区块链共识机制综述

2018 年 9 月

TokenClub 研究院

目录

1. 行业综述

传统的关系数据库管理系统、NoSQL 数据库管理系统都是由单一机构进行管理和维护，单一机构对所有数据拥有绝对的控制权，其它机构无法完整了解数据更新过程，因而无法完全信任数据库中的数据。所以，在多个机构协作模式下，中心化的数据库管理系统始终存在信任问题。以金融行业的清算和结算业务为例，传统中心化的数据库因无法解决多方互信问题，使得每个参与方都需要独立维护一套承载自己业务数据的数据库，这些数据库实际上是一座座信息孤岛，造成清结算过程耗费大量人工进行对账的情况，目前的清结算时间最快也需按天来计。如果存在一个多方参与者一致信任的数据库系统，则可显著减少人工成本及缩短结算周期。

区块链（Blockchain）是一种去中心化、不可篡改、可追溯、多方共同维护的分布式数据库，能够将传统单方维护的仅涉及自己业务的多个孤立数据库整合在一起，分布式地存储在多方共同维护的多个节点上，任何一方都无法完全控制这些数据，只能按照严格的规则和共识进行更新，从而实现了可信的多方间的信息共享和监督，避免了繁琐的人工对账，提高了业务处理效率，降低了交易成本。区块链通过集成 P2P 协议、非对称加密、共识机制、块链结构等多种技术，解决了数据的可信问题。通过应用区块链技术，无需借助任何第三方可信机构，互不了解、互不信任的多方可实现可信、对等的价值传输。

2008 年，一位化名“中本聪”的学者以一篇《比特币：一种点对点的电子现金系统》的文章，阐述了一种数字加密货币的实现思路。一年之后作者释放出了以论文为原型设计出来的加密货币——比特币。历经近 10 年的发展，比特币一直保持着交易量和市值全球第一的地位，与此同时，支撑比特币运行的核心技术—

—区块链，凭借去中心化、易验证、难篡改，已成为各国政府、国际组织关注的一个热点，许多金融巨头和研究机构纷纷在该领域投上宝贵的精力。各种区块链相关项目爆发式增长。对于区块链技术，目前普遍的观点是其对未来的改变是不可预估的。

1.1 区块链技术

作为支持比特币服务的核心技术，区块链是一种基础设施，是加密货币或者其他应用的底层根本。它使用链式数据结构来验证和存储数据，并使用分布式节点协商机制来生成和更新数据。根据不同的应用场景，区块链分为公共链、联盟链和专有链。

1.1.1 公有链（Public Blockchain）

公有链通常也称为非许可链（Permissionless Blockchain），无官方组织及管理机构，无中心服务器，参与的借点按照系统规格自由接入网路、不受控制，节点间基于共识机制开展工作。

公有链是真正意义上的完全去中心化的区块链，它通过密码学保证交易不可篡改，同时也利用密码学验证以及经济上的激励，在互为陌生的网络环境中建立共识，从而形成去中心化的信用机制。在公有链中的共识机制一般是工作量证明（PoW）或权益证明（PoS），用户对共识形成的影响力直接取决于他们在网络中拥有资源的占比。

公有链一般适合于虚拟货币、面向大众的电子商务、互联网金融等 B2C、C2C 或 C2B 等应用场景，比特币和以太坊等就是典型的公有链。

1.1.2 联盟链（Consortium Blockchain）

联盟链是一种需要注册许可的区块链，这种区块链也称为许可链（Permissioned Blockchain）。联盟链仅限于联盟成员参与，区块链上的读写权限、参与记账权限按联盟规则来制定。整个网络由成员机构共同维护，网络接入一般通过成员机构的网关节点接入，共识过程由预先选好的节点控制。由于参与共识的节点比较少，联盟链一般不采用工作量证明的挖矿机制，而是多采用权益证明（PoS）或 PBFT（Practical Byzantine Fault Tolerant）、RAFT 等共识算法。

一般来说，联盟链适合于机构间的交易、结算或清算等 B2B 场景。例如在银行间进行支付、结算、清算的系统就可以采用联盟链的形式，将各家银行的网关节点作为记账节点，当网络上有超过 2/3 的节点确认一个区块，该区块记录的交易将得到全网确认。联盟链对交易的确认时间、每秒交易数都与公有链有较大的区别，对安全和性能的要求也比公共链高。

1.1.3 私有链（Private Blockchain）

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。私有链的应用场景一般是企业内部的应用，如数据库管理、审计等；在政府行业也会有一些应用，比如政府的预算和执行，或者政府的行业统计数据，这个一般来说由政府登记，但公众有权力监督。私有链的价值主要是提供安全、可追溯、不可篡改、自动执行的运算平台，可以同时防范来自内部和外部对数据的安全攻击，这个在

传统的系统是很难做到的。

三种不同形式的区块链对比分析

	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	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	不需要
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	3-5000笔/秒	1000-1万笔/秒	1000-10万笔/秒
典型场景	虚拟货币	支付、结算	审计、发行
代币项目	比特币、以太坊	R3、Hyperleder	

1.2 区块链体系架构

从最早应用区块链技术的比特币到最先在区块链引入智能合约的以太坊，再到应用最广的联盟链 Hyperledger Fabric，它们尽管在具体实现上各有不同，但在整体体系架构上存在着诸多共性。如下图所示，区块链平台整体上可划分为网络层、共识层、数据层、智能合约层和应用层五个层次。

		比特币	以太坊	Hyperledger Fabric
应用层		比特币交易	Dapp/以太币交易	企业级区块链应用
智能合约层	编程语言	Script	Solidity/Serpent	Go/Java
	沙盒环境		EVM	Docker
数据层	数据结构	Merkle树 区块链表	Merkle树 Patricia树/ 区块链表	Merkle Bocket树/ 区块链表
	数据模型	基于交易的模型	基于账户的模型	基于账户的模型
	区块存储	文件存储	LevelDB	文件存储
共识层		PoW	PoW/PoS	PBFT/SBFT
网络层		TCP-based P2P	TCP-based P2P	HTTP/2-based P2P

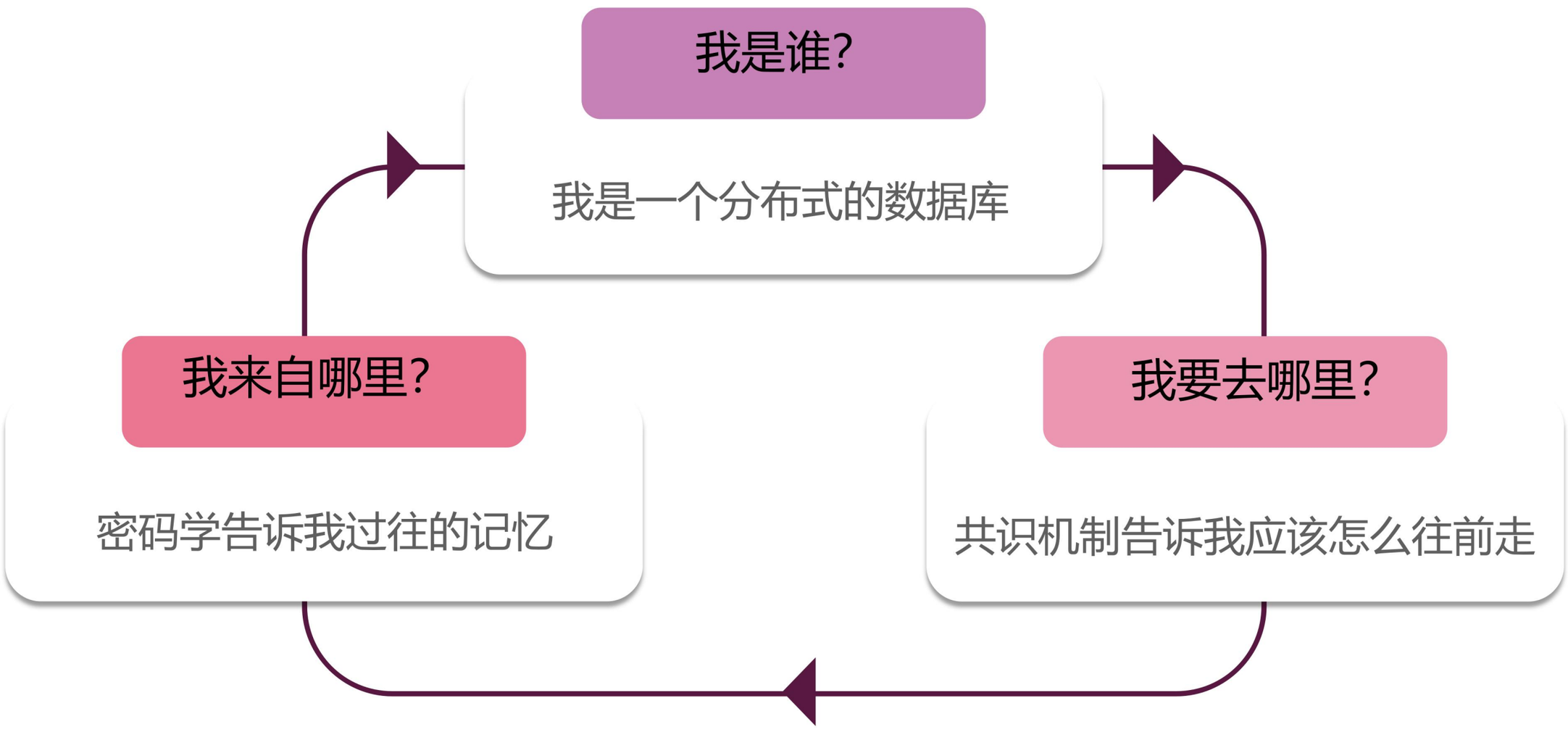
此篇报告重点介绍共识层的共识机制。

2. 共识机制简介

区块链有以下三个基本特征：

- 区块链是一个分布式数据库（系统）
- 区块链采用密码学，保证数据不被篡改
- 区块链采用共识算法来对于新增的数据达成共识

这三点可以简单的从哲学上理解为：



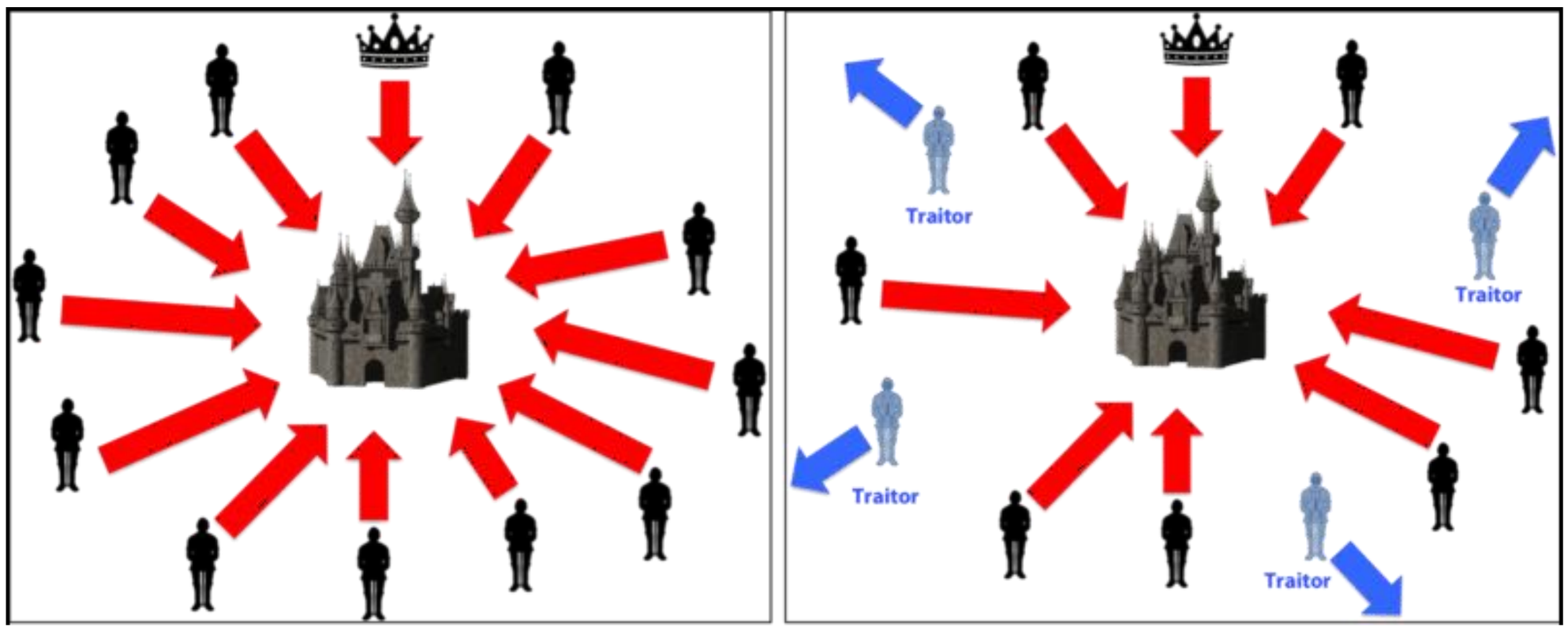
区块链技术的伟大之处就是它的共识机制，在去中心化的思想上解决了节点间互相信任的问题。区块链拥有众多节点并达到一种平衡状态是因为共识机制。尽管密码学占据了区块链的半壁江山，但是共识机制才是让区块链系统不断运行下去的关键。所以，要深入谈及区块链的共识机制，就避不开一个问题，拜占庭问题。

