主流区块链共识机制的简介与比较

——区块链技术引卷之三

通证通研究院
FENBUSHI DIGITAL
区块链研究报告

专题报告　　行业研究

2018.12.26

通证通 x FENBUSHI DIGITAL

分析师：宋双杰，CFA

Email:master117@bitall.cc

分析师：孙含儒

Email: sunhanru@bitall.cc

Fenbushi Digital

投资总监：Rin

Email: r.huang@fenbushi.vc

特别顾问

沈波

JX

更多研究请关注公众号获取

通证通研究院　　FENBUSHI DIGITAL

请务必阅读最后特别声明与免责条款

导读：本文介绍主流共识机制的特点，探讨共识机制分类的标准并作出分类。

摘要：

在区块链被发明后的近十年历程里，不断有新的共识机制被创造出来。有些算法在工作量证明的基础上作出改进，有些则将传统的分布式容错算法运用到区块链网络中。我们尝试将共识机制的“容错”、“节点参与共识过程的资格”、“形成共识的依据”、“共识的内容”等要素作为区分不同类别共识机制的标准，将共识机制分为竞争记账权间接形成共识的 Proof of X 类、投票直接形成共识的 BFT 类、选举代理人间接参与共识的代理类以及舍弃传统区块概念的 DAG 类共识。

BTC 的初衷是建设一个开放的公共区块链基础设施，网络中的节点可以自由地加入及退出，平等地竞争记账权。如果节点获得记账权的概率与该节点拥有某种难以垄断的资源的比例相关，并存在算法能够快速验证某个节点确实拥有这部分资源，就称这类共识机制为 Proof of X 类共识，X 代表竞争记账权所需要的资源。这类共识机制包括以算力竞争的 PoW、以权益竞争的 PoS，以及针对 PoS 的一些缺陷作出改进的 PoA、PoSV、Casper 等，以及按其他不易垄断的资源分配记账权的 PoST、Proof of Authority 等。

BFT 类共识机制与 Proof of X 采用了不同的思路形成非中心化的共识，并且同样能容忍网络中的拜占庭错误，即通过**对提案（区块内容）直接投票表决，相同意见的票数超过一定比例则作为决策共识的“直接形成共识”。**主流的 BFT 类共识机制有 pBFT、dBFT 以及 FBA。

代理类共识机制借鉴现实社会中的选举，节点可以作为参选人参加选举，也可以给参选人投票。节点控制的选票数量与其持有的某种权益或资源多少挂钩，网络定期按照节点的得票数选出一定数量的“共识节点”，**仅由共识节点按照一定的共识算法完成区块链网络的共识过程。**

DAG（有向无环图）是一类可以作为记录区块链交易历史的数据结构，不同于传统的将交易打包成区块，对区块形成共识的方式，IOTA 使用的 Tangle（缠结）共识能够对交易直接形成共识。

最后我们总结了区块链共识机制的分类方式，并且比较了 PoS、PoW、BFT 类共识的优势与缺陷。

风险提示：算力中心化风险、共识节点中心化风险

目录

图表目录

在上一篇专题中，我们以BTC为例分析了Proof of Work（PoW，工作量证明）共识机制。中本聪在BTC白皮书：《一种点对点的电子现金系统》中提出了一种能够应用到区块链中的PoW共识机制，其核心思想是通过要求网络中的节点付出一定量的算力竞争记录区块的权利（即记账权），来保证共识的一致性。

我们回顾一下上篇专题提出的“共识机制关键要素”，并将PoW共识机制的特点总结如下：

1.容错：PoW能够容忍拜占庭节点，并且容错能力为1/2；

2.CAP：PoW可以满足CAP，但网络效率较低；

3.哪些节点可以参与共识过程：网络中的全部节点；

4.节点如何获得记账权：通过解决Hash谜题；

5.需要形成共识的内容：若干交易打包的区块；

6.形成共识的依据：区块内的交易是否合法，以及当前链是否为最长链；

7.激励措施：记账节点可以获得区块奖励；

8.惩罚措施：没有对恶意节点**直接的**惩罚机制（但有挖矿的沉没成本）；

4和6分别代表了工作量证明的两个特点：一是工作量（Work），由于节点需要不断改变区块头中的nonce值使区块Hash满足一定的条件，**找到合法区块的节点必然需要付出相应的工作量**，即为Work；二是证明（Proof），其他节点可以迅速地验证区块的合法性，即**能够对节点的工作量进行检验**，即为Proof。

随着数字通证逐步被更多的人所认知，人们也对其采用的底层区块链技术的共识机制进行不断改进。其中有一类称为Proof of X。与PoW类似，这类共识机制主要针对PoW的节点**竞争记账权的方式**作出改进或替代方案。

1 记账权的竞争——Proof of X 类共识机制

BTC的初衷是建设一个开放的公有区块链基础设施，网络中的节点可以自由地加入以及退出，能够平等地竞争记账权。在这一类共识机制下，**节点获得记账权的概率与该节点拥有某种资源的比例相关，并且这种资源是难以垄断的。**此外还需要一个**能够快速验证某个节点确实拥有这部分资源的算法。**

在PoW共识机制中，这种资源是所谓的“算力”，即一定量的CPU或GPU计算时间，验证节点算力则是利用了Hash函数易于计算、内容隐秘的特性。在PoS（Proof of Stake）共识中，资源是所谓的“权益”，节点按照其持有的某种权益数量的比例分配记账权。此外还有PoSpace（Proof of Space）类共识，资源是节点提供的一定量磁盘或者内存空间；Proof of Bandwith，资源是节点提供的网络带宽；Proof of Ownership，资源是节点所持有的特定数据。

1.1 Proof of Work 工作量证明

我们将 PoW 的哈希解谜过程表示为节点不断改变区块头部的 nonce 使区块 Hash 满足**目标条件** Target 的过程，可以由以下的公式描述：

$$\mathrm{H}(nonce + Block) < Target$$

Target 根据网络的难度进行设定，难度每隔一段时间根据规定的算法进行调整，目的是保证网络中挖掘出区块的时间期望为固定值。H(x)表示 Hash 函数，我们把 x 的取值范围称为节点的**搜索空间**。

PoW 机制中节点的搜索空间是所有正整数，由于 Hash 函数的特性，不等式左边可以认为是在 Hash 函数值域上均匀分布的随机变量，**Target 对于全体节点都是相同的，节点获得记账权的概率取决于其计算 Hash 的速度。**

