HiZoco 区块链技术白皮书

1. 前言：

由于 HiZoco 区块链参考应用了大量应熟的区块链技术进行组合创新，本白皮书基于阅读者已经对主流区块链技术知识有一定理解的基础表述，不作针对区块链、以太坊区块链（ETH），以太坊虚拟机（后称 EVM）、各种哈希算法作普及性表述。

本白皮书将就 HiZoco 链的技术细节作表述。

2. 基本表述：

HiZoco 链是一条以太坊虚拟机（EVM）兼容链，目前兼容至以太坊上海升级，基本计量符号为 HZC，由共识证明者在每个区块上挖矿取得。

3. HiZoco 区块链的共识技术细节概述：

(1) HiZoco 区块链的共识方式称为 PoCT(Proof of Capacity Time)，和一般提法的 PoST（Proof of Space Time）有一点点表述上的差异，HiZoco 链中使用的 PoC（Proof of Capacity）表示证明了算力提供者有一定的容量，并不代表这些容量可用，而且，S 缩写易于与存储（Storage）、股权（Stock）等单词混淆，因此不使用空间这一词来表示算力。

(2) HiZoco 链设计为在一条密码学上兼容 CHIA 链的 PoST 算力的共识算法的双挖链（Dual Mining），旨为现有 CHIA 链的矿工即可同时提供

HiZoco 链共识所需的 PoC 算力，因此当 CHIA 链现有的矿工以极小代价即可同时也作为 HiZoco 链的矿工获得 HZC。

(3) VDF（可验证延迟函数）在 PoCT 共识中，通过迭代计数用于生成 PoT（时间证明），基于同样的挑战哈希和同样的迭代次数所生成的 PoT 是一致的，并可快速验证。HiZoco 链和 CHIA 链一样使用了 Wesolowski 算法，一种基于在未知顺序的类群中重复平方的迭代算法。

(4) HiZoco 链重新定义了矿工在区块链运转中的作用。 支持以太坊虚拟机的区块链作为一个分布式的 IT 体系，矿工的主要作用是驱动区块链前进，因此弱化了交易过程中对矿工的交易封装奖励（手续费），其中 45% 的手续费直接留存在锁定的托管账户中，目前，托管账户由项目方先代为管理，预期将来将使用去中心化组织（DAO）进行公平管理，留存的 HZC 将会有以下可能：根据地方权力机构的法律文书移交给权力机构作为税收上缴到指定账户或是在一定期限后由 DAO 作处置决定，比如用于举开发者办竞赛、安全审计等。

4. PoCT 共识流程及原理说明：

(1) 依据当前链顶最高块，PoT 生成器在完成指定迭代量（目前为 1M 次）计算完成延时后，生成当前高度的 PoC 收集任务的 PoT，称为 SP，按 2-3 所指，同样的块高度之下，只要得到验证正确的 SP PoT，即证明可依据它进行容器证明的查找，这个过程会持续以大约每 15 秒一次的速度推进。

(2) 依据完成延时的 SP　PoT，矿工在预先完成 P 图的已索引证据中，

查找符合当前难度要求的 PoC，同一个 SP PoT，有可能同时得到多个 PoC，矿工持 SP PoT、PoC 按当前区块高度，进行封装签名，该查找过程和 CHIA PoST 共识一致，因此 HiZoco 链可以直接使用 CHIA 链的 Harvester 进程来进行该过程。而依据 CHIA PoST 的技术白皮书可有参考推论：PoC 的查找过程有能效抵挡彩虹攻击（试图使用强大的计算能力实时地按 SP PoT 生成符合条件的 PoC）。因此该查找过程不会消耗大量的计算机算力资源。按共识要求，按照难度要求，该 PoC 可计算出需求的迭代量，为防止过多浪费的注入，该迭代量将会在两个 SP 后才生效，也就是需要的迭代量 = SP 迭代量 + PoC 迭代量。

(3) 针对收集到的 PoC 与当前的块高度、父块哈希、当前的 SP_PoT 等关键因素产生的未完成新块，首先会进行封装与哈希，矿工会使用对应生成该 PoC 的私钥作两次签名计算，一次使用 BLS 算法、一次使用 Secp256K1 算法，并将签名过的未完成块分别送给本地的验证器和广播给其它节点的验证器。

(4) 验证器类同于 CHIA 链的 Timelord（时间领主），但实际上它另一方面也用于验证未完成块是否签名有效，而且是本地调用 VDF 生成 PoT 的调度器，验证器验证了未完成块的有效性后，则会把未完成块的注入迭代任务加排入注入迭代器流程，在注入迭代器达到该块的 PoC 所要求的迭代次数时，则会生成注入的 PoT (IP PoT)并广播。基于此机制，解除了 SP PoT 的生成、PoC 的查找、IP PoT 生成的节点粘性，以上三步完全有可能在不同的节点上进行，而且由于 PoT 的一致性（同一个块高度上，所有 VDF 生成的 PoT 一样），节点之间并不会反复传播同一个 PoT 和 PoC，因此不会大

