比特元 BTY 白皮书

一种简单稳定、扩展性强的区块链网络

V2.0

2018 年 6 月

目录

摘要

比特元的目标是于打造最简单稳定、拓展性强的区块链代币系统，改善比特币和以太坊的既有问题，回归区块链去中心化、透明、平等的本质初衷，系统设计秉承简单稳定的原则，从而实现支付、C2C 交易、DApp 应用开发和商业应用落地，并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。

在技术实现方面，比特元透过平行链打造简单易用、灵活并且易于拓展的公链，兼顾效率和安全性，让开发者可以简便地在比特元公链上打造自己的微生态系。除此之外，比特元提供一键发币功能，所有人都可以在比特元公链上发行非原生代币。

比特元致力于打造去中心化的支付环境，C2C 交易让比特元上的原生代币和非原生代币都可以透过比特元互兑，实现个人和个人之间匿名、安全和去中心化的支付行为。在比特元生态系之外，比特元开发团队还透过 BTC Relay 和 Hash Locking（哈希锁定）两种技术方法，实现跨链、跨币种的 DEX 去中心化交易。

比特元采用自主创新 PoS 算法，比特元的目标是设计一种自我更新的系统，建构一个综合型的开发平台，我们希望，建立繁荣共好的生态，回归区块链公开、开放、透明、人人平权的本质， 让全球的开发人员参与进来，共同维护比特元系统的发展

1.比特元目标与使命

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，必须不断升级优化技术，完善功能和性能，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。比特元的主要使命就是实现去中心化治理，让持币者制定相关规则，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，都能获得比特元（BTY）作为回报。

比特元的核心目标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，以提升整体生态的多样性。

2.应用生态

2.1 数字资产管理

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。

2.2 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 10000 BTY 可以锁定并换取 1 张 Ticket，所有的在线 Ticket 皆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，拥有越多的 Ticket 会获得越高的产矿概率。

2.3 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。

2.4 钱包找回

比特元预设的钱包找回功能，解决了因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导致私钥丢失，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。

2.5 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。

2.6 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、可以交易的资产，

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。

3. 技术实现

3.1 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，加入了自主创新，解决了 POS 挖矿的安全问题，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。

3.2 一键 token

一键 token 是一种代币发行的方法，简而言之，任何人只要通过填送表单，通过审核，即可在比特元的区块链网络系统上，发行自己的代币。整个过程中有三个环节：区块链系统、非原生代币合约和原生代币合约，比特元区块链上的一键发 token 属于非原生代币合约，是比特元代币以外的代币。

代币建立在比特元区块链的生态上，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，代币的安全性由比特元主链保证，申请简便、安全性高。各个代币可以在比特元区块链上共建生态、共存共荣。

比特元区块链的一键 token 功能有以下优势：

- **发币简便**

无需技术团队研发，只要通过表单申请，符合比特元区块链生态需求即可发行 token。

- **安全性高**

建立在比特元区块链上，比特元区块链保证 token 的安全性，无须自行维护安全。

- **数据真实**

所有交易都被记录在区块链上，不可篡改，数据真实可信。

- **Token 的唯一性**

在比特元区块链上，除去一些特殊名称，token 名称和符号都是唯一的。

- **共享生态**

在比特元区块链生态系中的各种 token 既可以独立发展，又可以通过比特元通证互相联系，共建比特元生态，共创全新互联网生态。

3.3 匿名 C2C 交易

只要创建钱包，即可在比特元区块链网络中进行交易，且钱包和钱包之间可直接进行交易，每个钱包都是一个交易节点，无需透过交易所，也可以实现个人和个人之间的交易。

- **匿名**

比特元区块链网络中的交易可以实现匿名交易，不同于现有的交易模式，大多需要实名认证，个人数据被集中储存在交易所，个人隐私风险高。比特元个人钱包完全建构在区块链上，保有区块链匿名的特性，对个人数据的保护程度较高，跳过中心化平台，实现个人与个人之间的直接交易，

- **去中心化**

原有的传统中心化交易方式，仰赖平台做信用背书，以保证交易真实可靠，但也暴露出个人隐私和资产被盗的风险。个人无法掌握自身信息，但在比特元区块链网络中，个人交易信息分散式地储存在所有节点上，任何人都可以公开检阅，形成多中心化的数据储存模式。跳过中心化平台直接进行个人和个人之间的交易，交易效率较高。

在比特元区块链的系统中，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。

- **非原生代币兑换**

所有发行在比特元区块链网络中的代币（token），又被称为非原生代币，不同的非原生代币之间，可先行兑换成比特元，再互兑交易。无须透过中心化的交易所或交易平台，个人与个人之间即可在比特元网络中互换不同的代币，效率较高，简而言之，钱包即交易所。

