



Viacoin Whitepaper

Via 币白皮书

Via 币制作团队

9.12.2017

最后更新于 9.20.2017

Via 币是在 2014 年由比特币协定上创建的开源数字货币，它支持嵌入式共识，并支持延伸 OP_RETURN 120 字节辅助。Via 币的特点是 Scrypt 合并挖矿，也称为辅助工作证明(Auxiliary Proof-Of-Work)(通常简称 AuxPoW)，速度比比特币(24 秒的区块时间)快上 25 倍。

Via 币的采矿报酬减半每 6 个月进行一次(目前的区块报酬是每块 0.3125 个币)，总共供应量为 23,176,392.41459，使通货膨胀率和采矿回馈相对较低。为了保持 挖矿利益，合并采矿(AuxPoW)已经实施，其中最大份额的哈希源自莱特币网络。Via 币目前由世界上最大的矿池 F2Pool 开采，因此保持了非常高的哈希率。

Via 币的其他功能包括暗引力波挖矿难度调节算法(Dark Gravity Wave)，旨在解决 Kimotos Gravity Well、版本位(BIP9)中的缺陷，最多可允许 29 个并行软叉功能在代码库执行，也可执行隔离见证(Segwit)和闪电网络，这两项将在本档的后面探讨。



Viacoin Whitepaper

1. Scrypt

在密码学中，由Colin Percival创建的Scrypt 密钥衍生函数，通过巨量的内存 需求，来让大规模硬件攻击的成本高昂、不易实施。在 2012 年，这个算法被 IETF 指定为一个信息性 RFC 的互联网草案，Scrypt 现在则被 Via 币作为工作量证明 机制。

Scrypt 算法需要保存在内存中的大量伪随机位和从中导出的密钥。该算法基于 TM TO(时空数据折中算法)。

Scrypt 使用以下参数生成密钥:

- 密码: 用于散列的字符串
- Salt: 提供给 Scrypt 函数的随机字符串 - N: 内存/ CPU 成本参数
- P: 并行参数
- R: 区块大小参数
- dkLen: 密钥的预期长度, 以字节为单位

`kd = scrypt(P, S, N, P, R, dkLen)`

Via 币参数, 其中 $N = 1024$, $R = 1$, $P = 1$, S = 随机 80 字节输出的 256 位

2. 合并采矿AuxPoW

Via 币的合并采矿用意在重新利用其他 Scrypt 硬币的采矿能力, 允许矿工同时对多个区块链进行开采, 以增加 Via 币区块链的安全性。这意味着例如, 矿工可以通过采矿莱特币或任何其他 Scrypt 硬币来间接挖掘 Via 币。矿工贡献的每个单独哈希操作都会单独添加到双方区块链的总哈希值中, 从而提升了安全性。

AuxPOW 块类似于标准的比特币块, 除了两个主要区别: 首先, 区块头的哈希 不一定符合其难度目标。第二, 它有额外的数据元素, 显示区块先在原区块链上 开采(莱特币), 然后成为辅助区块链(Via 币)符合其难度目标的有效区块。

Via 币的 AuxPoW 功能可有效地确保矿工将继续无限期地开采 Via 币, 即使财务回馈减少(块收益变得太低而不能直接开采), 这是因为他们可以轻松地挖掘任

何其他 Scrypt 硬币并收取 Via 币而不需要增加成本。这种模式可导致 via 币通货膨胀率低于其他不支持合并采矿的货币, 并同时允许每 6 个月减半一次。



Viacoin Whitepaper

3. 引力波挖矿难度调节算法(DarkGravityWave)

引力波(DGW)是一种开源的难度调整算法。DGW 由 X11 / 暗黑币(Darkcoin)/ 达世币(Dash)的创始人 Evan Duffield 撰写。该算法用意在解决 Kimoto's Gravity Well 算法的缺陷，如时间扭曲攻击(time warp attack)。引力波首次在达世(暗黑币)中引进。

DGW 利用多指数移动平均线和简单移动平均线来稳定调整机制。它使用以下公式:
$$2222222 / (((Difficulty + 2600) / 9)^2)$$

Dark Gravity Wave 版本 3 是最新版本，与众所周知的 Kimoto Gravity Well 算法相比，可以改进难度重新定位。

4. 隔离见证(Segwit)

