# 比特坊（BTE）

以太坊上的类比特币价值储存手段

# Bitcoineum 白皮书

# v 1.1

BSC 翻译

# 比特坊（BTE）：以太坊上的类比特币价值储存手段

**Matt Branton** (bitcoineum@protonmail.ch)

比特币的价值存储 +以太坊的性能

**BSC**（超级熊猫 & yuanchao）

## 概述

比特币的可扩展性问题和政治僵局，呼唤新的解决方案。我们在此提出一种新代币——比特坊（bitcoineum），它建立在以太坊网络上，由一个去信任（trustless）、匿名的去中心化应用所控制。通过新颖的以用户为中心的挖矿算法，比特坊复制了比特币的值语义（value semantics），同时被赋予以太坊的原生性能。不同于把智能合约以及其他高级功能移植到比特币网络上，比特坊直接在以太坊上建立了一种价值存储的手段。相比于以太币，这种新代币在保留了以太坊可交互性和交易速度的基础上，引入了一些吸引人的特性。更进一步，它的交易速度和交易费用都将优于现有比特币网络，可以成为整个价值存储类代币生态体系的锚定物。比特坊拥有其他基础货币所没有的特性，它可以被看作更大货币体系中的一个模块化的组成部分：作为一种可以通过公平的在线挖矿获取的基本单位，用以引入其他功能。

## 代币分发

比特坊是一种通过公平的挖矿获取的加密货币。没有 ICO，没有预挖，没有创始人奖励。只要有 ether，就可以通过新颖的挖矿机制挖出比特坊，这是一种真正民主的代币获取途径，模仿了比特币早期的分发方式。尽管本文作者曾经考虑过是否要进行 ICO，但在这种挖矿机制下，ICO 既无必要，也不符合比特坊的长期目标。如果你认同比特坊在已有智能合约网络上建构强价值存储手段的理念，请通过挖矿支持它。

## 安全性

比特坊的安全性，依赖于现在正保护着以太坊区块链上价值超过 110 亿美元（白皮书写作时）的资产的安全机制，也取决于以太坊本身的性能。交易的安全性和完整性将由以太坊网络保证，其新代币的发行（上限为 2100 万）则取决于独立的概率挖矿机制。

## 代币

比特坊代币将遵从 ERC20 代币标准，从而保证比特坊与广泛支持 ERC20 协议的 DApp 间的互相可操作性。这将有利于创造一种具有流动性和可互换性的价值存储手段，并且允许次级代币直接通过（存入的）保证金（deposit）获取价值。这些次级代币可以对比特坊 ERC20 代币进行扩展或封装，增添附加功能，例如零知识证明，混币，以及其他高级功能，就像以太坊本身也可以添加这些技术那样。此外，比特坊还支持独特的转换接口，这是一种便捷的机制，借此机制，比特坊和其销毁证明（proof-of-burn）机制可被转换到任何支持这种接口的代币上。这将提供一个无门槛的机制，可以去信任（trustlessly）的将比特坊技术升级为以太坊的原生扩展性能，并能用以创建具有独特安全、隐私属性和其他特性的次级代币。

# 挖矿综述

## 概述

比特币挖矿，本质上是一种计算资源和概率的游戏。通过消耗现实世界中的资源来增加挖出区块的概率。比特坊引入了一种概率算法模仿比特币的挖币过程。每 50 个以太坊区块，开启一个新的挖矿窗口期，矿工们竞争获取比特坊区块奖励。普通用户就能做矿工，不需要投入专门的硬件，只要愿意将 ether 投入到一个基于概率竞争比特坊区块奖励的抽奖活动中。所有在这个过程中消耗的 ether，都会被销毁，这其实是一种价值转移，就好比比特币挖矿要烧掉电力。