BTC 以及其分叉通证、LTC、ETH（当前 Metropolis 版本）等大部分主流数字通证均采用 PoW 共识机制，它们之间的区别主要是采用的哈希算法不同，以及具体参数例如难度调节机制、区块激励机制的不同。例如 LTC 的总量为 8400 万个，区块速度改为 2.5 分钟，采用 scrypt 哈希算法。ETH 进一步减少了区块时间，并对引用孤块的矿工提供一定奖励，采用 GPU 挖矿算法削弱专业 ASIC 矿机的算力优势。XMR、ZCash 在 BTC 基础上增强了交易的匿名性等。

在上一篇专题中，我们总结了几种恶意攻击者可能采取的攻击方式。

女巫攻击是攻击者以大量制造节点“伪装”成不同身份加入网络的方式发起的攻击。在 PoW 共识机制下，节点虽然无需身份验证，但获得记账奖励的概率与节点的实际算力相关，女巫攻击是不可行的。

双重支付攻击需要攻击者在发出一笔交易后挖掘出比当前链更长的包含双花交易的攻击链，因此又称为重组区块历史类型的攻击。攻击者重组区块链历史成功的概率随他落后当前最长链的区块个数增加而降低。中本聪在 BTC 白皮书中给出如下计算公式：

$$\mathrm{P} = 1 - \sum_{k=0}^{\infty} \frac{\lambda^k e^{-\lambda}}{k!} \left(1 - \left(\frac{q}{p}\right)^{z-k}\right)$$

$$\lambda = z \cdot \frac{q}{p}, \qquad p + q = 1$$

其中 z 表示交易的接收者观察到这笔交易得到的区块确认个数，P 表示攻击者发动双重支付攻击成功的概率，q 表示攻击者掌握的算力占全网算力比例，且 q<0.5。例如在 q=0.1 的条件下，当 z=5 时，P 已经小于 0.001。

51%攻击。在以上公式中，若 q>p，即攻击者掌握的算力超过了全网算力的一半时，无论诚实的交易者观察到一笔交易被多少个区块确认，攻击者总是可以追上最长链，也就是所说的 51%攻击。但发动这种攻击所需的成本是巨大的，并且会使通证严重贬值。

1.2 Proof of Stake 权益证明

PoS 按节点持有的某种权益占网络中全部节点的比例来分配记账权，它的出现源自人们对 PoW“算力竞赛”中消耗大量能源的批判。PoS 尝试在不使用大量能源的情况下，仍然保证不弱于 PoW 共识机制的安全性。

点点（Peercoin）是首个将 PoS 理念加入到共识机制中的数字通证。严格来说 Peercoin 采用的是 PoS+PoW 混合共识机制，考虑到它在 PoS 发展历程中的重要地位，我们将 Peercoin 作为分析 PoS 共识机制的第一个例子。

1.2.1 Peercoin——PoS 共识的先驱者

Peercoin 提出了“币龄”的概念。**通证币龄等于通证的数量乘以该部分通证自上次交易经过的时间。**Peercoin 沿用与 BTC 相似的区块以及交易结构设计，因此同样有 UTXO（未使用交易输出）这一概念，一笔 UTXO 包含一定数量的通证，并记录了包含这笔交易的区块被挖掘的时间，从而可以计算出对应的币龄。**当 UTXO 被使用后，这部分通证的币龄也被清零。**Peercoin 使用 CoinDay 作为币龄的单位（1 单位通证 1 天积累的币龄）。

与 BTC 区块的 coinbase（币基）交易对应，Peercoin 的 PoS 区块还包含一个类似的 coinstake（币利）交易，它的输入包含核心（Kernel）输入与权益（Stake）输入两部分。节点可以将自己的 UTXO 作为核心输入，并通过**消耗币龄获取生产 PoS 区块的权利**。Peercoin 的 PoS 挖矿过程与 PoW 工作量证明类似，同样需要节点进行哈希计算并使结果满足目标值，目标值越大，则越容易获得生产区块的权利。其挖矿过程可以表示为：

$$\mathrm{H}(StakeModifier + Timestamp) < BaseTarget * CoinAge$$

不等式左边 Hash 函数搜索空间中的 Timestamp 表示当前时间。Peercoin 规定了一个区块的时间戳必须在由前一个区块所决定的时间范围之内，否则该区块不会被其他节点接受。StakeModifier 是每过一定数量区块就根据最新区块 Hash 重新计算的值，它的设计是为了防止节点提前计算未来某个时间的 Hash 值。这样得出的 Hash 可以保证是节点在规定的时间范围内计算出的。不等式右边 BaseTarget 由当前 PoS 挖矿的基础难度决定，CoinAge 表示节点投入参与记账权竞争的币龄。

与 PoW 网络的节点在一个非常广泛的搜索空间里寻找 nonce 不同，由于时间戳取整数进行 Hash 运算，Peercoin 网络中的**节点固定时间间隔内的搜索空间是有限的**，限制了节点因算力差异产生的竞争。**而节点币龄越大，目标空间也越大，Hash 值满足条件的概率越高。**

Peercoin 的激励机制在于，获得记账权的节点可以添加一笔权益输入，根据区块内所有交易消耗总币龄的多少生产一定比例的利息支付给自己，Peercoin 中每一单位的通证一年的币龄会产生 1%的利息。

与 PoW 的最长链原则类似（累计工作量最高），Peercoin 的区块也会记录该区块内交易的总币龄，**累计消耗币龄最多的链将成为主链。**

1.2.2 Nextcoin——“未来已经注定”

未来币（Nextcoin）是另一种以不同的方式实现 PoS 共识机制的数字通证。2013 年 9 月一个名为 BCNext 的用户在著名的 bitcointalk.org 发表了一篇帖子，宣布将发行一个“机制与代码与 BTC 完全不同”的数字通证，即 Nextcoin。它引入了“透明锻造”的概念，并由此实现纯粹的 PoS。

Nextcoin 没有采用 BTC 的 UTXO 设计方案，而是使用账户余额方案，更加接近传统银行的处理方式。每一个账户（Account）对应一个私钥，链上的区块都有独特的生成签名（generationSig）。当新一轮共识开始时，参与“锻造区块”的账户用自己的私钥对前一个区块的生成签名进行签名，采用 SHA256 散列算法计算该签名结果的 Hash，取前 8 个字节，称为 hit。只要 hit 值满足目标值，则该账户可以生产一个新区块。将其判定方式表示为：

$$\text{hit} < BaseTarget * EffectiveBalance * ElapsedTime$$
$$\text{hit} = \text{H}\big(sig(prevGenerationSig)\big)$$

