云矿

CPT
云矿币
白皮书

WHITE PAPER ON CPT
CLOUD MINING CURRENCY

摘要 ABSTRACT

几乎全部加密货币均需要基于各类共识机制产生，挖矿业务成为整个加密货币行业的基石。矿池业务也伴随整个行业的发展快速成长，截止2020年一季度整个挖矿服务的市场规模超过 20亿美元。随着业务的增长竞争随之而来。加密货币市场的蓬勃发展，使 得挖矿模式模式日新月异，为矿池业务带来机遇的同时也为行业带来众多挑战。如何为各类矿工带来更加全面的业务、更加稳定的收益、 更加贴心的服务，更加安全的保障成为每个矿池应该思考的问题。我们的使命我们认为可以为矿工提供全方位服务的矿池，是传统矿池业务的 转型方向。我们将矿池业务重新定义为“数字资产生产平台”，向包括以POS、POW、DPOS/POC等为诸多生产机制的代币生产者提供从生产到销售的一站式服务。

CPT云矿币是基于Cloud Proof Of Capacity (以下简称：CPOC)的新型加密货币。其主要的特点是使用硬盘作为共识的参与者，降低加密货币对电力资源的消耗，降低参与门槛，让其生产方式更趋向去中心化方式，并更加安全可信，让人人都能参与到加密货币的开采，通过数学算法以及分布式开采产生信用和价值。本文将从本加密货币系统塑造出的信用体系和技术特征分别对其进行阐述。

CONRENTS

目录

背景

BACKGROUND

A

A-1 CPT为何现在出现？

云矿

随着加密货币爱好者愈发增多，其去中心化的目标离我们更进了一步。每一个参与者都希望自己能够参与并且从中收益，这一合情合理的需求在POW领域愈发变得艰难。随着BTC的能源消耗越来越大，矿机厂商越来越中心化，甚至产生了戏剧化的分叉，而基于POC的加密货币比在2019年变得更为加密货币爱好者需要。再加上其特殊的共识算法保证了在上线可以迅速完成对算力的积累及难度的控制，在保证系统安全性、健全性的同时，对交易者及共识支持者进行奖励。

在这几个方向上CPT都是优于现有的加密货币的，共识的迭代也提供了高于Burst所提供的安全性，技术维度和信用维度完全超越其他加密货币。相较于高能源开销的POW算法，我们更相信低功耗也能赋予算法以足够的信用来保证未来每一个人都可以使用上加密货币。

POC+POW
设计机制

B B-1 CPOC权益证明

在资源被大量用来出块，成本逐渐提高的时候，加密货币爱好者开始致力于寻找更低功耗的替代者，主要分为两类：更低成本获得收益的替代者和更通用可堆叠组件的替代者，这就是ASIC挖矿以及抗ASIC算法开发的大航海时代。

其中ETH，Monero的初衷都是以抗ASIC为目的，他们希望出块的计算方式能够抵抗ASIC芯片，并且维持比较低的出块成本，让它变成一个不受控于ASIC芯片进行挖矿的加密货币，不过在加密货币发行之后，市值一旦达到ASIC芯片投入的范畴，ASIC的开发商依然会想办法将这些通过计算方式去挖矿的加密算法设计成为矿机。另外一个著名的加密货币LTC也是其中的代表，使用Scrypt算法的LTC，以对抗ASIC为技术亮点，不过很快ASIC设备生产商就优化了他的算法，将其做成了矿机，形成了设备以及算力的垄断，带来了巨大的能源消耗。电力的依赖和矿场的门槛让挖矿成为少数人的游戏。

而CPT则是一个集大成者，其即能达到更低的能源消耗，又能方便矿工自制通用组件参与其中，同时维持相对高的难度来保证系统的稳定性。CPT使用的CPOC共识，是非常去中心化的一个共识算法，相对于POW引起的算力证明大航海时代，CPOC将会开拓一个基于硬盘容量证明的新大航海时代。CPOC使用硬盘来作为共识的主要载体，让更多的普通人可以通过自己的电脑参与到算力的组建中，能够回归到中本聪设计POW的部分初衷，让每个人都能参与到去中心化的革新之路。

CPT与此同时继承了BTC的传统，因为BTC在设计之初便是一个服务于多数参与者的系统，即每一个参与的者都可以是一个思考、支持、甚至是颠覆系统的角色。CPOC继承了这种开放性、包容性，伴随着更加亲民的硬盘容量共识，可进一步将加密货币推向向大众视野，让更多的人参与到CPT 经济系统的建设。

