

# POC CONSENSUS INTRODUCTION

powered by **POC Lab**, @2019

# 内容提要

- 1 问题背景
- 2 解决方案
- 3 项目分析
- 4 参考文献

# 问题背景

- POW 算法
  - 安全性基于算力资源，挖矿速度与求解特定函数的速度相关
  - 不够经济、不够环保、不够去中心化
- POC 算法
  - 安全性基于磁盘资源，挖矿速度与磁盘容量相关
  - 解决 POW 算法的经济、环保和中心化问题

# 解决方案

1 问题背景

- Proof of Retrievability
- Proof of Space
- Proof of Spacetime

2 解决方案

3 项目分析

4 参考文献

# 非前向计算函数映射

- 原理
  - 构造需要更多 Time/space 才可逆转的函数
  - 函数不可前向计算，与 Time/space trade-offs 攻击不冲突
- 示例
  - 随机函数  $g : [N] \times [N] \rightarrow [N]$ , 随机置换函数  $f : [N] \rightarrow [N]$
  - $g_f(x) = g(x, x')$ ,  $f(x) = \pi(f(x'))$
  - 初始化: P 计算  $f$  函数表，并按照函数值排序
  - 验证过程: V 选择随机数  $y \in [N]$ , P 返回  $(x, x')$ , 满足  $f(x) = \pi(f(x'))$  且  $g(x, x') = y$
- 特性
  - 可配置安全级别，安全因子  $k$
  - 准线性， $S^k \cdot T \in \Omega(N^k)$ ,  $S = T \approx N^{k/k+1}$

# GRAPH PEBBLING

- 原理
  - 基于 Hard-to-pebbling Graph
  - 选择  $G = (V, E)$ , 对每个顶点  $i$  计算并存储  $I_i = \text{hash}(\mu, i, I_{p1}, \dots, I_{pt})$
- 特性
  - Time/space 下界跟选择 DAG 类型有关
  - 选择 1: 初始化和执行间或执行期  $\Omega(|V| / \log(|V|))$  空间
  - 选择 2: 初始化和执行间  $\Theta(|V|)$  空间或执行期  $\Theta(|V|)$  时间

# PROOF OF SPACETIME

- PoSpace 问题

- 分期共享同一块存储空间
- 当初始化和运行证明间存储数据的成本高于重新生成数据开销时，理性的证明者会选择重新生成，因而 PoSpace 算法沦落为 PoW
- 即便忽略能量开销，证明者需要生成很多证明数据，但只有小部分会被验证，不诚实的证明者可以不消耗资源用于存储不被验证的证明数据

- PoST 核心思想

- Space × Time：填充一定容量的磁盘空间并持续一段时间
- 时空证明

└ 项目分析

  └ 项目概览

# 项目概览

- ① Burstcoin: 内存复杂函数映射
- ② SpaceMint: Graph Pebbling
- ③ ChiaNet: 不可前向计算的函数映射 + PoW
- ④ BitcoinOre: 不可前向计算的函数映射
- ⑤ SpaceMesh: Proof of Spacetime
- ⑥ Filecoin: Proof of Replication + Proof of Spacetime

