三角”，难以同时实现一致性、可用性以及分区容错性三大要素。区块链公链在交易性能、节点去中心化，回滚问题、防攻击、激励、匿名隐私等问题上面临诸多严峻挑战。

本文将带领读者从基础概念出发，共同探讨公链技术所面临的挑战。我们将以比特币和以太坊为例，浅析其为克服去中心化挑战所提出的提案。同时，我们也将一窥交易所公链的技术特点及性能体现，介绍 GateChain 在公链交易安全方面的技术创新，帮助广大用户从技术角度进一步了解公链研发的重点难点。

- 公链技术最为关键的技术突破点即实现去中心化（Decentralization）。
- 从理论上看，去中心化系统受“分布式不可能三角”限制，只能从分区容错性（Partition Tolerance）、可用性（Availability）、一致性（Consistency）三者中同时实现其二。
- 目前与去中心化关联最为紧密、最迫于解决的问题主要包括交易处理能力（体现在 TPS 高低）、回滚问题、防攻击问题、激励问题、以及匿名隐私问题等。
- 比特币和以太坊作为最早的、使用人数最多的公链，存在上述问题；而相应的社区和团队也对其面临的挑战进行了创新和升级。

- 加密货币交易所为早日实现去中心化交易，纷纷投入公链研发。经过对比，GateChain 不仅具有创新性的安全解决方案，其性能亦优于主流交易所公链。

# 1 从公链“不可能三角”到去中心化挑战

自比特币诞生以来，关于区块链技术的进展和突破便不断涌现。以太坊的发布标志着区块链进入 2.0 时代，随后更有 EOS 等优秀公链逐渐进入我们的视野，在寻求技术突破的基础上，旨在为未来打造更完整的公链生态。

众所周知，区块链公链技术之所以难以突破是由于可扩展性（Scalability）、安全性（Security）以及去中心化（Decentralization）三者无法同时实现，又称区块链的“不可能三角”；其中，各大公链，尤其是对扩容性(即可扩展性)及去中心化方面做了许多努力和创新，试图寻求不可能三角的最优解。


*来源: Gate.io 研究院*

## 1.1 扩容性

提到扩容性，我们不得不提加密货币的始祖——比特币。

作为首个区块链支付网络和新型的加密数字货币，比特币（Bitcoin）采用了分布式账本技术（Distributed Ledger Technology，即 DLT）中的区块链结构，通过“工作量证明”（Proof of

Work，即 PoW，下文将详细介绍）机制巧妙地解决了信息传输的信任和储存问题，构建了首个能够进行点对点价值传输的去中心化网络系统。

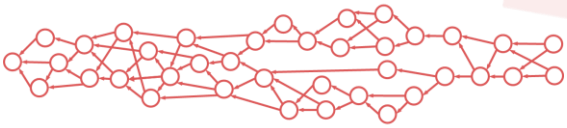
比特币将区块[1]的大小设置为 1M，使得更多节点能够加入到网络中，一方面网络更为去中心化，另一方面也提高了其安全性。

然而，受限于区块大小等原因，比特币网络每秒仅可处理 7 笔交易（7 transaction per second，即 7 TPS）。比特币在交易高峰期容易出现严重的拥堵，转账交易的费用也会大大增加。

面对这一问题，比特币现金（Bitcoin Cash）和比特币闪电网络[2]（Lightning Network）试图通过不同的方式提高比特币的扩容性。在这之后，其他公链提出了另一种分布式账本技术概念——有向无环图（Directed Acyclic Graph，即 DAG）来替代区块链结构，以提高网络的性能，如加快交易处理速度等。

**图 1 Blockchain 结构示意图**

**图 2 DAG 结构示意图**



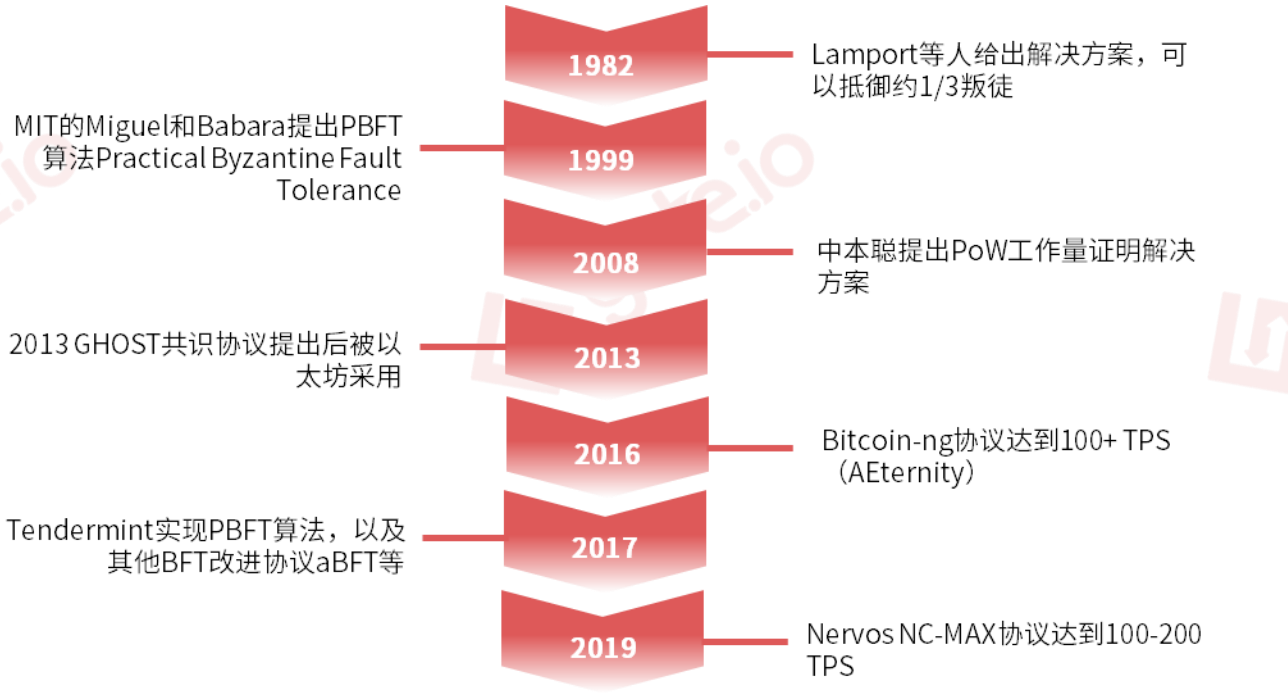
*来源：Gate.io 研究院*

在区块链结构中，交易被打包进区块中，每一个区块与前一个区块相连，形成一套单一的“账本”，交易只能按顺序逐一进行，不能同时处理，即并发性[3]低。DAG 结构中，单元从区块变成了 TX（交易），省略了打包多笔交易成块这一步，并且可以同时处理多笔交易，从而能够突破性能瓶颈，达到更高的 TPS。然而，由于 DAG 结构的并发性强，其交易的顺序难以确定，容易引发双花问题[4]。但从整体来讲，DAG 结构不失为提高去中心化网络扩容性的可行方式。