2.1 共识机制的起源

现代共识机制的基础于 1962 年提出。RAND Corporation 的一名工程师 Paul Baran 在论文《论分布式通讯网络》中提出了加密签名的概念。这些数字化签名不久就成为了系统对修改数据或文档的用户进行验证的方法。二十年后，三名学者发表了一篇关于去中心化系统可靠性问题的论文。在《拜占庭将军问题》中，作者 Leslie Lamport、Robert Shostak、和 Marshall Pease 提出了一个思维实验：拜占庭将军问题。

2.1.1 拜占庭将军问题

拜占庭问题是容错计算中的一个老问题，有莱斯特兰伯特等人在 1982 年提出。拜占廷帝国为公元 395 年直至 1453 年的东罗马帝国，拜占庭城邦拥有巨大的财富，令他的十个邻邦垂涎已久，但是拜占庭高墙耸立，固若金汤，没有任何一个单独的邻邦能够成功入侵，任何单个城邦的入侵行动都会失败，而入侵者的军队也会被歼灭，使得其自身反而容易遭到其它九个城邦的入侵。这十个城邦之间也互相觊觎对方的财富并经常爆发战争。



拜占庭的防御能力如此之强，非大多数人一起不能攻破。而且只要其中一个城邦背叛盟军，那么所有进攻军队都会被歼灭，并随后被其他邻邦所劫掠。因此这是一个互不信任的各个邻邦构成的分布式网络。每一方都小心行事，因为稍有不慎就会给自己带来灾难。为了获取拜占庭的巨额财富，这些邻邦分散在拜占庭的周围，依靠士兵传递消息来协商进攻目的及进攻时间，这些邻邦将军想要攻克拜占庭，但面临的一个困扰，邻邦将军不确定他们之中是否有叛徒，叛徒是否擅自变更进攻意向或者进攻时间？在这种状态下，将军们能否找到一种分布式协议来进行远程协商达成他们的共识，进而赢取拜占庭城邦的财富呢？

在拜占庭将军问题模型中，对于将军们有两个公认的假设：

假设一

所有忠诚的将军受到相同的命令后，执行这条命令，得到的结果一定是相同的，它的含义是所有节点对命令的解析和执行是一样的，这个命令必须是一个确定性的命令，不能存在随机性，也不能依赖节点自身的状态，也就是说这个秘密不能是心情好，就攻击敌人，心情不好就原地休息

假设二

如果命令是正确的，那么所有忠诚的将军必须执行这条命令，换句话说，忠诚的将军需要判断，接收到的命令是不是正确的

对于将军们的通讯过程，在“拜占庭将军问题”中也是有默认假设的：点对点通信是没有问题的，也就是说在这里，我们假设 A 将军要给 B 将军一条命令“M”，那么派出去的传令兵一定会准确的把命令“M”传给 B 将军。

但问题在于，如果每个城邦向其他九个城邦派出一名信使，那么就是这十个城邦，

每一个都派出了九名信使，也就是在任何一个时间有总计 90 次的信息传输，并且每个城市分别收到九条信息，可能每一条都写着不同的进攻时间，除此以外，信息传输过程中，如果叛徒想要破坏原有的约定时间，就会自己修改相关信息，然后发给其他城邦以混淆试听，这样的结果是，部分城邦收到错误信息后，会遵循一个或者多个城邦已经修改过的攻击时间相关信息，从而背叛发起人的本意。这样一来，遵循错误信息的城邦（包含叛徒），将重新广播超过一条信息的信息链，整个信息链会随着他们所发送的错误信息，迅速变成不可信的信息和攻击时间，变成一个相互矛盾的纠结体。

针对这个问题，人们主要提出了两种解决方法，一个是口头协议算法；另一个是书面协议算法。

口头协议算法的核心思想：要求每一个被发送的消息都能被正确投递，信息接收者明确知道消息发送者的身份，并且信息接收者知道信息中是否缺少信息。采用口头协议算法，若叛徒数少于 1/3 时，则拜占庭将军问题可以很容易解决。但是口头协议算法存在着明显的缺点，那就是消息不能溯源。

为解决该问题，提出了**书面协议算法**。该算法要求签名，不可伪造，一旦被篡改即可发现，同时任何人都可以验证签名的可靠性。

就算是书面协议算法，也不能完全解决拜占庭将军问题，因为该算法没有考虑信息传输延迟、签名体系难以实现的问题。且签名消息记录的保存，也难以摆脱中心化机构。

而这个问题该如何解决？中本聪的理念给出了一个比较好的答案：不能让所有人都有资格发信息，而是给发信息设置了一个条件：“工作量”。将军们同时做一

道计算题，谁先算完，谁才能获得给其他小国发信息的资格。而其他小国在收到信息后，必须采用加密技术进行签字盖戳，以确认身份。然后再继续做题，做对题的再继续发消息……对这种先后顺序达成共识的算法，开创了共识机制的先河。

2.2.2 区块链共识机制解决方案

中本聪所创建的比特币，通过对这个系统，做出一个简单的变化解决了这个问题。它为发送信息加入成本，这降低了信息传递的速率，并加入了一个随机元素，以保证在一个时间只有一个城邦，可以进行广播。

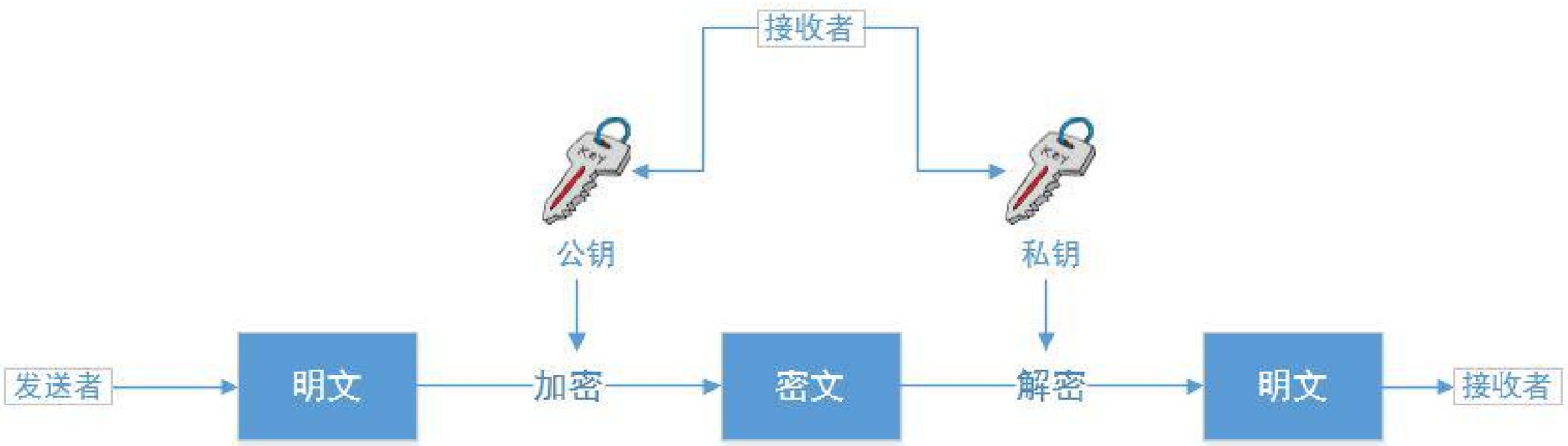
中本聪加入的成本是“工作量证明”——挖矿，并且工作量证明是基于计算一个随机哈希算法。哈希算法唯一做的事情就是获得一些输入，然后进行计算，并得到一串 64 位的随机数字和字母的字符串。

在比特币的世界中，输入数据，包括了到当前时间点的整个总帐。尽管单个哈希值用现在的计算机几乎可以及时的计算出来，但是比特币系统接受的工作量证明，是无数个 64 位哈希值中唯一的哈希值，而且这个哈希值前 13 个字符均为 0，这样一个哈希值是极其罕见，不可能被破解的，并且在当前却要花费整个比特币网络，总算力约十分钟的时间才能找到一个。

在一台网络机器随机的找到一个有效哈希值之前，上十亿个的无效值会被计算出来，计算哈希值就需要花费大量时间，增加了发送信息的时间间隔，造成信息传递速率减慢，而这就是使得整个系统可用的“工作量证明”。

而那台发现下一个有效哈希值的机器，能将所有之前的信息放到一起，附上他自己的辨识信息，以及它的签名/印章诸如此类，向网络中的其他机器广播出去。只要其他网络中的机器接收到并验证通过了，这个有效的哈希值和附着在上面的签名信息，他们就会停止他们当下的计算，使用新的信息更新他们的总账拷贝，然后把新更新的总账作为哈希算法的输入，再次开始计算哈希值。

哈希计算竞赛，从一个新的开始点重新开始，如此这般，网络持续同步着，所以网络上的电脑都使用着同一版本的总账，与此同时，每一次成功找到有效哈希值以及区块链更新的间隔，大概是十分钟，在那十分钟以内，网络上的参与者发送信息并完成交易，并且因为网络上的每一个机器都是使用同一个总账，所有的这些交易和信息都会进入每一份遍布全网的总账拷贝。当区块链更新，并在全网同步之后，在之前十分钟内进入区块链的所有交易也被更新并同步。因此分散的交易记录，是在所有的参与者之间进行对账和同步的。



最后在用户向网络输入一笔交易的时候，他们使用内嵌在比特币客户端的标准公钥加密工具来加密，同时用他们的私钥以及接收者的公钥为这笔交易签名，这对应于拜占庭将军问题中，他们用来签名和验证消息时使用的“印章”。因此，哈希计算速率的限制，加上公钥加密，使得一个不可信网络变成一个可信的网络，

所有参与者可以在某些事情上达成一致（比如说攻击时间、或者一系列的交易域名记录，政治投票系统，或者任何其他的需要分布式协议的地方）。

将比特币的共识机制引入拜占庭问题，就形成了这样一种情况，城邦 A 向其他九个城邦发送进攻相关信息，是直接将相关信息及其当时发送的时间，附加在通过哈希算法加密的信息中，并且加上独属于自己的数字签名传递给其他城邦。等其他城邦中相应的机器已经收到，并验证通过这个有效哈希值和附加在上面的签名信息，他们就会停止他们当下的计算，使用新的信息更新他们的总的进攻信息拷贝，然后把新更新的信息区块链作为哈希算法的输入，再发给其他城邦。其他城邦接受消息后，重复此流程直至所有城邦都收到消息。如此这般，网络持续同步着，所有网络上的电脑都使用着同一版本的总账。

如果叛徒想要修改进攻信息来误导其他城邦时，其他城邦的机器会立刻识别到异常信息，同步的虚假信息将不被认可，依旧会同步其他大部分共同的信息，这样叛徒就失败了，他无法破坏十个城邦当中的大多数节点，也就是至少六个节点，这样信息的一致性就得到了保证，完美解决了拜占庭问题。

这就是区块链共识机制为何如此特别的关键，他为一个算法上的难题提供了解决方案，区块链的共识机制，通过不断同步各个节点的信息，使得各分布式节点之间达到一种平衡，保证了绝大多数节点的一致性，即达成了共识。