不等式右边的目标值由基础难度、账户有效余额、当前时间与前一个区块生产的时间间隔相乘得到。基础难度是对所有账户都相同的、随全网有效总余额的变化不断调整，各账户独立的目标值与其有效余额有关，随时间的流逝增加。

由于在上一个区块产生时，其生成签名已经确定了，每个账户的 hit 值也由此确定了。相比 BTC 需要搜索合适的 nonce 值，Peercoin 要在一个有限区间中进行 Hash 计算，Nextcoin 的账户**没有任何搜索空间**，由于 hit 值仅有 8 字节，因此随着目标值的不断增加，总是有账户能够满足条件生产区块。hit 是一个对所有账户期望值相同的随机变量，因此**账户获得记账权的概率与其有效余额成正比**。

前一个区块确定后，hit、基础难度、有效余额都是确定的，因此每个账户可以立即计算出自己需要经过多长时间可以获得生产区块的权利，并将这一时间向其他节点广播，这样全部节点都可以预知在接下来的某个时刻，是哪个节点能够生产新区块，这就是所谓的“透明锻造”，在前一个区块生产出来时，下一个区块的“未来”就已经确定了。

以通证数量代替币龄作为竞争记账权依据的方式也被很多山寨通证如 Novacoin、Blackcoin 采用。

1.2.3 传统 PoS 的安全性与缺陷

在网络安全性方面，对 PoS 共识机制发起 **51%攻击**的可能仍然存在，但相比 PoW，**对 PoS 进行 51%攻击所需的成本通常可能会更高。**在以币龄为权益的 PoS 算法中，攻击者发起攻击不仅需要金钱成本，还要付出时间成本，恶意囤积通证的可能性也被限制。攻击者在记录一次区块后币龄会清零，该部分通证一段时间内不能再被用于竞争记账权，增加了重组区块链历史、发动双花攻击的难度。最后，攻击者必须持有通证才能竞争记账权，发起以破坏区块链为目的攻击会使攻击者本身遭受损失。

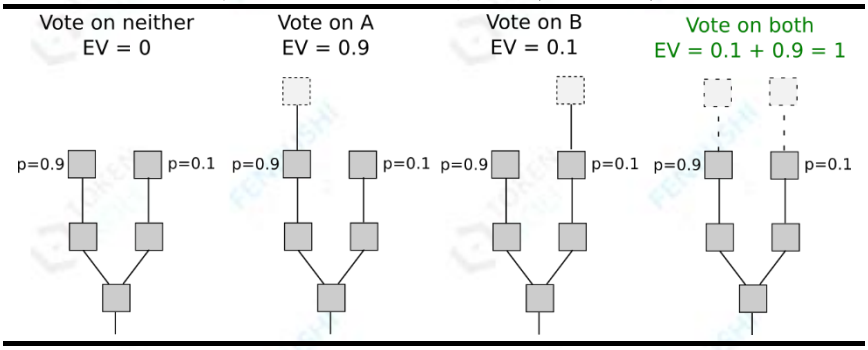
虽然解决了能源消耗问题，PoS 也引入了新的问题。

在传统 PoS 中，**节点不需要在线也可以累积币龄**，这可能导致网络在线的记账节点数量较低，网络安全得不到保障。

另一方面，PoS 对抗硬分叉的能力很弱，即所谓 Nothing at Stake（零成本，简写 N@S）攻击。

由于网络分叉后**节点可以同时在两条链上拥有记账权益并同时获得收益，理性的节点会默认分叉行为的产生**，反而可能造成通证价值的下降。甚至在攻击者没有掌握 51%以上记账权的情况下，发起分叉仍然是能够成功的。

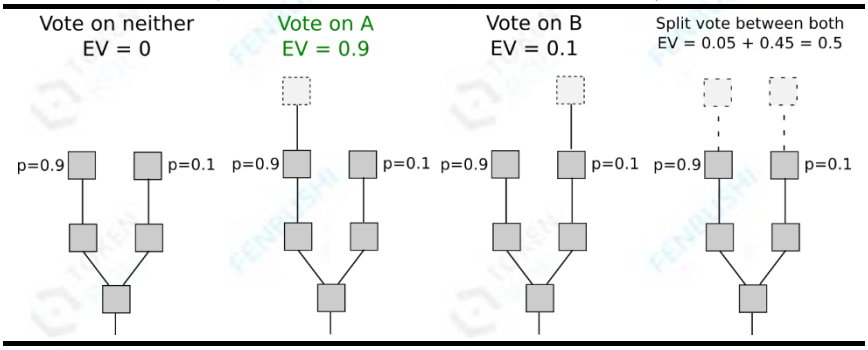
图表1：发生链分叉时 PoS 节点的决策



资料来源：Ethereum Wiki，通证通研究院

而 PoW 的矿工如果想在分叉链上挖矿，则必须切换一部分算力，这样造成在两条链上的收益均下降，因此理性的矿工只会在最长链（即成为共识链概率最大的链）上挖矿。

图表2：发生链分叉时 PoW 矿工的决策



资料来源：Ethereum Wiki，通证通研究院

解决 N@S 的方法主要是加入对不诚实节点的惩罚机制，将在 Casper 共识部分阐述。

类似 Nextcoin 的 PoS 机制的缺点还包括：高度依赖精确的时间轴，如果网络节点间的时间不统一，那么可能对区块的有效性无法形成共识。另外，当记账节点非常多的时候，最新区块附近不可避免地会产生很多分叉，因此需要交易确认需要一定时间以保证共识的一致性。

1.3 PoS 的改进共识机制

1.3.1 PoA（Proof of Activity）活跃证明

PoA 是一种 PoW+PoS 混合共识机制，最早在李启威（LTC 的创造者）和其他三位作者共同发表的论文中提出。针对**传统 PoS 离线也可以积累币龄或权益，没有机制促使节点保持在线以维持网络运作**的问题作出改进。

在 PoA 共识机制中，节点首先通过传统 PoW 的方式进行挖矿，但是这个新区块不打包任何交易，仅仅包含区块头信息和区块 coinbase 奖励的发送地址。

当空区块被产出后，系统切换到 PoS 模式，并随机选出若干个权益持有人（Stakeholder）向空区块中填充交易并签名，称他们为“验证者”（Validator）。**当随机选出的验证者全部签署了区块后，该区块便成为共识。**验证者和区块的 PoW 开采者将该区块的手续费按一定规则分配。