## 1.2 去中心化

除了扩容问题难以解决外，网络的去中心化一直是区块链社区所追求的，甚至将其视为与加密货币并存的特质。以太坊创始人 Vitalik Buterin 在早期的文章中写到‘去中心化’有三个优点分别为：容错性（Fault Tolerance）、防攻击性（Attack Resistance）、抗勾结性（Collusion Resistance）。早在上个世纪 80 年代，由 Leslie Lamport 为首的三位作者以“拜占庭将军问题[5]”比喻去中心化的决策过程中会遇到的问题。若分散在敌人四周的各个将军们中存在叛徒，或信息传递的过程中出现意外（如信使是叛徒，篡改信息；或信使在传信途中被杀害），则将军们无法达成共识。

Lamport 等人在其论文中指出要解决拜占庭将军问题，我们不需要使每个将军所获得的消息完全一致，只需要大概一致即可。论文中提出了解决方案（Byzantine Fault Tolerance[6]，即 BFT），但只有当叛徒数量少于总数的三分之一时才可实现。后来在 1999 年，Miguel Castro 与 Barbara Liskov 两人提出了实用拜占庭容错算法[7]（Practical Byzantine Fault Tolerance algorithm，即 pBFT），然而该算法只适用于节点数量较少的网络，若节点增加，需要处理的信息呈指数增长，使网络整体的沟通成本过高。




*来源: Gate.io 研究院*

随后，在 2008 年，中本聪提出了“中本聪共识”（Nakamoto Consensus，即 NC），分为四大部分。其中，帮助达成网络共识的“工作量证明[8]”机制（Proof of Work，即 PoW），通过增加个体发送信息的成本，降低其发送信息的速率，保证一个时间内只有一个(或很少)的个体在进行广播而不受干扰，从而解决了信任问题。

然而，PoW 共识机制仍存在一些缺陷，其中一个缺点即能源消耗问题，例如比特币挖矿[9]需要消耗大量的电力。考虑到所存在 PoW 的缺陷，在 2011 年，名为 QuantumMechanic 的用户在比特币论坛上提出采用“权益证明[10]”（Proof of Stake，即 PoS）的想法。在 PoS 机制中，持有代币越多者则对网络规则有更多的决定权。尽管这一机制在很大程度上降低了能源的消耗，但其中心化程度也因此增高；同时，由于创造分叉链的的成本比 PoW 低，PoS 出块节点更容易被长程攻击。

下表对 PoW 和 PoS 机制进行了简单的对比。

## PoW 与 PoS 对比

| PoW | PoS |
| --- | --- |
| 算法简洁容易实现 | 算法复杂度高 |
| 非常消耗能源 | 极少消耗能源 |
| 去中心化程度高 | 中心化程度高 |
| 无需授权随时加入 | 需要授权或选举 |
| 延迟高 | 低延迟 |
| 51%攻击[11] | BFT 1/3 攻击 |
| 有孤块问题 | 共识协议容易排除孤块 |
| 确定性差，需要多个确认 | 确定性强，甚至一个确认就可以 |
| TPS 低（通常低于 100） | TPS 高（可以达到数千） |
| 不易受到双花影响 | 易受双花影响 |
| 长程攻击（Long Range Attack）难 | 长程攻击（Long Range Attack）容易 |

*来源: Gate.io 研究院*

为了克服这些缺点，在“不可能三角中”拓展极限和寻找平衡，许多公链团队研发出了更多共识算法，而这一努力仍在进行中。正如上文所说，去中心化是区块链领域中最为核心的价值。如何通过解决公链中的各个技术难题从而实现真正的去中心化，正是对公链技术最大的挑战。

## 2 去中心化问题

尽管有比特币、以太坊等优秀公链先驱，公链的研发依然面临重重挑战。公链的交易处理能力及去中心化程度为其研发技术的核心，除此之外，共识确定性、验证节点防攻击、激励和隐私安全等问题的解决同样至关重要。我们将会在下文对每个技术难题进行深入浅出的分析，帮助

用户从技术层面出发理解公链研发的重点难点，加深用户对公链技术的认识。

## 2.1 去中心化的重要性

传统中心化系统存在信任问题，而且维护安全的成本很高，只要攻破主系统就可以盗取系统内的所有信息。

而去中心化以公信力取代了中心化当中具有承担这份公信力的单个中介，不需要依赖第三方而提高了自由度，私钥[12]掌握在自己手中，没有人知道你的资金，并且因为节点分散，攻破单个节点无法完成资金的盗取，安全性更高。因此，实现去中心化的意义重大。

## 2.2 造成中心化的原因

然而，在实际情况下，由于种种问题，公链难以实现完全去中心化。其中，许多公链中常出现的出块节点[13]中心化和非出块全节点[14]中心化问题也影响去中心化的实现。

以 EOS 为例，虽然 EOS 是传统公链中创新性较强的项目，通过采用 DPoS[15]共识机制，大幅度提升公链的 TPS，但是在长时间的运行过程中，追求高 TPS 的 EOS 也出现了比较多的问题。EOS 为了实现较高的 TPS，仅设置了 21 个验证节点，这也就导致了出块节点中心化的问题，还有就是 EOS 本身协议并未涉及惩罚机制，仅靠社区惩罚机制难以起到实质性的作用，如此一来有可能会发生节点贿选，交换选票等问题。

EOS 设置了 21 个验证节点的同时，有较高的区块产出频率，由此产生的数据量较大，同时因为其智能合约系统的较高要求，安装全节点会造成非常大的计算机性能要求。因此，用户很少会选择设置全节点，这也会造成非出块全节点中心化的问题。

## 2.3 去中心化问题的主要挑战

虽然去中心化实现困难，但是由于去中心化能够解决中心化系统下存在的问题，各公链都追求去中心化系统的建设。但目前去中心化面临着非常多的挑战，包括但不限于以下几个问题：

