时戳资本
TIMESTAMP CAPITAL

区块链公链项目研究报告

时戳资本区块链行业研究报告系列-03

时戳资本分析师 陈波涛

2018年5月3日

引言：

公链是区块链的底层协议，是区块链世界的“操作系统”。经历了第一代公链比特币和第二代公链以太坊的探索，第三代公链正着眼于解决系统的扩展性、安全性和监管兼容性问题，以承载大规模的商业应用。同时，第三代公链仍需保留区块链的开放、自治等特性。与互联网的架构不同，区块链底层协议的价值远远超过应用层，因此，区块链的研发和投资更关注底层公链技术。我们预计底层公链仍将是现阶段区块链行业的攻关重点，各公链在可扩展性、应用性、共识哲学，以及应用生态搭建上的角逐将长期延续。

本报告主要阐述：

- **区块链公链的定义**
- **区块链公链的发展路径**
- **区块链公链的核心要素**
- **区块链公链的技术实现形式**
- **区块链共识机制的讨论**

目录

一、区块链公链的定义

公链是区块链的底层协议，是区块链世界的“操作系统”。公链为区块链搭建分布式数据存储空间、网络传输环境、交易和计算通道，利用加密算法保证网络安全，通过共识机制和激励机制实现节点网络的正常运行。公链提供的 API 接口可供开发者调用，以开发符合公链生态的应用。

二、区块链公链的发展阶段

比特币是区块链上的第一代公链。比特币在设计之初定位为支付工具，只能进行价值传输。中本聪因此大幅删减了许多脚本指令，所以其安全性极高。但比特币的脚本语言是图灵不完备的，不能执行循环语句，可扩展性差，许多高级应用无法建立在比特币脚本之上。

区块链上的第二代公链以太坊，是一个具备图灵完备脚本的公共区块链平台，被称为“世界计算机”。除进行价值传递外，开发者还能够在以太坊上创建任意的智能合约。以太坊通过智能合约的方式，拓展了区块链商用渠道，比如众多区块链项目的代币发行，智能合约开发，以及去中心化 DAPP 的开发，目前基于以太坊的 DAPP 已经超过 1000 个[1]。然而，当前的以太坊网络存在扩展性不足、安全性差、开发难度高以及过度依赖手续费等问题，区块链的大规模商用遭遇了发展瓶颈。

第三代公链定位于能大规模商用，与实际资产和真实价值相关联，推动实体经济发展。目前正在竞争区块链 3.0 时代的公链项目有 EOS，Cardano，Bytom 等，但这些公链项目多数处于理论论证及测试阶段，少数主链完成开发的项目也

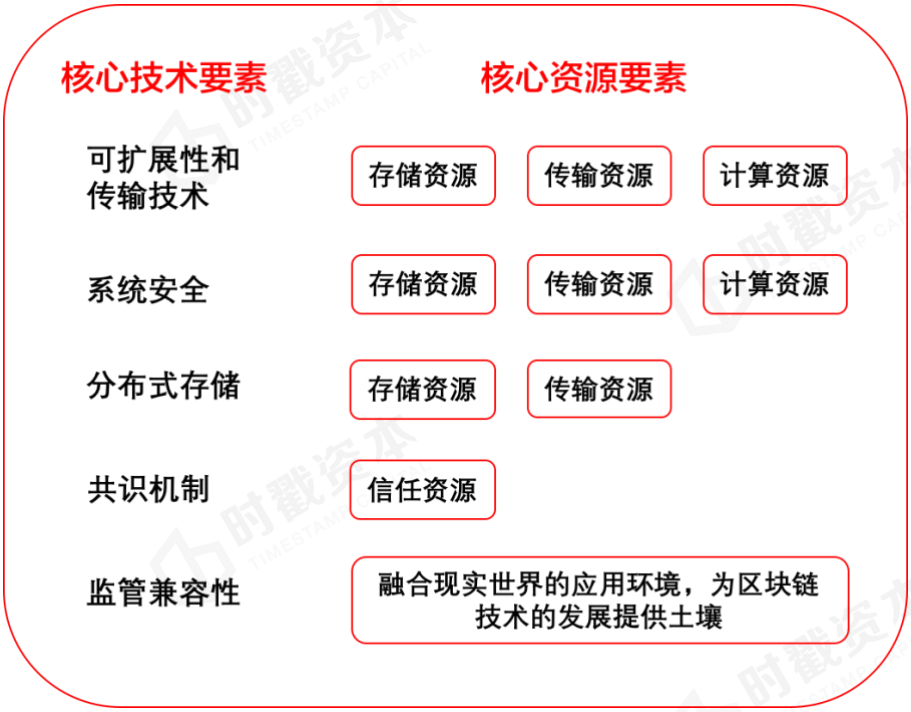
[1] 据 stateofthedapps.com 最新数据，基于以太坊上的 DAPP 数量已经达到了 1311 个。

仍处于早期探索阶段。而技术储备充足、财力雄厚的以太坊仍在不断地自我迭代，区块链 3.0 时代的公链之争群雄逐鹿。

三、区块链公链的核心要素

互联网世界里的核心资源要素包括存储资源、传输资源、运算资源三个方面，区块链技术作为互联网世界的延伸，其核心资源要素与互联网有很大的相关性。同时，区块链是信任的机器，在互联网传递信息的功能之外，还承载着价值传输的使命，因而区块链世界的核心资源要素可归结为存储资源、传输资源、运算资源和共识机制所产生的信任资源四个方面。