隔离见证(Segwit)指的是一种与交易流程分开，称为“见证人”的新结构。它用在增加各区块的交易吞吐量，有助于将交易事务的大小缩小 2-3 倍，同时允许区块对新节点进行更快的同步。隔离见证于 2017 年 7 月 31 日与 Via 币镶嵌，并于 2017 年 8 月 3 日正式启用。

隔离见证的主要目的不是增加事务量，而是修复可扩展性、使脚本易于升级。随着 Via 币的可扩展性修复，未来的各项实施将会更有可塑性。后期的各项升级如原子交换，双向支付管道和闪电网络也可因此成功执行，来增加 Via 币与比特币和莱特币互操作性的项目。



Viacoin Whitepaper

5. 闪电网络

闪电网络(LN)是在 Via 币块链上运行的转移网络，透过将共识总账外的大多数交易输至支付信道，来大量地改善交易吞吐量。链上脚本使这功能可能实施，首先允许各方进入一个双边合同，通过共享数字签名来更新状态，然后将证据发布到区块链上结束行动。

对于低量交易，闪电网络是一个杀手锏。它开启了新种的交易方式。通过多方开设付款通道，LN 的各个参与者可做为其他参与者付款之间的管道，藉由各个连接来构成一个完整的付款通道。

6. Schnorr 签名方案

椭圆曲线数字签名算法(ECDSA)是目前 Via 币利用的加密算法，作为零知识证明的货币所有权，来授权货币的输入与输出。在 2015 年，丹尼尔 J · 伯恩斯坦 (Daniel J. Bernstein)在椭圆曲线之上提出了类似 Schnorr 的数字签名。它在 加密货币市场中越来越受欢迎，且常被认为是继 ECDSA 后一种更有效的算法，主要用于比特币。

直到最近，它的应用实施会需要 Via 币链的硬分支，然而在启动隔离见证后又多了许多更新的可能性， Schnorr 签名就是其中之一。这一点便说明了 Via 币块链启用隔离见证的关键意义:因为所有的签名数据都被传送到证人身上，所以它 能更灵活地增加更多加密功能。为了确保 Via 币网络的发展，我们打算在 Via 币上开发及实施 Schnorr 签名。

Schnorr 签名的一些优点包括:

*根据标准假设提供安全保障 *抗延展性 *避免哈希函数碰撞 *批量验证， 2-3 倍加速
*k-k 多重签名

Schnorr 签名支持批量验证， 这意味着可以对一组公钥消息签名对执行简单的验证 测试，以确定此组整体上是否有效。比起单独验证其中的每一个签名对，可更快速地执行。这是一个非常理想的结果，因为从根本上来说，区块本身也是以批次的签名来验证。

k-of-k 多重签名是一个在 Schnorr 下得出的结果，单个签名可以被用来证明一起



Viacoin Whitepaper

签署的多个密钥已被签署，由于一个组可以创建一个代表整体的签名。为了说明这一点，假设 U1, U2 和 U3 用户。他们参与一个 2 轮交互方案，它们都提出了 nonce k1, k2, k3，然后计算相应的公共点 R1, R2, R3。再来，他们以公共点相互通信并将它们相加到一个聚合值 R。

然后每个用户将 R 值作为一个 nonce 与自己的钥匙，汇出 S1, S2, S3，然后将其合并成一个最终签名 S，S 对钥匙的总和有效。这显示了从 1 对 1 变换至 k-k 多重签名的明显优点，因为携带的数据量将与典型的单签名交易相同。

$$\begin{array}{c} U_1 \rightarrow k_1, R_1 \\ U_2 \rightarrow k_2, R_2 \\ U_3 \rightarrow k_3, R_3 \end{array} \left| \begin{array}{c} \longrightarrow R \longrightarrow \\ | \\ U_1 \rightarrow (R, s_1) \\ U_2 \rightarrow (R, s_2) \\ U_3 \rightarrow (R, s_3) \end{array} \right| \longrightarrow (R, s) \quad (1)$$

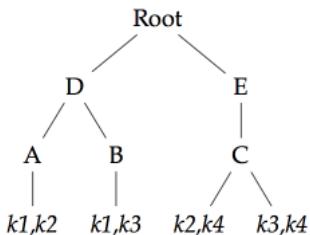
上述过程对于非 k-k 情况也是有效的。若知道什么钥的组合可以签名，那么仅需 Merkle 树及 Schnorr 功能便能构建一颗树，其中树的每个节点叶皆是可以被签名的密钥组合，将它们一起混合并导出根作为地址。OP CHECKSIG 和 OP CHECKMULTISIG 将被修改，以便它们将公钥堆栈在一起，对它们进行划分，连结受验证的输入，并为交易产生一个组合签名，从而将区块大小减去 20%。