3.4 平行链

关于平行链的三个关键字是扩展性高、效率高和安全 。平行链比分片方案扩展网络能力更简单，更加直观，功能更加强大；它不仅仅是一个 DApp 的应用，直接拥有自己的区块链生态；也比跨链交易更加高效简单。

3.4.1 背景

大部分区块链系统由两个紧紧耦合在一起的系统组成：共识和状态机。共识提供了区块链网络的安全，这也是区块链和传统软件系统最关键区别的本质，而状态机则提供了区块链网络的功能。区块链共识可以大致分成 3 类：PoW，PoW 和 DPoS，但是状态机千奇百怪，有无限种可能性，基本上每个链的状态机都不同，因为，他们提供了不同的功能。平行链的目标就是让不同的区块链，共享共识部分，让任何想开发区块链系统的人，只需要专注开发链状态机的部分即可。

3.4.2 为什么需要平行链

绝大多数人认为，区块链只要搭几个超级节点，就能保证安全，或者买点矿机挖矿就可以保证安全。事实上，最近发生的 PoW 51%攻击事件说明，PoW 不是最安全的。另一方面，DPoS 因为节点数少，验证的人就相对少，有心人士共谋的可能性便大大增加，可以说 DPoS 只是一种区块链为了性能妥协的替代性产物。所以，要维护区块链系统的安全，只是搭建几个节点是不够的，而是需要一个非常强大的技术团队支撑，同时需要众多社区成员参与搭建节点，交互验证，才能提高安全。既然安全的代价那么高，那么让区块链共享共识是最自然的选择。

3.4.3 平行链是什么

平行链（可并行化的链）是一简单、易扩展的区块链，它的安全性由附着的“主链”提供，而非自有的。平行链并非完全平行于主链，它和主链保持既独立又连结的关系，在主链之下，平行链可以拥有自己的超级节点和状态机，但平行链的安全性是由主链提供的，平行链上的原始交易数据，和交易的执行

状态哈希值最终也保存在主链上。

主链不仅可以保证平行链的安全，并且可以在不同的平行链之间简单、安全地做跨链操作，从而在同一个平行链网络内的链条可以形成自己的生态系统。最简单的一个例子就是积分联盟，如果每一个公司，组织，都自己搭一条链，发积分，那么最直接的结果是这些积分都不能互通，或者互相交换非常麻烦。如果这些积分不能互通，它和传统的系统之间便没有任何区别，但若在平行链上搭建积分系统，那么不同链上的积分便能自动实现互换。这就是平行链生态和单链生态的不同，在单链系统中，你必须建立自己的生态，每一条链之间都是独立的，而在平行链生态中，你不但可以利用系统的共识保证安全，还可以共享原有的生态。

3.4.4 平行链的本质

平行链的一个关键特征是它们执行的计算本质上是独立，但又跟主链连结在一起。平行链之间有明确的隔离分界线，可以立即执行所有交易，而不用担心和其他链产生冲突。

打个比方，如果有十条平行链，在同样的时长之内，相较于现有的传统区块链交易方式，每一次都只能是每个节点一笔、一笔地处理交易，平行链可以多条链同时处理交易，效率可提升十倍，好比同样开车从 A 点到 B 点，原先只有一条公路，一小时内能通过的车流量可能只有两千，现在加开了十条，能处理的车流量就提升了十倍。

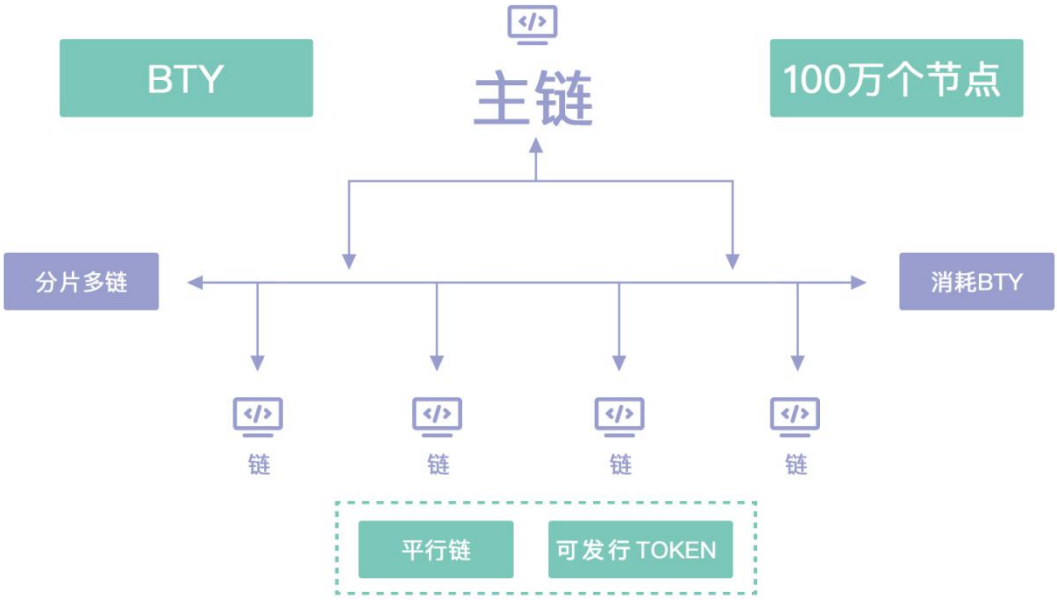
因此，平行链可以在主链的架构之上，开发自己的功能，同时又无需自己维护安全性，这让平行链的可扩展性较现有的区块链系统要高很多，大部分开发 DApp 的人，都希望拥有自己的生态。在比特元主链上，只要执行一个智能合约，就能让原先不懂区块链技术的程序开发员，也能开发区块链应用，这是我们引入平行链，希望解决的业内痛点。