PoA 选择验证者（即为记账节点）的算法称为“Follow the Satoshi”（跟随中本聪）。“聪”是 BTC 的最小货币单位，PoA 将随机数映射到目前已经开采出的 1“聪”通证上，并且从这 1 聪通证被开采出的区块开始追溯每一笔交易，直到它目前的持有人，该名持有人就成为验证者。由于区块的开采和交易的排列是规定顺序的，所以能够以这种方式追溯交易历史。

通过“Follow The Satoshi”方式，**每个节点成为验证者的概率与其持有权益的大小成正比。**另外，如果被选出的验证者没有对区块进行签名，那么这个区块将作废，因此**希望竞争记账权利的节点需要保持在线以准备签署区块。**这也是 Activity（活跃）的原意，有别于传统的节点离线也可以积累币龄的 PoS 共识。目前采用 PoA 的数字通证有 Decred 等。

1.3.2 Casper——下一代 ETH 投注共识

Casper 是目前第二大公链 Ethereum 最受期待的升级之一，是 ETH 接下来的升级中将采用的 PoS 共识机制，**通过加入对恶意节点的惩罚措施来解决 N@S 零成本攻击。**

Ethereum 升级的最初阶段将采用 Casper FFG——一个 PoW+PoS 的混合共识机制。

区块仍然通过传统 PoW 方式产出，并且**每隔一定数量的区块设置一个 PoS 检查点（Checkpoint）**，选出一定数量的验证人对检查点进行验证并投票，投票阶段采用类似 BFT 的容错算法（BFT 会在接下来部分讨论），若表决通过则检查点之前的所有区块不会再被撤销，即**在最长链协议对链达成概率共识的基础上再对一定数量的区块达成最终共识。**降低了对网络发动双花、分叉攻击的可能性。

Casper 协议的主要特点是：

问责制。Casper 协议中，验证人需要向智能合约支付一笔“押金”，并作为分配区块收益的凭证。违反协议规则的节点是可以被识别的，**如果在共识过程中节点表现出恶意、消极或投机行为，押金会被合约没收，这样极大地提高了攻击者发动攻击的成本。**例如网络出现分叉时，验证人在检查点高度投票给两个不同的区块，即同时在两个分叉上“投注”，此类行为被认为是支持 N@S 攻击的投机者，将受到没收“押金”的惩罚。

动态选择验证人。网络每隔一段时间根据投票动态地切换验证人，相对于传统 BFT 类共识机制更加非中心化。

PoW+PoS 混合共识。由于区块还是以 PoW 的方式生产的，有一定的算力支撑，可以在一定程度上避免 N@S 攻击。

1.3.3 Ouroboros——首个可证安全的 PoS 共识算法

Ouroboros（俄洛波洛斯），是北欧神话中一条衔着尾巴的巨蛇，象征着“循环”与“无限”。有些 PoW 共识的支持者认为，PoS 共识机制以自身发行的通证为资源来生产新的通证，没有任何的外部资源

作为区块链安全与通证价值的担保，以“一条衔住自己尾巴的蛇”来比喻 PoS。

Ouroboros 作为新一代数字通证 Cardano 的共识机制，是首个被学术界证明是安全健壮的 PoS 共识算法，以此作为共识的名称，体现了其信心与技术水平。**相比传统 PoS 选择验证人的随机算法，Ouroboros 实现了一个安全的、无法被大量算力或其他计算资源操纵、并且可验证的随机数协议。**并以此随机数算法为工具，通过类似 PoA 的“Follow the Satoshi”算法按照节点持有的权益选择验证者生产区块。

Ouroboros 同样能有效地防止 N@S 攻击。通过随机算法选择验证者生产区块，因此不会像 PoW 共识机制存在网络中几乎同时挖掘出多个合法区块的可能性，从根源上减少了网络分叉发生的几率。另外，在共识算法中加入使验证者忽略在自己上次在线时收到的区块之前的所有分叉的协议，来增强共识的最终性。

1.3.4 PoSV（Proof of Stake Velocity）权益流通证明

PoSV 由 Reddcoin 提出，针对**传统 PoS 机制鼓励人们持有通证，从而减少了网络活跃度**的问题作出改进。它借鉴经济学“货币流通速度”的概念，认为数字通证的价值在于**“所有权”（Stake）的确认和价值的“流通”（Velocity）**两方面。

PoSV 同样根据节点参与竞争的币龄分配记账权，但是**将币龄的计算公式修改为增长率指数衰减的函数**。Reddcoin 将币龄增长率的半衰期设为 1 个月。假设单位通证在第 1 天能够积累 1CoinDay 币龄，在第 31 天只能积累 0.5CoinDay 币龄，第 61 天只能积累 0.25CoinDay 币龄，以此类推。通过这种方式促使节点在持有通证一段时间后用它进行一笔交易，从而重新开始计算币龄，提高网络中通证的流通速度。

1.4 其他 Proof of X 类共识

1.4.1 Proof of Authority

节点用于竞选记账权的资源不再是算力或是权益，而是“Authority”，可以理解为权限、身份之意。节点必须具有真实可验证的身份，才能获得成为区块验证者记账的权限。而一旦被发现恶意行为，成为验证者的权限会被移除。节点的身份认证可以由初始的一组“管理员”节点授予。

举例：ETH 测试网 Koven、VEN

1.4.2 Proof of Believability

采用类似“换届选举”的方式，节点通过抵押通证投票选出若干验证者组成的“委员会”轮流生产区块，每 10 分钟进行一轮投票，并且通过扣除已经生产过区块的节点的的票数等方式增加区块生产者的流动性。

举例：IOST

1.4.3 IPFS 与时空证明

在信息技术日益发达的时代，存储资源的过剩与如何有效利用也成为一个难题。IPFS 希望在 PoST（Proof of Space and Time）与 PoR（Proof of Republication）共识机制的基础上搭建一个**非中心化**

的共享存储网络。根据 IPFS 白皮书的描述，节点可以通过 PoST 生成一个可验证的、表明自己**在一段时间内存储了规定数据**的证明，根据提供存储空间的大小获得相应 Filecoin 挖矿及交易费用产生的权益。