2.2 共识机制的概念

由于加密货币多数采用去中心化的区块链设计，节点是各处分散且平行的，所以必须设计一套制度，来维护系统的运作顺序与公平性，统一区块链的版本，并奖励提供资源维护区块链的使用者，以及惩罚恶意的危害者。这样的制度，必须依赖某种方式来证明，是由谁取得了一个区块链的打包权（或称记账权），并且可以获取打包这一个区块的奖励；又或者是谁意图进行危害，就会获得一定的惩罚，这就是共识机制。

区块链的共识机制通常包含了两个方面：

达成共识的计算机算法，即共识算法
（Consensus Algorithm）

达成共识的规则，即共识规则
（Consensus Rule）

我们经常说的“共识机制”，多数情况下同时包含了共识算法和共识规则，少数情况下单指其中一方，这也是大家经常在认识上存在的误区。

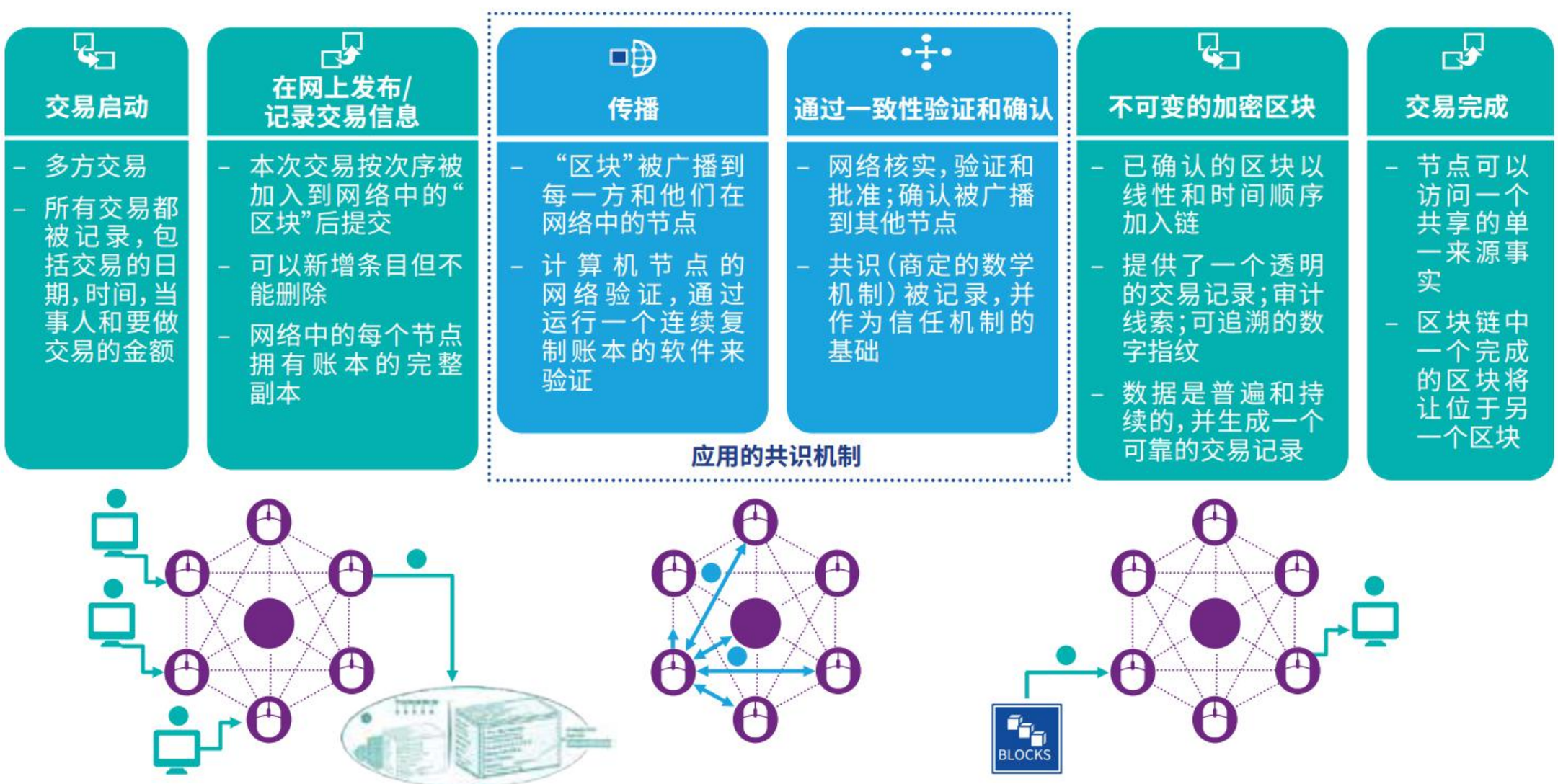
由于点对点网络下存在较高的网络延迟，各个节点所观察到的事务先后顺序不可能完全一致。因此区块链系统需要设计一种机制对在差不多时间内发生的事务的先后顺序进行共识。这种对一个时间窗口内的事务的先后顺序达成共识的算法被

称为“共识机制”。这里解释的其实只是共识算法，也就是节点依照共识规则达成共识的计算机算法。

而共识规则（Consensus Rule）则是指每个区块链里面都有自己精心设计好的规则性协议，这些协议通过共识算法来保证共识规则得以可靠地执行。譬如我们通常所说的比特币的挖矿，就是比特币记账的共识规则，其专业术语为 PoW（Proof of Work），即工作量证明。比特币的工作量证明共识规则是通过 SHA（Secure Hash Algorithm）系列安全散列算法之一的 SHA256 来得以可靠地执行的。

2.3 共识机制的作用

区块链的核心是参与者之间的共识（参见下图蓝色标识的第三、四步）。共识机制之所以关键，是因为他的作用：在没有中央机构的情况下，参与者必须就规则及其应用方法达成一致，并同意使用这些规则来接受及记录拟定的交易。

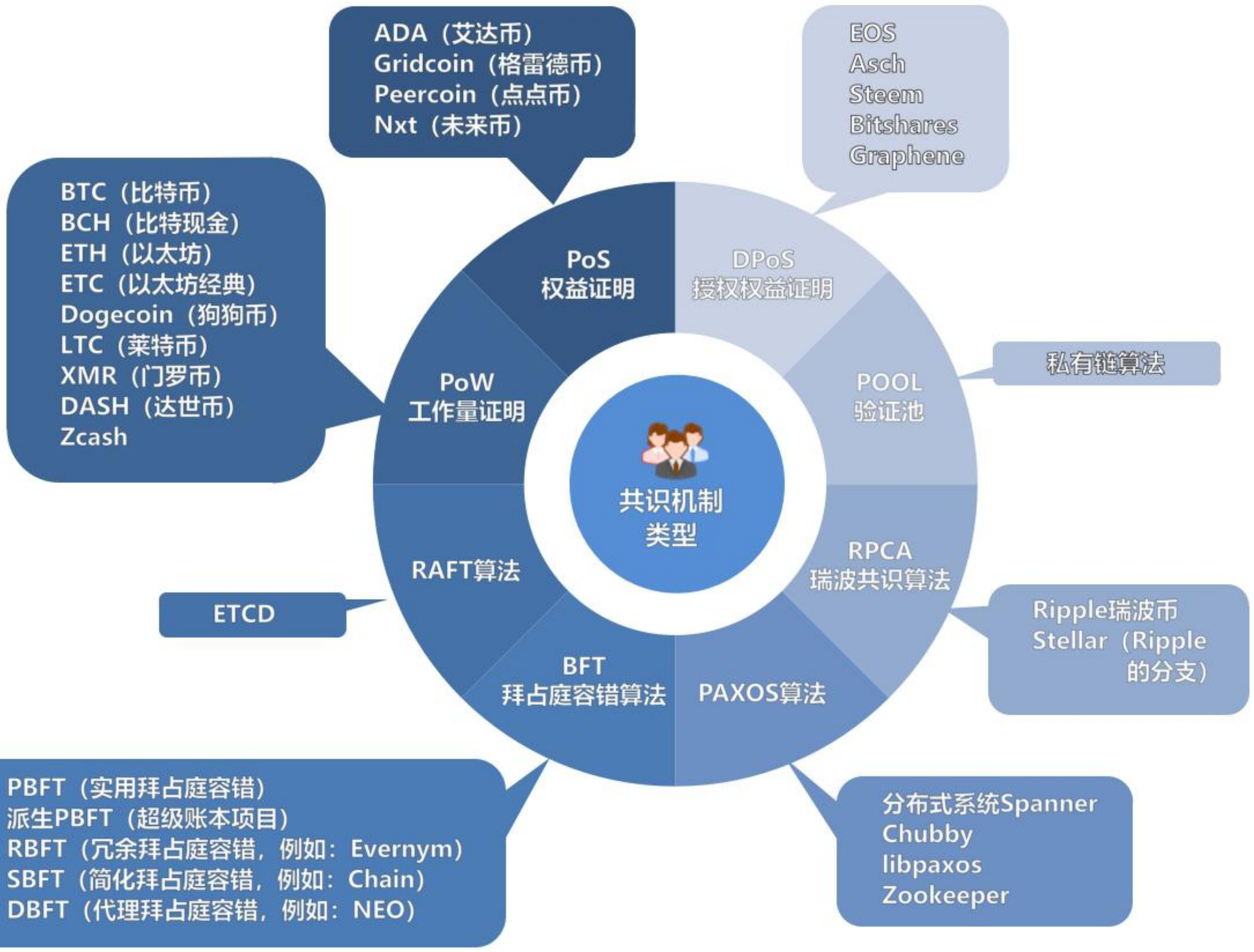


如上图所示，交易一经创建和发布，即署有交易发起人的签名，签署表示获得授权以支付金钱、订立合同或传递与交易相关的数据指标。交易在签署后即可生效并包含执行需要的所有信息。

一旦交易被验证并纳入区块，该交易便会在整个网络中传播。在整个网络达成共识和网络中的其他节点接受新区块后，该区块就并入区块链中。一经区块链的记录和足够多的节点确认，该交易将成为公共账本的永久组成部分，区块链网络中的所有节点亦会视之为有效。

3. 共识机制的原理

共识机制被用来决定区块链网络中的记账节点，并对交易信息进行确认和一致性同步。早期的比特币区块链采用高度依赖节点算力的工作量证明（Proof of Work，PoW）机制来保证比特币网络分布式记账的一致性。随着区块链技术的发展和各种竞争币的相继涌现，下图展示了当前市面常见的共识机制极其有代表性的项目。

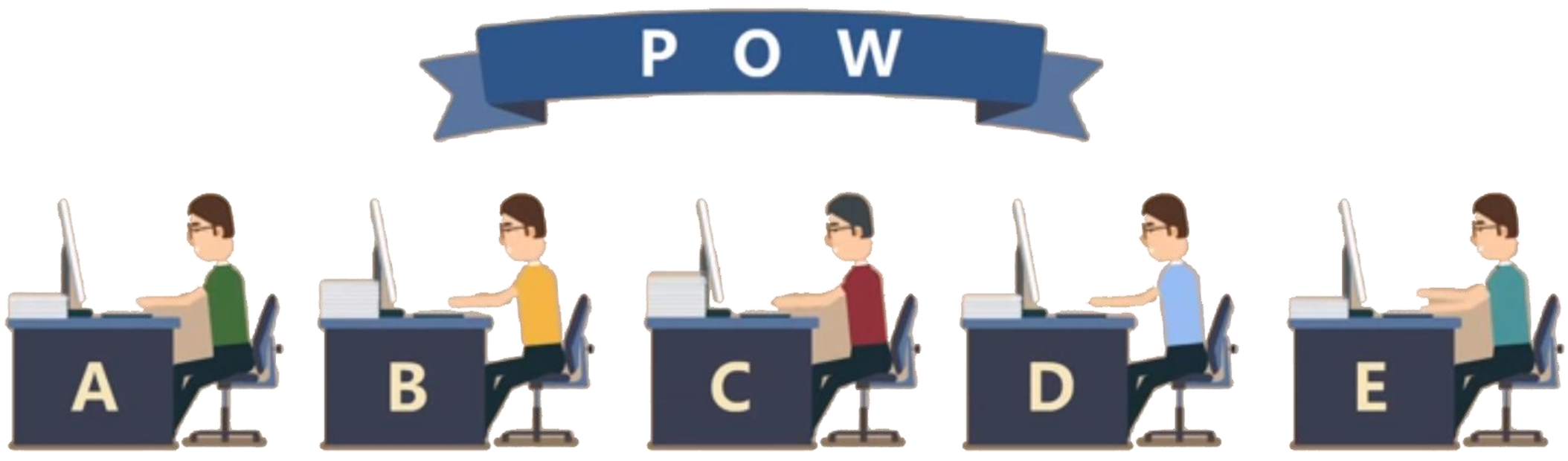


因技术更新日新月异，以上共识机制的种类和描述仅是近期某一时点（2018 年 9

月）的概览。本文的目的并不是完整展示当前所有共识机制，而仅描述那些当前作为区块链建立的技术选项而被热切讨论和探索的机制。本文并非进行学术讨论，所以关于共识机制的具体技术细节并没有深入讲解，仅仅是进行概略性的简介。以下介绍的共识机制中的大部分在区块链和分布式账本产生前已被应用。