## 作为概率游戏的挖矿奖励

对于每个区块，接下来的五十个区块为一个“挖矿窗口”。矿工通过对窗口结束后第一个区块的根哈希值押注代币，获得可能的收益。按以太坊区块时间计算，大约是十分钟下注一次。这个 256 位的哈希值对应着 2^256 种可能性的解空间。难度被映射到这个解空间（key space）中，即挖矿难度为搜索整个解空间的总成本。在五十个（以太坊）区块时间的窗口内，所有矿工的下注占总成本比例，代表了在这个下注轮中，会被搜索到的解空间的百分比。根据每一个矿工在整体（下注）中的贡献，他们将分得对应比例的搜索区间。搜索范围覆盖了这个未来的 SHA256 哈希值的矿工，将获得这个挖矿窗口的比特坊区块奖励。

我们举一个简单的例子。在挖矿难度为 1 时，假设挖矿难度等于需要花费的以太币数，即难度为 1 等于需要花费 1 个以太币。在这种情况下搜索整个 2^256 的解空间将要花费 1 个 ether。Alice 提交一个 0.1 ETH 的挖矿尝试， Bob 提交了一个 0.3 ether 的挖矿尝试，还有 0.6Ether 的工作价值没有被分配。这意味着 Alice 搜索 1/(1/0.1) = 10% 的解空间 , Bob 搜索 1/(1/0.3) = 30% 的解空间，还剩余 1(1/0.6) = 60% 的解空间无矿工搜索。我们根据每个矿工交易提交的顺序依次排列搜索区间。Alice 搜索 0 ~ 0.1 * 2^256, Bob 搜索 0.1 * 2^256 + 1 ~ (0.1 + 0.3) * 2^256，剩余的解空间不搜索。然后计算挖矿窗口关闭后的第 51 个块的状态根哈希，并与每个参与者的搜索区间进行比较，以确定谁获得块奖励。如果在这一轮中所有投注的以太币总额，超过了挖矿难度，挖矿难度为投注总额。

$$T_{\text{diff}} = max C_{\text{diff}}, \sum_{i=1}^{n} M_{\text{bet}} \qquad (1)$$

Where:

$T_{\text{diff}}$ : Total difficulty for this mining attempt
$C_{\text{diff}}$ : computed network difficulty
$M_{\text{bet}}$ : miners current bet
$n$ : number of miners

$T_{diff}$ : 当前挖矿难度　$C_{diff}$ : 算力网络难度　$M_{bet}$ : 当前矿工的下注　n: 矿工数

$$M_{\text{alloc}} = 1/(T_{\text{diff}}/M_{\text{bet}}) \tag{2}$$

Where:

$$\begin{aligned} M_{\text{alloc}} &: \text{allocated \% of total key space} \\ T_{\text{diff}} &: \text{total difficulty} \\ M_{\text{bet}} &: \text{miners current bet} \end{aligned}$$

$M_{alloc}$：解空间的占比 $T_{diff}$：挖矿难度 $M_{bet}$：当前矿工下注

我们可以使用上述方程来构建一个奖励表，用于任何预计的难度，并使用它来公平分配比特坊。

| Miner | $M_{\text{bet}}$ | $M_{\text{alloc}}$ | Range |
|---|---|---|---|
| Alice | 0.1 | 0.1 | $[0, 0.1 * k)$ |
| Unallocated | 0.2 | 0.2 | $[r_{\text{alice}}, r_{\text{alice}} + (0.2 * k))$ |
| Bob | 0.3 | 0.3 | $[r_{\text{unalloc}}, r_{\text{unalloc}} + (0.3 * k))$ |
| Kate | 0.4 | 0.4 | $[r_{\text{bob}}, r_{\text{bob}} + (0.4 * k)]$ |

difficulty is 1

$k$ key space $2^{256}$

$t_{\text{miner}}$ search range for miner

## 难度

每隔 120960 个以太坊区块，或者 2016 个比特坊区块，难度将被重新计算，和比特币保持一致，周期约为两周。难度的调整，将根据被销毁的 ether 数量与这两周内预期估值的比值来计算。同时将根据待发总量，减少或增加挖矿难度。每个调整窗口的上限为 4 个因素，以便挖矿可以随时间可控的加压 / 减压而不至于剧烈波动。