① 由单节点吞吐量、节点数量增多但缺少并行写入能力引发的 TPS 问题

② 由节点故障以及网络无法达成共识引发的回滚问题

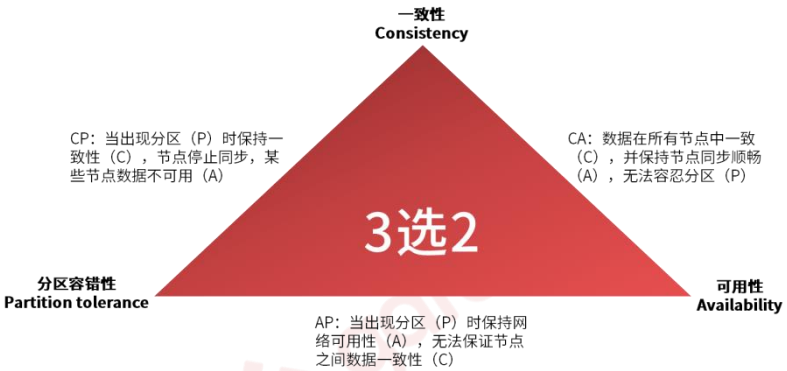
③ 由节点被攻击、数据篡改以及作弊引发的防攻击问题

这几个方面的问题都会使网络去中心化程度受到影响，下文将会着重对这些问题分析探讨。

## 2.4 去中心化的影响因素

区块链技术的初衷是为了实现去中心化，但因为不可能三角的问题，目前还没有一个分布式系统能够完美实现去中心化。

去中心化不可能三角（下文简称 CAP 理论）是上文区块链不可能三角的去中心化一角，包括一致性、分区容错性和可用性。一个网络只能在这三个特性中选择其中两个特性。当网络选择了一致性[16]时，那么其势必要在分区容错性[17]和可用性[18]上作出选择，三者不可兼得。



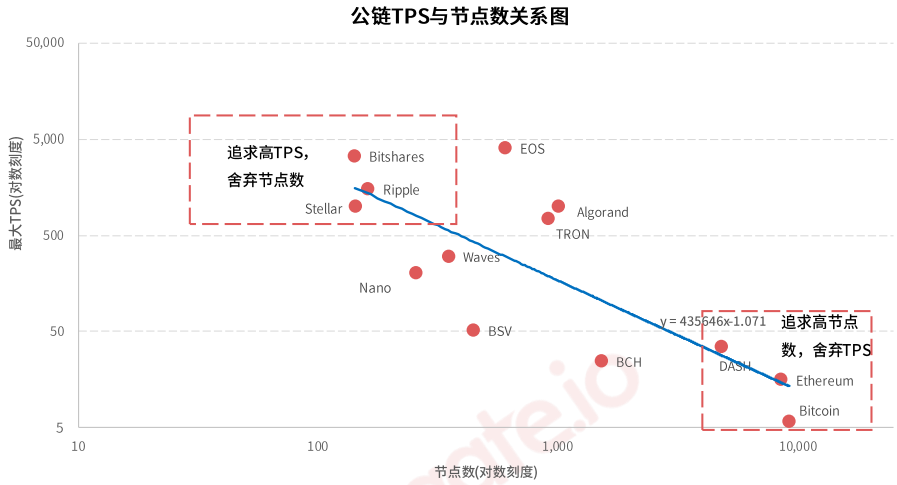

*来源：Gate.io 研究院*

目前影响网络去中心化的主要因素有 TPS、回滚、防攻击、激励和匿名，下文将对这五个维度

具体如何影响网络去中心化展开讨论。

### 2.4.1 TPS（每秒事务处理量/系统吞吐量）

TPS 是公链性能的直观表现，许多公链都会追求高 TPS，但 TPS 并非越高越好，很多公链选择高 TPS 往往意味着牺牲去中心化程度。




*来源：Gate.io 研究院，其中 TPS 数据为公链公开披露数据但未经检测*

上图为各公链 TPS 和节点数的关系图（图中横纵坐标轴均已作底数为 10 的对数处理）。由图可知，当网络选择高节点数时，则会降低网络最大可达的 TPS；相反，当网络选择高 TPS 时，其网络节点数也会减少，降低去中心化程度。对于公链而言，在 TPS 和节点数上目前没有“最优解”，只能实现各自的“满意解”，单纯为了追求 TPS 而降低去中心化程度并非好的方案。

### 2.4.2 回滚问题

回滚问题是指由于网络中记账过程发生共识冲突，回滚恢复到最近一个共识的状态。由于 CAP 理论中一致性与可用性的冲突，实际上 NC 和 BFT 共识在回滚问题上有着不同的表现。这是因为不同机制的共识确定性[19]是不同的。

比特币所使用的 NC 共识机制拥有概率确定性。比特币共识中规定工作量最大的链即为主链，也就是说想要交易不被篡改首先要保证正常的主链不会因为遭受恶意攻击而被取代，在概率确定性当中，交易区块埋得越深，交易被撤销的可能就越小，所以这也是为什么包含交易的区块必须要在此基础之上当区块链深度达到 6 的时候才会被确定交易的完成，以此降低交易被撤销的可能性。

然而 BFT 拥有的共识确定性就是绝对确定性，这种不依赖工作量证明的方式除了解决能源消耗外，还解决了 NC 中交易确认，交易分叉，性能较低等问题。

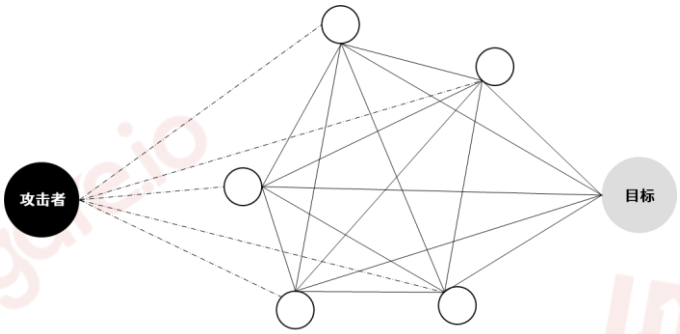
看起来绝对确定性比概率确定性更优，但是许多项目还是选择使用 PoW 机制，这是因为实际上还要考虑到应用场景等一些其他因素，可以参考分布式网络中的 CAP 理论来进行简单解释：在同样保证分区容错性的情况下，选择可用性则无法保证一致性。追求可用性的系统即使收到未共识的交易信息提交，同样会继续运行，而追求一致性的系统如果发现共识无法达成一致时会因为系统追求一致性而迫使系统停止运行，不让非共识信息通过。