3.1 PoW

工作量证明（Proof of Work，PoW）的主要特点是将解决计算困难问题所需要的计算代价作为新加入块的凭证和获得激励收益。



中本聪在其比特币奠基性论文中设计了 POW 共识机制，其核心思想是通过引入分布式节点的算力竞争来保证数据一致性和共识的安全性。比特币系统中，各节点（即矿工）基于各自的计算机算力相互竞争来共同解决一个求解复杂但验证容易的 SHA256 数学难题（即挖矿），最快解决该难题的节点将获得区块记账权和系统自动生成的比特币奖励。

该数学难题可表述为：根据当前难度值，通过搜索求解一个合适的随机数

（Nonce），使得区块头各元数据的双 SHA256 哈希值小于或等于目标哈希值，比特币系统通过灵活调整随机数搜索的难度值来控制区块的平均生成时间为 10min 左右。

一般说来，POW 共识的随机数搜索过程如下：

- 第一步：搜集当前时间段的全网未确认交易，并增加一个用于发行新比特币奖励的 Coinbase 交易形成当前区块体的交易集合。

- 第二步：计算区块体交易集合的 Merkle 根记入区块头，并填写区块头的其他元数据，其中随机数 Nonce 置零。

- 第三步：随机数 Nonce 加 1，计算当前区块头的双 SHA256 哈希值如果小于或等于目标哈希值，则成功搜索到合适的随机数并获得该区块的记账权；否则继续执行第三步直到任一节点搜索到合适的随机数为止。

- 最后一步：如果一定时间内未成功则更新时间戳和未确认交易集合，重新计算 Merkle 根后继续搜索。

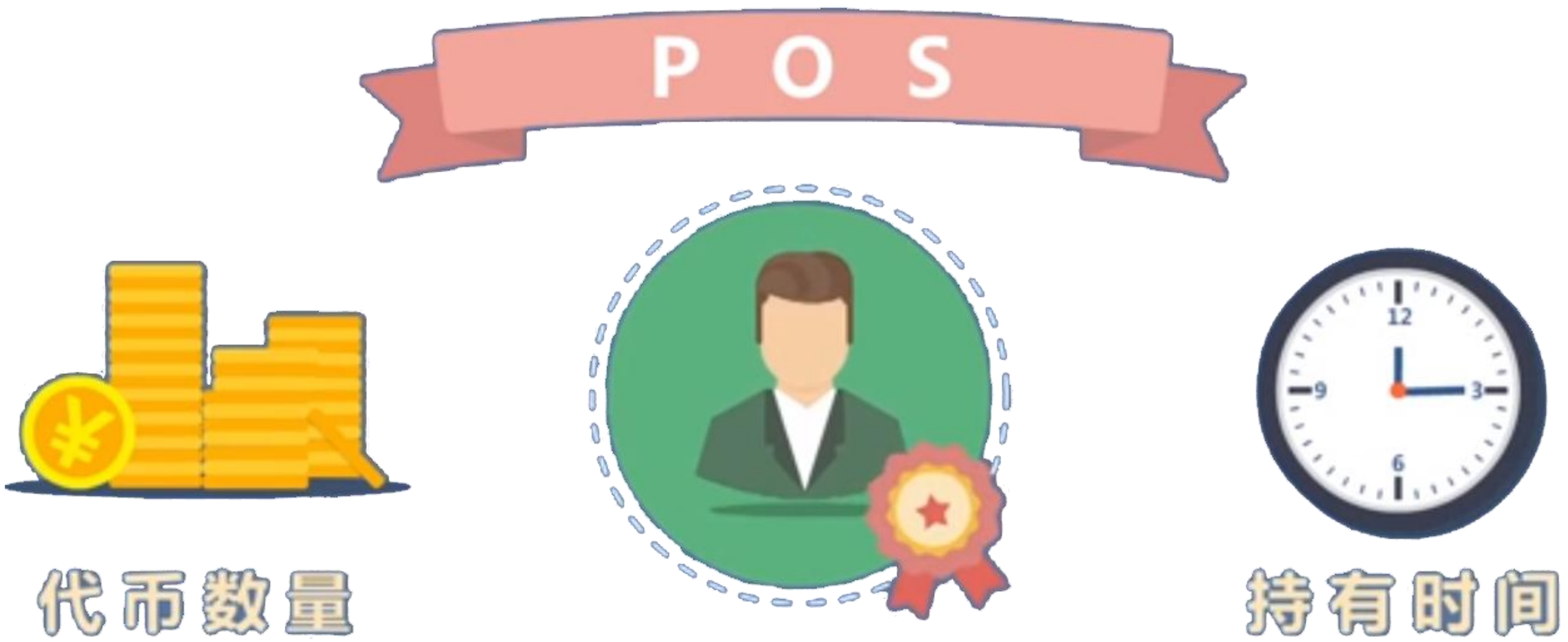
符合要求的区块头哈希值通常由多个前导零构成，目标哈希值越小，区块头哈希值的前导零越多，成功找到合适的随机数并挖出新区块的难度越大。由此可见，比特币区块链系统的安全性和不可篡改性是由 POW 共识机制的强大算力所保证的，任何对于区块数据的攻击或篡改都必须重新计算该区块以及其后所有区块的 SHA256 难题，并且计算速度必须使得伪造链长度超过主链，这种攻击难度导致的成本将远超其收益。正是由于这种机制保证了区块链的数据一致性和不可篡改性，但是同时也带来了资源浪费，甚至由于超大矿池的出现而失去了去中心的优

势。

举个简单的例子，如果算法得到的哈希值总是在 0-10000 之间，而算法要求得到的（哈希值）小于 1，一台机器如果一秒钟能够计算一次,那么平均计算一万次，就有一次值可能小于 1；或者反过来说，每次计算，有万分之一的机会小于 1。如果有一万台节点同时在计算，那么每秒都有可能有一台节点得到符合条件的结果，得到符合条件结果的节点就是出块成功。而每一秒，得到结果的机器都可能不一样。这样就获得了足够随机的结果。

3.2 PoS

权益证明（Proof of Stake，PoS）的主要特点以权益证明代替工作量证明，由具有最高权益的节点实现新块加入和获得激励收益。



由于工作量证明机制资源消耗大且计算资源趋于中心化，权益证明机制受到广泛关注。如果把工作量证明中的计算资源视为对区块进行投票的份额，那么权益证

明就是将与系统相关的权益作为投票的份额。合理假设，权益的所有者更乐于维护系统的一致性和安全性。

假设网络同步性较高，系统以轮为单位运行。在每一轮的开始，节点验证自己是否可通过权益证明被选为代表，只有代表可以提出新的区块。代表在收到的最长的有效区块链后提出新的待定区块，并将自己生成的新的区块链广播出去，等待确认。下一轮开始时，重新选取代表，对上一轮的结果进行确认。诚实的代表会在最长的有效区块链后面继续工作。如此循环，共同维护区块链。

权益证明机制在一定程度上解决了工作量证明机制能耗大的问题，缩短了区块的产生时间和确认时间，提高了系统效率。权益证明每一轮产生多个通过验证的代表，也就是产生多个区块，在网络同步性较差的情况下，系统极易产生分叉，影响一致性。若恶意节点成为代表，就会通过控制网络通信，形成网络分区。向不同网络分区发送不同待定区块，就会造成网络分叉，从而可进行二次支付攻击，严重影响系统安全性。恶意敌手也可以对诚实代表进行贿赂，破坏一致性。权益证明的关键在于如何选择恰当的权益，构造相应的验证算法，以保证系统的一致性和公平性。不当的权益会影响系统公平性。例如，PPCoin 采用币龄作为权益的一个因子，若部分节点在进入系统初期就保持一部分小额交易不用于支付，则币龄足够大，该节点更容易被选为代表，影响系统公平性。

在 PoS 出现后，一些针对其中某个缺点进行修改而诞生的新协议被称作 PoS 的衍生协议，比如 PoSV 和 PoA。

PoSV 针对 PoS 中币龄是时间的线性函数这一问题进行改进，致力于消除货币持有者的屯币现象。PoSV 意为权益和活动频率证明，是瑞迪币(Reddcoin)目前使用的共识机制，瑞迪币在前期使用 POW 进行币的分发，后期使用 PoSV 维护

网络长期安全。PoSV 将 PoS 中币龄和时间的线性函数修改为指数式衰减函数，即币龄的增长率随时间逐渐减少最后趋于零，因此新币的币龄比老币增长得更快，直到达到上限阈值，这样在一定程度上缓和了货币持有者屯币现象。

PoA 意为行动证明，也是 PoS 的一种改进方案。它的本质是通过奖励参与度高的货币持有者而不是惩罚消极参与者来维护系统安全。PoA 将 PoW 和 PoS 结合在一起，主要思想是将 PoW 挖矿生成币的一部分以抽奖的方式分发给所有活跃节点，而节点拥有的股权与抽奖券的数量即抽中概率成正比。

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。

3.3 DPoS

为了进一步加快交易速度，同时解决 PoS 中节点离线也能累积币龄的安全问题，Daniel Larimer 于 2014 年 4 月提出 DPoS。

股份授权证明（Delegated Proof of Stake，DPoS）是 PoS 的一个演化版本，首先通过 PoS 选出代表，进而从代表中选出块生成者并获得收益。

DPoS 共识机制的基本思路类似于“董事会决策”，即系统中每个股东节点可以

将其持有的股份权益作为选票授予一个代表，获得票数最多且愿意成为代表的前 101 个节点将进入“董事会”，按照既定的时间表轮流对交易进行打包结算并且签署（即生产）一个新区块。每个区块被签署之前必须先验证前一个区块已经被受信任的代表节点所签署，“董事会”的授权代表节点可以从每笔交易的手续费中获得收入，同时要成为授权代表节点必须缴纳一定量的保证金，其金额相当于生产一个区块收入的 100 倍。授权代表节点必须对其他股东节点负责，如果其错过签署相对应的区块，股东将会收回选票，从而将该节点“投出”董事会。因此授权代表节点通常必须保证 99%以上的在线时间以实现盈利目标。

显然，与 PoW 共识机制必须信任最高算力节点和 PoS 共识机制必须信任最高权益节点不同的是，DPoS 共识机制中每个节点都能够自主决定其信任的授权节点，且由这些节点轮流记账生成新区块，因而大幅减少了参与验证和记账的节点数量，可以实现快速共识验证。

运用 DPoS 机制的最典型的是 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。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。

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。

3.4 RPCA

瑞波共识算法（Ripple Protocol Consensus Algorithm，RPCA）是一种数据正确性优先的网络交易同步算法，它是基于特殊节点（也称“网关”节点）列表达成的共识。在这种共识机制下，必须首先确定若干个初始特殊节点，如果要新接入一个节点，必须获得 51%的初始节点的确认，并且只能由被确认的节点产生区块。

瑞波共识机制的工作原理如下：

- 第一步，验证节点接收存储待验证交易，将其存储在本地。本轮共识过程中新到的交易需要等待，在下次共识时再确认。

- 第二步，由活跃信任节点发送提议。信任节点列表是验证池的一个子集，其信任节点来源于验证池，参与共识过程的信任节点须处于活跃状态，验证节点与信任节点间存在保活机制，长期不活跃节点将被从信任节点列表删除。信任节点根据自身掌握的交易双方额度、交易历史等信息对交易做出判断，并加入到提议中进行发送。