# 算法术语

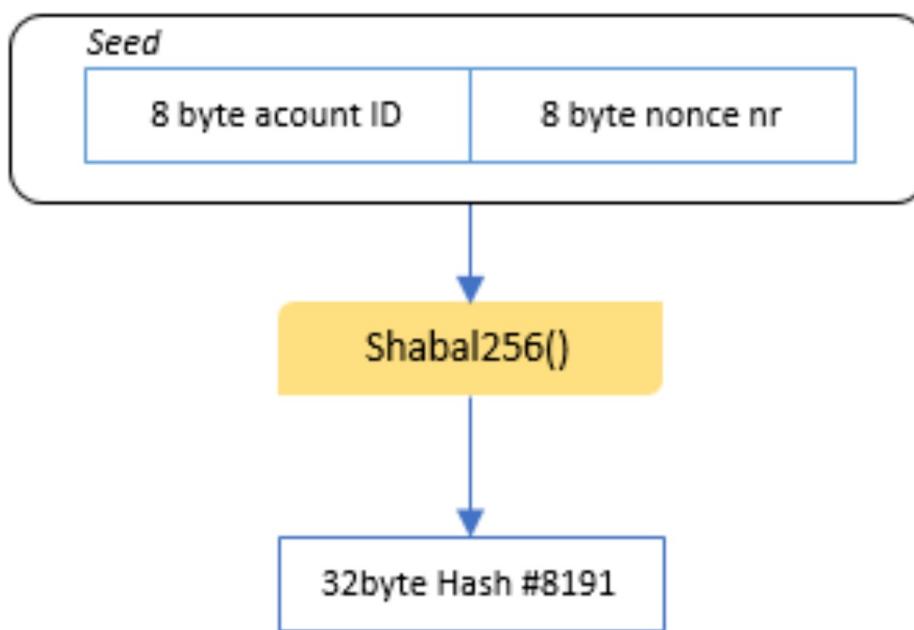
- Shabal/Sha256/Curve5519: 哈希算法
- Plot 文件: 挖矿需要读取 Plot 文件中存储的预计算哈希值
- Nonce: 一个 plot 文件包括一组或多组 nonce, 每个 nonce 包括 8192 个哈希, 总共 256KB, nonce 编号范围  $[0, 2^{64}]$
- Scoop: nonce 包含的 4096 个有序数据分片 (两个哈希值)
- Account ID: 每个 plot 文件都绑定特定 Burstcoin 账号
- Deadline: 这个时间范围内不允许出块
- Block reward: 区块奖励
- Base target: 由前 24 个区块计算而得, 难度自动调整, 平均每 4 分钟出一个块

# 算法术语

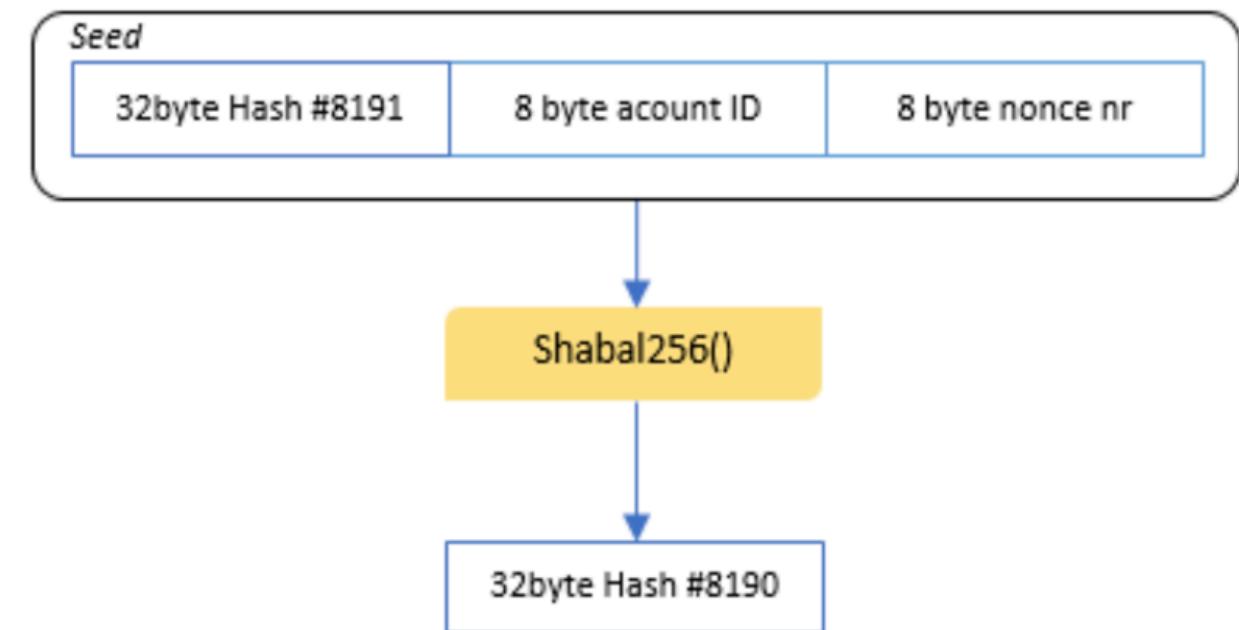
- Network Difficulty: 贡献用于挖矿的总磁盘空间评估值
- Block Height: 区块高度
- Block Generator: 区块构建者
- Generation Signature: 由前一个 Generation Signature 和 Block Generator 计算而得
- Block Signature: 区块签名
- Reward Assignment: 奖励分配