每条平行链都可以自行定义其自身的功能。如果平行链出现 bug，平行链的共识各方可以轻易地升级更新，对主链没有任何影响。

区块链的另一痛点就是，数据是全量的，要验证一条链的正确性，我们要下载所有的数据才能验证。但是平行链不同，验证平行链的正确性，只需要下载和平行链相关的数据就能验证。

比特元的平行链其实就是比特元主网上的分支，这些平行链使用比特元的共识，只需少量部署 3f+1 个节点即可。f 表示错误节点。它们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，同时，生态越丰富，平行链之间的交互功能就会越多，整个生态的力量会更加强大。

这些平行链开枝散叶，可以打造自己独有的生态系，就像在一个大型生态系中，又各自长出不同的微型独立生态系，如同热带雨林生态一样。全球有一半的物种生存在热带雨林，热带雨林是生态多样性最丰富的自然地貌，平行链就如同热带雨林一样，致力于打造最多元丰富的生态系，让微型生态系在稳定且高效的主链系统中自然生长，蓬勃发展。



3.5 DEX 去中心化交易

相较于集中式的交易，由于监管客户资金需要遵守管理机构的相关规定，需要跨越很多障碍。通过这种方式来进行交易的用户，必须遵守集中式交易服务商的各种规则且支付相应的费用。比特元的 DEX（Decentralized Exchange）去中心化交易则能解决这方面的问题，实现既便捷又安全的交易。比特元区块

链实现 DEX 去中心化交易的方式有两种：BTC Relay 和 Hash Locking。

3.5.1 BTC Relay

使用 BTC Relay 指的是在比特元区块链上置入 BTC 轻钱包，从而实现 DEX 去中心化交易。

轻钱包（Simplified Payment Verification）指的是简单支付验证。中本聪在论文中简要地提及了这一概念，他指出：不运行完全节点也可验证支付，用户只需要保存所有的区块头（block header）就可以了。用户虽然不能自己验证交易，但如果能够从区块链的某处找到相符的交易，他就可以知道网络已经认可了这笔交易，而且得到了网络上多少个节点确认。

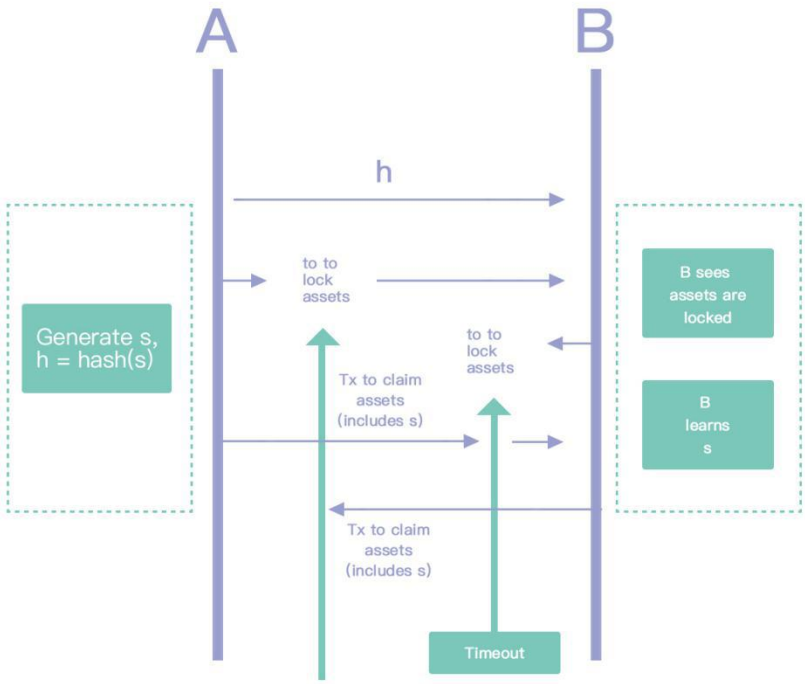
BTC Relay 指的就是把比特币区块头拷贝到比特元上，在比特元上虽然无法验证交易，但是能够从比特币的某处找到相符的交易，就可以得知网络已经认可了这笔交易。采用这种方式，可以撮合任何有交易意向的双方进行交易，交易保证会在 6 小时内完成。整个过程交易双方信息都是匿名的，无需第三方担保。

