比特元 BTY 白皮书

——一种简单稳定、扩展性强的区块链网络

目录

一. 比特元设计目标

目前，以比特币为代表的分布式记账、代币激励的时间戳系统，被普遍认为有望成为未来金融的支柱。对一种新兴技术来说，能够不断的技术升级优化，完善功能、性能，才能得到市场的认可，得到广泛的应用落地，从而引领一个时代的变革。比特元的主要目标就是实现去中心化治理，让持币的人来制定相关规则，并有足够的发展基金，调动全社会的力量来推动比特元的发展。

比特元的核心会如比特币一样稳定，同时兼备灵活高效的扩展性，开发者可以在比特元上建立强大的 DApp 和 多链的生态，共同维护比特元系统的发展。任何个人或者团体，只要为生态系贡献力量，都能拿到比特元作为回报。

1. 数字资产

以电子数据形式存在的资产被称为数字资产。区块链技术的运用，使数字资产拥有去中心化、去信任、可追踪朔源的特点。比特元主要实现了资产数字化、一键 Token 的功能。

- 用户可在比特元主链上登记资产，实现资产数字化。一些流动性不足的资产，诸如房产、黄金、大宗商品、积分、白条等，可以通过数字化、证券化，增加流动性，实现价值的转移。
- 用户可通过填写表单一键发行 token，无需编写代码，也不用担心代码的错误对比特元网络产生影响。同时 token 名字具有全网唯一性，避免了重复和混淆。

2. 应用生态

比特元的核心是致力于打造一种简单稳定、扩展性强的区块链代币系统，整个系统的设计秉承着简单稳定的原则，从而实现安全快速支付、隐私交易和原子互换等功能，同时运用离线钱包和钱包找回等功能来保障比特元数字资产的安全性。为了维护整个比特元生态系统，比特元还将在积分、预付卡、游戏等多个领域开发应用，以提升整个生态的多样性。

a. 挖矿

比特元推出的 PC 版比特元钱包，除了支付、存储功能以外，还具有挖矿功能，持币人通过锁定一部分的币来换取选票（Ticket）。比特元采用创新式 POS 算法，预计全球部署 100 万个同步节点，其中挖矿节点约 3 万个。每个区块生成时间约 15 秒，每个新区块产出 30 个 BTY，其中 18 个 BTY 由矿工获得，另外 12 个 BTY 则进入发展基金。当前版本，每 10000BTY 可以锁定并换取 1 张 Ticket，所有的在线 Ticket 会参与新区块生成的挖矿，平均每张 Ticket 被选中的时间是 5 天，拥有更多的 ticket 会获得更高的产矿概率。

b. 支付

比特元底层系统经过多次迭代优化，已具备高性能、低延时的支付特性，这不仅为比特元在支付清算领域提供了强劲的竞争力，同时也为比特元系统内的代币转账搭建了高速通道。比特元力争成为全球资产交易的主要媒介，用户大部分费用可以减免。

c. 钱包找回

比特元的预设钱包找回功能，解决了私钥丢失而导致数字资产损失的问题。当用户因遗失钱包或者存储设备突然损坏引起的私钥丢失，可以通过低权限的备用私钥（自己保存或者托管给信任的机构/人）找回自己的数字货币，找回指令并不会立刻转移数字资产，而是会在预告一段时间后生效，所以若备用私钥被冒用，用户也可及时发现，并用原私钥将数字资产转移到安全钱包，避免损失。

d. C2C 交易

在一个有众多节点分布的系统中，每个节点都具有高度自治的特征。任何一个节点都可能成为阶段性的中心，但不具备强制性的中心控制功能。节点与节点之间，会通过网络形成非线性因果关系。实现去中心化、开放、扁平、平等的系统。

比特元区块链上的交易，只需要创建钱包，不需要个人实名信息，抛弃了第三方机构，真正实现了去中心化交易。所有节点都置于链上，由智能合约执行全部操作，交易过程无需信任任何第三方，即可实现所有比特元链上 token 的交易，降低了交易成本，也提高了交易的效率。

e. 区块链浏览器

用户通过比特元区块链浏览器，可以查看区块链上所有的相关信息，包括区块产出情况，每个区块包含的交易，token 发行的记录，token 转账的记录，每个区块的产矿记录，账户地址资产余额等。