- 第三步，本验证节点检查收到的提议是否来自信任节点列表中的合法信任节点，如果是，则存储；如果不是，则丢弃。

- 第四步，验证节点根据提议确定认可交易列表，假定信任节点列表中活跃的信

任节点个数为 M (比如 5 个)，本轮中交易认可阈值为 N (百分比，比如 50%)，则每一个超过 M×N 个信任节点认可的交易将被本验证节点认可，本验证节点生成认可交易列表。系统为验证节点设置一个计时器，如果计时器时间已到，本信任节点需要发送自己的认可交易列表。

- 第五步，账本共识达成。本验证节点仍然在接收来自信任节点列表中信任节点的提议，并持续更新认可交易列表，验证节点认可列表的生成并不代表最终账本的形成以及共识的达成，账本共识只有在每笔交易都获得至少超过一定阈值（比如 80%）的信任节点列表认可才能达成，这时交易验证结束，否则继续上述过程。

- 第六步，共识过程结束，形成最新的账本，将上轮剩余的待确认交易以及新交易纳入待确认交易列表，开始新一轮共识过程。

瑞波共识机制使得一组节点能够基于特殊节点列表达成共识。初始特殊节点列表就像一个俱乐部，要接纳一个新成员，必须由一定比例的该俱乐部会员投票通过。因此，它区别于其它共识机制的主要因素是有一定的“中心化”。

3.5 PAXOS

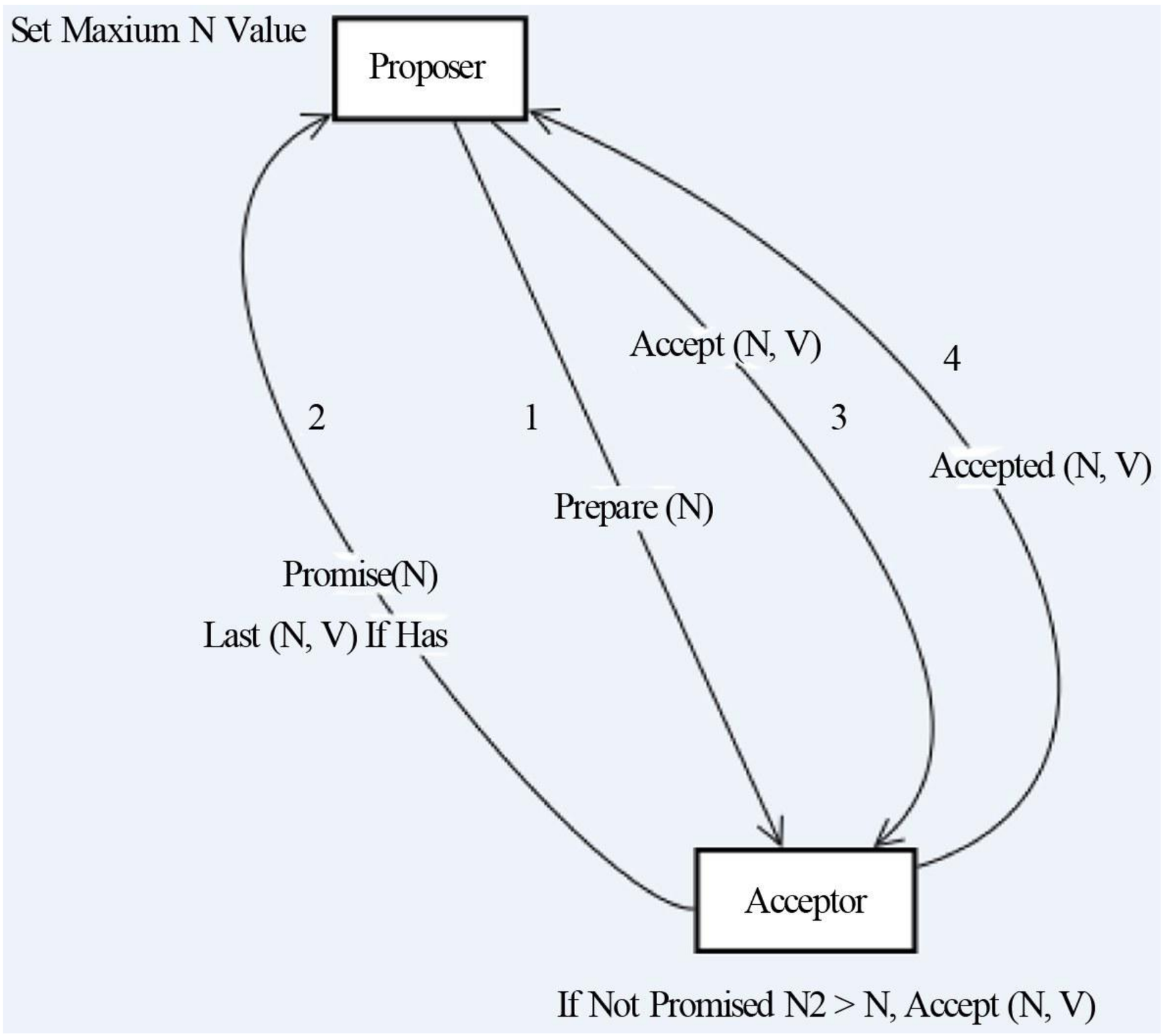
PAXOS 是一种基于消息传递且具有高度容错特性的一致性算法，PAXOS 算法中将节点分为 3 种类型：

ProPoSer 角色	负责提出一个提案，等待大家批准，往往是客户端担任该角色
Acceptor 角色	负责对提案进行投票，往往是服务端担任该角色
Learner 角色	被告知提案结果，并与之统一，不参与投票过程，可能为客户端或服务端

基本共识过程是先由 ProPoSer 提出提案，先争取大多数 Acceptor 的支持，超过一半支持时，则发送结案结果给所有人进行确认。如果 ProPoSer 在此过程中出现故障，可以通过超时机制来解决。极为凑巧的情况下，每次新的一轮提案的 ProPoSer 都恰好故障，系统则永远无法达成一致（概率很小）。

- 第一阶段，ProPoSer 向网络内超过半数的 Acceptor 发送 Prepare 消息，Acceptor 正常情况下回复 Promise 消息。

- 第二阶段，在有足够多 Acceptor 回复 Promise 消息时，ProPoSer 发送 Accept 消息，正常情况下 Acceptor 回复 Accepted 消息。PAXOS 中 3 类角色的主要交互过程在 ProPoSer 和 Acceptor 之间（见下图）。



其中 1、2、3、4 代表顺序。PAXOS 协议用于微信 PaxosStore 中，每分钟调用 PAXOS 协议过程数 10 亿次量级。PAXOS 协议被用于分布式系统中典型的例子就是 Zookeeper，它是第一个被证明的共识算法，其原理基于两阶段提交并进行了扩展。

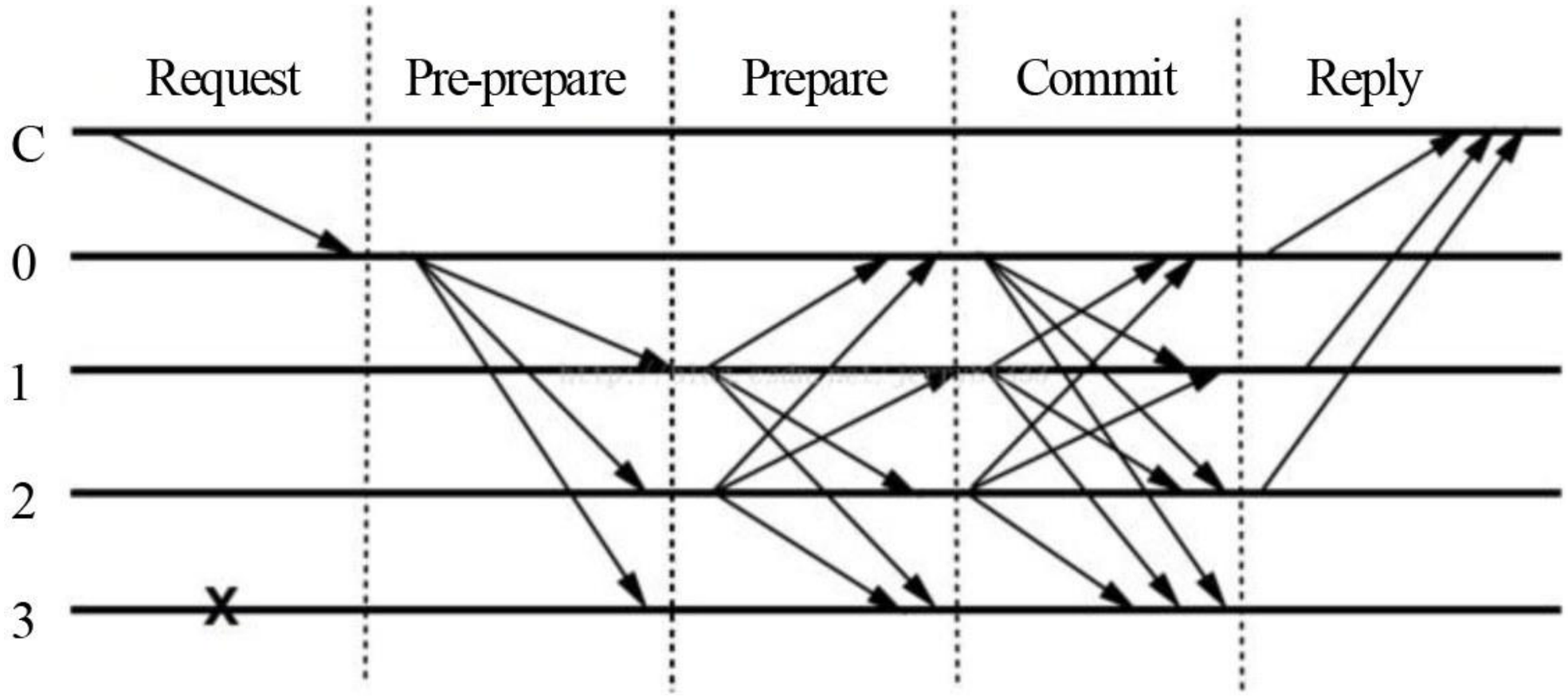
3.6 BFT

拜占庭将军问题提出后，有很多的算法被提出用于解决这个问题。这类算法统称拜占庭容错算法（BFT: Byzantine Fault Tolerance）。BFT 从上世纪 80 年代开始被研究，目前已经是一个被研究得比较透彻的理论，具体实现都已经有现成的算法。

3.6.1 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 算法分为 5 个阶段：请求（Request）、预准备（Pre-prepare）、准备（Prepare）、确认（Commit）、回复（Reply），共识过程如下图所示。



图中 C 为发送请求端，0、1、2、3 为服务端，3 为宕机的服务端，具体步骤是：

- 第一步，请求阶段。从全网节点选举出一个主节点（Leader），这里是 0，新区块由主节点负责生成，请求端 C 发送请求到主节点。

- 第二步，预准备阶段，每个节点把客户端发来的交易向全网广播，主节点 0 将从网络收集到需放在新区块内的多个交易排序后存入列表，并将该列表向全网广播，扩散至 123。

- 第三步，准备阶段，每个节点接收到交易列表后，根据排序模拟执行这些交易。所有交易执行完后，基于交易结果计算新区块的哈希摘要，并向全网广播，1→023，2→013，3 因为宕机无法广播。

- 第四步，提交阶段，如果一个节点收到的 2f（f 为可容忍的拜占庭节点数）个其他节点发来的摘要都和自己相等，就向全网广播一条 Commit 消息。第五步，回复阶段，如果一个节点收到 2f+1 条 Commit 消息，即可提交新区块及其交易到本地的区块链和状态数据库。

这种机制下有一个叫视图的概念，在一个视图里，一个是主节点，其余的都叫备份节点。主节点负责将来自客户端的请求排好序，然后按序发送给备份节点们。但是主节点可能是有问题的，它可能会给不同的请求编上相同的序号，或者不去分配序号，或者让相邻的序号不连续。备份节点应当有职责来主动检查这些序号的合法性，并能通过超时机制检测到主节点是否已经宕掉。当出现这些异常情况时，这些备份节点就会触发视图更换协议来选举出新的主节点。

