因子链 ChainFA 白皮书

目录

1 摘要

比特币（BitCoin）的概念最初由中本聪在 2009 年提出，根据中本聪的思路设计发布的开源软件以及建构其上的 P2P 网络。比特币是一种 P2P 形式的数字货币。点对点的传输意味着一个去中心化的支付系统。

比特币已经证明，一个去中心化的电子系统确实可以工作和完成付款处理。然而，要基于一个完全分散的，对等解决整个电子经济，就必须做到以下几点：过程中的交易安全、迅速和有效；为人们提供参与网络安全奖励；规模与全球最小的资源占用；提供一系列基本的交易类型；提供一个灵活的架构，使新的核心功能的加入，并允许先进的应用程序的创建和部署；并能够运行在一个范围广泛的设备，包括移动的。ChainFA 满足所有这些要求。

2 引言概述

ChainFA 是 100% POS 方式的工作证明，基于开源的 JAVA 语言编写，具有独特的 POS 算法和抗攻击风险。创世块中共有 70 亿个可用 CFA。随着 SHA256 算法越来越受欢迎，Curve25519 密码术用于提供安全性和所需处理能力的平衡，以及更常用的 SHA256 哈希算法。

平均每 60 秒产生一个块，由网络节点上解锁的帐户生成。由于完整的令牌供应已经存在，所以 ChainFA 通过包含在成功创建块时

向账户授予的交易费来重新分配。 这个过程被称为锻造，类似于其他加密货币采用的挖掘概念，交易在经过 10 次交易确认后被认为是安全的。

ChainFA 是基于一系列核心功能类型，不需要任何脚本处理或者网络节点的事务输入/输出处理。 通过这些基础功能，ChainFA 核心可以被看作是一个敏捷的基础层协议，在这个协议上可以建立无限范围的服务，应用程序。

3 基础技术

3.1 工作证明

在大多数加密货币使用的传统工作证明模式中，网络安全由节点进行工作。他们调配资源（计算/处理时间）来调和双重支出交易，并为试图扭转交易的人付出非常高的成本。以资产奖励换取工作证明，频率和金额随每个加密货币的操作参数而变化。这个过程被称为采矿。确定每个加密货币的可用挖掘奖励的块生成频率通常保持不变。因此，随着网络工作量的增加，要求获得报酬的工作的难度必须增加。

随着“工作证明”网络变得越来越强大，为了追求利润，矿工须不断增加资源，采用专有硬件，需要大量的资金投入和持续的能源需求。随着时间的推移，网络将变得越来越集中。

在 ChainFA 使用的工作证明模型的证明中，网络安全由网络中有利害关系的节点来管理。这种算法所提供的激励机制并不像 POW 算法那样促进集中化。

ChainFA 使用一个系统，每个资产在一个帐户可以被认为是一个小型的矿机。帐户中存储的资产越多，帐户获得创建块的权限就越大。由于区块生成而收到的总收益是区块内交易费用的总和。ChainFA 的重新分配是由于区块生成者接收交易费用而产生的，因此使用术语“锻造”而不是采矿。

随后的块基于来自前一块的可验证，唯一且几乎不可预知的信息而生成。块之间通过这些连接链接，创建了一系列的块（和交易），可以追溯到创始块。

3.2 令牌

ChainFA 的总资产供给量为 70 亿个 CFA，可以被整除到小数点后第八位。所有的令牌都是创建了创世区块（ChainFA 区块链中的第一个区块），创始账户初始值为-70 亿 CFA。

在生成帐户中存在反标记有类似如下的副作用：

创始账户不能发行任何形式的交易，因为其余额为负数，不能支付交易费用。

任何发送到创建账户的令牌都被有效地销毁，因为这个账户的负数将会被取消。

3.3 网络节点

ChainFA 网络上的节点可以是向网络提供交易或数据的任何设备。任何运行 ChainFA 软件的设备都被视为一个节点。

节点可以细分为两种类型：标记和正常。 一个带标记的节点就是一个标记有从一个账户私钥导出的加密标记的节点；该令牌可被解码以揭示与节点相关联的特定 ChainFA 帐户地址和余额。在节点上放置标志的行为增加了一定程度的问责性和可信度，因此标志性节点比网络上的非标志性节点更可信。绑定到标记节点的帐户的余额越大，对该节点的信任度越高。

ChainFA 网络上的每个节点都有能力处理和广播交易和块信息。如果它们从其他节点收到验证块，并在块验证失败的情况下，节点可能会暂时列入黑名单，以防止传播无效块数据。