f. 商业应用

比特元独特的生态系统能够让数字资产和数字代币在不同链上无障碍的流通、接收、存贮、交易。

比特元区块链生态系统中的代币可以代表任何有价值、可以交易的东西，应用于众多产业，比如：积分、预付卡、游戏、竞彩、不动产、大宗商品、智能清算等等。

二、管理模式

1. 发行机制

比特元的管理代币是 BTY，2014 年初发行，自主创新 POS 算法，目前流通量 3.2 亿左右。比特元每个区块生成时间约 15 秒，每个新区块产出 30 个 BTY，一年新增约 6300 万 BTY，其中 18 个 BTY 由矿工获得，另外 12 个 BTY 则进入发展基金，BTY 的最小单位为 10^{-8}。每 1 万个比特元可以购买一张票进行挖矿，诚实的节点可凭票进行挖矿，票数越多，挖到的概率越高。恶意节点，试图分叉比特元，或者任何系统能检测到的恶意行为，都可能会被惩罚，每次惩罚会损失 20%的资产。挖矿必须以比特元基金会发布的标准钱包进行，篡改挖矿行为，如果被系统自动判定为恶意，都会给矿工造成巨大的损失。

2. 发展基金

比特元一直致力于自治的方式解决区块链的治理问题，社区志愿者制定社区运营规则，将比特元打造为自主和去中心化的数字货币，所有参与者都可能因其付出的努力而获得相对应的奖励。

比特元基金会特设发展基金，通过挖矿持续获得的 BTY 激励，可用于支持比特元网络的开发、运维和生态发展，这部分包括用于激励比特元开发者和理事会成员、周边生态开发者、其它机动使用等。此外，还有一部分将用于税收减免以及公益活动。

比特元基金会都会在相关渠道和社区公示比特元发展基金的使用情况。

3. 比特元发展路线图

- 2018.05

比特元主网上线，限速 100 笔/秒。

主要功能：转账、挖矿、平行链（有自己独立的钱包和服务，平行链共识安全由主链提供），钱包找回，一键 Token，hash 锁定；

- 2018.09

比特元实现和比特币原子跨链互换功能（BTC relay），实现和比特币的去中心化的兑换和交易。例如比特币打到某个地址后，比特元或者比特元中的 Token 就会自动发送给对方 ；

- 2018.11

推出隐私交易功能，实现完全匿名交易；

- 2019.02

比特元推出区块链提案机制，完全透明使用发展基金。

三、技术实现

1. 共识机制 POS

POS 全称为 Proof of Stake，是一种通过权益证明来投票以实现大规模节点参与共识的机制。比特元代币的持有者通过投票，来实现相关决策。比特元的 POS 算法，加入了一些自主创新，解决了挖矿的安全问题，可以和传统的 POW 一样安全。

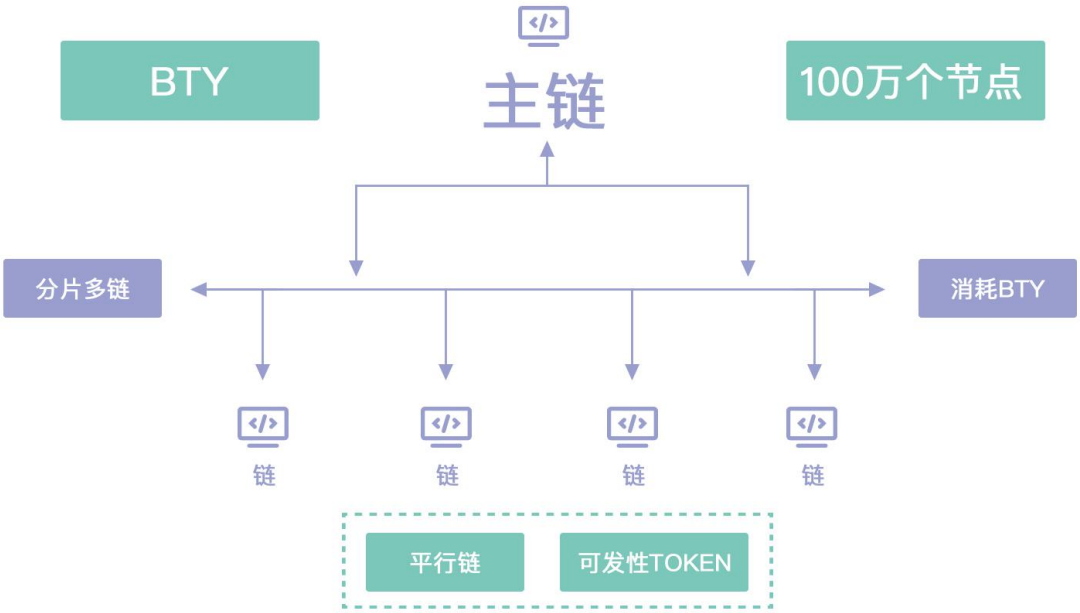
在 POS 共识机制之下，不再需要大量消耗能源挖矿，在一定程度上缩短了共识达成的时间。比特元平均每 15 秒生成一个区块，交易吞吐量实测可达到