时戳资本区块链行业研究报告系列一将区块链的架构分为五个层面，分别为数据层、网络层、共识层、合约层和应用层，我们将其中的核心技术要素提炼成五个维度，包括可扩展性和传输技术、系统安全、分布式存储、监管兼容性和共识机制。



图：区块链公链的核心资源要素和技术要素

- **可扩展性和传输技术**:可扩展性包括系统节点数和交易吞吐能力两个方面，由区块容量、出块时间和节点间的传输速度等因素决定，可扩展性和传输技术相辅相成。
- **系统安全**：包括双花攻击、交易及合约漏洞的防范机制，身份识别和匿名性，数据库安全等方面。
- **分布式存储**：充分利用节点存储资源，解决区块链系统中日益增长的数据存储需求，提高系统传输效率，保证分布式账本的安全可靠运行。
- **监管兼容性：**区块链最核心的理念是去中心化，许多区块链技术在设计之初即将中心化的政府视为对立面。但不容否认，中心化依然是目前社会运行的主体模式，区块链的去中心化思维难免会和中心化的传统监管之间产生冲突和摩擦。因此，公链架构中与现实中心化世界的兼容性设计将是公链大规模应用的前提。
- **共识机制**：共识机制是区块链的灵魂，共识机制的设计决定了一条公链能否建立完善的激励机制，鼓励更多的节点参与其中，增加系统的去中心化属性。而在多数公链中，节点数量与传输速率呈负相关关系，节点数量和系统性能的平衡是共识机制需要考虑的另一个要素。

四、区块链公链的技术实现形式和共识机制

目前，研发中的区块链公链项目众多，每条公链的设计哲学和应用场景各有千秋，下文将对主流公链从可扩展性和传输技术、系统安全、分布式存储、监管兼容性、共识机制五个维度的技术实现展开分析。

表：主流公链的技术特性

项目	共识机制	出块时间	节点数	技术特色
BTC	POW	约 10min	10441	UTXO 架构
Ethereum	POW+POS	约 15s	16379	虚拟机 EVM、智能合约
Cardano	Ouroboros（DPOS）	约 20s	/	分层架构、交互性强
NEO	DBFT	15～20s	7	数字证书、智能合约、跨链互操作
EOS	DPOS	3s	21 个生产节点，100 个备用节点	石墨烯技术、多链并行
Qtum	IPOS	1-3min	7757	UTXO、分层架构
Bytom	POW	2.5min	/	人工智能 POW 、BUTXO、侧链

（一）可扩展性和传输技术

1. 扩容技术

比特币、以太坊等公链将区块大小设计得很小，以降低普通设备成为全节点的门槛，保证系统的去中心化属性。

然而过小的区块大小限制了每个区块的交易承载量，给公链系统带来运算瓶颈。目前，比特币系统的 TPS 仅 7 笔/秒，以太坊系统的 TPS 仅约 13 笔/秒。

公链的扩容技术分为链上扩容和链下扩容两大体系。其中链上扩容技术包括大区块、隔离见证、分片技术等，链下扩容技术包括侧链技术、状态通道技术等。

各主流公链对扩容技术的已经开展了以下实践：

- 针对比特币的扩容方案：BCH 分叉（大区块）、闪电网络 Lightning Network（状态通道技术）。

- 针对以太坊扩容方案：Sharding（分片）、Plasma（侧链）、雷电网络 Radien Network（状态通道技术）等。
- 针对 NEO 的扩容技术有 Trinity 提供的状态通道技术。
- Bytom 实行的类隔离见证技术，在区块设计中将数据和见证、签名部分分离，在一定程度上提升了每秒交易速率。同时，还采用了基于多资产的状态通道技术，基于 BUTXO 的分片机制。

2. 跨链技术

区块链之间的互通性问题极大程度地限制了区块链的应用空间，而跨链技术能让价值跨过链与链之间的障碍直接流通，是区块链实现价值互联网的关键。知名的跨链技术有连接比特币与以太坊的 BTC Relay、Cardano 的 NIPoPoW 和 Bytom 的 XRelay 技术等。

BTC Relay 是一种基于以太坊区块链的智能合约，将以太坊网络与比特币网络以一种安全去中心化的方式连接起来。BTC Relay 通过使用以太坊的智能合约功能可以允许用户在以太坊区块链上验证比特币交易。BTC Relay 使用区块头创建一种小型版本的比特币区块链，以太坊 DApp 开发者可以从智能合约向 BTC Relay 进行 API 调用来验证比特币网络活动。BTC Relay 进行了跨区块链通信的有意义的尝试，打开了不同区块链交流的通道。

Cardano 的跨链技术通过 NIPoPoW（Non-interactive Proofs of Proof of Work）侧链实现，它可以让 CSL 与任何其他的区块链链协议进行交互。Cardano 能够成为其它数字货币的粘合剂，通过侧链和快照技术让不同的货币都可以通过 Cardano 相互流通。

Bytom 上的资产互通采用 XRelay 技术（与比特币的 BTC Relay 类似），以此来支持不同形式的区块链数字资产在比原链上流动。

3. 点对点传输技术

从系统性能角度而言，现有的区块链网络节点，除了见证系统账本之外，对系统的性能提升没有贡献，反而降低了系统的活跃度，因为节点越多，账本同步至所有节点所需的时间也越长。