每个节点都具有的 DDOS（分布式拒绝服务）防御机制，将来自其他任何节点的网络请求数限制为每秒 30 个。

3.4 区块

与其他加密货币一样，ChainFA 交易信息也被建立并存储在一系列区块中，称为区块链。这个账本提供了已经发生的交易的永久记录，并确定交易的发生顺序。区块链的副本保存在 ChainFA 网络的每个节点上，并且每个在节点上解锁的帐户（通过提供帐户私钥）都能够生成块，只要至少有一个到帐户的传入交易已经确认了 1440

次。任何符合这些标准的帐户都被称为活动帐户。

在 ChainFA 中，每个区块最多包含 255 个事件，所有事件都以包含标识参数的块标题开头。块中的每个事件由常用事件数据表示，具体事件类型也包括事件附件，并且某些事件可以包括一个或多个附加附件。最大块大小是 42KB。所有块包含以下参数：

- 区块版本，块高度值和块标识符
- 一个块时间戳，以秒为单位表示，因为起始块阻塞
- 生成该块的帐户的 ID 以及该帐户的公钥
- 前一个块的 ID 和区块中存储的事件数
- 以交易和费用为代表的 CFA 总资产
- 包含在块中的所有交易的交易数据，包括他们的交易 ID
- 块的有效载荷长度以及块有效载荷的散列值
- 该块的签名
- 块的基本目标值和难度

3.4.1 锻造区块

为了成功锻造（生成）出块，所有活动的 ChainFA 帐户通过尝试生成低于给定基本目标值的散列值进行竞争。此基础目标值随着块的不同而不同，并且是以前一个块为基础目标乘以 60 秒平均块时间的公式所需的时间量得出的。

区块链上的每个块都有一个生成签名参数。为了参与块锻造过程，活动账户用自己的公钥对前一个块的生成签名进行数字签名。这将创建一个 64 字节的签名，然后使用 SHA256 进行散列。结果散列的前 8 个字节被转换为一个数字，称为帐户匹配。

命中与当前目标值进行比较。如果计算出的命中率低于目标值，则可以生成下一个块。如目标值公式中所指出的那样，目标值随着每秒通过而增加。即使网络上只有少数活跃帐户，其中一个最终会生成一个块，因为目标值会变得非常大。因此，您可以通过比较帐户命中值与目标值来计算锻造块的时间。

3.4.2 账号

作为其设计的一部分，ChainFA 运用了脑钱包形式：所有帐户都存储在网络上，并为每个账户地址直接生成私钥。每个帐户私钥使用 SHA256 和 Curve25519 的加密组合产生账户地址。

帐户地址始终以 CFA-前缀开头，使得 ChainFA 帐户地址容易被其他区块链使用的地址格式识别和区分。

3.4.3 交易

交易是 ChainFA 账户改变其状态或余额的唯一方式。 每笔交易只执行一项功能，一旦该交易包含在一个区块中，其记录永久存储在网络上。

交易费用是 ChainFA 重新回到网络的主要机制。 每笔交易都需

要最低的费用。 当一个 ChainFA 账户锻造一个区块时，该区块中包含的所有交易费用都会被奖励给该锻造账户。与其他区块链不同，最小交易费用由区块链强制执行，因此没有指定大于此交易类型的最小费用的交易将不被节点接受。

所有 ChainFA 事件都被认为是未经确认的，直到它们被包含在一个有效的网络块中。新创建的块由创建它们的节点（和相关联的帐户）分配到网络，并且包含在块中的事件被认为已经接收到一个确认。 随着随后的块被添加到现有的区块链中，每个附加区块为事件的确认数量增加一个确认。

每个交易都包含一个截止时间参数，从交易提交到网络的时间开始，设置为一个分钟数。默认截止时间是 1440 分钟（24 小时）。已经被广播到网络但尚未被包括在块中的事务被称为未确认的事件。

如果事件在交易截止日期到期之前没有被包含在一个块中，则交易将从网络中移除。

3.5 加密类型

ChainFA 中的密钥交换基于 Curve25519 算法，该算法使用快速，高效，高安全性的椭圆曲线 Diffie-Hellman 函数生成共享密钥。

4 核心说明

4.1 COTP 基于区块链的动态口令令牌技术

4.1.1 前言

因基于区块链的动态口令令牌目前无任何案例，范围适用于基于区块链动态口令令牌产品的开发和应用产品的依据，其中各项技术指标可随技术进步和产品改进而提高标准。

4.1.2 文献与名词

HMAC:Hash-based message authentication code RFC 2104

HOTP: HMAC-Based One-Time Password RFC 4226

TOTP: Time-Based One-Time Password RFC 6238

COTP:Chain-Based One-Time Password

4.1.3 技术细节

HMAC 算法公式 HMAC(K, m) = H((K’ xor opad) || H ((K’ xor ipad) || m))