1.4.4 Proof of Burn

是一类较为有趣的共识机制，节点需要通过“燃烧”一定数量通证或其他链上的通证如 BTC、ETH 来换取一定的权重，并根据此权重竞争记账权，并且权重会随着时间流逝降低。“燃烧”通证的方式可以通过将通证转给一个不存在或者通过合约锁定的地址上完成。

1.5 将“浪费”的算力用于有意义的计算

为解决 **PoW 共识过程大量节点的算力被浪费**的问题，一些共识机制对节点重复计算哈希值的过程作出改进，将 Hash 函数替换为其他验证结果很容易但寻找满足目标的解非常困难的函数，例如寻找大素数，希望能够尽量利用这些被“浪费”的算力。例如 Primecoin 等。

2 直接形成共识——BFT 类共识机制

Proof of X 类共识通过验证节点持有一定比例的某种资源如算力、权益，节点有相应的概率被选为某个区块的生产者（取得记账权），在**符合一定规则的前提下，由该节点决定区块的内容**，再经其他节点验证。生产合法区块的节点通常可以获得一定的激励。通常称这类共识是“间接形成”的。

BFT 类共识机制与 Proof of X 采用了不同的思路形成非中心化的共识，并且同样能容忍网络中的拜占庭错误，即通过对提案（区块内容）**直接投票表决，相同意见的票数超过一定比例则作为决策共识**的“直接形成共识”。主流的 BFT 类共识机制有 pBFT 以及 FBA。

2.1 pBFT——实用拜占庭容错

pBFT 最早在 1999 年提出，原目的是为了解决传统分布式系统中的一致性问题，与区块链共识机制的目标不谋而合，是首个高效地解决拜占庭容错问题的算法。目前超级账本 Hyperledger Fabric 采用 pBFT 共识机制。

pBFT 算法引入“视图”（View）和“主从节点”（Replica）的概念。Replica 包括主节点（Primary）以及备份节点（Backups），主节点通常在每一轮共识过程开始时随机选取或者轮流担任。“视图”表示一次主节点分发请求的过程。

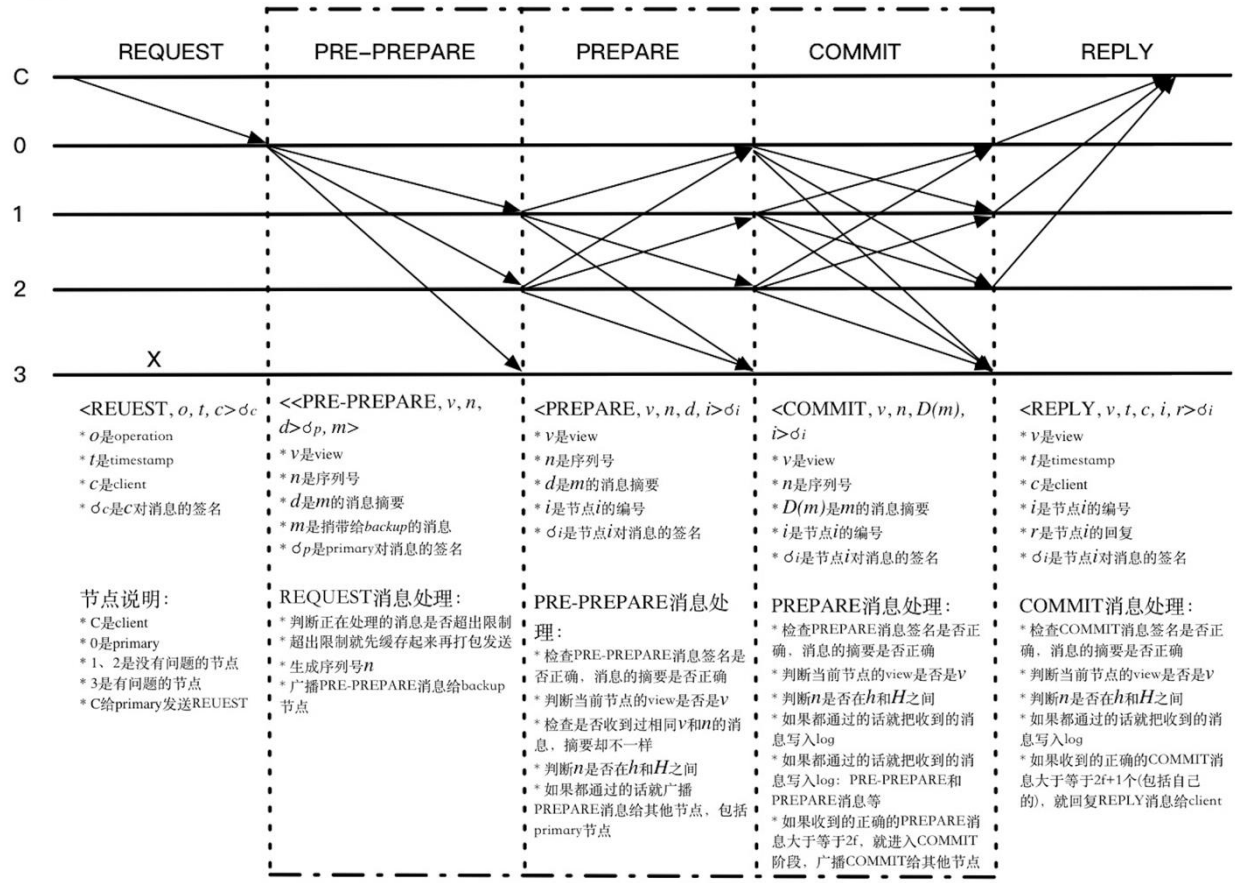
当一轮共识开始时，首先检查主节点的有效性。如果备份节点检测到主节点失效，需要选举出新的主节点，称为“视图更换”。共识过程分为包括预准备、准备、确认阶段，又称**“三阶段协议”**。

如果将 pBFT 算法应用到区块链中，假设 n 个节点中最多有 f 个拜占庭节点。所有共识节点独立监听全网的交易广播，当主节点确定后，将区块及签名信息以预准备消息的形式广播到备份节点，备份节点收到交易并确认合法后就会进入准备阶段，向包括主节点在内的其他节点发送一条准备消息；否则会认为主节点发生故障，发出一条更改视图的消息。

