**MATRX TESTNET vs ETHEREUM**

**版本: V1.0**

**作者：MATRIX 基金会北京研究院**

**日期：2018.10.02**

任何情况下，与本系统及其衍生产品，以及与之相关的全部文件（包括本文件及其任何附件中的全部信息）相关的全部知识产权（包括但不限于版权、商标和技术秘密）皆属于 MATRIX 基金会所有。

本文件中的信息是保密的，且仅供用户指定的接收人内部使用。未经 MATRIX 基金会事先书面同意，本文件的任何用户不得对本产品和本文件中的信息向任何第三方（包括但不限于除用户指定接收人以外的管理人员、员工和关联公司）进行披露、出借、许可、转让、出售、分发、传播或进行与本产品和本文件相关的任何其他处置，也不得使该等第三方以任何形式使用本产品和本文件中的信息。

未经 MATRIX 基金会事先书面允许，不得为任何目的、以任何形式或任何方式对本文件进行复制、修改或分发。本文件的任何用户不得更改、移除或损害本文件所使用的任何商标。

本文件按“原样”提供，就本文件的正确性、准确性、可靠性或其他方面，MATRIX 基金会并不保证本文件的使用或使用后果。本文件中的全部信息皆可能在没有任何通知的情形下被进一步修改，MATRIX 基金会对本文件中可能出现的任何错误或不准确之处不承担任何责任。

在任何情况下，MATRIX 基金会均不对任何因使用本软件产品和本文件中的信息而引起的任何直接损失、间接损失、附带损失、特别损失或惩罚性损害赔偿（包括但不限于获得替代商品或服务、丧失使用权、数据或利润；或商业中断），责任或侵权（包括过失或其他侵权）承担任何责任，即使 MATRIX 基金会事先获知上述损失可能发生。

MATRIX 基金会保留所有权利

# 目 录

[目 录 1](#_Toc20734)

[变更记录 2](#_Toc20591)

[1 引言 3](#_Toc27568)

[1.1 文档用途 3](#_Toc22177)

[1.2 术语 3](#_Toc863)

[1.3 使用对象 3](#_Toc2404)

[2 共识机制完全重构 4](#_Toc5066)

[3 网络架构重构 5](#_Toc7081)

[4 交易类型重构 6](#_Toc22917)

[5 存储接口重构 7](#_Toc32633)

[6 钱包优化 8](#_Toc3887)

[7 更多（待续） 9](#_Toc15049)

# 变更记录

| 修订日期 | 设计内容 | 作者 | 评审者 | 评审日期 |
| --- | --- | --- | --- | --- |
| 2018-10-02 | 初版 | 李庆华 |  |  |
|  |  |  |  |  |

# 引言

## 文档用途

本文档旨在从几个重要方面比较MATRIX 测试链相比以太坊的优势。

## 术语

| **术语** | **备注** |
| --- | --- |
|  |  |

## 使用对象

# 共识机制完全重构

MATRIX采用的是HPOW算法，核心包括：可以验证随机选举的验证者，支持（3个/11个/21个以及可配置）生成交易区块，可验证随机选举的矿工，并支持任务分配的计算节点（目前是由验证者直接将任务分发给AI server，通过自行编写的三个Python程序，未来由AI矿工加入）。可以在区块链浏览器中看到这个的体现，就是节点和出块。

（详细框架可以看我们的文档）。

这一全新架构大大提升了共识的处理速度，并完成了打包和矿工HASH的分离。另外，矿工HASH的分离，很快将修改为基于随机视频流的inference结果判断，并根据这个结果计算出来一个HASH，作为挖矿过程。其目标就是最终进化到MCMC矿机。

上述实际蕴含了一个可验证随机函数的概念VRF，我们将这个固化到代码，并通过随机数服务体现

# 网络架构重构

由于MATRIX为了保证处理速度和负载均衡，将整个拓扑网络进行了层级优化。现在已经没有洪泛的概念，而是按照有序网络的方式对外提供，这里面加入了nodelevel的概念，每个选举周期内，每层都会进行层级轮换，并进行新加入和退出层的合并。从而保证整个传输网络的稳定性。

这个也是我们发布的代码中的一个核心内容。这部分相对以太坊，解决网络优化和传输效率问题。

# 交易类型重构

由于MATRIX需要面向较多复杂的交易场景，并试图解决交易的安全性问题，目前提供了一对多交易/定时交易类型，并在下个月版本提供白名单、黑名单机制，还提供了token直接基于交易的转换技术。这部分代码也基本上重构。由于提高了链的交易速度，所以我们将提供基于链的多token直接兑换技术，通过简单交易函数实现，从而避免基于合约实现。

另外，为避免普通用户的合约交易风险，除了提供安全智能合约，我们也提供了直接的内置go函数方式实现，用户直接通过钱包就能实现一些复杂的但相对固化的交易。

# 存储接口重构

为保证交易不会出现类似EOS的验证节点或者矿工作弊，我们提出了广播节点的概念，每300个周期会有一个广播周期，该周期仅用于广播交易和申诉，验证者需要优先执行，从而避免验证者作弊，这个在本次发布中也体现出来了。

另外，由于AI数据很大，需要借助IPFS和广播接口，我们也在本次发布中体现了原型。

此外，我们的区块数据，也是直接通过具备集群的IPFS主节点进行发布，从而可以快速广播到全网，从而避免很多时候，节点无法下载到完整数据的。

# 钱包优化

由于具备验证节点和矿工节点以及AI节点，这些都需要进行安全授权，并进行交易，所以我们重新构造了抵押交易，并集成其中。

另外，从安全性和扩展性设计出发，我们设计了第三方付费业务，支持A与B交易，C提供Gas费用，并提供交易费用批量减免，多个周期集中付费，以及gas费用分级，这些都是需要对交易进行重构才能完成。

在上述基础上，我们将实现信用交易，核心是为支付提供新的实现手段。

# 更多（待续）