- H 散列函数
- K 共享密钥
- K’ 通过 K(密钥)计算所得(当散列函数是 SHA-1, MD5, RIPEMD-128/160,K’大小为 64 字节不足后面填充 0)
- xor 异或
- opad 外层 HASH 填充值,0x5c5c5c….长度与 K’相当
- ipad 内层 HASH 填充值,0x363636….长度与 K’相当
- m 一个消息输入
- || 表示连接

HOTP 算法公式 HOTP(K,C) = (Truncate(HMAC(K,C)) & 0x7FFFFFFF) mod 10d

- C 计数器,对应 HMAC 中的 m
- & 与
- T HMAC sha1 后得到的结果太长,经过 Truncate 处理后我会得到一个 32bit 的无附号整数
- mod 取余,与 10 的 d 次方模运算得到 d 位的一个数字口令

COTP 算法公式 COTP = HOTP(K, CH)

- K 基础因子
- HC BlockId，最新区块唯一 id 信息，具备不可预测性。

4.2 网络节点

node1.chainfa.org

node2.chainfa.org

4.3 服务

官网：http://chainfa.org

在线钱包：http://wallet.chainfa.org:17876（安装及使用教程见官网说明）

区块链客户端：http://chainfa.org/chainfa-core.zip

Telegram 讨论：https://t.me/chainfa

QQ 群：337574426

5 应用方案

5.1 因子链认证

5.1.1 介绍

因子链认证是指结合密码和基于区块连的动态口令令牌两种条件对用户进行认证的方法。为减轻必须携带专用因子链口令令牌设备所带来的阻力，可以利用现在无处不在的移动计算平台（如支持 Java 的手机应用传递的一次性口令）作为因子链客户平台。

5.1.2 为什么我们需要因子链验证

传统的密码认证方式，如果在用户名密码在其他网站上泄露，任何用户都可以使用你的账号密码进行登陆做任何操作。但有了因子链认证就能在一定程度上有效的避免这种情况的发生。因为在每次登录时，不仅需要输入您的帐户密码，还需输入移动设备为您生成的因子链动态口令令牌。

5.1.3 特点

无需记忆，不会产生 password 这样的泄漏问题。

动态生成，约每 71 秒更新一次，安全性大大提高。

客户端与服务端通过区块链非中心化模式进行动态口令同步。

低成本，无需购买硬件和软件。

5.1.4 认证流程

1. 服务器随机生成一个类似于『GEZDGNBVGY3TQOJQGEZDGNBVGY3TQOJQ』的 40 位基础因子，并且把这个基础因子保存在数据库中。

2. 在展示面显示一个二维码，内容是一个 json 格式信息 {“accoName”:accoName, “domain”:domain, “optsk:” otpSk}

3. 客户端扫描二维码，将基础因子『GEZDGNBVGY3TQOJQGEZDGNBVGY3TQOJQ』保存在客户端。

4. 客户端定时（5 秒）使用基础因子『GEZDGNBVGY3TQOJQGEZDGNBVGY3TQOJQ』和最新区块信息通过 COTP 算法生成一个 8 位数字的动态口令。

5.1.5 认证其他情况

1. 客户端在认证时需要连接公有或私有网络区块链网络以确认最新区块信息。

2. 在遇到利用遍历所有 8 位数字进行暴力破解时，建议服务端对错误次数进行限制。

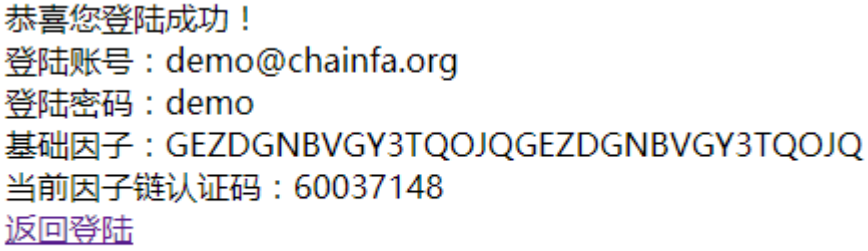
5.1.6 案例 DEMO

访问地址：http://www.chainfa.org/login.jsp

客户端：android：http://chainfa.org/chainfa-release1.0.1.apk

5.1.6.1 DEMO 图片

平台登陆：



Android 端：


10:23
ChainFA [Chain Factor Authentication]
60037148
chainfa.org$demo@chainfa.org$Sep-08-2017
60037148
chainfa.org$demo@chainfa.org$Sep-08-2017
SCAN QR CODE 扫面二维码