量产生节点间的传播通讯。

(5) 当持有最佳 PoC 的节点从 VDF 收到 IP VDF 时，首先该 IP VDF 是最先生成的（需要的迭代量最少），其次对同一 SP 在当前节点查找到的其它 PoC，它也是迭代量最少的，在下一个 SP PoT 出现之前，矿工节点会选择出自己持有的最优 PoC。

(6) 当 VDF 生成了最新的一个 SP PoT 时，矿工节点依据自己持有的最优 PoC 及其它所有关键因素（SP PoT、PoC、IP PoT）依据当前最新的链高度，从交易池中优选手续费最佳交易封装出最新块来，这一步与以太坊一致，都是完成交易封装，智能合约的执行等进行记账封装，并计算出封装的新块并重新使用生成 PoC 时的私钥重新签名完成新块并广播。

(7) 最新的块在块头识记了链的总迭代量与预期的每块迭代量（2M 次）增长的误差积分与计算的微分，当误差积分达到算法要求的阈值时，则会计算出难度调整值来并记录下一个块必须要难度。

(8) 新块明显依据共识约定及当前链高度可被验证，按 4-2 节所述，同一矿工节点在同一 SP 内，已经进行了 PoC 优选并只会为最优证据宣称出块，由于网络迟时等原因，不排除短时间内其它节点也依据它们的优选 PoC 宣称出块，这种情况即为短时间内的分叉，应对分叉的情况，共识算法首先依据以太坊的分叉选择方式：同一块高度下，只选择总难度最高的链，同一总难度下，只选择分叉块难度最高的链，由于 PoCT 共识不同于以太坊的 EthHash 共识算法，在总难度、分叉块都一致的时候，只选择分叉块的 PoC 需求迭代量最小链。被放弃的无效块则为孤块，不作挖矿奖励，节点会依据最新的块高度，循环 4-1 步骤，放弃旧块进行中的迭代重新开始一轮迭代。

(9) 和 CHIA 一样，为防止被预测生成 SP 挑战的可能，会每 64 个 SP 就作为一个小阶段总结（称为子槽），会依据前一个子槽的总结更新 SP 的挑战。

5. 矿工奖励：

(1) 前 11,212,800 个块，每块矿工挖矿基础奖励为 5 个 HZC

(2) 11,212,801 高度至 22,425,600，每块矿工挖矿基础奖励为 2.5 个 HZC

(3) 之后每个块的矿工挖矿基础奖励为 1.25 个 HZC

性能：

由共识算法的流程可得知，VDF 函数计算生成 SP 的速度是整条链的驱动时钟，依据算法的常数值可算出平均每 2.5M 次迭代会生成一个块，目前平均大约是 35~40 秒一个块，每个块的交易 Gas 上限为 3M，与以太坊的每块交易容量一致。

考虑到初期创世的原因和有可能出现大量的算力动荡，目前选择 1M 一次的固定迭代量，按照计划，将会在随后提出升级以实现预期每 11.25 秒每个块的出块频率。

6. 推进线路：

(1) 当前阶段，代号为夏，技术白皮书公开，算法依据及参数常量公开，

完成代码开源和审计，当前阶段仍在持续进行，依照白皮书，会有快速的调整升级分叉以调整修正。

(2) 代号湘江，完成内部世纪更迭，实现针对现实时间的基本校正，将目标出块间隔提升至11.25秒,实现多共识跨链预言机,在L1层实现跨CHIA、ETH 链的预言机。

(3) 代号乌江，克服零知识证明 = 零服务证明的难点，保留 VDF 带来的节能优势，实现内容流量服务的证明，以证明存储并交换了有效的内容数据作为记账依据，并与 PoCT 共识并行。

(4) 构建并行链生态，提供更节能，容量更丰富的实时区块链网络。

7. HiZoco 链、CHIA 链横向参考：

组件用途	HiZoco 链	CHIA 链	差异
密码学验证与 VDF 调度	Verifier	Timelord	扩展了 RPC API
POC 筛选	POC_Filter	Farmer	增加了使用的签名算法
POC 收集	POC_Collector	Harvester	一致
区块链主节点	Node	Full_node	Hizoco 的主节点基于以太坊主节点扩展
密钥管理器	Daemon	Daemon	一致

VDF 迭代器	VDF	VDF	一致

引用参考：

《Efficient verifiable delay functions》，由 Benjamin Wesolowski 发表，基于在在未知顺序的类群中重复平方而实现的可延证延时函数算法。

《Beyond Hellman’ s Time-Memory Trade-Offs with Applications to Proofs of Space》，由 Hamza Abusalah

Jo¨el Alwen

Bram Cohen

Danylo Khilko

Krzysztof

Pietrzak

Leonid Reyzin 联发发表，提供一种基于 BLS 聚合签名算法构建空间证明的应用方法。