BHD 比特硬盘

BitcoinHD

01

BitcoinHD(BHD)的愿景是降低挖矿门槛，实现绿色节能的新型矿业体系；但如果从Bitcoin分叉而来，那么剩余的挖矿份额将只有20%，这一点是跟我们愿景相悖的，我们更希望将更多的份额留给辛苦贡献的矿工们。

我们决定启动这个伟大的实验，BitcoinHD（BHD）即将面世，BHD 将改变比特币挖矿目前面临的金字塔现状：矿机被寡头高度垄断随意涨价，矿场越来越趋向中心化导致的大户垄断和国家政策压力，超过159 个国家的巨大电力消耗以及矿机噪音热量的挖矿环境限制，整个挖矿被精英化阶层统治，如此下去，普通用户根本无法参与，BHD 的最终梦想继承比特币的初衷，实现中本聪人人挖矿，一人一票的白皮书构想。

02

BHD的分发以及挖矿机制

供应总量：2100万枚

开发团队：210万枚(10%预挖)

推广团队：105万枚(5%随挖矿产出)

矿工挖矿：1785万枚(85%供矿工)

出块时间：5分钟

初始块大小：25BHD / Block， 8MB区块大小

减半周期：4年，首次减半时间约为420480区块高度

初始TPS：70笔交易/秒

抵　　押：1T硬盘抵押3个BHD

03

BHD算法共识机制：CPoC

BHD的算法共识机制在传统的PoC (Proof of Capacity)基础上进行了改进，我们称之为：CPoC (Considering-Proof of Capacity)，即“条件化容量证明“，意在解决现有情况下的以下尴尬问题：

1.矿工不持币，挖矿所得全部用于砸盘，价格越来越低，利润越来越薄，恶性循环

2.推广团队缺少资金支持，导致推广效率低下，市场信心不足

3.电力占比太高，拿比特币来说，目前电力占比已达65%，矿工不得不砸盘付电费

03

算法共识机制的基础：PoC

BHD 将采用严谨证明的 Consider - Proof of Capacity(CPoC)容量证明共识机制，基于BurstCoin的PoC共识机制改进而来。

简单就是用硬盘的容量存放哈希值，寻找正确的哈希值就是挖矿过程，也许大家觉得用硬盘挖矿是个匪夷所思的思路，其实最初显卡拿来挖矿也是改变了显卡玩游戏的功能，而且显卡工作的热量，巨大的功耗并不适合家庭挖矿，从显卡发展到 FPGA 挖矿，从 FPGA 衍生到ASIC芯片的矿机，最终均无法摆脱热量和功耗的问题，不能想象在家里放几十张显卡，几台矿机的场面。而硬盘天然存在耗电低，无热量，无需散热，低噪音，无法被 ASIC化，购买门槛低的优点，每家部署几十块硬盘角落一丢就行，无需担心巨额的电费支出，未来挖矿收益提高需要升级更大容量的硬盘，旧硬盘可以拿来存放影片，资料，做整列盘等。因此硬盘的残余价值，保值率是非常高的。我们认为硬盘挖矿才能真正的降低挖矿门槛，实现家家户户有矿机，人人都参与挖矿的愿景。

03

算法共识机制：CPoC的实施细节

BHD将于2018年8月3日正式上线，为了鼓励更多矿工参与进来，我们制定了以下上线计划：

1. 上线首月免条件挖矿，矿工持有或不持有BHD，均可以拿到100%收益，即25BHD per Block，收益和你的总Plot数据容量成正比

2. 次月开始实施条件性挖矿，即运行1个1TB节点，需要在节点账户中保留3个BHD，出块的同时全网会验证该节点账户余额，如果不足3个BHD，则只能获得25*30%=7.5个奖励，其余的17.5个直接会被划转到推广团队账户：3F26JRhiGjc8z8pRKJvLXBEkdE6nLDAA3y

3. 运行的节点容量越大，账户中需要保留的BHD越多，由于全网是根据出块比率来逆推你的总容量，会随着你的运气值而上下浮动，所以建议按照1TB=3BHD来部署您的算力以免被误判抵押币不足而影响收益

4. 实际挖矿时，可以直接调用现成的BurstCoin Plot 数据，无需重新Plot硬盘，可以和BurstCoin实现同时挖矿，互不影响

04

官方

1. www.btchd.org
2. 微信：btchd01
3. 邮箱：master@btchd.net
4. BitcoinTalk创始帖：

https://bitcointalk.org/index.php?topic=4750368.0

愿景

容量证明从根本上解决比特币网络巨大的能源浪费，同时永久的杜绝挖矿 ASIC 化。容量证明必将是区块链网络最正确的出路，只有容量证明可以长期保证挖矿环保、公平以及低门槛。