处理Deadline

钱包收到矿工提交的信息，创建对应的nonce，以便找到并验证的dead-line。然后钱包现在将检查deadline对应时间的流逝，直到deadline对应的时间（秒）用光。如果在deadline之前在网络上收到其他钱包的有效区块，则钱包将丢弃提交的Mining信息。如果矿工提交新信息，钱包将创建nonce，并检查deadline值是否低于之前的deadline。如果新deadline较小，钱包将使用该deadline。Deadline有效时，钱包现在开始锻造一个新的区块。

锻造

首先，钱包获取从用户或网络收到的所有未经确认的交易。钱包将尝试包含尽可能多的交易，直到达到8M的上限，或者直到处理完所有交易。钱包对交易进行合法性检查。例如如果交易具有有效签名，如果它具有正确的时间戳等。钱包还将总结所有添加的交易金额和费用。

CPT VS BTC

参数	BTC	CPT
供应总量	2100万	2100万
出块时间	10分钟	1分钟
区块大小	1M	8M
减半周期	4年减半	4年减半
初始出块奖励	50	5

CPT继承自BTC，相对BTC：CPT增加区块到8M/Block，区块变大，单个区块可以包含更多交易，提升转账速度；出块时间调整为1分钟，提升转账速度；初始出块奖励调整为5CPT/block，4年减半；
初始出块奖励减半，可以让社区有更多得时间，聚集社区资源，矿工群体可以分享更多收益，同时维持2100万货币供应总量。

B-3 矿工挖矿流程

P盘(Plot)

Miner（矿工）在本地硬盘Plot文件，用含有自己公钥的哈希值，综合Shabal算法填充硬盘。我们将plot文件（p盘）认为是软件制造“poc矿机”的过程，将垄断矿机厂商的权力释放给每个普通的人。硬盘容量越大，填充的Hash值越多，爆块的概率越高。Hash算法采用Shabal256，具有抗ASIC特性。

转账(Transaction)

钱包组成的P2P网络（基于BTC）；钱包之间进行转账操作。

打包 (Forging)

Miner通过钱包，侦听P2P网络，每当收到一个块，就开始下一块的打包过程。钱包组织一个Block,把block的哈希值发给Miner，Miner寻找最匹配的Nonce。钱包收到Nonce后，把Nonce转成Deadline（时间），然后等待这个时间结束后，把块广播出去。

验证(Verify)

收到Block之后，进行验证。

CPT技术特性

1. POC2共识算法；
2. 出块时间1分钟，交易速度更快；
3. 8M区块大小，提升网络效率；
4. 全网容量达到3000P计划加入零知识证明；
5. 使用硬盘挖矿，抗ASIC，无需专业设备即可挖矿；
6. 绿色环保，低能耗，低噪音；

CPT分发及挖矿共识算法

供应总量	2100万枚
推广团队	5%：105万枚。方式：随挖矿的每个块产出
矿工	95%：1995万枚。方式：挖矿
出块时间	1分钟
初始块大小	5CPT / Block， 8MB区块大小
减半周期	4年，首次减半时间约为420000区块高度
初始TPS	70笔交易/秒
条件化容量证明	每T持有3个CPT作为条件。 说明：1T硬盘是根据爆块率对全网占比进行评估，不是绝对值。

在挖矿初期的前十五天，矿工挖矿完全免条件；从第十六天开始，矿工实行条件挖矿，如果矿工不满足条件挖矿，只能获得50%的收益，50%的币将会纳入基金会用于系统开发、市场推广和运营；如果矿工满足条件挖矿，将会获得95%收益，5%纳入基金会用于市场推广。

CPOC条件挖矿的发行方式会让矿工、矿池和基金会等参与方的产生正向商业博弈，使整个系统始终会有一个较为主力的临时商业既得利者（这个既得利益者会随着时间和价格挖矿难度等变量条件而变化）去无形推动整个生态。

CPT技术特性

项目将把所获得管理费投入到其他币种的算力上，比如BTC/BCH/BSV/ETH同时也将纳入更多小众矿币；投入CPT云矿币，真正实现一台矿机多种币收益。

CPT架构及共识算法

CPT钱包源自BTC，共识源自BurstCoin。BTC(Bitcoin)始于2009年1月，经过10年的迭代，其钱包稳定性及交易链稳定性已得到广泛的认可， 在其QT钱包基础上进行POC共识的部署将会非常安全可信。
BurstCoin始于2014年8月，经过4年的迭代，于2018年升级到POC2，技术相对成熟、完善。把这两者结合，取长补短，CPT钱成为目前POC共识算法下最可信赖的公链。CPT自2020年6月上线以来，算力稳步增长，经受了无数的测试、攻击和破解，至今无大的漏洞出现。
通过采用成熟的POC2共识算法，CPT 瞬间获得一个稳定，可信赖的共识算法，社群具备对CPT钱公链的信心。通过兼容BurstCoin Plot文件，矿工仅仅需要增加微小的投入，便可以获得CPT钱和BurstCoin两份收益。