Cardano 采用了一种类似于 BitTorrent 的点对点传输协议一样，参与的节点数量越多，传输的速度越快。随着系统节点的增多，Cardano 每秒可以处理非常庞大的交易量。

（二）系统安全性

以太坊计算层的计算和存储没有分离机制，只是采用了 Gas 机制（以太坊网络的执行的每个操作、交易或合同执行都要求支付其相应的费用）来平衡主网上的算力资源，这种架构设计存在两个方面的问题：

- **主网计算资源不分隔。**一个热门 DAPP 可能占据以太坊主网的绝大多数计算资源，导致网络拥堵，其他 DAPP 或交易无法执行。
- **合约行为和交易行为不分离。**太坊 Parity 钱包中 15 万 ETH 被盗，就是因为合约计算和价值传输不分离导致的。

针对以太坊主网没有分离机制的问题，许多后起公链以计算层分层、侧链或多链架构等方式解决。实行合约层分层的有量子链和 Cardano，这种分层机制一般将计算层分为交易层和合约层，而交易层仍模仿比特币采用 UTXO 链式结构，保证价值传输的安全可靠；实行多链或侧链隔离架构的有 Aelf 和 EOS 等。

1. 分层

（1）Cardano

Cardano 将计算层分为两层。一层专注于交易和结算，另一层专注于智能合约的计算。

第一层，Cardano Settlement Layer (CSL) 加密货币结算层，是整个 Cardano 系统的基础，其代币 ADA 只在结算层内流动，主要用来处理数字货币价值转移。CSL 的脚本结构与比特币的 UTXO 类似，只支持交易，虽然简单，但可确保复杂可编程脚本的漏洞不会出现。

第二层，Cardano Computation Layer (CCL)智能合约层，允许智能合约相关的所有高级可编程功能存在。

Cardano 结算层与合约层分开运行的方式，可以针对不同的分层进行有针对性的部署和升级。针对结算层，可以通过软分叉对数字货币交易中遇到的问题进行升级和换代，而对于合约层，则可以根据 DAPP 的运行需求进行针对性的拓展和改良。因此，分层的方式实现了在一个生态内建立清晰、有边界的系统运行秩序，实现更好的可拓展性和交互性。

（2）量子链（Qtum）

量子链将系统中的交易行为和合约行为分离。在量子链系统中，除了基于 UTXO 模型的可追溯的 Transaction Ledger，还将构建一个合约内容的 Contract Ledger。账户抽象层（Account Abstract Layer, AAL）对 UTXO 账户和 EVM 合约账户之间进行了适配，使得量子链兼容符合 EVM 规范的智能合约，为 Dapp 提供一个新的基础平台，同时 UTXO 的安全、稳定、隐私性等优点能得以保留。

2. 多链或侧链隔离

（1）EOS

与以太坊不同，EOS 是一个多链并行的区块链架构。开发者可以自由地在 EOS 上创建公链，链与链之间不会影响彼此的资源。使用 EOS 系统中的计算不会消耗费用，也不会出现因个别应用资源消耗而造成网络大面积拥堵的情况，EOS 以此来解决底层公链的性能和系统安全问题。

（2）Aelf

Aelf 系统采用“主链+多侧链”结构，每条侧链都可对应一个特定的计算场景，这种设计对主网的计算资源进行了有效的隔离。Aelf 还可以用侧链去链接其他的主链，扩展 Aelf 的边界。

（三）分布式存储

区块链的数据以分布式账本的形式存储，分布式的存储能力是区块链的发展瓶颈之一。对于目前大部分的基础公链而言，如何让大量的数据存储在自己的主链上是急需解决的问题。

1. Filecoin

IPFS 是 Inter-Planetary File System 的简称，由 Protocol Lab 提出，是一个 P2P 的分布式文件系统。与现有 Web 不同的是，对于一个存放在 IPFS 网络的文件资源，通过这个文件资源的内容生成的唯一编码去访问。IPFS 可以将数据分片存储到分布式的存储节点，与 BitTorrent 类似，在访问时不需要关心存储在哪里，可以从多个存储节点分片获取。

Protocol Lab 提出了与 IPFS 相辅相成的 Filecoin，这是一个公有的区块链，是 IPFS 的经济激励系统。世界各地的数据中心和硬盘中有大量闲置存储空间，

Filecoin 网络允许全球任何一方作为存储提供商参与其中，通过“桥接”功能与其他区块链公链相连接，为区块链提供了巨大的存储规模。

2. NeoFS

除 Filecoin 之外，NEO 也有其专属的分布式文件存储技术 NeoFS。NeoFS 是一套利用了 Distributed Hash Table 技术的分布式存储协议。NeoFS 通过文件内容（Hash）而非文件路径（URI）来对数据进行索引。大文件将被分割为固定大小的数据块分布式地存储在众多节点中。

该类系统的主要问题是需要在冗余度和可靠性之间寻找平衡点。NeoFS 计划通过代币激励机制和建立骨干节点的方式来解决这一矛盾。用户可以选择文件的可靠性要求，低可靠性的文件可以免费或几乎免费的被存储和访问，高可靠性的文件将由骨干节点提供稳定可靠的服务。