### 2.4.3 防攻击问题

任何展望都是基于安全性之上的，作为区块链去中心化发展中最重要的一环常面临一系列的攻击，常见的攻击包括 DDoS 攻击、女巫攻击和长程攻击，无利害关系问题等。

- DDoS 攻击

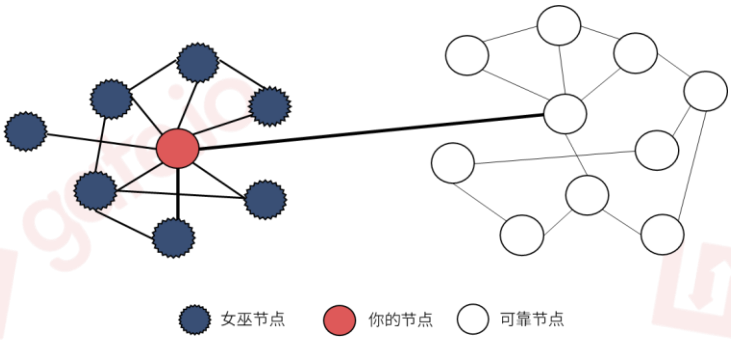
DDoS 攻击是目前对互联网信息安全威胁最大的恶意攻击之一，区块链网络同样受到 DDoS 攻击的威胁。DDoS 攻击者侵入控制大量的服务器形成僵尸网络，利用这些服务器对区块链共识节点同时发动攻击致使共识无法达成，造成网络瘫痪，甚至可以在正常共识节点瘫痪的情况下，冒充共识节点伪造数据。因此对于共识节点的隐藏和保护至关重要。



来源：Gate.io研究院

- 女巫攻击

女巫攻击是常见的一种攻击形式，其通过创建虚假节点对网络造成危害。比如在社交媒体上的僵尸账号，通过扮演不同的角色来达到欺骗他人并损害他人利益的目的。

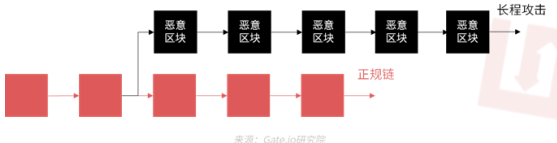


来源：Gate.io研究院

针对此类攻击，比特币网络采取的规避方式是设定一个网络连接数，在只能和 6 个节点进行联系的情况下，受到攻击的可能性就会比较大。另外比特币网络通过增加女巫节点的成本来减少被攻击的可能性，算法中规定当一个节点的区块工作量不足时，比特币网络不会接受该节点的数据。

- 长程攻击

纯 PoS 机制还面临着长程攻击的威胁。长程攻击会出现的根本原因来自于 PoS 机制本身的设定。



来源：Gate.io研究院

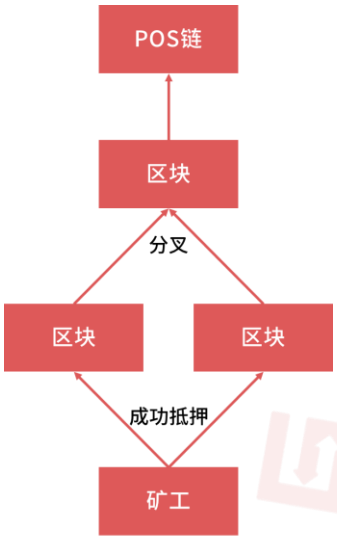
由于股权证明机制所需算力成本很低，即使重新计算大量区块也不需要很大的工作量，假

如一个攻击者获得了一些在过去某个历史时间点拥有大量股权的秘钥，那么攻击者完全可以在那个时间点开始分叉攻击而不用付出太多代价，新来的节点因为主观性而无法判断哪条是主链，进而对网络造成危害。

对于长程攻击，Cosmos 通过设置较长时间的抵押撤回等待时间来规避此危险。除此之外，还可以通过设置 checkpoint 检查点，不允许回滚一定长度的区块来解决长程攻击问题。

- 无利害关系问题

除了上述的攻击方式，由于无需算力，签名廉价等缘故，矿工可以在所有同一层级的分叉上同时签订多份协议，为多条链出块，这样任意一条链最终胜出自己收益都有保障，无利害关系（nothing-at-stack，下文简称 NAS）问题也是 PoS 机制中的一个典型问题。这样恶意分叉很有可能造成一些虚假，破坏性交易混杂，严重危害区块链的安全。



来源：Gate.io研究院

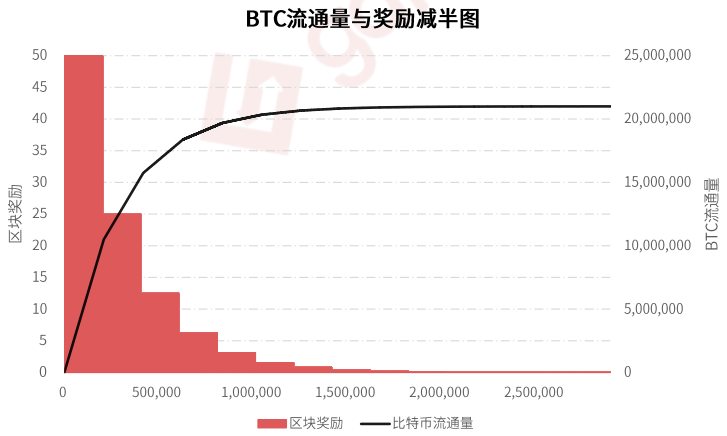
针对 NAS 攻击，目前已有解决方案是设置 Slashing 惩罚机制，包括 Tendenmint 和 Tezos 都采用此惩罚机制；同时要求矿工在挖矿前需要进行抵押，目前比较知名的 Cosmos 公链便是通过此方法防止 NAS 攻击。

### 2.4.4 激励问题

此外，网络的激励机制也会对整体网络去中心化产生较大影响。无论任何一个体系下，有效的激励机制都是推动发展、增加生产力不可或缺的一部分。比如说在公司这一体系中，升职加薪就是一种激励机制，可以增加员工动力，推动公司更好的发展。区块链最终是为了实现完全去中心化，所以不可能像企业一样，人为地提供激励机制。因此，如何设定区块链当中的激励机

制显得格外重要。比如说，比特币的激励机制是挖矿，如果没有“挖矿可以得到比特币作为奖励”这种机制存在，矿工们不会愿意耗费大量的算力去维护比特币网络，导致算力减少，很容易出现算力攻击，严重威胁到比特币网络的安全性。