# NONCE 生成

① 由账号 ID 和 nonce 编号生成哈希 #8191



② 由账号 ID、nonce 编号和哈希 #8191 生成哈希 #8190

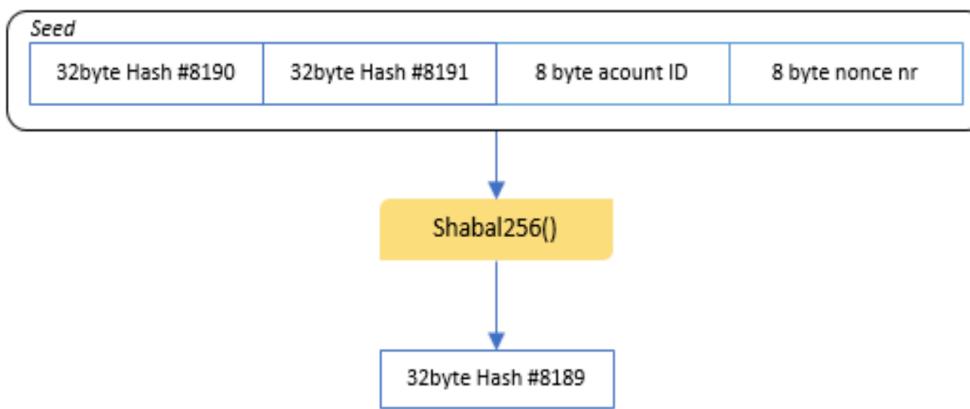


└ 项目分析

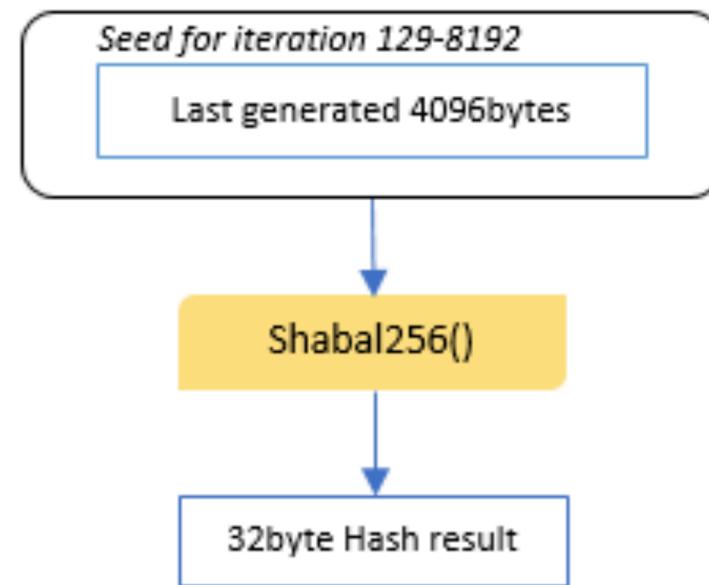
└ Burstcoin

# NONCE 生成

③ 由账号 ID、nonce 编号、哈希 #8191 & 8190 生成哈希 #8189



④ 生成其他哈希值，总共 8192 个

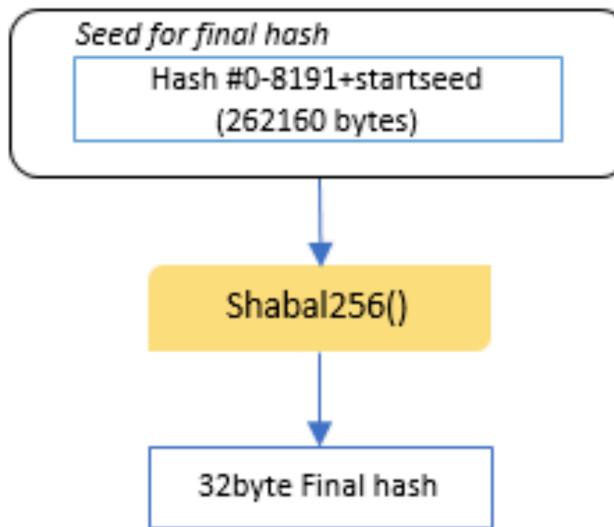


└ 项目分析

└ Burstcoin

# NONCE 生成

⑤ 计算最终 Hash 值



⑥ 初始 Hash 值与最终哈希值异或



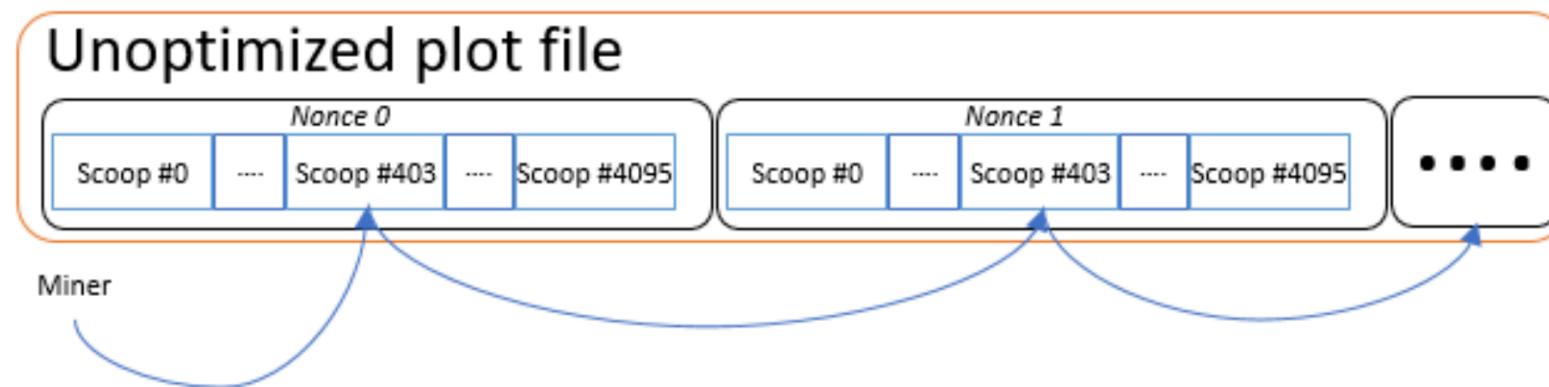
⑦ Nonce 结构

## Nonce



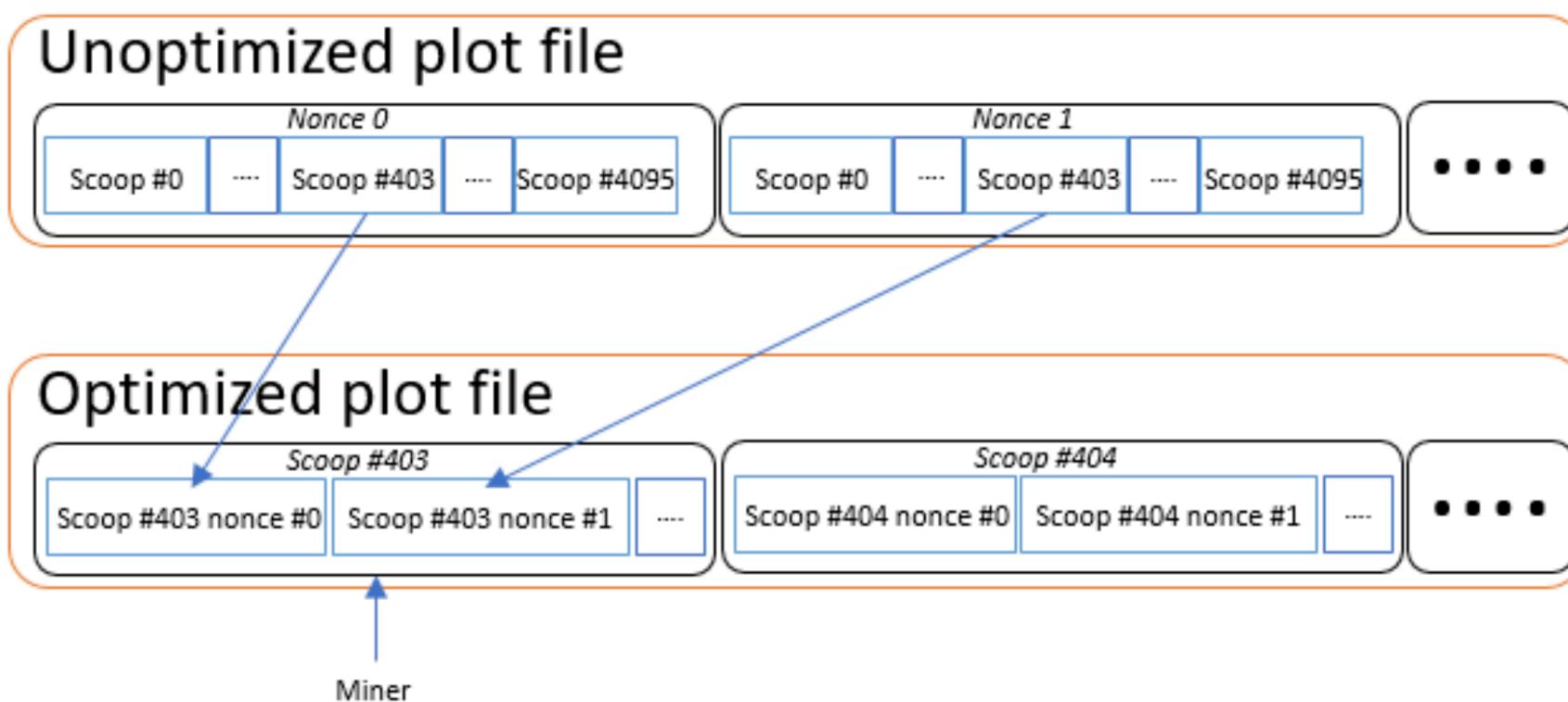
# PLOT 结构

- 优化前存储结构



# PLOT 结构

- 优化后存储结构：按照 Scoop 编号对数据分片进行分组，以便一次性读出所需的 Scoops，提高效率