（四）监管兼容性

区块链最核心的理念是去中心化，以太坊等公链在设计之初是以现实世界的挑战者的姿态出现的。然而，区块链技术最终要应用到解决社会问题，提升生产效率中去。如果要实现商业化应用和社会价值，公链的架构设计必须要考虑如何与现实社会的融合。NEO、量子链、Cardano 等公链在架构设计上都考虑到了区块链与监管的兼容性问题。

1. NEO

NEO 的愿景是普及区块链技术，帮助企业和政府完成区块链技术落地，最终实现智能经济。NEO 通过数字资产、数字身份和智能合约这三者来构筑智能经济体系，同时从合规和可审查性角度，让数字身份和数字资产能获得现有法律的许可和政府监督。

2. 量子链

许多现有公链不被政府或金融机构所采纳的重要原因之一是，没有设计身份认证或者准入环节。量子链定位于符合行业监管的区块链去中心化应用开发平台，在设计之初就为监管者的角色设计了很多可选项。

- 在量子链中引入数字身份（Identity）和第三方征信平台，第三方服务商可以通过智能合约标记量子链参与者的身份，从而区分已验证和未验证的 Qtum 地址，已验证的地址有权优先使用基于 Qtum 的金融服务 DAPP。
- 在智能合约（Smart Contract）之外，量子链引入新的主控合约（Master Contract），主控合约的执行逻辑可以通过链下执行，把监管者的角色引入，从而避免类似以太坊 DAO 事件的悲剧再次重演。
- 监管者可以作为 Qtum 系统中的喻言和数据源的提供者（Oracle 和 data feed），比如某一合约的执行结果取决于当季的 GDP 增长速度，那么监管者可以作为可信数据的提供者。

3. Cardano

与量子链类似，在 Cardano 的设计哲学中，充分考虑了监管需求，同时也尽可能考虑用户的隐私性，并设法达到二者之间最优平衡点。比如，在必要且用户自愿的情况下，可以针对性的选择提交 KYC（客户身份）和 AML（资金流向）等信息，满足最基本的监管需求。这一切的目的都是希望让区块链金融被社会主流群体更容易接受和使用。

（五）共识机制

共识机制是区块链的核心基石，是区块链系统安全性的重要保障。区块链是一个去中心化的系统，共识机制通过数学的方式，让分散在全球各地成千上万的

节点就区块的创建达成一致的意见。共识机制中还包含了促使区块链系统有效运转的激励机制，是区块链建立信任的基础。

区块链公链常用的共识机制有 POW、POS、DPOS、BFT 以及多种机制混合而成的共识机制等。共识是指系统节点达成一致的过程，而分布式系统的一致性体现在三个方面[2]：

- 最终性（Termination）：所有进程最终会在有限步数中结束并选取一个值，算法不会无尽执行下去。
- 统一性（Agreement）：所有进程必须同意同一个值。
- 合法性（Validity）：输出内容是输入内容按照系统规则生成的，且输出内容合法。

最终性衡量了达成共识的效率，在一些对交易确认的实时性要求高的场景显得非常重要，而统一性和合法性表征了共识的安全性。在区块链系统中，去中心化程度表征了分布式系统的大规模协作程度。因此，我们从效率、安全性和去中心化程度这三个维度去评价各种共识机制，也就是长铗提出的著名的“不可能三角”[3]理论。

1. POW 共识机制

比特币采用的 POW 工作量证明共识机制，在生成区块时，系统让所有节点公平地去计算一个随机数，最先寻找到随机数的节点即是这个区块的生产者，并获得相应的区块奖励。由于哈希函数是散列函数，求解随机数的唯一方法在数学上只能是穷举，随机性非常好，每个人都可以参与协议的执行。由于梅克尔树根

[2] George Coulouris.分布式系统概念与设计[M].北京：机械工业出版社，2008.

[3] 区块链“不可能三角”：指平等共识（去中心化）、安全性、效率（非计算性）三者不能同时共存，只能取其二。该理论由巴比特创始人长铗提出。

的设置，哈希函数的解的验证过程也能迅速实现。因此，比特币的 POW 共识机制门槛很低，无需中心化权威的许可，人人都可以参与，并且每一个参与者都无需身份认证。

同时，中本聪通过工作量证明的机制破解了无门槛分布式系统的“女巫攻击”问题。对系统发起攻击需要掌握超过 50%的算力，系统的安全保障较强。

POW 共识的优点可归纳为：

- 算法简单，容易实现，节点可自由进入，去中心化程度高。
- 破坏系统需要投入极大的成本，安全性极高。
- 区块生产者的选择通过节点求解哈希函数实现，提案的产生、验证到共识的最终达成过程是一个纯数学问题，节点间无需交换额外的信息即可达成共识，整个过程不需要人性的参与。

比特币系统的设定在保证安全性的的前提下，牺牲了一部分最终性。因此，POW 共识算法也存在一些问题：

- 为了保证去中心化程度，区块的确认时间难以缩短。
- 没有最终性，需要检查点机制来弥补最终性，但随着确认次数的增加，达成共识的可能性也呈指数级地增长。

由于这两个方面的问题，一笔交易为了确保安全，要在 6 个新的区块产生后才能在全网得到确认，也就是说一个交易的确认延迟时间大概为 1 小时，这无法满足现实世界中对交易实时性要求很高的应用场景。