2(共 4 个)(k1 ... k4)

O(1)验证时间

O(log n)签名大小

O(n)签约时间



在单笔交易中聚合所有签名是有可能的。其背后的想法是启用如 Via 币节点的系统验证器来换算出一个包含每笔交易输入的钥匙。



Viacoin Whitepaper

7. 非原子冲洗

为了使系统更加耐用，磁盘上的状态必须对应于区块。这样，即使钱包意外停止，我们仍然可以启动和回转，或者在其内部滚动，并且可以在磁盘上获得一致的提示。通常每当缓存满时，我们便强制冲洗。如果它在启动时出现，这意味着我们在刷新期间死机了，我们可以回滚/前滚区块，以便在继续操作之前获得一致的提示。

8. 彩色币(colored coins)

Via 币的脚本语言允许在区块链中存储少量的元数据来作为资产操作指令。一笔 Via 交易首先进行编码，以便传输新流入 x 个单位的资产，并将其记入 Via 币地址。

这个词源自于一个把名义金额的货币着色的想法。通过 Via 币的“着色”，它变成可以代表用户欲交易任何东西的代币，例如公司股票，房屋所有权契约，期货合约或任何现实世界的资产。虽然这似乎与合约币(XCP)类似，但还是有一些关键的区别。

它使用 Viacoin 区块链(如未来币 NXT)。这意味着它不会发行辅助硬币(例如合约币和万事达)来锚定资产。

此外，彩色硬币交易由通常存储在 OP RETURN 操作码之一中的元数据指示。包含 OP RETURN 的输出称为标记输出，值可以为零或不为零。标记输出从 OP RETURN 操作码开始，后面可以接续任何序列的操作码，但它们必须包含一个含有 Open Assets 标记酬载的 PUSHDATA 操作码。资产数量列表用于确定每笔资产输出的数量，每个整数皆使用 LEB128 编码。如果超过 9 个字节，标记输出会被视为无效。产出的最大资产量为 $2^{63}-1$ 个单位。彩色硬币开放资产协议(Open Assets Protocol)建立于 Via 币协议之上，并且不需要对其进行任何更改。

9. 抽象语法树 MAST (Merkelized Abstract Syntax Trees, BIP 0114)

MAST 允许 Via 币交易验证脚本以部分散列的形式存储，并允许节点与默克尔树进行交互。消费时，使用者只需提供正在执行的分支，与将分支连接到默克尔根的哈希。这可将偿还堆栈的大小从 $O(n)$ 减少到 $O(\log n)$ (n 这里表示分支数)。

原本因脚本大小和操作码限制而不可能实行的复杂兑换条件，可因此实现，隐私也通过隐密的未执行分支来改善，也可在非常低的成本下允许共识之外的数据。BIP 0114 是一个重要的升级，因为 MAST 可在不堵塞块链下创建智能合约，而不会发生智慧合约在区块链上可见或占用空间等等常见的错误。



Viacoin Whitepaper

MAST 只显现已完成的智慧合约，空间更节省因节点只读取默克尔树顶层。这说 法虽然与以太坊听起来很相似，但有一个重要的区别。以太坊利用了以太坊虚 拟机(EVM)运行环境，但 VIA 币将通过 RootStock(RSK)使用 VM。RSK 旨在成为以太坊(或应该是)的一个:去中心化的，图灵完备的智慧合约平台

10. Via 币 RSK 智能合约

Rootstock 是一个双向挂钩的智慧合约平台。想法是让 Via 币能够支持智慧合约。Rootstock 运行一个称为 Rootstock Virtual 的图灵完备虚拟机，与以太坊的虚拟 机兼容，并允许 Solidity 编译的智能合约运行。它可以通过与 Via 币合并开采 来实现，使得 RSK 块链与 Via 币具有相同的安全级别。性能方面，它能允许大 约每秒 2000 个链上交易和每秒 20,000 个链外交易。

11. 匿名交易

基于 Tumblebit 上的 Via 币原子性匿名交易中心

<https://github.com/viacoin/documents/blob/master/whitepapers/styx/Viacoin-Styx-Whitepaper.pdf>