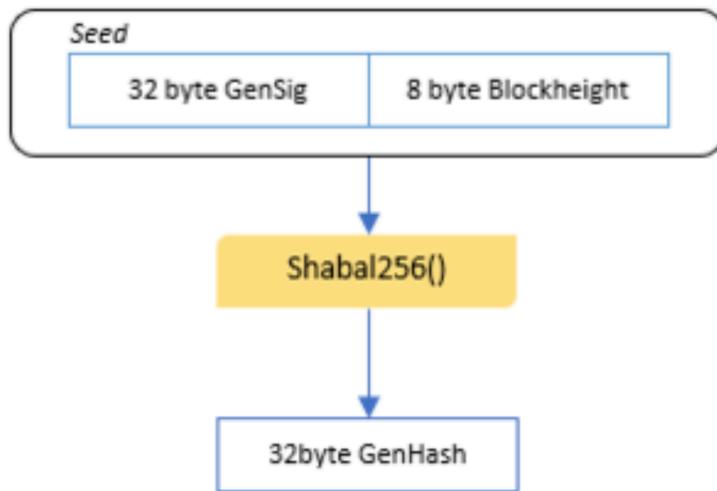


└ 项目分析

└ Burstcoin

# 挖矿过程

- ① 根据 Generation signature 和区块高度生成 Generation hash



- ② 对 Generation hash 求模获得 Scoop 编号

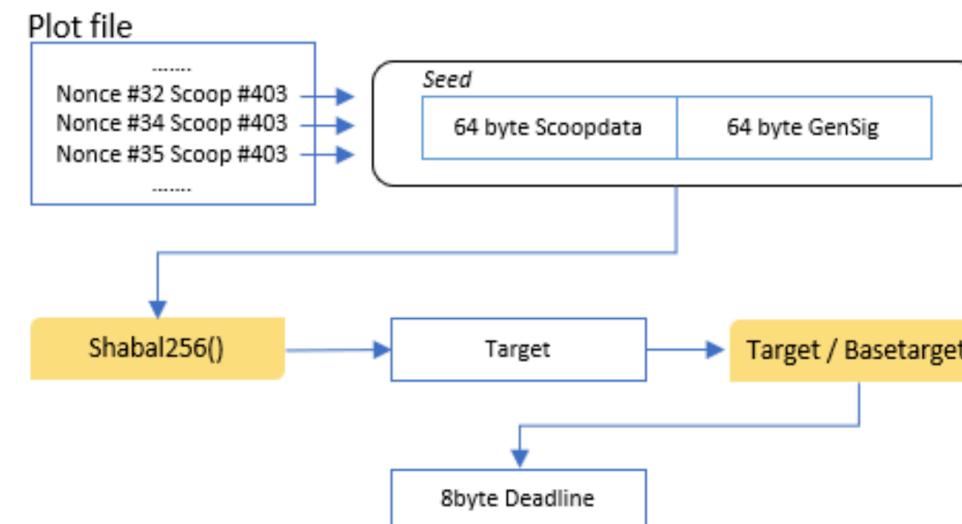


└ 项目分析

└ Burstcoin

# 挖矿过程

## ③ 计算 Deadline



# 构造区块

- 选择目前为止使得 Deadline 最小的 nonce
- 没有接受到区块并且 Deadtime 有效，则开始构建新区快
- 区块内容：Block version number、List of Transaction ID、Payload Hash、Timestamp、Total amount of coins、Total amount of fees、The length of the payload、Public Key、Generation Signature、Previous block hash、Previous block ID、Cumulative Difficulty、Base Target、Height、Block ID、Nonce、AT、Block Signature