激励机制的设计需要考虑算力与代币通胀之间的平衡。以 BTC 为例，中本聪在设计比特币时，规定了比特币会随着挖矿进度而逐渐减产（具体减产影响可参考 Gate.io 研究院“发布未来大事件对比特币价格影响预测”）。这一规定导致越到后期比特币矿工获得奖励的越少，提供的算力保护越薄弱，虽然网络交易手续费可以给矿工提供部分奖励，但跟挖矿初期的区块固定奖励相比占比很低。当 BTC 不再产出时，比特币网络的保护将会变得很弱，此时容易出现 51%攻击。




*来源：Gate.io 研究院*

由上图可以看出，BTC 是递减式的激励机制。针对挖矿激励危机，增加激励是一个可行处理方式。但如果发行的代币本身没有上限数量，那么持续挖掘下去，代币越来越多就会导致代币通胀。所以如何平衡算力保护与代币通胀对区块链未来的发展有着重大的意义。

针对网络激励逐渐枯竭造成的网络保护减弱的问题，Gate.io 研究院认为可以从升级产量和改用 PoS 算法这两种形式出发，但这两种方法各有优缺。

| 处理方式 | 优点 | 缺点 |
| --- | --- | --- |
| **升级产量，增发比特币** | - 网络会更健康，有更多算力参与保护比特币网络 | - 年通胀率升高<br>- 增加比特币市场价格压力 |
| **改变挖矿算法为 PoS** | - 通过权益证明的方式保证比特币网络健康<br>- 保证年通胀率不会过高 | - 可能会引起分歧和争斗<br>- 实现难度大 |

对于网络保护减弱的问题，目前还没有一个确定性的方案。不论是升级产量亦或是改变算法，对于原有 BTC 网络而言都会有相应的缺陷，未来技术的进步可能会带来更完美的处理方案。

### 2.4.5 匿名隐私问题

除了激励问题外，有不少项目开始关注网络的匿名隐私问题。目前，在匿名隐私问题上，有很多技术开发人员提出了各自的处理提案。下文重点讨论环形签名、Mimblewimble 模型和零和协议三种算法。

- 环形签名通过将交易以环形的形式排列，隐匿了交易顺序，从而实现隐私性，是最为古老的算法。XMR 便是采用此签名算法实现匿名性，此签名算法最早可以追溯到 BTC 刚开始的时候。
- Mimblewimble 模型通过隐藏交易地址和交易金额，合并中间状态的交易，从而实现你隐私匿名性。该算法的特点是占用空间小，签名算法的实现速度快，更为关键的一点是有较好的匿名性，Grin 和 Beam 是采用该模型的两个知名项目。

- 零和协议，又称零知识证明，指不向验证者提供任何有用的信息的情况下，使验证者相信某个论断是正确的，是目前技术型更强的算法之一。Zcash 和 Sero 都通过此协议保证其隐私性。此外，在以太坊的未来规划里，零和协议也将添加到网络中。

除此之外，还有达世币采用的混币方式，同样能够实现匿名隐私性。混币是指在进行交易时，会把各种交易进行拆分。例如当接收到 1100 个代币的交易活动时，网络便会自动拆解为 1000 和 100 个代币，然后再和其他的转账做一个混合，最后再发出去。

在保障网络匿名隐私的算法上，与环形签名、Mimblewimble 模型和零和协议相比，混币的匿名性是最弱的。

# 3 传统公链剖析

除了上述去中心化的技术问题，公链项目在开发和维护过程中也存在各自的难题。在长时间的运营过程中，参与交易的人数越来越多，公链性能的问题逐渐显现。下文我们将会对传统公链中的经典项目比特币和以太坊进行问题剖析，重点阐述公链项目长期运行下产生的问题以及目前的处理方式，帮助用户更清晰地了解公链项目的发展。

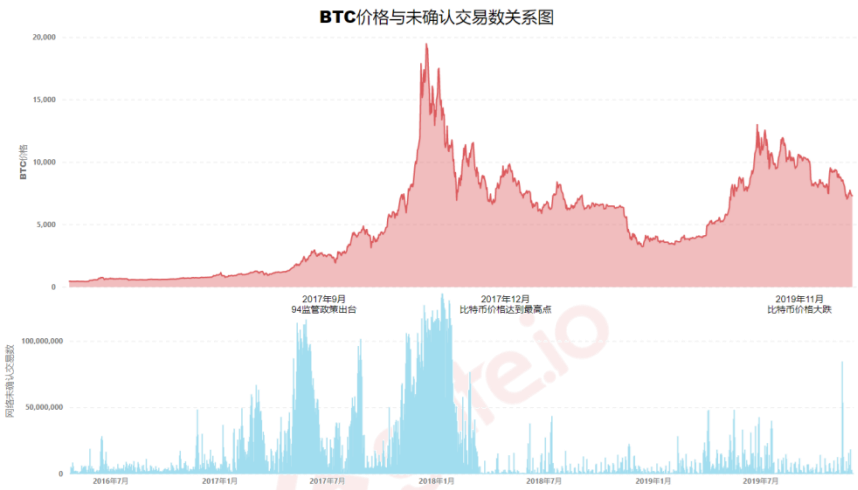
## 3.1 BTC

比特币网络是整个区块链技术的先驱，开创了区块链 1.0 时代。由于技术设计较早期，比特币网络拥堵等问题渐渐暴露出来。目前比特币网络中有一些弊端，主要是容易出现网络拥堵和算力有集中趋势。

### 3.1.1 网络拥堵情况

比特币网络拥堵会增加用户交易确认时间，同时由于网络优先处理手续费高的交易，造成交易时手续费升高的现象，影响网络的正常运行。

根据蜜蜂查（Block.cc）平台的交易行情数据，可以对照 2016 年至今 BTC 价格和网络未确认交易数的具体情况，以此来观察网络拥堵与顺畅运行时与 BTC 价格变化之间的关系。




*来源：blockchain.com、block.cc，截止 2019 年 12 月 4 日*

由图可知，当比特币价格波动较大时，容易出现网络拥堵现象，原因是价格波动说明买卖交易活跃，即比特币的买入卖出活动频繁。买卖交易活跃时大家在各个交易所来回充提交易，比特币网络记账不及时，待处理交易过多，造成网络拥堵。