3.6.2 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(2n+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。

3.7 RAFT

RAFT（The Raft Consensus Algorithm）算法是对 PAXOS 算法的一种简单实现。核心思想是如果数个数据库的初始状态一致，只要之后进行的操作一致，就能保证之后的数据一致。因此 RAFT 使用的是日志方式进行同步，并且将服务器分为 3 种角色：Leader、 Follower、Candidate，角色之间可以互相转换。

Leader 即领导者	负责处理来自客户端的请求，管理日志复制以及与 Follower 保持心跳以维持其领导者地位
Follower 即追随者	负责响应来自 Leader 的日志复制请求，响应来自 Candidate 的选举请求，初始时所有节点均为 Follower
Candidate 即候选者	负责发起选举投票，RAFT 启动后或 Leader 宕机后，一个节点从 Follower 转为 Candidate，并发起选举，选举成功后，由 Candidate 转为 Leader

RAFT 算法主要分为两个步骤。

第一步，选举 Leader。Follower 自增当前任期，转换为 Candidate，对自己投票，并发起投票申请，等待下面 3 种情形发生：

➢一是获得超过半数服务器的投票，赢得选举，成为 Leader；

➢二是另一台服务器赢得选举，并接收到对应的心跳，成为 Follower；

➢三是选举超时，没有任何一台服务器赢得选举，自增当前任期，重新发起选举。

第二步，Leader 生成日志，并与 Follower 进行心跳同步。Leader 接受客户端请求，更新日志，并向所有 Follower 发送心跳信息，并同步日志。

所有 Follwer 都有选举超时机制，如果在设定时间之内，没有收到 Leader 的心跳信息，则认为 Leader 失效，重新选举 Leader。在 RAFT 算法中，日志的流向只有 Leader 到 Follower，并且 Leader 不能覆盖日志，日志不是最新者不能成为 Candidate。

3.8 POOL

POOL（验证池）共识是基于传统的分布式一致性技术，加上了数据验证机制，这种共识方法的主要特点是基于当前成熟的分布式一致性算法（PBFT、Pasox、Raft 等），来实现秒级共识验证，是目前私有链和联盟链中大范围在使用的共识机制，此处不再赘述。

除了常见的以上所述的几类共识机制，在区块链的实际应用过程中，也衍生出了像 POW+PoS、行动证明（Proofofac-tivity）等多个变种机制。还存在着五花八门的依据业务逻辑自定义的共识机制，如小蚁的“中性记账”、类似瑞波共识的 Stellar 共识机制、Factom 等众多以“侧链”形式存在的共识机制等，这些共识机制各有优劣势，比特币的 POW 共识机制依靠其先发优势已经形成成熟的挖矿产业链，支持者众多，而 PoS 和 DPoS 等新兴机制则更为安全、环保和高效，从而使得共识机制的选择问题成为区块链系统研究者最不易达成共识的问题。

3.9 混合共识算法及其他

3.9.1 Proof of Luck

伯克利大学的研究人员基于 TEEs（trustexe-cutionenvironments）设计了一种新型的共识机制，他们运行在支持 SGX 的 CPU 上，来抵御挖矿以及对能源的消耗。算法分为 2 个函数：PoLRound 和 PoLMine，其中所有参与者都运行这 2 个函数，得到以同一区块为祖先的不同区块。PoLMine 会选择一个介于 0 到 1 之间的随机数字（运气），最大数字意味着运气最好，将所持有的区块作为被用作区块链中的下一个块。由于在 SGX 环境中发生随机数选择，所以不能伪造它。在论文中研究人员使用的是 Intel 的 TEE——SGX，基于 Intel 的硬件环境提出了对应的共识协议————POET（proof of elapsedtime）。据 Intel 自己的实验数据该算法可以拓展到数千节点。但是问题就是这些算法依赖底层 CPU 需要把信任交给 Intel，这却与区块链去中心化的思想相悖。

3.9.2 PoDD（proof of DDos）

在 USENIX 技术研讨会上，一个新的加密数字货币 DDosCoin 被科罗拉多大学和密歇根大学的研究人员提出，旨在用于奖励用户使用他们的电脑参与 DDos 攻击。在 DDosCoin 中，矿工工作量的计算是依据建立的 TLS 连接，这导致其只适用于已启用 TLS 加密的网站。他们使用的共识机制就是 PoDD，参与 DDos 攻击会给矿工数字货币，矿工便可将货币转换成比特币或其他法定货币，这可以认为是 PoW 的另一种形式。恶意的“DDos 身份验证”操作是让矿工连接到 Web 服务器。将响应作为链接证据，在现代版本的 TLS 中，服务器在握手过程中签署客

户端提供的参数，并在连接的密钥交换中使用服务器提供的值。这允许客户向其他人证明他已经与服务器通信。此外，服务器返回的签名值对于客户端来说是不可预知且随机分布的。

3.9.3 PoB（proof of burn）

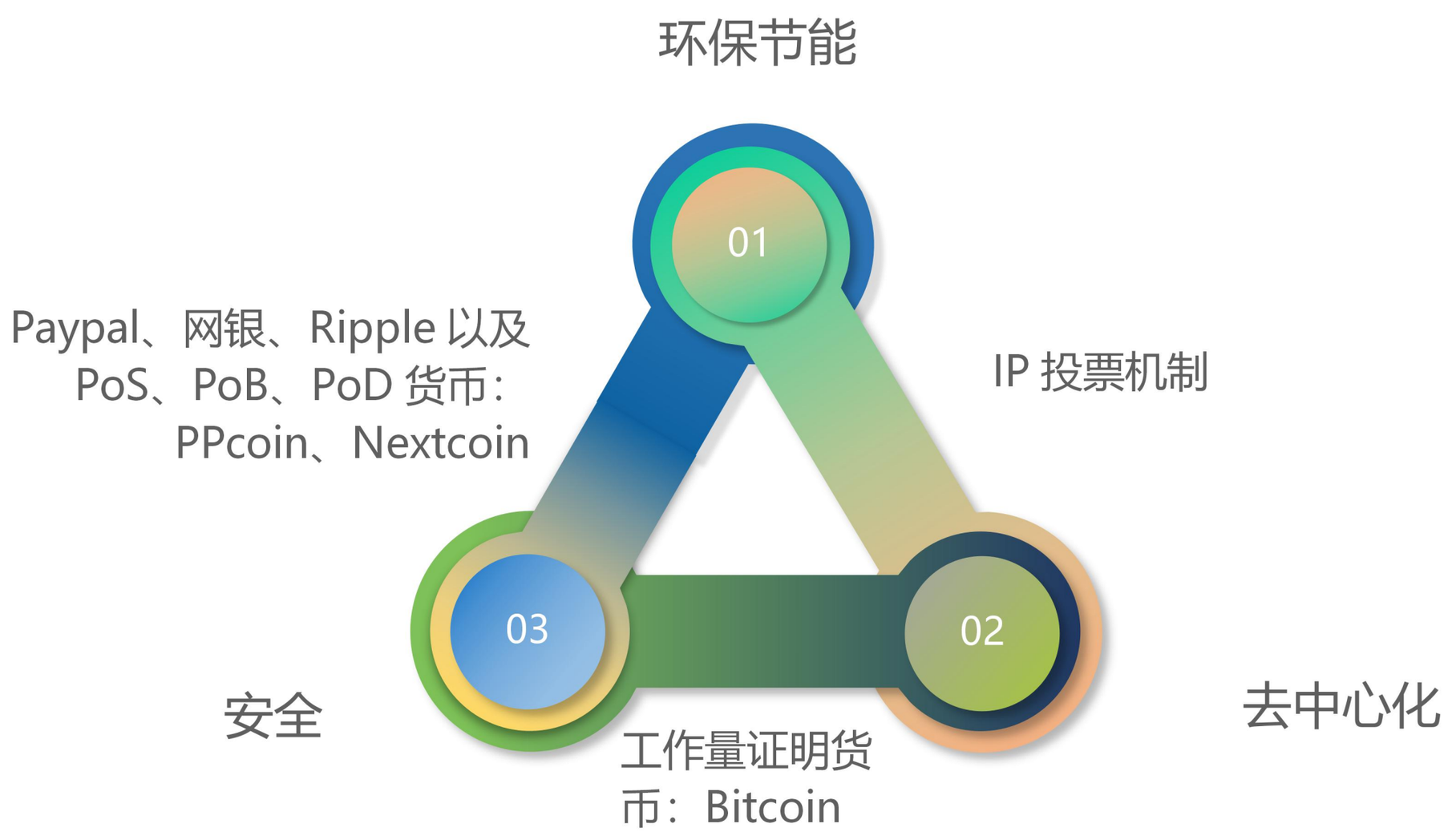
POB(Proof of Burn)，即烧毁证明，和开发比特币的过程也很相似。但 PoB 是通过将货币转移到不可逆转的地址上以销毁货币，而不是投资到计算硬件上。这种转移也叫作“燃烧”。货币被你转到了某个很难找到的地址。

创建新区块的人必须为创建新的货币支付费用。这些费用将按照预先规空的比例或者算法转换为新的货币。合约币(XCP)就是通过烧毁比特币而产生。

4. 共识机制的对比

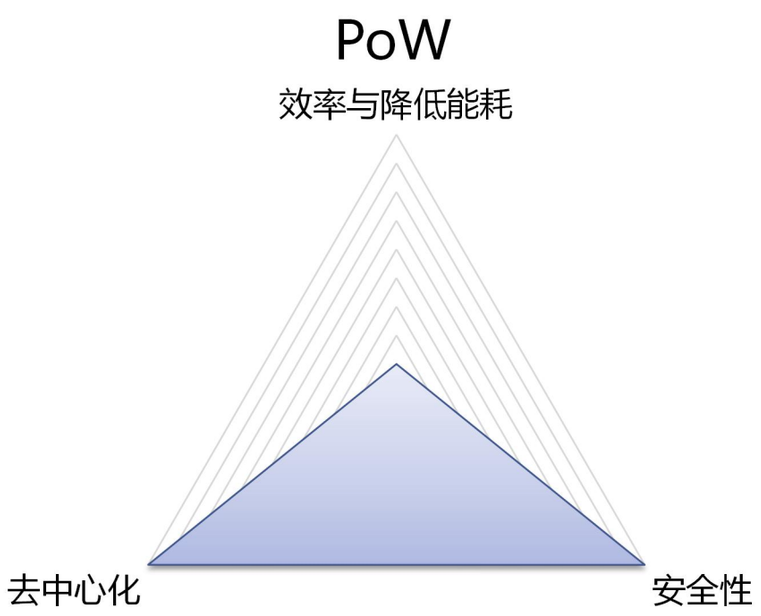
4.1 评价标准

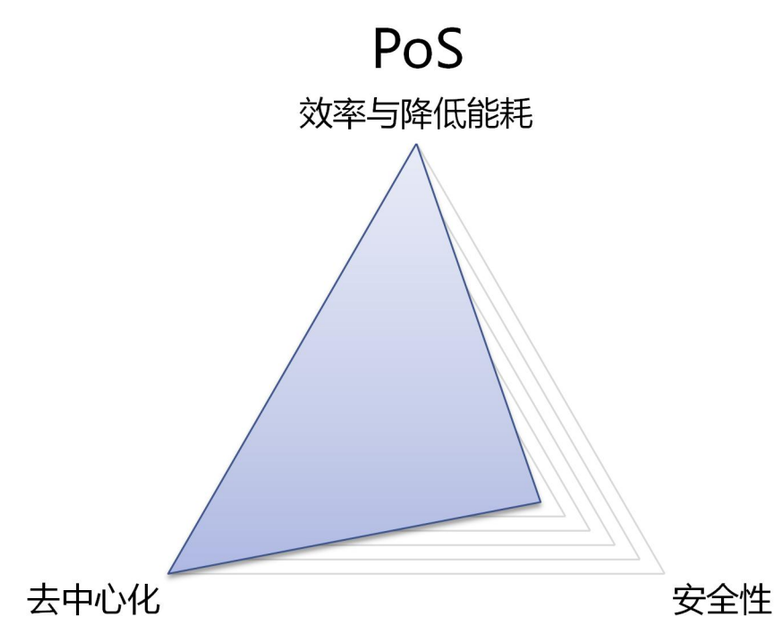
巴比特创始人长铗提出了区块链“不可能三角”理念：去中心化、安全、环保构成一个不可能三角形，设计一个符合其中两个特性的数字货币，则必然会使得第三个特性无法达成。