另一方面，POW 共识算法带来了硬件设备的大量浪费。随着比特币价值的增长，比特币算力竞赛经历了从 CPU 到 GPU，再到 ASIC 专用芯片的阶段。算

力强大的 ASIC 芯片矿机将挖矿算法硬件化，而 ASIC 芯片矿机在淘汰后，没有其他的用途，造成了大量的硬件浪费。

2. POS 共识机制

POS（Proof of Stake）共识机制，是一种由系统权益代替算力决定区块记账权的共识机制，拥有的权益越大则成为下一个区块生产者的概率也越大。POS 的合理假设是权益的所有者更乐于维护系统的一致性和安全性。如果说 POW 把系统的安全性交给了数学和算力，那么 POS 共识机制把系统的安全性交给了人性。人性问题，可以用博弈论来研究，POS 共识机制的关键在于构建适当的博弈模型相应的验证算法，以保证系统的一致性和公平性。

POS 共识机制没有像 POW 那样耗费能源和硬件设备，缩短了区块的产生时间和确认时间，提高了系统效率。但存在的缺点也有很多，包括：

- 实现规则复杂，中间步骤多，参杂了很多人为因素，容易产生安全漏洞。
- 与 POW 共识机制一样没有最终性，需要检查点机制来弥补最终性。

（1）POS 共识机制的最早实践

早期 POS 共识机制的实现一般是结合了 POW 共识机制，如点点币（Peer Coin）、黑币（Black Coin）等。其主要思想是区块记账权的获得难度与节点持有权益的币龄成反比。相比于 POW 共识机制，一定程度减少了数学运算带来的资源消耗，达成共识的时间也相应地缩短，出块效率提高。

但这种 POS 共识机制的致命弱点在于币龄依赖问题，攻击者在积累长时间币龄后，挖矿的难度大大降低，容易对系统发起双花攻击。

（2）纯 POS 共识机制

纯 POS 共识机制由节点所持权益（持有数量乘以持有时间）决定区块生产者，权益比例越高，被选为区块生产者的概率也越大，区块生产者选举过程中没有挖矿。这种机制的践行者有未来币（NXT）和量子链（QTUM）等。

纯 POS 共识机制没有引入外部资源，仅仅依靠自身的权益来维护网络安全，因此其不需要消耗能源来进行计算；而且由于其没有引入外部的资源，因此不会担心外部攻击，例如外界的算力攻击。但是，这种 POS 共识依然存在很多问题：

- **无利害关系攻击（Nothing-at-Stake attack）**

基于权益的挖矿不需要像 POW 共识一样投入物理算力和能源的消耗，只需要持有权益。假设系统中出现了两个分支链，那么对于持有币的“挖矿者”来讲，矿工的最佳的操作策略就是同时在两个分支上进行“挖矿”，这样无论哪个分支胜出，对币种持有者来讲，都会获得本属于他的利益，而不会有利益损失。

这导致的问题是，只要系统存在分叉，“矿工们”都会同时在这几个分支上挖矿；因此在某种情况下，发起攻击的分叉链是极有可能成功的，因为所有人也都在这个分叉链上达成了共识；而且甚至不用持有 51%的权益，就可以成功发起分叉攻击。

- **马太效应**

POS 共识机制下的权益累计由持币数量乘以持币时间得到，它势必形成赢家通吃的局面。假设电力成本均为 3 币，大户持有 100 币天获得 100 利息币，小户持有 1 币天，获得 1 利息币。这样大户会倾向于开机获得更多的币天，而小户倾向于关机，（97，0）是最终博弈的选择。如此，大户获得的币越来越多，造成富者愈富，贫者愈贫的局面。

表：POS 博弈收益矩阵[4]

大户 / 小户	开机	不开机
开机	97，-2	0，-2
不开机	97，0	0，0

■ **记账节点激励问题**

尽管 POS 中的“挖矿”不用消耗算力，运行成本很低，但是也存在如何激励 POS 矿工的问题。因为一般的 POS 系统是没有新币产生的，矿工只能赚取交易费，而且在交易费不高的情况下，对矿工的激励十分有限。

（3）改进的 POS 共识机制

针对纯 POS 共识机制存在的问题，改进的 POS 共识机制通过设立惩罚制度来保证系统安全，区块验证者以存入押金的形式参与，对系统恶意攻击的惩罚力度要比奖励大成百上千倍。

POS 共识的这种改进方便区块链进行分叉选择和在链上设置检查点，解决了纯 POS 共识机制的分叉问题，并使共识结果获得了最终性。但是对于如何判定恶意攻击依然是个备受争议的问题[5]，POS 共识的实行过程始终是一个复杂的人性博弈过程。

以太坊的 Casper FFG 版 POS 机制将于以太坊第三阶段 Metropolis 中的第二部分 Constantinople（君士坦丁堡）中投入使用，这是一种融合了改进的 POS 共识和 POW 共识的混合共识。以太坊 Casper FFG 版本的记账人选择和出块时间都由 POW 共识完成，POS 共识在每 100 个区块处设置检查点，为交

[4] 引用自巴比特创始人长铗在 2018 年全球区块链（杭州）高峰论坛的演讲——我所认为的区块链思维，2018 年 3 月 26 日。
[5] BitMEX Research: Complete guide to Proof of Stake - Ethereum's latest proposal & Vitalik Buterin interview, April 11, 2018.中文版见 http://www.8btc.com/vitalik-pos，对话 V 神：权益证明 POS 新趋势。