除了价格波动因素外，网络运行情况还会受到国家政策的影响。在 94 国家监管时，大量用户从各交易所中提取代币，造成比特币网络的拥堵，不利于网络的正常运作。

### 3.1.2 拥堵处理方式之扩容

针对比特币网络拥堵的情况，有人提出了为比特币网络扩容的想法，目前较为主流的扩容方案

有隔离见证[20]和增加区块大小两种，下文以 BTC、BCH 和 BSV 三种代币为例进行分析。

① BTC 是通过 Segwit 隔离见证保持 1M 区块的情况下，将交易量容量提高 30%左右。

② BCH 则是通过修改协议代码，升级区块链的大小将区块大小上限提高到 8M。

③ BSV 同样是通过增大区块大小来实现扩容，其区块上限为 2000M，并且后续可能继续提高。

三者各自采用不同方法来缓解网络拥堵的问题，BTC 是通过隔离见证来实现，而 BCH 和 BSV 处理的思路大致相当，均是通过增大区块大小来实现网络的扩容，但在具体细节上有所不同。

虽然通过提高区块大小来实现扩容的确会降低手续费，使整个网络的吞吐量提高，从而降低网络拥堵，但这也会引起很多严重的问题。由于账本本身能够记录的转账条数有限，且每个转账的大小相近，所有转账都是共用一个账本。此外，区块链里面的资源是恒定的，而所有转账记录都会记录在账并同步到所有全节点，使得区块链内的空间永远被占用并对每一个全节点造成压力，因此区块大小也并非越高越好。

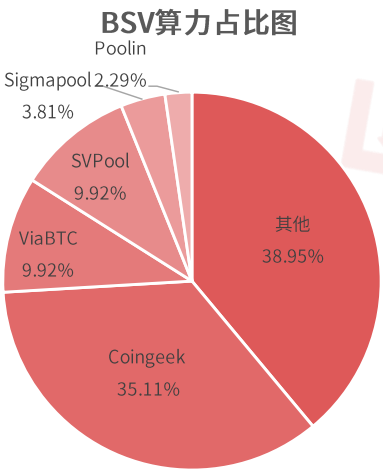
### 3.1.3 增加区块大小的弊端

目前，为实现扩容增加区块大小的 BCH 和 BSV 的中心化趋向已经逐渐显露。

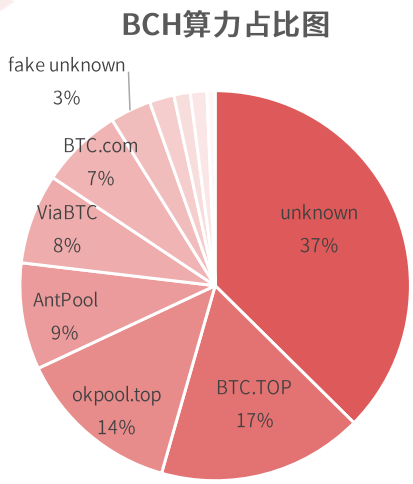
■ BSV

虽然 BSV 通过增大区块大小缓解了网络拥堵问题，但相应的也对网络带来了不同的问题，其中比较明显的问题在于全节点严重中心化。全节点会变得越来越大，随着时间变化，有的电脑支撑不住就会退出全节点，这样包含全节点的电脑就会越来越少，从而造成严重的中心化问题。

同时，由 BSV 算力占比图可知，BSV 算力非常集中，前三矿池算力将近 55%，对网络安全性埋下巨大的隐患。




来源：viabtc.com，截止 2019 年 12 月 4 日




来源：bch.btc.com，截止 2019 年 12 月 4 日

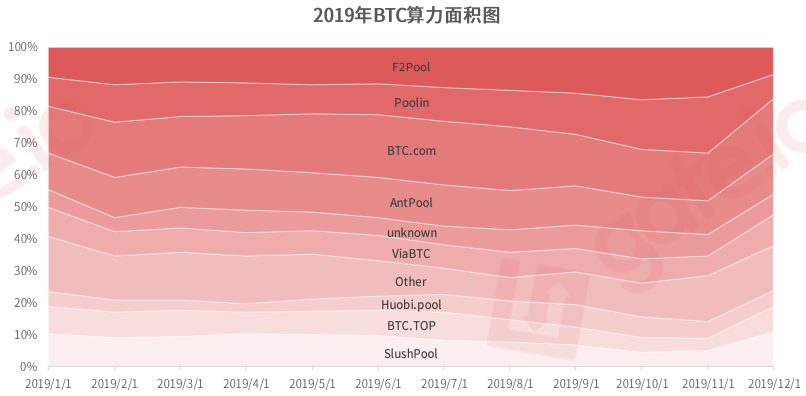
■ BCH

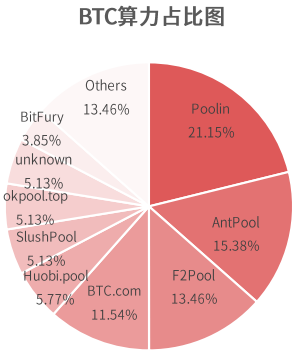
和 BSV 一样，BCH 采用大区块来实现扩容。有所不同的是，BCH 将区块提高到 8M。但同样存在全节点趋于中心化的问题。

在 BCH 算力分布中还一度出现高达 37%的未知来源算力，且目前前三矿池算力将近 40%。与 BTC 相比，BCH 的 TPS 有所提高；但去中心化程度减弱，并且 BCH 依旧是采用 PoW 共识机制，未能有效解决非常消耗电力的问题。

### 3.1.4 算力集中使去中心化程度减弱

比特币网络使用 PoW 共识机制，有着非常高的算力。但随着科技的发展，矿机技术不断提升，算力不断集中到挖矿实力强大的矿池中，算力中心化趋势明显。




*来源：BTC.COM，截止 2019 年 12 月 4 日*

由算力面积图可知，一年前三大矿池算力已占全网 32%，现已上升至将近 50%，由于矿机技术提升，挖矿的成本会越来越低。Gate.io 研究院认为，在未来，算力将会越来越集中，届时将会产生严重的危害。

## 3.2 ETH

作为比较传统的公链，以太坊 1.0 阶段采用的是 PoW 共识机制，节点数量较多，去中心化程度也比较高。此外，平均 15 秒产生一个新区块的设置，在没有突发需求的情况下，对于用户来说已经满足日常的交易需求。但也出现了以下几个问题：

① TPS 不高且在交易频繁时，网络容易出现交易拥堵和产生高昂手续费的问题

② PoW 机制本身会消耗过多电力，造成资源浪费

③ 代币基于智能合约发行，非原生方式，执行的效率低

④ 虽然智能合约的灵活性高，但容易出现错误，漏洞较多

⑤ 节点集中有中心化的趋势，存在 51%攻击的可能性

下文将着重分析以太坊在网络拥堵和中心化方面出现的问题。

### 3.2.1 拥堵处理方式之分片（Sharding）&二层（Layer2）Plasma 扩容协议

在以太坊 1.0 阶段，一旦市场中有热点事件，网络便会非常拥堵。针对这个问题，以太坊 2.0 阶段在以太坊虚拟机[21]中增加了分片[22]，同时在 Layer2[23]层进行了扩容，采用 Plasma 方案。