$$C_{\text{diff}} = \begin{cases} C_{\text{diff}} * 0.25 & \text{if } (T_{\text{burned}}/(b * T_{\text{expected}})) \leq 0.25 \\ C_{\text{diff}} & \text{if } 0.25 < (T_{\text{burned}}/(b * T_{\text{expected}})) \leq 4 \\ C_{\text{diff}} * 4 & \text{if } (T_{\text{burned}}/(b * T_{\text{expected}})) > 4 \end{cases} \tag{3}$$

Where:

$$C_{\text{diff}} : \text{current difficulty}$$
$$T_{\text{burned}} : \text{total Ethereum burned in period}$$
$$T_{\text{expected}} : \text{total Ethereum expected in period}$$
$$b : \text{numer of blocks in a retargetting window}$$

$C_{diff}$：当前难度

$T_{burned}$：实际周期内销毁的 ether 数量

$T_{\_\ expected}$：周期内销毁的 ether 预期数量

$b$：从新定义的窗口区块数量

## 挖矿奖励的分配

和比特币类似，比特坊挖矿奖励的数量会递减，每 21 万个比特坊区块减半一次。初始的区块奖励是 100 比特坊，用以抵消比例奖励的效应。每一个区块阶段，只有赢家的销毁的贡献的比例会被放出。例如，假设两个矿工，在区块中的赌注一样，且难度目标被达到或者超过，则挖到矿的矿工只能得到 50% 的区块奖励。这种设计，是专门用来限制一个不友善的矿工可能做一个小押注而对比特坊哈希 grinding 攻击的吸引力。这种攻击，除了极度昂贵外，不会产生不成比例的比特坊消耗。这将减缓初始的货币扩张，这种扩张会使得一个更高的基础区块奖励成为必须，同时也能提高已有比特坊持有者通过挖矿贡献得到的代币的价值，即使从比例上说区块奖励相对较小。

## 矿池

挖矿的发展将会刺激更多的，提供共享挖矿机制的矿池出现。这样不仅提高了获得收益的可能性，也增加了这一回报的比例。然而，由于以太坊网络的性质，这些矿池可以是他们自己的智能合约，也可以是一个具有更高级用户界面和其他优点的中心化服务。比特坊合约若内置矿池，将变得过于复杂，这也将抑制第三方用户界面或智能合约设计的生态。作者希望保持这些激励措施，同时在既定的代码复杂程度条件下，保持比特坊代码尽量小而安全。

## 代币上限

总共 2100 万枚比特坊将以与比特币大致相同的机制被挖出，由于其独有的架构，会有些许差别。

# 收益

## 以太坊持有者

比特坊拥有一个和比特币相似的价值生成和通货紧缩架构，使其可以成为以太坊网络上一个完美的价值存储工具。从本质上说，ether 是通胀性的，它的设计是用于智能合约的，这使其很难成为一种长期的价值存储手段。现在持有以太坊的人，可以无门槛的将以太币转换为比特坊，将后者作为一种具有结构安全性的避险资产，同时还能保留以太坊本身的智能合约和网络性能。这种混合两大品种优点的方案，将能大大增加以太坊网络对长期投资者的实用性。

## 比特币持有者

比特币有内部政治风险，中心化挖矿的风险，以及未来潜在的因为公司利益而出现可以造成经济不稳定的变化的风险。比特坊可以作为一种对冲，以及附加的价值存储手段，同时给比特币持有者一个通往智能合约系统的途径，这将优于比特币现有的功能。作为一种自治应用，它可以永远运行下去，而无需谁的监管，很大程度上也不会受到比特币社区频繁发生的那种政治争吵和幕后交易的影响。更进一步，它可以以无需信任的方式升级，还可以孵化出衍生价值的智能代币，产生类似安全升级那样的附加功能。