目前行业的怪圈是如果一个算法适合于CPU/GPU，矿工收益以及算法市值达到一定程度，就必定有ASIC厂商生产ASIC矿机夺取本属于CPU/GPU矿工的领地，而CPOC共识天然杜绝ASIC，矿工的领地永远属于自己。

如果说比特币挖矿属于精英、资源占有者，那么 BHD 将把挖矿带进千家万户，BHD 属于人民的挖矿。

05 技术特点

1.BHD 创新的攻克了全球容量证明研究中一直视为技术难点的众多问题.

比如Hellman's time memory trade off、Multiple chain、Block grinding 等。比特币之所以获得今天的地位，在于其技术及网络的严谨和稳定。在今天浮躁的数字货币世界里，BHD 与 ZCASH 一样，开发团队以顶级学术研究标准来进行算法的研究。

2. BHD 从诞生起便将具备 8MB 大区块，5 分钟出块时间的性能，大幅拓展网络效率。

3. BHD 将在 2019年加入零知识证明。

05 硬件特性

A. 用户使用硬盘就能挖矿，无需昂贵的显卡和矿机。

B. 传统的矿机功耗高，噪音大，热量大，专业矿场趋向中心化，普通用户参与门槛高。

C. 目前 POW 挖矿使用的电力已经超过了 159 个国家的电力总和，数字货币的发展不应该以消耗过多能源为代价。

D. CPoC 容量证明数分钟扫描一次硬盘，平时硬盘处于待机状态，功耗极低，矿场收取不到电费，具备能源天然抵抗优势。

E. 相对于基于算力的 POW 挖矿，CPoC 容量证明绿色节能，低功耗，低噪音，无热量，回归中本聪白皮书人人可以挖矿的初衷，是真正的去中心化人人挖矿。

F. 固态硬盘价格昂贵，CPoC 对快速吞吐数据无要求，只需容量，因此 CPoC 天然杜绝ASIC 芯片。

G.用户可以购置硬盘，用开源程序写入数据，硬盘挂载在家用 PC 上挖矿。也可购置已经完成挖矿数据写入的专用多硬盘矿机，同样矿机硬件也开源。

开源的硬盘矿机

05 挖矿电力消耗对比

1. 在 BHD 网络中，使用 5T 硬盘挖矿平均功耗不到 7W。以相同矿机价值计算（1.5 万元）， 比特币 ASIC 矿机耗电约 1350-2000W，而 BHD 所需硬盘矿机仅耗电 70-90W。仅为比特币 ASIC 矿机耗电量的 1/20。一台 ASIC 矿机，每年消耗电力约 17520 度，而硬盘矿机仅耗电约 700 度，硬盘矿机不仅耗电量极小，与比特币 ASIC 矿机相比，噪音极小且几乎没有发热量。
2. 比特币网络年耗电超过 180 亿度，并且仍在以每月 16%以上的速度增长。每笔比特币交易耗电约 175 度， 是 VISA 网络的 8500 倍，而刚果人均全年消耗电量仅为 91 度。如果比特币是一个国家，耗电量超过古巴、冰岛、斯洛文尼亚，位列 71 位。