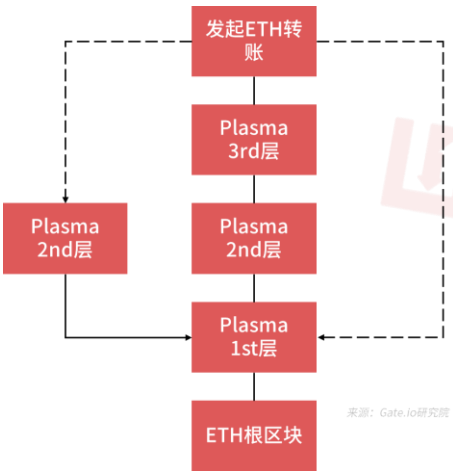
- 增加分片

  增加分片能够解决以太坊原有网络存有量和性能不够的网络固病，但同时也会丧失一些交易的原子性[24]。

  在分片数量上，预计最终只会有 64 个分片，远远小于设想的 1024 个。这是因为如果设置 1024 个分片，将会大大提高网络的复杂性。

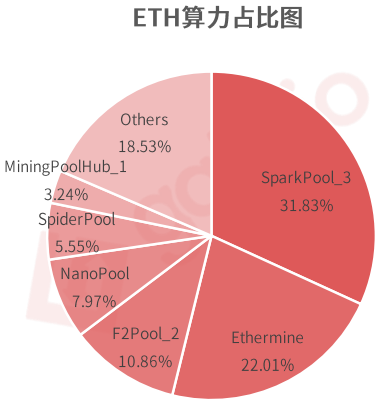
- Plasma 扩容方案

  由右图可知，Plasma 是将以太坊链作为一个仲裁，搭建数条子链。子链通过根合约预定规则与主链关联，链上所有资产均在主链创建。当子链出现资产纠纷时可以通过主链进行仲裁，将资产从子链转回主链时需要比较长的时间。每条子链的 TPS 可以很高从而实现较好的性能，但子链本身的安全性容易出现问题。




### 3.2.2 算力集中有中心化的趋势

与比特币网络相同，长时间使用 PoW 共识机制的以太坊也出现算力集中的问题。




*来源：eth.btc.com，截止 2019 年 12 月 4 日*

由 ETH 算力占比图可见，前 2 名矿池总算力已经超过 51%，大大增加了 51%攻击发生的可能性。尽管 PoS 机制本身也存在趋于中心化问题，但是“V 神”曾在访谈中表示，以太坊从 1.0 升级为 2.0 之后，能够保证各种大小的验证者都能享有参与的机会，不再重演 PoW 矿池过于集中化，小型矿池与独立矿工丧失生存空间的历史。

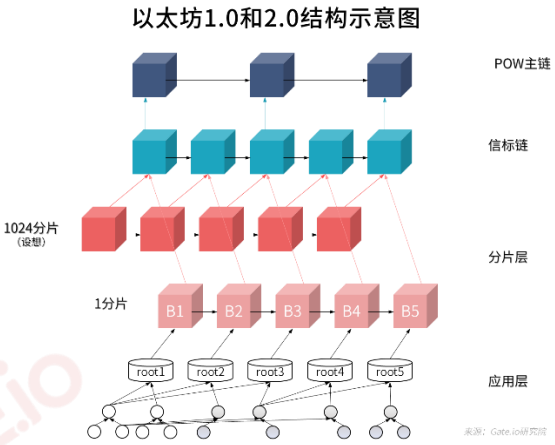
### 3.2.3 以太坊转换升级难度高，持续时间长

以太坊从 1.0 过渡到 2.0，主要是在共识机制上做出了改变，将原有的 PoW 机制更改为 PoS 机制，以解决 PoW 带来的电力损耗问题。为了要保持转换过程中以太坊网络的稳定性，整个升级过程将会持续较长时间。其一是因为目前 Dapp 大多都是在原有网络上，如果突然转换的话会造成很多的问题。其二，在主网上线后再进行升级的难度较高。因此，以太坊的升级并不会一蹴而就，而是通过采用逐年过渡的方案，逐渐把现有网络上的资产转换到新的网络系统中。

在转换升级方案上，ETH 主要是采用 Casper 协议[25]完成分步推进。该协议共有两个版本，分别是 FFG 和 CBC。其中，Casper FFG 是 以太坊创始人 Vitalik 提出来的一个 PoW/PoS 混

合的算法，目的是为了让 Ethereum 平滑过渡到 PoS。而 Casper CBC 由以太坊著名研究员 Vlad 等人提出，在搭建协议时不断对其进行修正，以保证协议的正确性。这两种方案都可以实现 ETH 分步推进升级的目的。

### 3.2.4 以太坊 1.0 和 2.0 对比




ETH 1.0 与 2.0 对比表

| 内容 | ETH 1.0 | ETH 2.0 |
|---|---|---|
| 共识机制 | PoW | PoS |
| 分片 | × | √ |
| 原子性 | √ | × |

## 4 交易所公链剖析

除了传统公链，近两年很多不同的行业也开始涉足公链项目，有越来越多交易所开始在公链方面进行布局，BinanceChain 是首个成功上线的交易所公链。其他交易所布局的公链仍处在开发或设想阶段。下文将根据已披露信息对 BinanceChain、HuobiChain 和 GateChain 进行简单的分析。