## 估值

比特币和比特坊有不同的优点和缺点，但它们的架构是如此相似，比特坊完全可以作为可行的比特币替代品。因为比特坊需要不断增加 ether 的销毁数量来产生新币，所以它比其父币 ether 是更好的价值存储手段。这种机制保证了在以太坊网络上的真正的稀缺性。只要看一看代币发行曲线，就能清楚反映出：相较于长期持有以太币，比特币和比特坊的价值。

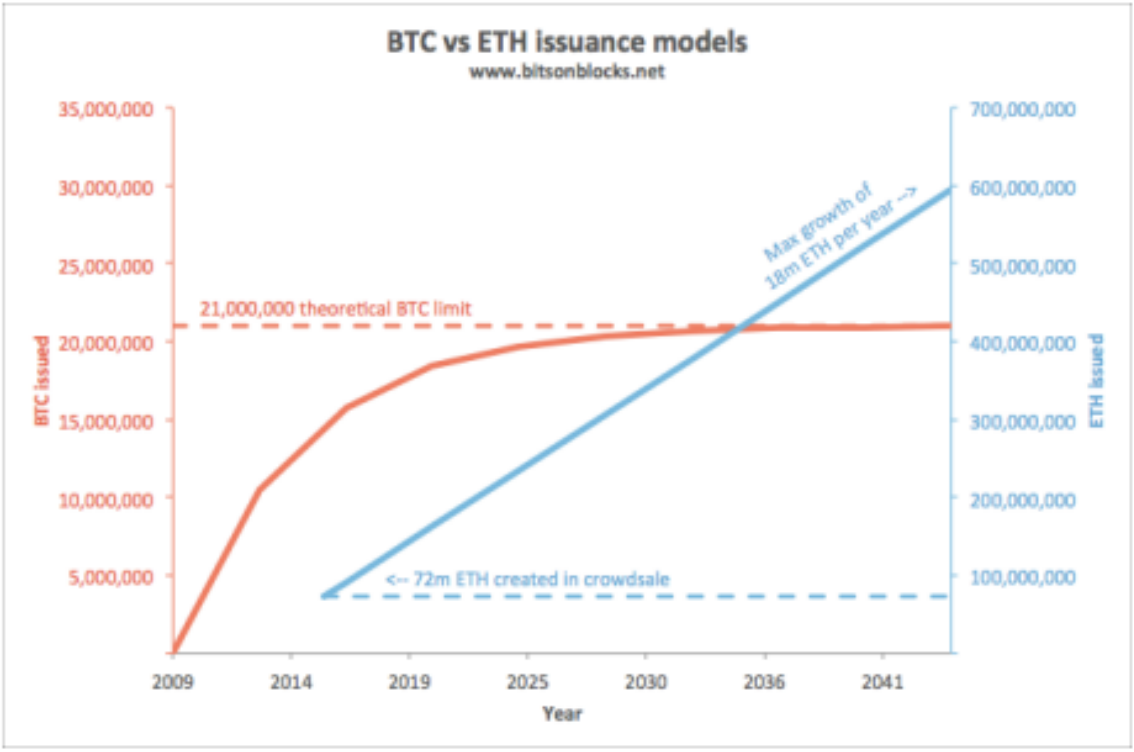


Figure 1: Ethereum vs Bitcoin and Bitcoineum issuance

**图：以太坊发行 VS 比特币和比特坊发行**

## 结论

比特坊的目标是模仿比特币的价值属性，同时提供更好的用户体验，并且提供一种真正公平、均等的网络挖矿体系，同时为错过早期比特币的人提供一个参与机会。它天然是对以太坊现有能力的一个补充，同时还拥有一些独特而有力的特性，是电子黄金（digital gold）信仰者的一个选项。