经过两轮消息广播后每个节点会收到一个来自预准备消息的区块和若干条来自其他节点准备消息的区块。节点使用预准备区块验证准备区块的合法性，如果任意节点收到合法的区块（包括自身的准备消息）大于等于 2f+1，则节点进入确认阶段，广播一条确认消息。若节点收到 2f+1 条确认消息（包括自身的确认消息）表明该区块得到最终确认，一轮共识完成。

pBFT 算法对于一个 n=3f+1 个节点组成的区块链网络，可以提供 f 的容错能力，容错能力近似为 1/3。由于一轮共识过程中节点间的通信次数与n^2成正比，考虑到通信延迟的存在，当**节点的数量达到一定规模后，pBFT 的效率会严重下降。目前实践中还没有拥有大规模共识节点的采用 pBFT 算法的区块链网络应用。**

图表3：pBFT 的“三阶段协议”



资料来源：网络资料，通证通研究院

2.2 基于联邦拜占庭协议的共识机制

FBA（Federated Byzantine Agreement，联邦拜占庭协议）是另一种解决拜占庭将军问题的算法。它通过一种**在子网络内部形成信任**（即联邦），将子网络作为整体视为网络的节点的协议。类比节点之间保持通信，子网络之间也应该保证最低的连通度。

基于 FBA 的共识机制有 RPCA（瑞波共识机制）、恒星共识机制等。

在瑞波共识机制中，节点分为验证节点和不参与共识过程的非验证节点。验证节点是被服务节点加入信任列表的节点。服务节点由瑞波基金会选出，并且拥有自己的信任节点列表（UNL, Unique

Node List），在共识过程中，**服务节点只接受来自 UNL 的投票，并且信任它们不会联合作弊。**这样服务节点以及它的 UNL 就组成一个“联邦”，在其内部可以按一定的规则达成共识，从而将其看作一个整体。

瑞波共识机制分两阶段进行：形成交易集的共识以及形成新区块的共识。在一轮共识开始后，每个节点监听网络中的需要确认的交易，将其放到一个交易候选集中。服务节点对自己 UNL 节点的候选集做并集，并且对每一个交易在 UNL 中投票表决，最终得到 80%投票的交易会被放入交易集中，不满足条件的交易会被丢弃或重新放入候选集。

形成交易集后，每一个节点开始将交易集打包为新的区块并计算区块 Hash，广播到网络中。服务节点接收到来自 UNL 广播的 Hash 值，若计算出比例最高的 Hash 值占比超过 80%，则说明该 Hash 对应的区块成为最新的共识。网络的容错能力为 1/5。

恒星共识机制与 RPCA 类似，恒星共识机制的特点是通过节点可以自由地选择要加入的“联邦”，无需中心化的组织预先选出“服务节点”。具体共识机制实现方式较为复杂，此处不再详细介绍。

3 通过选举间接形成共识——Delegated 共识机制

前面提到 pBFT、FBA 等共识机制有一些局限：**参与共识的节点数量有限制，或者参与共识的部分节点必须是可信任的。**但一些公共区块链希望尽可能多的节点参与到共识过程中去，因此一类“代理”共识机制被发明了。借鉴现实社会中的选举，节点可以作为参选人参加选举，也可以给参选人投票。节点控制的选票数量与其持有的某种权益或资源多少挂钩，网络定期按照节点的得票数选出一定数量的“共识节点”，**仅由共识节点完成区块链网络的共识过程。**

3.1 DPoS（Delegated PoS）

虽然 PoS 针对 PoW 能源消耗等不足做出了改进，但它们仍然存在区块容量、出块速度等方面的局限。为了解决这些问题，Dan Larimer（BM）于 2013 年启动了 BitShares 项目，采用了一种通过代理投票实现大部分节点参与共识的共识机制 DPoS。

在 BitShares 网络中，通证被称为“股”，通证的持有者被视作股东。股东拥有每股一票选举“见证人”的权利，以及成为候选人参与竞选的权利，获得选票前 101 名的节点获得参与网络共识过程的资格，被称为“见证人”。**各见证人的记账权利是相同的**，不因获票数的多少产生区别。网络中的投票是实时进行的，间隔固定的时间重新统计获票数。

见证人的义务包括提供带宽以及计算能力以维持网络的运作、参与共识过程生产区块、维护网络的安全。见证人可以通过生产区块获得区块奖励及交易费用，但如果股东们发现**见证人未能履行义务或作出不符合整体利益的行为，见证人会被取消记账权，**由获票数最多的候选人替补。

每个见证人按照一定的顺序（BitShares 中是随机的）轮流获得生产区块的机会，再根据一定的规则对区块链达成共识。在

BitShares 中，见证人根据类似 PoW 的最长链原则选择在高度最高的区块后添加自己的区块。

3.2 DPoS-BFT

继 BitShares 之后，BM 又开发了 Steemit、EOS 等同样使用 DPoS 共识机制的区块链项目。EOS 使用的 DPoS-BFT 共识机制**在以股权投票选举出见证人（EOS 称为 BP，Block Producer）的基础上，使用 BFT 类算法在 BP 之间形成共识**。EOS 的见证人共有 21 名，在 BFT 的三阶段协议中，区块得到 15 个 BP 的确认就可最终确认。

另一种 dBFT 是由 NEO 提出的对 pBFT 共识算法的改进。以 NEO 为例，NEO 网络中有两种通证，管理通证 NEO 以及燃料通证 GAS。节点根据持有管理通证的份额获得相应数量的选票，选举出一定数量的见证人（共识节点），由见证人通过改进的 pBFT 算法形成共识，生产区块，区块中会有奖励的燃料通证，按持有 NEO 的比例分配给各节点。

从本质上来说，NEO 的 dBFT 与 EOS 的 DPoS-BFT 共识类似。**所谓“dPoS”是指见证人根据获得获得权益支持的多少选出，见证人形成共识的算法可以是 BFT 或其他算法**。NEO 网络中燃料通证奖励是直接按权益比例分配的，不涉及 PoS 共识过程。

代理类共识机制中，最终参与共识的只有数量有限的若干个见证人，见证人是由网络中的全体节点投票选出的，理论上见证人因担心不符合选民利益的举动会让自己失去选票，会对自己的行为有所约束。此类共识机制既保证了一定的非中心化程度，相对 PoW 提高了网络效率，是两者的相对均衡，但同样存在着一些缺陷。

由于见证人的数量有限并且公开，攻击者想要发动 DDoS 攻击较为容易，见证人需要额外的保护措施，增加了运行共识节点的成本。

类似 PoS 共识中的“富者更富”，掌握了更多具有投票权的通证的节点通常有更大的话语权，甚至可以操纵投票结果。而如果限制节点的最高投票权重，也可以通过转移通证到不同的节点来规避。如果实行“一节点一票”的机制，又会导致“女巫攻击”变得可行。寻找一个平衡安全性与非中心化的投票算法是较为困难的。