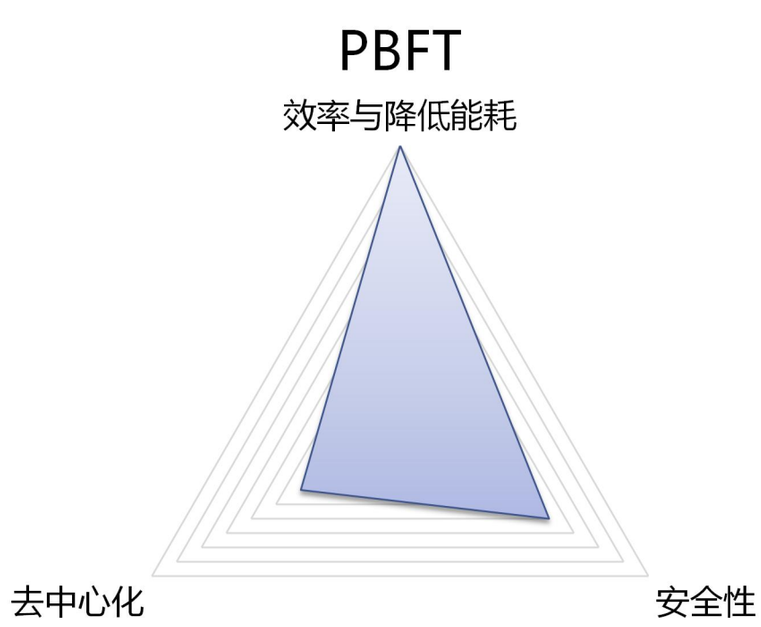


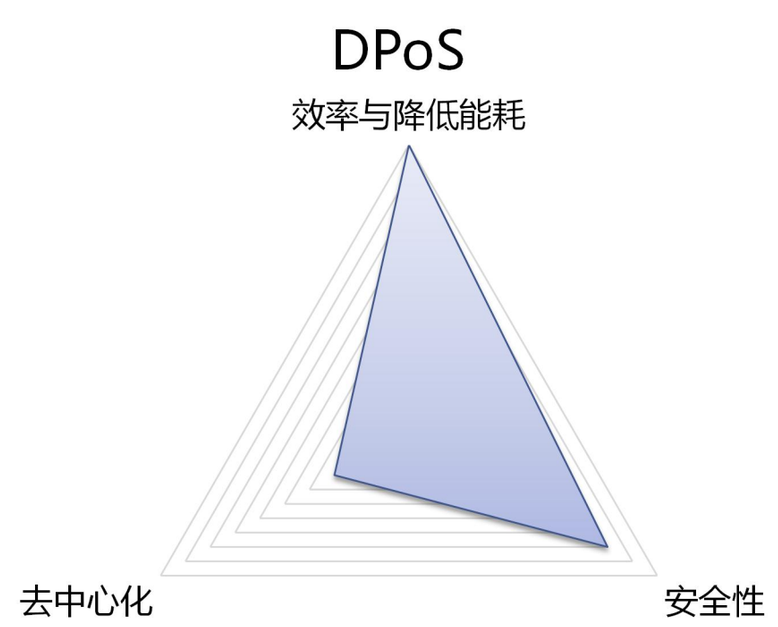
对于共识机制而言，去中心化、效率与降低能耗和安全性三个方面，也不可能面面俱到，想要完全的去中心化，则会牺牲一定的效率与降低能耗和性能，想要达到很高的可扩展，也必然面临着中心化的危险，在这两者之外，还要权衡系统的安全性。就目前的共识机制来看，都还无法完美实现三者的融合。

如下图所示：









上图常见 4 种共识机制 PoW、PoS、DPoS 和 PBFT，在去中心化、安全性和效率与降低能耗上面都有自己的不足。

比如 EOS 采用 DPOS 共识算法，从形式上有些中心化，但在可扩展性、效率、维护成本等方面寻找平衡。

比如比特币和以太坊采用 PoW 共识算法，造成大量的资源浪费；同时 PoW 共识算法的网络性能太低，需要等待多个确认，容易产生分叉，区块的确认共识达成

的周期较长（10 分钟），现在每秒交易量上限是 7 笔（visa 的平均每秒交易量上万，支付宝峰值接近 9 万），不适合商业应用。

比如 PoS 虽然在效率和去中心化达到了较好的效果，但是在安全性上偏弱。主要原因在于 PoS 容易遭受无利害关系攻击(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。

4.2 各共识机制的对比

4.2.1 PoW

PoW（工作量证明），也就是像比特币的挖矿机制，矿工通过把网络尚未记录的现有交易打包到一个区块，然后不断遍历尝试来寻找一个随机数，使得新区块加上随机数的哈希值满足一定的难度条件，例如前面 10 位是零。找到满足条件的随机数，就相当于确定了区块链最新的一个区块，也相当于获得了区块链的本轮记账权。

矿工把满足挖矿难度条件的区块在网络中广播出去，全网其他节点在验证该区块满足挖矿难度条件，同时区块里的交易数据符合协议规范后，将各自把该区块链接到自己版本的区块链上，从而在全网形成对当前网络状态的共识。

优点：完全去中心化，节点自由进出，避免了建立和维护中心化信用机构的成本。

缺点：目前比特币挖矿造成大量的资源浪费。挖矿的激励机制也造成矿池算力的高度集中，背离了当初去中心化设计的初衷。更大的问题是 PoW 机制的共识达成的周期较长，每秒只能最多做 7 笔交易，不适合商业应用。

4.2.2 PoS

PoS 作为 POW 的一种升级共识机制，它主要解决了 POW 工作量计算浪费的问题。当前 PoS 已有很多不同的变种，但基本还是根据每个节点所占有代币的数量和时间（即权益）来决定其挖矿的难度，根据每个节点所占代币的比例和时间，等比例的降低挖矿难度，从而加快找随机数的速度。

优点：相比 POW，PoS 算法的优点包括，避免了挖矿造成大量的资源浪费，缩短了各个节点之间达成共识的时间，网络环境好的话可实现毫秒级，对节点性能要求低。

缺点：仍需要挖矿，并且 PoS 会使得“富者更富”，有可能支配记账权，拥有权益的参与者也未必希望参与记账。无法达成最终一致性，容易产生分叉，需要等待多个确认。PoS 依然是基于哈希运算竞争获取记账权的方式，可监管性弱，容错性和 POW 相同。

4.2.3 DPoS

DPoS 与 PoS 的原理相同，主要区别在于节点选举若干代理人，由代理人轮流验证和记账，其合规监管、性能、资源消耗和容错性与 PoS 相似。

优点：DPoS 相比 PoS，它的优点是，能大幅缩小参与验证和记账节点的数量，可以达到秒级的共识验证。

缺点：整个共识机制还是依赖于代币，而很多商业应用是不需要代币存在的。并

且牺牲了去中心化的概念，选举固定数量的见证人作为记账候选人有可能不适合于完全去中心化的场景。在网络节点数少的场景，选举的见证人的代表性也不强。

以上三种算法多用于共有链。

4.2.4 RPCA

瑞波共识协议所创建的区块链是由所有参与者中部分被称作为“网关”的受信任的节点所维护，同时网关节点之间存在信任关系，而其余的一般参与者则被称为“用户”。用户只能产生交易，并不参与创建区块和记录交易的工作。

优点：确认交易可以在很短的时间内完成验证，每 3s 左右就能产生一个区块，任何时候都不会产生硬分叉。

缺点：包括对网关节点的可靠性要求很高，网关节点的可靠程度将影响整个交易网络的正常运行。由于存在网关节点，不能算做是完全的“去中心化”，新加入节点要取得与其他节点的共识所需时间也比较长。

4.2.5 PAXOS

PAXOS 属于传统的分布式一致性算法，是一种基于选举领导者的共识机制，PAXOS 能保证在超过 50%的正常节点存在时，系统能达成共识。

优点：包括允许强监管节点参与，性能高，资源消耗低。

缺点：缺点是仅用于具有较高容错性的分布式系统中。

4.2.6 PBFT

PBFT 解决了原始拜占庭容错算法效率不高的问题，使得拜占庭容错算法在实际系统应用中变得可行，可容错节点数为 N/3-1。与 PAXOS 类似，它也是一种采用许可投票、少数服从多数来选举领导者进行记账的共识机制，但该共识机制允许拜占庭容错。

优点：效率高，秒级出块，可配置为 1 到几秒出块，满足交易短时间内响应的需求。允许强监管节点参与，具备权限分级能力，相比 PAXOS，性能更高，耗能更低。安全性高，该算法每轮记账都会由全网节点共同选举领导者，允许 33% 的节点作恶，容错性为 33%。高一致性、高可用性，抗欺诈能力较强，是联盟链里较为实用的一种共识算法。

缺点：包括当有 1/3 或以上记账人停止工作后，系统将无法提供服务。当有 1/3 或以上记账人联合作恶，且其他所有的记账人被恰好分割为两个网络孤岛时，恶意记账人可以使系统出现分叉，但是会留下密码学证据。

4.2.7 RAFT

RAFT 更注重协议的可理解性和落地性，其特点是任何时刻最多只有一个合法 Leader，可容错节点数为 N/2-1。Raft 算法是 PAXOS 算法的一个简化实现，因此其合规监管、性能、资源消耗和容错性与 PAXOS 相似。

优点：相比 PAXOS 和 PBFT 算法，性能更高，耗能更低，秒级出块，可以配置为 1 或多秒出块。高一致性，候选区块超过半数赞成票才提交到区块链中。高可用性，如果超时没有收集超过半数的回复票，则重新发起选举，保证系统的容错恢复能力。支持 1/2 节点容错，整个系统中少于 1/2 数量的节点出现故障，均不影响共识进行。数据安全性高，在选举过程和区块同步过程中严格校验签名。

缺点：与 PBFT 共识的拜占庭容错特性对比，RAFT 共识并不严格保证抗欺诈性，适用于互信程度较高的联盟链。

4.2.8 POOL

POLL (验证池) 共识机制是基于传统的分布式一致性技术 (PBFT、PAXOS、RAFT 等），加上数据验证机制。

优点：不需要代币也可以工作，在成熟的分布式一致性算法（Pasox、Raft）基础上，实现秒级共识验证；Pool 验证池，基于传统的分布式一致性技术，加上数据验证机制；是目前行业链大范围在使用的共识机制。

缺点：性能会随着节点数的增加而变差，并且去中心化程度不高，更适合多方参与的多中心商业模式。

基于以上分析，这里做一张表，将上面这些共识算法从各角度做一个比较。

共识算法	PoW	PoS	DPoS	RPCA	PAXOS	PBFT	RAFT	POOL
性能效率	低	较高	高	高	高	高	高	高
去中心化程度	完全	完全	完全	半中心化	半中心化	半中心化	半中心化	半中心化
最大允许作恶节点数量	50%	50%	50%	20%	50%	33%	50%	同选取的分布式一致性算法
是否需要代币	是	是	是	是	否	否	否	否
应用场景	公有链	公有链	公有链	私有链 联盟链	私有链 联盟链	私有链 联盟链	私有链 联盟链	私有链 联盟链
安全威胁	算力集中化	候选人作弊	候选人作弊	网关节点作弊	Proposer 节点故障	主节点故障	Leader 节点故障	同选取的分布式一致性算法
一致性	有分叉	有分叉	无分叉	无分叉	无分叉	无分叉	无分叉	无分叉
资源消耗	高	中	低	低	低	低	低	低
可监管性	弱	弱	弱	强	强	强	强	强

5. 共识机制面临的问题

5.1 性能和扩展性不能满足要求

从目前的情况来看，区块链的性能问题主要表现为吞吐量及存储带宽远不能满足整个社会的支付需求。同时，比特币随着时间的推移，累积的交易数据越来越大，对于普通电脑的存储来说，这是个不小的负担。如果只是简单提高区块大小来提高吞吐量，比特币很快就会变成只有少数几个大公司能够运行的系统，有违去中心化的设计初衷。在比特币、以太坊等公有链系统中，上述矛盾是系统设计时面临的最大挑战。

