The Dagger 加密货币：白皮书 v0.3

April 4, 2018。翻译：Nikoni

摘要: Dagger 社区引进了一种新的的加密货币。它基于有向无环图（DAG），而不是区块链（Block Chain）,并且不像其它以 DAG 为导向的加密货币，XDAG 可以挖矿。这个项目的目标是创造一个可以每秒处理上千笔交易的去中心化的支付系统。

请注意：在本白皮书中，加密令牌（CryptoGraphic tokens）指的是在有向无环图上运行的加密令牌。它指的不是在以太坊区块链上分配的的 ERC-20 标准代币与 XDAG 令牌分配有关

介绍

Dagger (XDAG 币) 是一种新的的加密货币。它基于有向无环图（DAG），而不是区块链（Block Chain）,并且不像其它以 DAG 为导向的加密货币，XDAG 可以挖矿。

概念

每个区块恰好包含一笔交易。同时，该区块也是一个地址。在所有交易中，主链是被指定的-它是难度最高的链。在主链中，新的代币大约每隔 1 分钟生成一次。

DAG 中的每个区块（Block，简称块）有着最多 15 个通往其它区块的链接（输入和输出）。如果我们能从区块 A 的链接到达区块 B，那么我们称块 B 是被块 A 引用的。一系列被前一个块引用的块成为链（Chain）。如果一个链的每一个区块属于单独的 64 秒间隔，那么这个链被称为不同的（distinct）。块的难度（Difficulty_of_block）是 1/hash。hash=sha256(sha256(block))，用小尾数（little-endian number，一种数字存储格式）表示。主链中的区块被称作主块（main_blocks）。

Daggers 在每个主块开采。在最初 4 年，每个主块可以开采出 1024 个 XDAG。在第二个 4 年，512 个，以此类推，每隔 4 年产出减半。所以，XDAG 的产出总量大约是 2^32。每个 dagger 等于 2^32 cheatoshino（译者注：比特币的最小单位 satoshi 来源于创始人中本聪名字中的聪。XDAG 的创始人是 Daniel Cheatoshin，因此 Cheatoshin 被用作 XDAG 的最小单位）。如果一笔交易被主块引用，那么它是有效的。有效的交易在主链上严格地按照链接的顺序排列。双花（double spending）被禁止，因为只有并发的第一笔交易（按此顺序）被应用。

安全性

拥有 256 位私钥的 ECDSA 算法被用于签名，以确认钱包拥有者对其地址中的代币拥有所有权。所有在主机中传输的数据使用作者的半对称（semi-symmetric ）加密算法加密。会话密钥的传输使用 8192 位密钥的 RSA 算法。

路线图

主网已于 2018 年 1 月 5 日上线。没有 ICO 计划。没有预挖矿。每个人可以在同等条件下参与挖矿。

目前可以使用 CPU/GPU 挖矿，现存的 ASIC 矿机不适用于挖矿。

团队

Dagger 最初的开发者是一位化名 Daniel Cheatoshin 的匿名人士。(cheatoshin@mail.com).

现在，这个项目由 Dagger 社区开发团队维护。

翻译

本白皮书由 Nikoni 翻译并校对。(Nikoni5151@gmail.com,XDAG:6PjsAe4w/336/rOXy6VAxey4NzBanm2v)