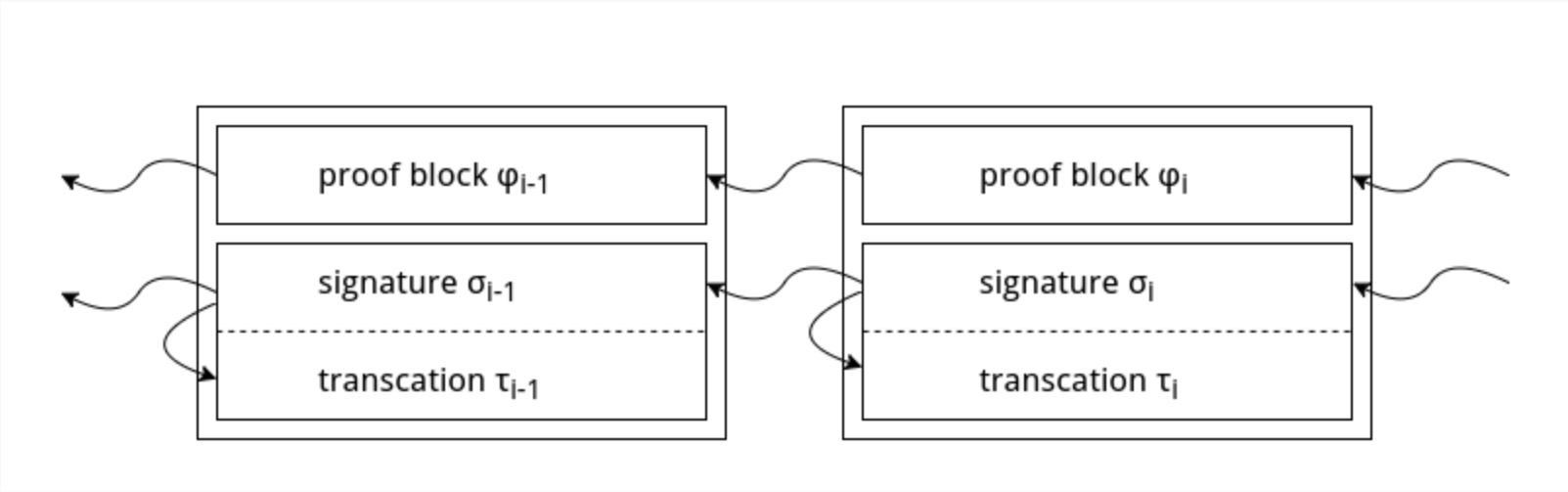
06 开源代码

Proof of Capacity 容量证明

- 提供 $h(x)$ 让证明者存储，询问任意的 $y = h(x_0)$，让证明者通过 y 返回 x。如果证明者存储了所有排序后的 $h(x)$，只需要通过简单的二分查找就可以得到答案。
- Hellman’s time-memory trade-off。攻击者可以将空间和时间进行交换，使得花费一些计算而不存储所有 $h(x)$。
- 但是我们能构造出这样的$h(x)$使得攻击者进行 Hellman’s time-memory trade-off，但是trade-off之后，如果攻击者存有 S bits 额外的信息，且进行 T 次 oracle queries, 那么它们满足关系 $S^2T \in \Omega(N^2)$。
- 这样，即使攻击者进行 trade-off，他每次需要进行计算的时间成本。

Btchd

Blockchain 区块链



- 我们的块包括 proof sub block, signature sub block and transaction sub block。
- 箭头表示该子块包含矿工对箭头指向子块的签名。
- 我们的 challenge 由 Δ 块之前的 proof 子块的 hash 生成。

Btchd

Block grinding

- 矿工可以在创建块的时候, 尝试不同的交易组合, 使得创建的块对自己有一定偏向性。
- 我们的区块结构中 proof 子块的独立性可以防止这个攻击。

Btchd

Challenge grinding

- 矿工在挖矿的过程中, 可以将自自己己的空间分成 m 份, 然后对区块链上的连续 $t = 2\Delta$ 块进行重构，如果区块链的 Quality 定义如下:
- 那么可以通过尝试第 i 块的 proof，使得 i + Δ 的 Quality 最大。在以上基于线性求和的 Quality 下，按照上述的攻击方法，将会导致攻击者可以获得 $\frac{m}{2}$ 倍的机会取得更大 Quality。
- 通过重新定义区块链的 Quality 的，来降低这种攻击的获得收益倍数，将 Quality 的计算由线性叠加改变为乘积的方式，定义如下:
- 在该定义下，攻击者获取的概率提升将会降低为 $\log(m)$。同时，让连续的 Δ 块的 challenge 由同一个块来决定，将会进一步降低该攻击的影响。

Transaction 交易

我们的交易结构同 bitcoin 一样，即一条 UTXO 到 UTXO 的链，与 bitcoin 相比，我们主要有两点变化：

- 新增 punishment 交易，该交易结构为：
  (输入 UTXO, 输出 UTXO, (signature1, signature2))

- 其中输入 UTXO 为矿工 A 挖出高度为 n 的块的收益，
  (signature1, signature2) 为矿工 A 对高度为 n 的两个不同块的签名。

- 当输入 UTXO 是矿工挖矿所得时要额外校验该 UTXO 所在的块与当前块高度相差是否小于 5，如果小于 5 则拒绝交易。

Btchd

07 答疑

Q1:为什么选择与Burst共享数据架构？是抄袭Burst的吗?
A1: 绿色节能环保的矿业结构是BHD团队的基本愿景，依托于Burst的Plot数据可以在不增加任何硬盘/电力资源浪费的情况下实现早期的容量收集工作，并且在确保网络和交易安全的情况下留出足够的时间来开发新的Plot格式以及文件存储方案。我们并不是对Burst的抄袭，开源代码以后一切关于抄袭的猜测将会不攻自破。