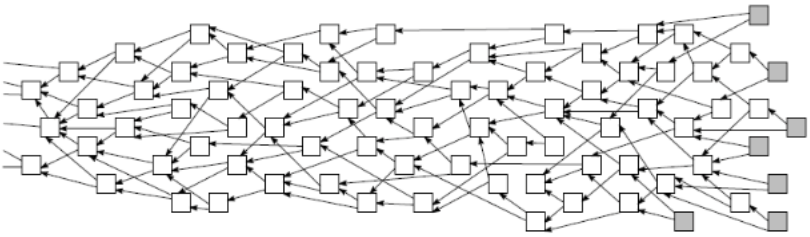
4 不再是区块“链”——DAG 类共识机制

4.1 使用 DAG 作为记录账本的数据结构

我们之前分析的共识机制中，节点所维护的交易历史是一个由区块组成的哈希链表，它具有单向、线性的特点。区块只能作为唯一一个区块的后继区块，并且区块只能有唯一的后继区块。记账节点收集一段时间内的未确认交易，打包进区块，并对区块或者链达成共识。

而 DAG（Directed Acyclic Graph，有向无环图）是一种计算机科学领域常用的数据结构，它满足每条边都是有向的并且从任意顶点出发无法经若干条边回到该点。IOTA 就是采用 DAG 作为记录交易历史的数据结构，使用 Tangle（缠结）技术对交易形成共识的创新型数字通证。

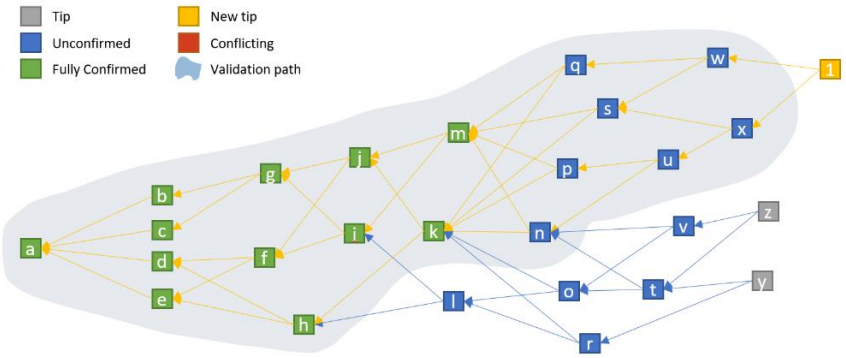
图表4：Tangle 结构示意



资料来源：互联网，通证通研究院

在 IOTA 中，一笔交易视为顶点，它可以选择两笔已经存在于区块链历史（IOTA 称为 Tangle）中的交易验证其合法性并引用（又称“连接”）。这样就形成了两条有向的边，由于节点加入 Tangle 的时间存在顺序关系，因此 Tangle 中不会存在环路。

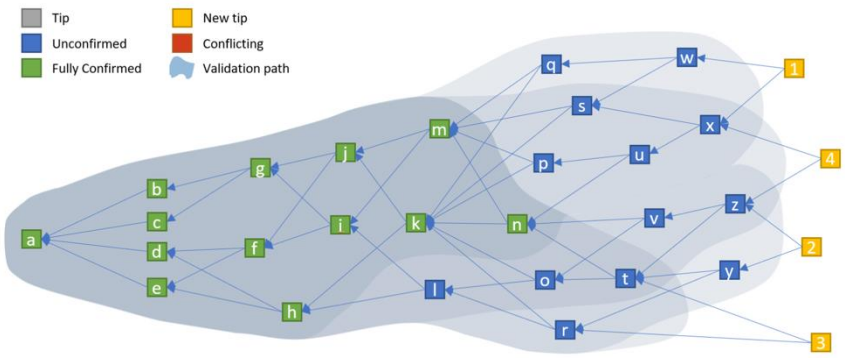
图表5：向 Tangle 中添加新交易



资料来源：互联网，通证通研究院

如图，没有被任何交易验证过的交易称为 tip（末端，图中灰色顶点），一笔新的交易需要选择两个 tip 进行验证，并确保它们与之前的任何的交易没有冲突。如果验证合法则验证路径（按交易引用的交易遍历下去得到的交易集合，图中灰色阴影）上的交易就得到一次确认。

图表6：Tangle 共识中交易的确认等级



资料来源：互联网，通证通研究院

按交易得到确认次数的多少可以划分不同的确认级别，如果一笔交易得到所有 tip 的确认，那么称它是被完全确认的（图中绿色顶点）。

Tangle 共识**不需要专门负责记账的矿工，而是由新交易给历史交易提供验证，因此不需要交易费用**。交易者要付出的代价是付出算力验证两个 tip 是否与 tangle 中的历史交易冲突，为网络提供安全性。

Tangle 共识的优势在于，不需要将交易打包成区块。由于单个节点验证 tip 的效率很高，因此**交易得到确认的速度取决于新交易加入 Tangle 的速度。**

Tangle 共识的缺点是对交易缺乏过滤机制，因此容易遭到大量垃圾交易的攻击，并且没有有效的机制过滤作恶的节点。

5 几类共识机制的对比

5.1 共识机制分类标准

区块链的近十年历程里，不断有新的共识机制被创造出来。有些算法对工作量证明作出了改进，有些则是将传统的分布式容错算法运用到区块链网络中。我们尝试将共识机制要素作为区分不同类别共识机制的标准。

图表7：主流共识机制总结

分类				举例
不能容忍拜占庭错误	Paxos，RAFT			
能容忍拜占庭错误	间接形成共识（竞争记账权）	PoW		BTC
		传统 PoS		Nextcoin
		PoW+PoS 混合共识	Casper FFG	ETH 君士坦丁堡
			PoA	Decred
		改进的 PoS	PoSV	Reddcoin
			Ouroboros	Cardano
		其他	PoST、PoBurn 等	IPFS 等
	直接形成共识	基于拜占庭容错	pBFT	Openledger
		基于联邦拜占庭协议	瑞波共识机制	Ripple
			恒星共识机制	Stellar
	通过选举间接形成共识	验证人通过 PoX 形成共识	早期 DPoS	Bitshares
		验证人直接形成共识	DPoS+BFT, DBFT	EOS, NEO
	直接对交易形成共识	DAG 类共识	Tangle	IOTA