5.2 企业级账户认证（私有链）

5.2.1 说明

基于现有因子链代码，可为企业架设基于区块链的认证架构，甚至在脱离外网的情况下实现企业内部安全认证。隔离各类入侵风险。

5.2.2 服务器系统安全

随项目进展，逐步更新。

5.2.3 机房应用入口认证

随项目进展，逐步更新。

5.2.4 远程管理认证

随项目进展，逐步更新。

5.2.5 企业应用系统员工签名认证

随项目进展，逐步更新。

5.3 区块链领域安全认证

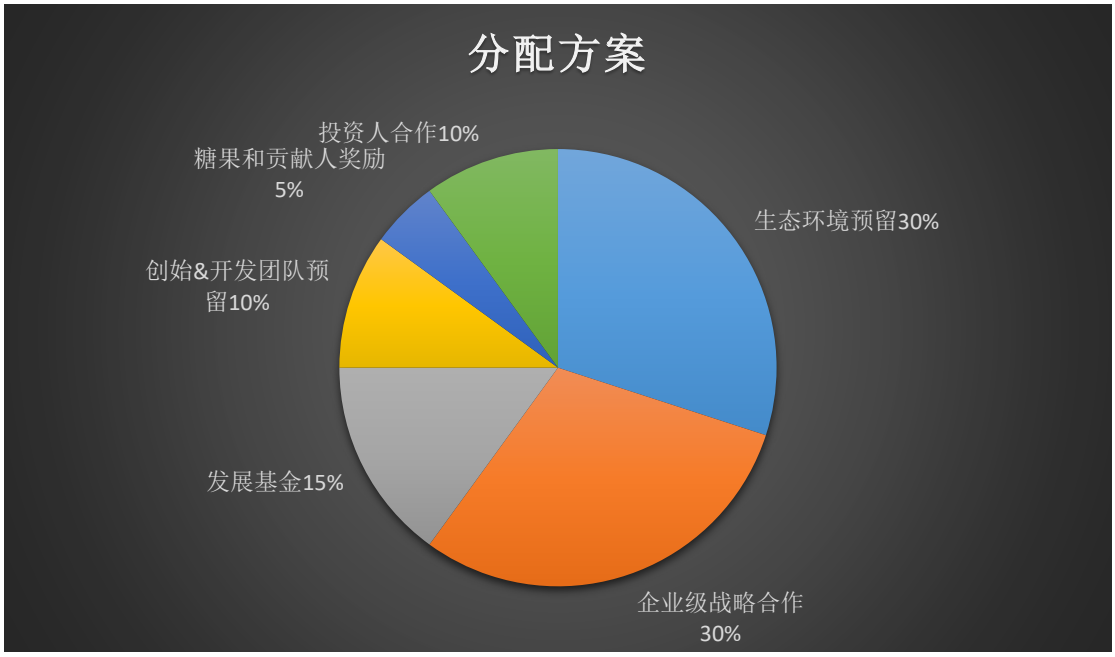
随项目进展，逐步更新。

6. 分配计划

设计资产总量：70 亿

为防止因价格波动导致交易费用过高问题，总资产设计多于其他常见区块链资产总量。

分配方案	数量	比例
运营&生态环境预留	21 亿	30%
企业级战略合作	21 亿	30%
发展基金	10.5 亿	15%
创始&开发团队预留	7 亿	10%
糖果&贡献人奖励	3.5 亿	5%
投资人合作	7 亿	10%



运营、生态、发展

包括但不局限于：因子链 ChainFA 社区区块链应用生态孵化、激励、开发者社区建设、商业合作、教育、学术研究及各类机构发展等。

合作

基于发展需要进行企业和个人合作预留。

创始&开发团队预留

因子链 ChainFA 发展过程中，从组织架构、研发、运营、客服、行政、财务、业务等持续做出贡献的团体和个人，在分配机制上预留 10%作为团队激励，这部分初始状态锁定，分 3 年逐步分发至创始&开发团队。

奖励

市场推广过程中，对项目普及、用户认知、平台测试&运行、信息反馈等作为奖励媒介。

7 总结

随着互联网发展的逐渐完善，尤其在金融业、通信业起到了巨大的作用，由此信息安全在各个行业逐渐受到重视，ChainFA 正是基于此环境下孕育而生，希望在不久的将来，ChainFA 能够在信息安全领域占有一席之地。