易确认提供最终性，也是这种 POW-POS 混合共识机制优于 POW 共识机制的地方。

3. DPOS 共识机制

DPOS（Delegated Proof of Share），代理权益证明共识机制，是一种基于投票选举的共识算法，类似代议制民主。在 POS 的基础上，DPOS 将区块生产者的角色专业化，先通过权益来选出区块生产者，然后区块生产者之间再轮流出块。

DPOS 共识由 BitShares（比特股）社区首先提出，它与 POS 共识的主要区别在于节点选举若干代理人，由代理人验证和记账。DPOS 相比 POS 能大幅度提升了选举效率，在牺牲一部分去中心化特性的情况下得到性能的提升。

DPOS 共识机制不需要挖矿，也不需要全节点验证，而是由有限数量的见证节点进行验证，因此是简单、高效的。由于验证节点数量有限，DPOS 共识被普遍质疑过于中心化，代理记账节点的选举过程中也存在巨大的人为操作空间。

（1）EOS

EOS 系统中共有 21 个超级节点和 100 个备用节点，超级节点和备用节点由 EOS 权益持有者选举产生。区块的生产按 21 个区块为一轮。在每轮开始的时候会选出 21 个区块生产者。前 20 个区块生产者由系统根据网络持币用户的投票数自动生成，最后一名区块生产者根据其得票数按概率生成。所选择的生产者会根据从区块时间导出的伪随机数轮流生产区块。

EOS 结合了 DPOS 和 BFT（拜占庭容错算法）的特性，在区块生成后即进入不可逆状态，因而具有良好的最终性。EOS 采用的石墨烯技术使其在理论上

能够达到百万级别的 TPS，目前上线的测试网络的 TPS 达到数千量级。同时，由于 EOS 的记账节点有严格的筛选制度，系统的安全性也很高。

DPOS 作为 POS 的变形，通过缩小选举节点的数量以减少网络压力，是一种典型的分治策略：将所有节点分为领导者与跟随者，只有领导者之间达成共识后才会通知跟随者。该机制能够在不增加计算资源的前提下有效减少网络压力，在商业环境的实现中将会具有较强的应用价值。

DPOS 为了实现更高的效率而设置的代理人制度，背离了区块链世界里人人可参与的基本精神，也是 EOS 一直被质疑的地方。

（2）Cardano

Cardano 实行的共识机制 Ouroboros 可认为是 DPOS 共识的一个变种，而 Cardano 团队更愿意将其表述为 Dynamic POS。与 DPOS 共识的相同之处是，只有 Cardano 的代币 ADA 持有量超过一定数量的地址（官方数据 ADA 前 2%的地址）才有资格参与区块生产者的选举，持有 ADA 越多的用户，被选为区块生产者的概率越大。

Ouroboros协议将物理时间分为纪元（epoch），然后再将纪元划分为区块（slot），每个纪元持续5天，每个区块持续约20s。每个纪元的区块生产者在上一个纪元就已经选定，并在下一个纪元中随机选定某个候选人充当各个区块的生产者，一个候选生产者可能在一个纪元中对生产多个区块。

Cardano 团队认为 Ouroboros 不同于 DPOS 之处在于，Cardano 记账人的选举过程是完全随机的，而不是利益相关方选举而来。Ouroboros 共识算法中引入了一种抛硬币协议（coin tossing protocol），可以保证选举过程的完

全随机性。据 Cardano 团队称，Ouroboros 是目前为止唯一在数学上证明能够达成近似纳什均衡的 POS 共识机制，但其有效性仍需实际运行效果来检验。

4. BFT 共识机制

（1）PBFT

最常用的BFT共识机制是实用拜占庭容错算法PBFT（Practical Byzantine Fault Tolerance）。该算法是Miguel Castro和Barbara Liskov在1999年提出来的，解决了原始拜占庭容错算法效率不高的问题，将算法复杂度由节点数的指数级降低到节点数的平方级，使得拜占庭容错算法在实际系统应用中变得可行。

PBFT是针对状态机副本复制为主的分布式系统执行环境开发的算法，旨在让系统中大部分的诚实节点来覆盖恶意节点或无效节点的行为。PBFT算法的节点数量是固定的，节点身份提前确定，无法动态添加或删除，只能适用于节点数目固定的联盟链或私有链场景中。

PBFT算法存在的问题：

- 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区块链系统，扩展性差。
- 系统节点是固定的，无法应对公有链的开放环境，只适用于联盟链或私有链环境。
- PBFT算法要求总节点数$n >= 3f + 1$（其中，f代表作恶节点数）。系统的失效节点数量不得超过全网节点的1/3，容错率相对较低。

（2）DBFT

考虑到BFT算法存在的扩容性问题，NEO采用了一种代理拜占庭容错算法——DBFT（Delegated Byzantine Fault Tolerant）。它与EOS的DPOS共识机制

一样，由权益持有者投票选举产生代理记账人，由代理人验证和生成区块，以此大幅度降低共识过程中的节点数量，解决了BFT算法固有的扩容性问题。

为了便于在区块链开放系统中应用，NEO的DBFT将PBFT中的将C/S（客户机/服务器）架构的请求响应模式，改进为适合P2P网络的对等节点模式，并将静态的共识参与节点改进为可动态进入、退出的动态共识参与节点，使其适用于区块链的开放节点环境。