# 问题汇总

- 验证者需要计算哈希次数  $4096 \cdot \frac{4096+1}{2}$ ，约等于 800 万，计算复杂度偏高
- 证明者需要访问  $\frac{1}{4096}$  比例的存储空间，效率低下
- Time/space tradeoffs 攻击

# 参考文献

- █ Ateniese G., Bonacina I., Faonio A., Galesi N. (2014) Proofs of Space: When Space Is of the Essence. In: Abdalla M., De Prisco R. (eds) Security and Cryptography for Networks. SCN 2014. Lecture Notes in Computer Science, vol 8642. (ePrint 2013/805)
- █ Stefan Dziembowski, Sebastian Faust, Vladimir Kolmogorov, and Krzysztof Pietrzak. Proofs of space. In CRYPTO 2015, 2015. (ePrint 2013/795)
- █ Abusalah, Hamza et al. “Beyond Hellman’s Time-Memory Trade-Offs with Applications to Proofs of Space.” ASIACRYPT (2017)
- █ Sunoo Park and Albert Kwon and Georg Fuchsbauer and Peter Gai and Joël Alwen and Krzysztof Pietrzak, SpaceMint: A Cryptocurrency Based on Proofs of Space (ePrint 2015/528) Original Publication: Financial Crypto 2018
- █ Martin E. Hellman. A cryptanalytic time-memory trade-off. IEEE Transactions on Information Theory, 26(4):401–406, 1980.
- █ Amos Fiat and Moni Naor. Rigorous time/space tradeoffs for inverting functions. pages 534–541, 1991.

# 参考文献

- █ <http://www.burst-coin.org/>
- █ <https://filecoin.io/>
- █ <https://spacemesh.io/>