Q2:BHD是不是开源项目？会在何时开源?
A2:BHD是一个开源项目，目前我们还在微调CPOC相关代码，会在CPOC上线并稳定运行后完全开放源代码。

Q3:BHD可以和Burst双挖吗?
A3:可以的，Burst的出块时间是4分钟，BHD是5分钟，交错出块时间就是为了让两个币种双挖时互不影响。

Q4:BHD钱包看起来很简陋，像是传统的比特币钱包，后续能添加更复杂的功能吗?
A4:BHD团队目前的主要工作是调试CPOC代码以及底层文件存储代码，在目前容量收集阶段使用成熟的比特币钱包代码可以减少代码维护量，提高系统安全性，我们愿意将更多的时间和精力用在更有意义的代码上面。

Q5:BHD的远景目标和IPFS是否冲突?
A5:IPFS是一个伟大的项目，不过现阶段团队认为并不应该开放文件上传权限给所有人。团队后续主要的应用场景是医疗DNA大数据的存储，院线电影等业内大数据的存储传输，至少在文件存储上线后的短时间内，所有文件上传者都必须要将身份信息上传到BHD区块链，我们认为管控好文件上传这一环节是现有监管政策下的折中选择。BHD团队也会持续关注IPFS完全开放模式带来的优势与风险，必要的时候会对我们的文件存储策略作出调整。做一个简单的比喻，IPFS的模式像eBay，而BHD的目标是做分布式存储产业中的Amazon。

08 长远发展计划

2018年8月3日： BHD的创世区块被挖出，开启一个创新性的挖矿征程。

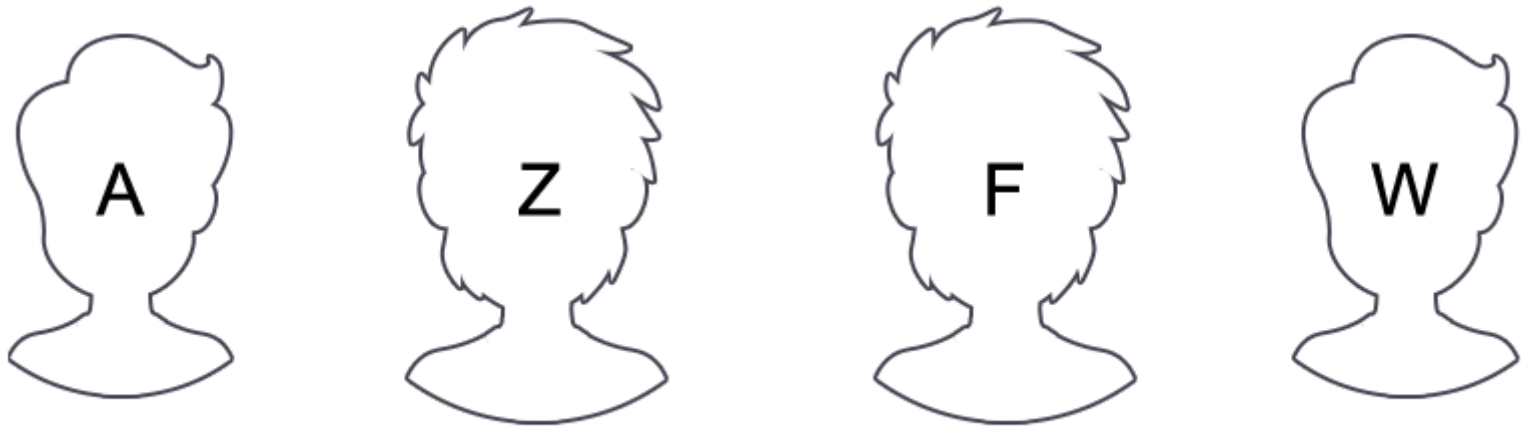
2019年：加入零知识证明，加入弹性区块链大小，并将TPS推高至100+

2019年末或全网算力2000P：放弃与Burst共享数据结构，部署自有BHD Plot数据，实现完善的私密/公开文件存储功能。

2020年：实现基于分布式网络的版权分发系统，目前已与某大型影业公司在合作，后续会有更多的版权类数据加入，如 电影、音乐、视频、游戏 等，充分发挥区块链分布式存储的高速，健壮等特性

更多后续特性持续开发中…

团队



THANK YOU