### 4.1 BinanceChain

BinanceChain 是基于社区开源构架 Cosmos 和 Tendermint 开发的更专注于交易功能的公链。

#### 4.1.1 技术特点

① 增加链上 DEX 去中心化交易

② 采用 Tendenmint 协议

#### 4.1.2 性能体现

① 继承了 Tendermint 的 TPS 较高，节点数少的特点

② 验证节点数量少，存在被攻击的问题

③ 采用 PoS 共识机制，不具备虚拟机和智能合约功能

④ 搭建链上 DEX 去中心化交易功能

### 4.2 HuobiChain

HuobiChain 是 Huobi 和 Nervos 联合开发的公链，基于 Muta，CKB-VM,nervos-p2p 等开源项目定制。

#### 4.2.1 技术特性

① 虚拟机、网络层和区块链框架均来自于 Nervos

② 共识协议采用 CryptApe 对 PBFT 的优化协议，Overlord

#### 4.2.2 性能体现

① 支持智能合约

② 采用 PBFT 共识算法，TPS 较高，节点数较少

## 4.3 GateChain

GateChain 是主要针对资产安全和底层优化的高性能公链，Gate.io 是其重要的生态合作伙伴。

### 4.3.1 技术特性

① 使用区块链的数据结构

② 发明可撤回交易和私钥丢失、资金找回的功能

③ 设置创新保险账户，保障资金存储安全

④ 针对节点防攻击，在技术上进行了新的改进，有效地提高了防攻击性

⑤ 对拜占庭算法进行了优化，从而实现更好的平衡性

### 4.3.2 性能体现

① 具有较高的 TPS、吞吐量

② 具有较高的去中心化程度

③ GateChain 计划在链上搭建自己的去中心化交易所

## 4.4 交易所公链对比

根据目前各大交易所公开披露的信息，我们对比了各平台公链的技术特性。值得一提的是，尽管交易所公链仍处于初期阶段，随着技术的发展与进步，未来的公链性能将会日益增强，公链生态也将日趋完善。

| 技术特性 | GateChain | HuobiChain | BinanceChain |
| --- | --- | --- | --- |
| **可撤回交易** | 有（独创） | 无 | 无 |

| | | | |
|---|---|---|---|
| **私钥丢失资金找回** | 有（独创） | 无 | 无 |
| **TPS** | ~1000 | ~1000 | ~500 |
| **去中心化程度** | 高 | 低 | 低 |
| **节点防攻击** | 好 | 差 | 差 |
| **DEX** | 开发中 | 有计划 | 已上线 |
| **当前市值** | 低 | 中 | 高 |

*来源：Gate.io 研究院*

## 5 总结

区块链技术是现阶段新兴技术之一，在当前的具体实现中尚且临各方面的巨大挑战，去中心化账本技术仍然是一个活跃的研究性课题，新的方法和机制正在不断使其完善。

目前公链亟需解决资产安全问题，性能瓶颈，以及去中心化的问题。在 CAP 理论下，去中心化实现难度高，受网络 TPS、回滚问题、防攻击问题、激励问题和匿名问题影响较大。现阶段仍然没有一个公链能够完美解决。如 BTC 的节点去中心化程度高，但是 TPS 较低，并且算力越来越集中，导致出块节点中心化程度上升；同时，机制本身带来的电力损耗问题严峻。另一个传统公链 ETH 虽然初期同样是采用 PoW 机制，但由于资源损耗问题严重，以太坊后期将共识机制调整为 PoS，并在原有的基础上增加了分片以缓解网络拥堵状况。

最近几年，越来越多行业开始在公链赛道有所布局，交易所也是其中一员。而 Binance 是首个

将公链成功上线的交易所，HuobiChain 和 GateChain 仍在开发中。HuobiChain 目前已知信息不多，主要基于开源组件深度定制；而 GateChain 对区块链共识机制等底层协议进行优化，能够有效地平衡 TPS 和去中心化程度以及保护网络节点。

对于交易所而言，最为重要的莫过于资金安全问题。在资金安全问题上，GateChain 通过创造性地设置安全账号以及开创性的可撤回交易、私钥找回功能，为用户的资金安全提供保障。

# 6 参考资料

## 6.1 参考资料

GateChain 首席构架师一休公链的战争主题直播文稿：

https://www.gate.io/help/livetext/17145

区块链不可能三角原出处：

https://en.wikipedia.org/wiki/CAP_theorem

Vitalik 去中心化讨论文章：

https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

拜占庭将军问题论文：

https://people.eecs.berkeley.edu/~luca/cs174/byzantine.pdf

中本共识：

https://blockonomi.com/nakamoto-consensus/

PBFT 共识论文：

http://pmg.csail.mit.edu/papers/osdi99.pdf

PoS 出处：

https://bitcointalk.org/index.php?topic=27787.0

BTC 白皮书：

https://bitcoin.org/bitcoin.pdf

ETH 白皮书：

https://github.com/ethereum/wiki/wiki/%5BSimplified-Chinese%5D-Ethereum-TOC

## 6.2 名词解释

[1] 区块：本质是账本，所有交易数据都会被打包进入区块，然后在区块链上以区块作为单元进行传输和存储

[2] 比特币闪电网络：将大量交易放到比特币区块链之外进行

[3] 并发性：多个事务同时处理的能力

[4] 双花问题：一个交易被记录在两个区块中。也称“双重支付”，一笔钱被花了两次或以上

[5] 拜占庭将军问题：在存在消息丢失的不可靠信道上试图通过消息传递的方式达到一致性是不可能的

[6] 拜占庭容错算法（BFT）：能够抵抗拜占庭将军问题所导致的一系列失败的理论性大于实践性的系统

[7] 实用拜占庭容错算法（pBFT）：降低了拜占庭协议的实践复杂度，是拜占庭协议在分布式系统中的应用变成可能

[8] 工作量证明（PoW）：通过一定的工作量来获取奖励的机制

[9] 挖矿：在区块链所属机制下，参与区块的生产，并在此过程中获得奖励

[10] 权益证明（PoS）：按照持有币的数量比例以及持有的时间，来提高挖矿成功并获取奖励的机制

[11] 51%攻击：指一旦有人掌握了比特币网络中 51%的算力，就能够篡改网络中的所有数据，使得信任崩塌

[12] 私钥：公钥与私钥是通过加密算法得出的一组密钥对

[13] 出块节点：生产区块的节点

[14] 非出块全节点：与出块节点相反，本次挖矿中除出块节点以外的其他节点

[15] 股权委托证明（DPoS）：币的持有者可以进行投票选举，选举出一些节点作为代表来记账

[16] 一致性：各区块数据保持一致

[17] 分区容错性：指系统的一部分不可用并不会影响其他部分

[18] 可用性：全部节点的可用程度

[19] 共识确定性：共识是指想要达成一致性的人或组织达成一致性的一个过程，而达到共识的程度与范围可以用共识确定性表示

[20] 隔离见证：是区块链扩容的一种方法，把区块内的数字签名信息从基本结构拿出去，让每个区块可以承载更多笔交易

[21] 以太坊虚拟机：以太坊虚拟机 EVM 是智能合约的运行环境，它被完全隔离运行

[22] 分片：通过缩小验证规模和大量事务并行处理来达到性能提升的效果

[23] Layer2：用于价值传输且不需要通过共识层的方案

[24] 原子性：把一个事务可看作是一个程序，要么完整的被执行，要么完全不执行

[25] Casper 协议：通过验证者抵押保证金，并通过赌注形式验证区块，有效地防止恶意攻击