100tps，在公有链中性能较高，商业化应用性强。

2. 平行链

比特元的平行链其实就是独立的应用链，这些链使用比特元的共识，只需少量部署 5-10 个节点即可。这些平行链依附于比特元区块链平台，又有自己独立的钱包和服务，例如发行数字资产等。只要保证比特元区块链的安全性，即可保证比特元生态系统中其它平行链的安全性。随着平行链的增加，比特元节点也将迅速增多，并且更加分散，DDOS 攻击力也会减弱，就可以保证比特元区块链生态的安全。

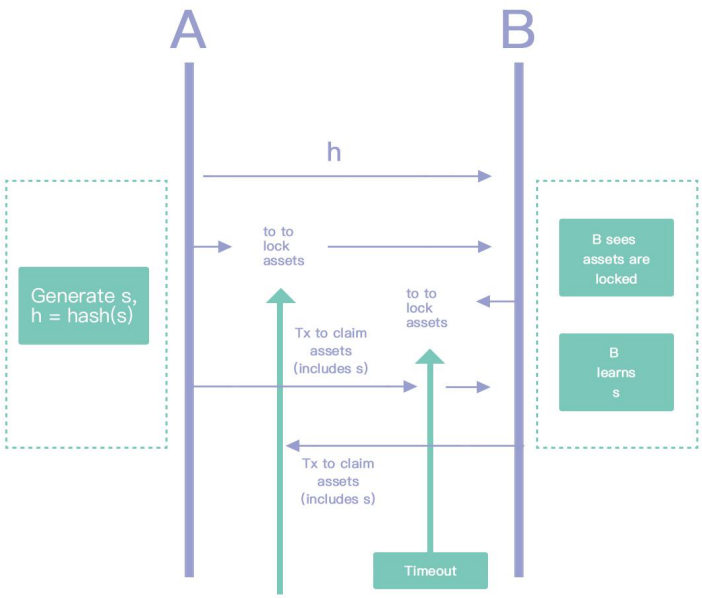
在比特元生态的基础上，结合开放平台的 API 和 SDK 就可以开发独立逻辑、容易升级的平行链，这就像安装 Windows 系统一样简单，可节约巨大成本，各行业机构不必再为区块链底层基础设施研发消耗庞大的人力物力。



3. 跨链原子交易

比特元在跨链交易上采用 Hash Locking（哈希锁定）的方法，可以用非常简单的方式实现跨链原子交易。原子互换就是在利用比特元的脚本语言来构建智能合约，授权进行跨链交易。

哈希锁定起源于闪电网络的 HTLC（Hashed TimeLock Contract），它的实现过程如下，以 20ETH 和 1BTC 的原子交换过程为例：



1）A 生成随机数 s，并计算 h = hash(s)，将 h 发送给 B；

2）A 生成 HTLC，超过时间设置为：2 小时，如果 2 小时内 B 猜出随机数 s，则取走 1BTC，否则 A 取回 1BTC；这里 A 用 h 锁住 BTC 合约，同时 B 也有相同的 h。这样 A 和 B 都有相同的锁 h，但 A 有钥匙 s；

3）B 在以太坊里部署智能合约，如果有谁能在 1 小时内提供一个随机数 s，让其 hash 值等于 h 则可以取走智能合约中 20ETH；

4）A 调用 B 部署的智能合约提供正确的 s，取走 20ETH；

5）B 得知 s，还有 1 小时时间，B 可以从容兑现 A 的 HTLC 的 1BTC。

一旦超时，交易失败，符合原子性。

Hash Locking 极大地提升了比特元生态网络的交易处理能力。交易双方若在区块链上预先设有支付通道，就可以多次、高频、双向地实现快速确认的交易支付；双方若无直接的点对点支付通道，只要网络中存在一条连通双方的、由多个支付通道构成的支付路径，闪电网络也可以利用这条支付路径，实现双方之间资金的可靠转移。

后期，比特元研发团队还将开发一些工具，用于各种币之间的原子交易、提高原子交易的便捷性，直接和安卓客户端结合起来。

四、总结

比特元的主要目的是设计一种便于自我更新的系统，从而形成一个综合型的开发平台，各行各业都可以在这个平台存储数据，并且进行撮合交易。它可以支付、接受、贮存多种货币，支持钱包找回、抵押发币、跨链币币交易、POS 环保挖矿等，而且拥有较高扩展性。