在联盟链中，因为参与记账的节点可选可控，最弱节点的能力上限不会太低，并且可以通过资源投入获得改善，再针对性地替换掉共识算法等组件最终获得性能的全方位提升。但作为智能合约基础支撑的联盟链另有考验：智能合约运行时会互相调用并读写区块数据，因此交易的处理时序特别重要，如果只能逐笔进行，这会严重制约节点的处理能力。

5.2 数据隐私和访问控制有待改进

现有公有链中，各参与方都能够获得完整数据备份，所有数据对于参与方来讲是透明的，无法使参与方仅获取特定信息。比特币通过隔断交易地址和地址持有人真实身份的关联，达到匿名效果。所以虽然能够看到每一笔转账记录的发送方和

接受方的地址，但无法对应到现实世界中的具体某个人。对于比特币而言，这样的解决方案也许够用。但如果区块链需要承载更多的业务，比如登记实名资产，又或者通过智能合约实现具体的借款合同，这些合同信息如何保存在区块链上，验证节点在不知晓具体合同信息的情况下如何执行合同等等，目前业内尚未有成熟方案。

5.3 治理机制有待完善

公有链社区摸索出了“硬分叉”和“软分叉”等升级机制，但遗留问题有待观察。由于公有链不能“关停”，其错误修复也异常棘手，一旦出现问题，尤其是安全漏洞，将非常致命。

实际上，通过放松去中心化这个限制条件，很多问题能找到解决的方案。比如在联盟链这样的多中心系统中，通过关闭系统来升级区块链底层，或者紧急干预，回滚数据等，必要时都是可用的手段，这些手段有助于控制风险、纠正错误。而对于常规代码升级，通过分离代码和数据，结合多层智能合约结构，实现可控的智能合约更替。

6. 共识机制应用场景分析

共识机制不但是计算机之间的算法和数据共识，也是合作伙伴之间进行协作的共识，共识机制使区块链的参与者通过约定的方式进行共同记账，确保合作者之间的记账正确性、一致性、持续性，避免少数出现故障的节点影响网络运行，并防御少数故意作恶者的破坏。在不同的应用场景下，需要使用不同的共识机制。现实生活中常见以下两种应用场景：需要加密数字货币的公有链和不需要货币体系的私有链和联盟链。

6.1 需要加密数字货币的公有链

公有链如比特币、以太坊等使用的共识算法通常为工作量证明或权益证明等，可以根据投入权益和记账的行为，对记账者制定奖励和惩罚制度。公有链上的共识算法一般确认时间较长，或需要较多的算力投入。

PoW 作为无授权协议，最适合公有链系统，虽然网络维护费用高但却是完全去中心化系统安全运行的保障。PoS 作为需要授权但授权程度较低的共识机制，在需要许可的、公共的共享系统中更有发挥空间，而 DPoS 则是需要许可的、私有的共享系统的较好选择，因为委托人群体的更值得信任，保障系统安全运转无需较大花费。

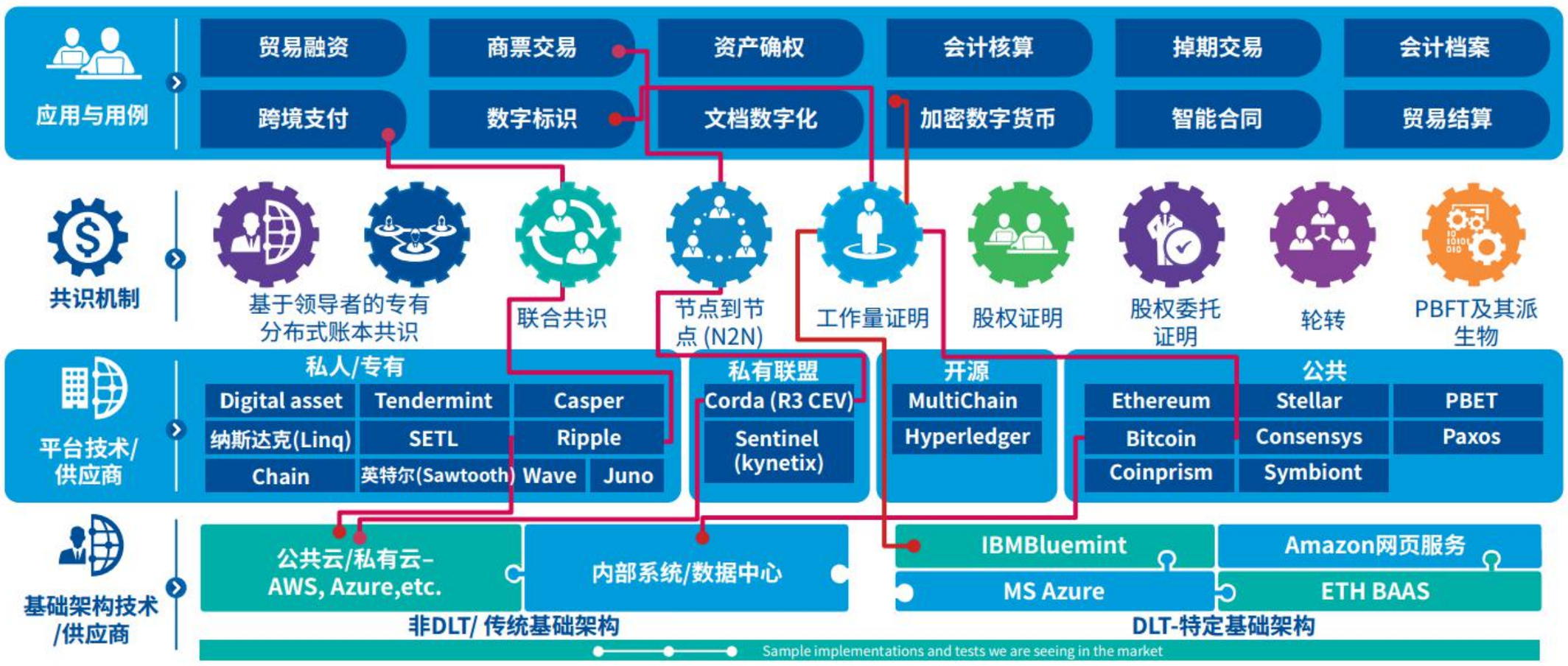
6.2 不需要货币体系的私有链和联盟链

而对于不需要货币体系的私有链或者联盟链而言，需要有绝对信任的节点，以及高效的需求，因此对于这样的区块链，传统的一致性算法成为首选，如 RPCA、PAXOS、PBFT、RAFT、POOL。

私有链和联盟链共识机制的设计目标和公有链有所不同，系统不需要根据记账的计算量对记账者进行经济奖励，而是鼓励参与者在共同维护区块链、促进生态系统发展、推进节点合作的过程中获得价值或收益。在此过程中产生的纠纷或非法行为，将采用监管审计和法律仲裁结合的方式解决。这样共识机制的实现符合私有链或联盟链场景需求，可避免算力浪费、防分叉和提升运行稳定性。

私有链和联盟链的共识机制在节点总数不多、网络规模不太大时，可以提供较高的交易并发处理能力。但随着节点数量增多，比如达到几百个共识节点的规模时，由于需要共识节点之间交换较多的信息，会出现明显的性能下降。所以一般会通过协商，在保证公平公开的前提下，控制参与者共识的节点数量，以保证共识算法的效率。

下图列举并展示了现阶段区块链、分布式账本技术和技术供应商是如何紧密合作，以适应市场的需求。



7. 共识机制选择标准

区块链上采用不同的共识机制，在满足区块链数据一致性和有效性的同时会对系统整体性能产生不同影响。综合考虑各个共识机制的特点，可以从以下 5 个维度作为对共识机制的选择标准。

7.1 安全性

指共识机制防攻击、防欺诈的能力，即是否可以防止双重支付（即双花）、自私挖矿等攻击，是否有良好的容错能力。以金融交易为驱动的区块链系统在实现一致性的过程中，最主要的安全问题就是如何防止和检测双重支付行为。另外，自私挖矿通过采用适当的策略发布自己产生的区块，可以获得更高的相对收益，也是一种威胁比特币系统安全性和公平性的攻击方法。

7.2 扩展性

指区块链是否支持网络节点扩展，扩展性是区块链设计要考虑的关键因素之一。根据对象不同，扩展性又分为系统成员数量的增加和待确认交易数量的增加两部分。扩展性主要考虑当系统成员数量、待确认交易数量增加时，随之带来的系统负载和网络通信量的变化。

7.3 性能效率

指区块链交易达成共识被确认的效率。即从交易达成共识被记录在区块链中至被最终确认的时间延迟，也可以理解为系统每秒可处理确认的交易数量。与传统第三方支持的交易平台不同，区块链技术通过共识机制达成一致，因此其性能效率问题一直是研究的关注点。比特币系统每秒最多处理 7 笔交易，远不能支持很多应用场景下的业务量。

7.4 资源消耗

指在达成共识的过程中，系统所要耗费的计算资源大小，包括共识过程中耗费的 CPU、网络输入输出、存储等计算机资源。区块链上的共识机制借助计算资源或者网络通信资源达成共识，以比特币系统为例，基于工作量证明机制的共识需要消耗大量计算资源进行挖矿来提供信任证明完成共识。

7.5 可监管性

指是否支持超级权限节点对全网节点、数据进行监管。区块链的匿名性与弱中心化的架构，与现有的监管体系存在某种程度的天然冲突。所以，比特币才会被用于暗网黑市交易、跨国境洗钱等场景。未来，区块链技术最终必然演化为“监管融入技术”的模式，区块链的难以篡改、共享账本、分布式的特性，更易于监管接入，获得更加全面实时的监管数据。让监管机构本身也参与到技术中去，通过技术本身实现对技术的监管，将最终化解区块链与监管的冲突。

8. 未来展望

共识机制作为区块链技术中至关重要的一个组成部分，备受学术界和企业界关注。良好的共识机制有益于区块链技术在理论和实践中的推广。然而，现有的可用于区块链技术的共识机制都不尽完善，未来创新之处主要在于降低共识机制的复杂度，资源消耗大的共识机制市场占有率会逐步减小，而那些不消耗能源的共识算法会进一步发展，这是一种长期的发展趋势。

在达成一致性的前提下，平衡效率、扩展性和资源是共识机制的痛点。在此基础上如何因地制宜结合共识机制，设计最佳协商机制，是未来研究的主要方向。而且我们可以看到，依据系统授权程度的高低，依次分为无需许可、公共的共享系统、需要许可、公共的共享系统，需要许可的、私有的共享系统。越开放的系统达成共识的代价越高。鉴于共识机制的优缺点，我们可以尝试将不同的共识机制结合起来，形成一种新的共识机制。比如将 PoW 和 PoS 结合，将 PoS 和 BFT 结合。

对于现存区块链的一些问题，要结合加密算法和底层存储技术的改进，共识机制才能发挥出最大效果，比如零知识证明、环签名、闪电网络、DAG、HashGraph。随着全球对区块链的关注，越来越多的人投入其中研究开发，未来会有更多工作高效设计巧妙的共识机制被设计出来。

共识机制永远需要在效率与安全之间达成最佳平衡，在比特币应用中采用了完全去中心化的共识机制，而在联盟链和私有链中，我们也看到去中心化不是那么完全的共识机制，相信基于区块链技术演化和发展，会有更多的技术和机制进入到我们的视野和应用场景中，区块链在比特币中的应用为我们打开了一扇通向未来

数字货币的大门，而从数字货币到数字金融最终达到数字社会之路仍然任重道远，共识机制需要不断完善和创新。

风险提示

本报告所采用的数据均来自合规渠道，分析逻辑基于作者的职业理解，本报告清晰准确地反映了作者的研究观点，力求独立、 客观和公正，结论不受任何第三方的授意或影响，特此声明。

本报告的信息来源于已公开的资料，TokenClub 研究院对该等信息的准确性、完整性或可靠性不作任何保证。在任何情况下，本报告中的信息或所表述的意见均不构成对任何人的投资建议。

TokenClub
研究院

TokenClub 是国内领先的数字货币投资社区，致力于构建一个自治、信任、高效的数字资产投资服务生态。

“TokenClub 研究院”是 TokenClub 旗下研究区块链的专业机构，专注于区块链行业研究、项目评级。

扫码关注
TokenClub 研究院

扫码下载
TokenClub APP