CPT钱钱包继承了BTC优良的P2P网络架构，及UTXO体系，成熟、稳定。继承自BTC钱包，可以保持对BTC社区最新进展的跟踪：如闪电网络，脚本升级等。 保持跟BTC的相同的接口规范，钱包，交易所对接获得了极大便利。

CPOC：Cloud Proof Of Capacity，即有条件的容量证明。
参与挖矿有条件，需要条件3CPT钱/T。通过条件属性，有助于整个社群的稳定，可持续发展。POC：Proof Of Capacity，即容量证明。

CPOC经济模型博弈
角色：矿池、矿工、持币者、钱包、交易所、硬件服务商。

CPT
综合介绍

C-1 CPT介绍

CPT发行总量为2100万枚。CPT在2020年6月22日零时诞生的时候，区块奖励是5个CPT。诞生10分钟后，第一批5个CPT生成了，而此时的货币总量就是5。随后CPT就以约每10分钟50个的速度增长。当总量达到1050万时（2100万的50%）,区块奖面咸半为2.5个。当总量达到1575万（新产出525万，即1050的50%）时，区块奖励再减半为1.25个。在4年内不超过1050万个，之后的总数量将被永久限制在约2100万个。

CPT伴随看每个新区块的生成而产生。其中在上线前根据联盟创始30个创世矿机超级节点的算力数量，上线后在创世区块中直接生成，映射给初期的这部分算力贡献者。不同于传统哈希值计算，云矿币的矿机采用POC+POW相结合的机制：每台矿机等同于一个算力，CPT的分发是基于节点算力在全网总算力中的权重比例来进行配比分发。根据智能合约，CPT上线后每1分钟产生5个CPT，每天7200个。随看全网总算力的提高，单独算力的权重比例越低，每个算力所配比分发的CPT越少。

C-2 权益

算力币（简称CPT ）是原生代币，也就是权益代币。

算力产出分成权益：

CPT为算力生态提供基础服务的同时，会分享一定比例算力产出做为收益费用。

云算力收益权：

项目所有节点将享受POC+POW的收益权，也支持平台内通过CPT购买云算力。

有收益的 POC钱包 ：

为矿工提供内置挖矿服务的钱包，通过钱包内置的挖矿业务，使得矿工在储存代币的同时取得稳定的挖矿收益。矿池的钱包立足于客户的隐私安全，通过交易所级别的安全风控措施，在保证客户财产安全的同时为客户带来稳定收益。

FPPS 收益模式 ：

采用FPPS结算模式，在区块拥堵时可以大幅度提高矿工收益。相比传统的PPS模式及矿池按全网难度、默认块收益，FPPS将块手续费也加入块收益中，以FPPS计算的挖矿收益将大幅提高矿工收益，将原有收益提升5%–8%。

多币种支持：

目前支持的 BTC、BCH、BSV等币种。我们将上线更多币种，甚至更多小众矿币。

C-2 权益

多语言支持：

目前已经上线中英语双语，后期会逐步支持其他语言，为打造世界级区块链资产生产平台扫清语言障碍。全平台客户端支持火币提供全平台客户端的支持，赚钱从未如此简单。

高性能支持：

系统内采用领先架构，通过多层，多集群的系统架构，大幅度提高了性能、安全、稳定性。解决了传统矿池算力数据掉线、算力乱切换、数据不稳定等问题。

盈利模式：

作为区块链数字资产生产平台，主要收入和利润主要来自于为平台用户提供服务以及对外提供服务所获得的报酬盈利方式说明手续费客户在平台进行挖矿时，需要向平台支付一定的手续费技术服务费平台为各类区块链提供技术服务时需要收取一定的费用包括项目方提供的技术报酬，社区支付的节点奖励等。

金融产品：

手续费后期平台会上线包括算力套保，云算力等业务并向客户收取一定的手续费DApps投资平台通过深度参与各类主链生态建设，发掘和培养有潜力的项目，获得投资收益其他收入其他通过各类自身资源输出所获得的收入。

风险提示及免责说明

D D-1 风险提示及免责说明

1、数字资产投资作为一种新的投资模式，存在各种不同的风险，潜在投资者需谨慎评估投资风险及自身风险的承受能力。

2、本文档用于指导CPT项目的进展，只用于传达信息之途，并不构成买卖CPT的相关意见，以上信息或分析不构成投资决策。

3、本文档不构成任何投资建议，投资意向或教唆投资。

4、本文档不组成也不理解为提供任何买卖行为或任何邀请买卖任何形式证券的行为，也不是任何形式上的合约或者承诺。

5、相关意向用户明确了解CPT项目的风险，投资者一旦参与投资即表示了解并接受该项目风险，并愿意个人为此承担一切相应结果或后果。

云矿