DBFT 的算法中，参与记账的是超级节点，普通节点可以看到共识过程，并同步账本信息，但不参与记账。总共 *n* 个超级节点分为一个议长和 *n*-1 个议员，议长会轮流当选。每次记账时，先有议长发起区块提案（拟记账的区块内容），一旦有至少（2*n*+1）/3 个记账节点（议长加议员）同意了这个提案，那么这个提案就成为最终发布的区块，并且该区块是不可逆的，所有里面的交易都是百分之百确认的，区块不会分叉。

NEO 的 DBFT 共识机制下只设置了 7 个超级节点，以一种弱中心化的模式实现较高的共识效率。目前，这些代理节点是静态选出的，并完全由项目方部署，NEO 由此被外界质疑为过于中心化。

DBFT 的优点一方面是效率高，NEO 每 15~20 秒生成一个区块，交易吞吐量可达到约 1000TPS，通过适当优化，性能可达 10000TPS；另一方面是其良好的最终性，区块不会分叉，以此来验证参与者的身份，保护网络安全，使区块链能够适用于对交易确认实时性要求高的真实金融场景。

DBFT 的缺点也不容忽视，一方面体现在较低的容错率，当有 1/3 或以上超级节点为恶意节点或宕机后，系统将无法提供服务；另一方面体现在超级节点数量过少，中心化程度高。

5. POW 共识机制的回归

（1）各种共识机制的比较

比特币是解决了拜占庭将军问题的分布式账本，在完全开放的环境中，实现了数据的一致性和安全性。但比特币采用的 POW 共识机制被广泛质疑为：

- 消耗大量能源和硬件设备；
- 区块同步时间长，扩展性弱，TPS 低。

于是效率更高、被认为更加节能环保的 POS、DPOS、BFT 等共识机制相继问世，并得到广泛的应用。各种共识机制的特点：

- 在 POS 共识机制下，全网节点根据权益大小按照某种规则参与区块生产者的选举，共识过程中节点系统开放。但选举过程效率低下，同时由于选举过程复杂，伴随着许多安全问题。
- DPOS 共识通过代理人制度，大幅度提升了 POS 共识的选举效率。但在共识过程中，节点系统是封闭的，而且去中心化程度低。
- BFT 类的共识机制性能较高并具备良好的最终性，但其容错率低，且由于节点的扩展性问题，更加适用于相对封闭的节点系统。

表：各类共识机制的特性

共识机制	特性	
	优势	劣势
POW	1. 安全稳定，节点自由度高 2. 去中心化程度高，节点系统开放	1. 扩展性弱，性能低 2. 没有最终性 3. 造成硬件设备浪费
POS	1. 能源耗费少 2. 去中心化程度较高，节点系统开放	1. 实现过程复杂 2. 存在安全漏洞
DPOS	1. 能源耗费少 2. 性能高 3. 具备最终性	1. 去中心化程度弱，节点系统相对封闭

BFT	1. 性能较高 2. 具备最终性 3. 安全性好	1. 去中心化程度弱，节点系统封闭 2. 容错率低

（2）POW 共识机制能源消耗的必要性

正如张首晟教授所言，现实世界的熵总是在增加的[6]。POW 共识机制将虚拟世界和现实世界连接起来，分布式系统中达成共识的过程是一个熵减的过程，这需要现实世界的熵增来平衡，能量消耗即是提供熵增的平衡方式。

相比于 POW 共识把系统的安全性交给了数学和能量消耗，POS 共识把系统的安全性交给了人性的博弈。POS 共识是虚拟世界中的一个封闭系统，如果共识的达成没有付出任何代价，共识的可靠性就可能存疑，人性博弈过程中的混乱一定会暴露出来。

POS 的升级模式 DPOS 共识机制的共识过程类似于精英代议制，是一种常设特权的治理架构，容易产生腐化。卢梭对代议制的描述是："民意一旦被代表，终究会被扭曲"。DPOS 共识机制是为了效率而生的，它更加适用于对性能要求极高的相对封闭的商业系统。

而对于 BFT 共识机制，由于节点扩展性的缺陷，其共识节点的选择过程一样是封闭或者需要验证的，因而也更加适用于相对封闭的应用环境。

信任的产生是需要付出代价的，POW 共识机制所消耗的能量，不仅不是缺陷，反而是信任产生过程中最有效的平衡机制。

（3）POW 共识在新一代公链中的大规模应用

就现实可执行性角度而言，BitMEX 的研究报告[7]指出，POW 共识机制解决了区块链分叉的选择、数字货币分发、谁产生区块、什么时间产生区块这四个问

[6] 引用自张首晟教授的演讲——区块链技术是互联网世界新的分合转折点。
[7] BitMEX Research: Complete guide to Proof of Stake - Ethereum's latest proposal & Vitalik Buterin interview, April 11, 2018.中文版见 http://www.8btc.com/vitalik-pos，对话 V 神：权益证明 POS 新趋势。

题，而改进的 POS 共识机制只是解决了区块链分叉的选择问题，其他三个问题都是开放的，需要更好的解决路径。

包括 Bytom、Aeternity、Aelf、Zilliqa 在内的新一代公链都包含了 POW 共识机制，第二代公链以太坊第三阶段的 Metropolis 也仍是 POS 和 POW 的混合体。