资料来源：通证通研究院

根据“容错”可以将共识机制分为能够容忍拜占庭错误与不能容忍拜占庭错误两类。传统的分布式共识算法如 Paxos、RAFT 便属于前一类，本文不再赘述，而是主要分析适用于分布式对等网络的具有拜占庭容错能力的共识机制。

根据“节点如何获得记账权”和“形成共识的依据”可以将共识机制分为间接形成共识和直接形成共识两类。PoW、PoS 等属于前者，而 pBFT、FBA 等属于后者。

根据“节点参与共识过程的资格”可以将共识机制分为全体参与共识、投票选举见证人、需要身份认证非中心化程度不同的三类。

根据“共识的内容”可以将共识机制分为对区块（交易的集合）形成共识以及对交易直接形成共识。例如 IOTA 采用的共识机制就属于后者。

此外，在共识的不同阶段结合不同算法的优势产生的“混合共识机制”也是未来共识机制演进的趋势。

5.2 BFT 类共识与 Proof of X 类共识的比较

BFT 和 PoX 都是在存在拜占庭节点的分布式对等网络中达成共识的算法。两者存在若干区别。

从**参与共识的节点规模**来说：

在 n 个节点组成的网络中，BFT 类算法完成一轮共识所需的时间复杂度为$O(n^2)$，因此网络的规模有一定的限制。共识过程开始需要在节点中选出“主节点”发出提案，因此需要维护一个可信任的节点身份列表，可扩展性较低。大规模的网络通常采用联邦拜占庭协议或代理投票共识，中心化程度较高。

采用 PoX 类共识的网络中所有节点都根据其拥有的某种资源来竞争记账权，理论上可以实现较低的中心化程度以及相对较高的扩展性。

从**选择记账节点**的角度来说：

BFT 类共识是轮流更换“主节点”发出区块提案，所有节点直接对区块进行投票表决，称为直接达成共识，不存在严格意义的记账节点。PoX 类共识通过固定的规则先选出记账节点，由记账节点决定区块的内容，再通过一定规则对可能出现的分叉链进行选择，称为间接达成共识。

从**共识的最终性**来说：

BFT 类共识在区块被记录到区块链历史上之后，不会发生重组或分叉。而 PoX 类共识即使在没有恶意节点的情况下，也有发生分叉的可能性，需要通过一定的规则对链达成共识。PoX 共识通常需要一定的区块确认，牺牲交易效率以保证非中心化的共识一致性。

从**共识的激励层**来说：

BFT 类共识没有挖矿过程，可以没有激励机制。而 PoX 类共识需要激励机制来约束记账节点不会作出破坏区块链的行为，并增加恶意节点发动攻击的成本。

从网络的实际性能来说：

BFT 类共识由于直接达成共识，因此响应时间（指一笔交易从广播到得到确认的时间）快，交易承载力高。PoX 类共识由于客观的区块容量、出块速度、网络通信延迟的限制，为了保证网络安全性，只能牺牲交易承载力与响应时间。而相比 BFT，PoX 的优势在于扩展性和非中心化程度。

5.3 PoW 和 PoS 的比较

从共识机制层面来说，PoX 类共识的主要区别在于节点竞争记账权的依据和验证节点确实拥有等量资源的算法。以 PoW 与 PoS 的对比为例。

PoW 共识中节点根据拥有算力的多少竞争记账权。验证节点算力的方式是通过让节点完成哈希解谜（一定的工作量），根据采用的哈希函数或其他符合规则的函数又有细微差异。例如 BTC、BCH 有专门用于计算 SHA-256 的 ASIC 矿机，而有些通证为了减少挖矿设备专业化可能带来的矿池中心化影响采用了其他特殊的哈希算法。但它们的共同缺点是浪费大量的能源。此外，BTC 及类似的分配方式决定经过一定时间后，区块激励会减少，此时节点记账的成本被转嫁到交易手续费上。如果网络的交易量或者交易者愿意付出的交易手续费无法支撑记账的能源消耗，势必会造成网络算力的减少，导致安全性降低。

PoS 共识中节点获得记账权的概率与持有的权益相关，解决了能源消耗高的弊端，但同时也带来了新的问题。一是前面提到的“零成本攻击”，可以通过加入对作恶节点的惩罚遏制此类现象；二是由于持有的权益越多，节点预期将来能够获得的收益也越多，因此相当于鼓励人们持有通证，导致网络的交易量下降。另一方面，也导致卡特尔的形成，即寡头垄断区块链的记账权，造成中心化和安全问题。有几种对 PoS 的改进针对这些问题提出了解决方案，但仍不成熟。三是大量的通证是通过募资分配或“预挖”的，造成初始分配的不均衡。

附注：

因一些原因，本文中的一些名词标注并不是十分精准，主要如：通证、数字通证、数字 currency、货币、token、Crowdsale 等，读者如有疑问，可来电来函共同探讨。

免责声明

本报告由通证通研究院和FENBUSHI DIGITAL提供，仅供通证通研究院和FENBUSHI DIGITAL客户使用。本报告仅在相关法律许可的情况下发放，所提供信息均来自公开渠道。通证通研究院和FENBUSHI DIGITAL尽可能保证信息的准确、完整，但不对其准确性或完整性做出保证。

本报告的完整观点应以通证通研究院和FENBUSHI DIGITAL发布的完整报告为准，任何微信订阅号、媒体、社交网站等发布的观点和信息仅供参考，通证通研究院和FENBUSHI DIGITAL不会因为关注、收到或阅读到报告相关内容而视相关人员为客户。

本报告所载的资料、意见及推测仅反映通证通研究院和FENBUSHI DIGITAL于发布本报告当日的判断，相关的分析意见及推测可能会根据后续发布的研究报告在不发出通知的情形下做出更改，投资者应当自行关注相应的更新或修改。

市场有风险，投资需谨慎。本报告中的信息或所表述的意见仅供参考，不构成对任何人的投资建议。投资者不应将本报告为作出投资决策的唯一参考因素，亦不应认为本报告可以取代自己的判断，通证通研究院或FENBUSHI DIGITAL、通证通研究院或FENBUSHI DIGITAL员工或者关联机构不承诺投资者一定获利，不与投资者分享投资收益，也不对任何人因使用本报告中的任何内容所引致的损失负责。

通证通研究院和FENBUSHI DIGITAL对本免责声明条款具有修改和最终解释权。