3.5.2 Hash Locking（哈希锁定）

比特元 DEX 去中心化交易的另一种实现方式是使用 Hash Locking（哈希锁定）来完成跨链原子交易。

跨链原子交易指的是不经由第三方完成的安全可靠的跨区块链交易，只要双方互相约定，就能安全地达成跨链的资产交易。原子性指的是一笔交易像原子一样，被视为最小的、不可再分割的单位（一般意义上）。比特元的跨链原子交易就是利用脚本语言来构建智能合约，允许跨两个区块链安全地转移资金，如此可以避免不同加密货币之间进行交易时，还需要第三方来授与交易信任。

Hash Locking 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，但只有 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。

具体而言，在使用 Hash Locking 来实现跨链原子交易的过程如下：假设甲要用持有的 1 万个 BTY 交换乙的 1 个 BTC 。假设甲生成随机数 N，使得哈希值成为特定数值 R，甲把特定数值 R 发给乙。同时，甲部署智能合约，如果乙在两小时能提供正确的随机数 N，使哈希值为 R，即可拿走 1 万个 BTY；乙同样设置在 1 小时内，如果甲能提供正确的 N，即可拿走 1 个 BTC。

当交易开始时，甲的 1 万个 BTY 和乙的 1 个 BTC 都会被转到一个特殊的暂存位置，按照先前规定智能合约，只有两种方式能把这些币转走：一是出示随机数，能使哈希值变为约定的数值；二是在超过了约定的时间，还没有提供正确的随机数，那么币被退回给原来的双方。

这些设置都完成后，甲指出正确的随机数 N 就可以把乙的 1 个 BTC 取走，因为是区块链是公开的，乙就可以查看到正确的随机数 N，取走甲的 1 万个 BTY。

需要注意的是：一、甲乙双方的智能合约只针对于交易双方，并不是任何知道随机数的人都可以领取，所以，即使甲在领币的时候，随机数被广播，其他人也不能拿走币；二、甲乙双方智能合约设置的时间是有差异的，甲设置的时间要比乙长，这样才能保证在甲拿到乙的币之后，乙有足够时间去拿甲的币。在这两个前提下，跨链原子交易就得到了保证，不会存在一方拿了币跑路的情况。

综上所述，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；即使双方没有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，直接和手机客户端结合起来。

简言之，使用 BTC Relay 和 Hash Locking 皆能达成不同通证之间的跨链交换，但交易所需时间、交易双方的身份真实性和交易所需时间的区别主要如下图：

	BTC Relay	Hash Locking
币种	目前限于 BTC	不限币种
交易所需时间	6 小时内保证完成	不定
交易身份	匿名	交易双方知晓
第三方	无	无

比特元除了是一种简单稳定、扩展性强的区块链网络，也通过 BTC Relay 和 Hash Locking 两种方式，实现轻便、可信赖的支付。DEX 去中心化交易的功

能，和比特元区块链本身去中心化的理念相符。

4.管理模式

4.1 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，会对矿工造成巨大的损失。

4.2 发展基金

比特元一直致力于以社区自治的方式解决区块链的治理问题，由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。

比特元基金会将会在相关渠道和社区公示比特元发展基金的使用情况。

4.3 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，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，比特元或者比特元网络中的 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，发展基金使用情形透明化。

5.总结

比特元的目标是设计一种自我更新的系统，建构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和开发应用，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、一键发 token、跨链币币和去中心化交易、POS 环保挖矿等，而且拥有较高扩展性，容易迭代开发。

我们希望，建立繁荣共好的生态，回归区块链公开、开放、透明、人人平权的本质， 让全球的开发人员参与进来，共同维护比特元系统的发展。任何一个个人或者团体，希望给这个生态贡献力量，都能拿到比特元作为回报，共同打造最安全且平等多元的生态系，让真正的科学技术成为第一生产力