表：新一代公链的共识机制选择

公链项目	共识机制特性
Bytom	**POW**：人工智能 ASIC 芯片友好型 POW 共识机制。
Aeternity	**POW+POS**：POW 机制生产区块，重大决策由 POS 机制完成，赋予代币持有者权利。
Aelf	**POW+POS**：主链采用 POS 共识机制，侧链采用 POW 共识机制。POS 共识机制的管理成本很高，因而适用于主链，侧链采用 POW 共识机制可安全、自主运行。
Zilliqa	**POW+PBFT**：利用 POW 共识机制的安全性对节点进行验证，验证过的节点交于 PBFT 共识机制决策。
Ethereum 第三阶段 Metropolis	**POW+POS**：POW 共识机制生产区块，只是在每 100 个区块处利用 POS 人为的设置检查点，赋予最终性。

上表所列的公链共识机制选择告诉我们，尽管许多公链有自己独特的设计哲学，但出于安全性考虑，它们依然绕不开 POW 共识机制的保护。**对于开放的、自治度高的公链环境，POW 共识机制有更好的适用性；而 POS 共识过程的管理成本很高，在算法更改、分叉选择等重大决策过程中，POS 共识机制才有其使用价值，但这已经是一种相对中心化的决策机制。**

（4）Bytom 的 POW 共识算法

虽然 POW 共识机制的能源消耗是一种有效的平衡机制，但是 POW 算法的 ASIC 芯片在淘汰之后的大量硬件浪费问题仍需引起关注。Bytom 采用的人工智

能 ASIC 友好型 POW 算法能够减少资源和设备浪费，提升去中心化水平，为 POW 共识机制的进化提供了一个极具建设性的方案。

Bytom 在 POW 共识机制中引入了 Tensority 算法，是区块链挖矿和人工智能的桥梁。Tensority 算法包含的矩阵乘法是人工智能中最通用的算法，几乎所有人工智能设备都能友好地兼容这种算法。同时，Tensority 算法选取的数据类型是 int8，是一种在插电型 AI 设备通用的数据类型。Tensority 算法的这些设计可以让智能摄像头、正在充电的 AI 手机等通用型人工智能设备都能参与比原币挖矿。Tensority 算法可能带来以下的一些场景：

- 区块链共识所需的计算也可以应用于 AI 硬件加速服务，这将产生更大的社会效益。
- 人工智能友好型挖矿将扩大市场对人工智能 ASIC 芯片的需求，促进芯片产业的发展，这与当前 GPU 友好型 PoW 区块链对 GPU 市场的提振效应如出一辙。
- 降低了矿工部署算力的成本，当矿机被淘汰或者闲置时，仍然可以用于人工智能的加速服务，避免硬件资源的浪费。
- 更多通用型人工智能设备将参与到区块链挖矿中，这将有助于扩大区块链的渗透率。

可以预见，Bytom 的人工智能 ASIC 友好型 POW 共识算法可以给区块链挖矿和人工智能芯片的发展带来双赢的局面。

五、总结

公链是区块链发展的前提基础，是区块链技术的底层架构，也是众多区块链应用的操作系统。目前区块链的发展现状是，底层公链的性能尚有诸多技术瓶颈，

在这些公链上构建的各类 DAPP 严重受限于性能、安全性，以及区块链和真实资产、价值的关联性，因而，大规模商业应用难以展开。

公链的核心资源要素可归结为存储资源、传输资源、运算资源和共识机制所产生的信任资源四个方面，对应的核心技术要素表现为可扩展性和传输技术、系统安全、分布式存储、监管兼容性和共识机制五个维度：

- 公链的可扩展性是其承载大规模商业应用的关键，可扩展性和传输技术包含大区块、隔离见证、分片等链上扩容技术，侧链、状态通道等链下扩容技术，点对点传输技术，跨链传输技术等。
- 公链的系统安全体现在系统计算资源的合理分配、数据存储安全和用户的账户财产安全等方面，技术实现方式有对系统计算层的分层处理，侧链和多链技术等。
- 分布式存储问题在于建立一套激励机制，充分利用节点的存储和传输资源，安全地存储数据和稳定地传输数据，降低存储成本，为区块链公链提供基础设施。
- 监管兼容性是指公链在系统设计中需要为监管留出接口，使得现实世界中的商业应用能够在区块链中有序运行，进而为区块链技术的发展提供土壤。
- 共识机制是区块链的灵魂，目前区块链公链的共识机制之争仍众说纷纭。相比于 POW 共识机制把系统的安全性交给了数学和能量消耗，POS 类的共识机制把系统的安全性交给了人性的博弈。因此，对于开放的、自治度高的公链环境，POW 共识机制有更好的适用性；而 POS 共识过

程的管理成本很高，在算法更改、分叉选择等重大决策过程中，POS 共识机制才有其使用价值。

传统互联网底层协议是免费的，所以互联网世界更关注应用层；但由于激励机制的存在，在区块链世界里，底层协议是最大的受益者，因此，区块链的研发和投资更关注底层公链技术。我们预计底层公链仍将是现阶段区块链行业的攻关重点，各公链在可扩展性、应用性、共识哲学，以及应用生态搭建上的角逐将长期延续。