万物魔坊
白皮书

以顶尖区块链技术引领全球资产数字化进程

AMFC

版本：0.8.1

2018-07-01

目　录

4.共识层

5.激励层

6.合约层

7.应用层

七、万物魔坊（AMFC）的分解

八、万物魔坊AMFC账户

九、信用体系

1.什么是信用体系?

2.万物魔坊（AMFC）为什么需要信用体系?

3.万物魔坊（AMFC）的信用体系

十、关系型数据库

十一、POC共识机制

1.共识准入

2.浮动保证金机制

3.全网效验

4.确定单点广播权限

(1)申请共识

(2)效验信用和保证金

(3)申请包含进区块，被确认

(4)等待当前共识轮次结束

(5)当前共识轮次结束，下一轮共识开始，下一轮变当前轮

(6)确定当前轮次共识人数

(7)初始化当前轮次共识顺序，各自节点计算出自己的共识时段

(8)接收新块，并进行区块权限验证和容错监控，等待自己共识时段的到来

(9)到了自己的共识时段开始时间，开始打包区块

(10)打包程序从内存池中获取新交易并验证

(11)预估到了自己的共识时段结束时间，停止打包

(12)询问容错监控器是否有违规需要处理，发放信用

(13)验证区块交易数据

(14)广播区块到全网

(15)继续接收新块，并进行区块权限验证和容错监控，等待下一轮开始

5.容错监控与处罚机制

6.POC总结

(1)节点之间通讯，引入先进的压缩技术。

(2)优化新区块同步到全网的流程。

(3)实现隔离见证技术，减少新区块广播大小。

十二、激励机制

十三、账户分级认证系统

十四、改进的UTXO交易模型

十五、专为商业应用而设计的通用底层协议

十六、万物魔坊（AMFC）的商业应用及落地规划

1.令牌系统

2.交易合约

3.去中心化交易所

4.存在性证明

5.物联网

十七、万物魔坊（AMFC）后继规划

十八、万物魔坊（AMFC）后继商业整合

(1)万物魔坊（AMFC）为企业提供资产发行交易服务

十九、万物魔坊（AMFC）的发展路线图

二十、风险

二十一、免责声明

二十二、万物魔坊（AMFC）智能合约(发行代币)新定义函数类型

(1)万物魔坊（AMFC）MVM对以太坊EVM的改变（指令集）

摘 要

我们正在为每个加密货币持有人创造机会，以投资于领先公司的股票和主流金融国家交易所的区块链对应实体债券。

万物魔坊（AMFC）加密货币是基于区块链的集体投资产品/工具。 同时可以在国际主流加密货币交易所进行交易，并可供任何人购买。

使万物魔坊（AMFC）代币独一无二的是蓝筹股和债券的可靠支撑， 其价格与相关证券的当前市场价值是相关联的。

万物魔坊（AMFC）代币使您能够投资于澳大利亚主要股票市场的一部分，由与其链接到的固定的股权代码作为代表， 投资组合由AXS排列，为万物魔坊（AMFC）持有人提供了完整的体验。

这些代币是在万物魔坊（AMFC）购买股票和债券等资产时发行的，然后万物魔坊（AMFC）公布这些区块链，公司将保留现有资产的直接比例,并发出万物魔坊（AMFC）。其是基于在区块链中的智能合约，每组资产将对应一个特定的万物魔坊（AMFC）。

当资产在购买时,万物魔坊（AMFC）将被颁发。当资产出售时，对应数量的万物魔坊（AMFC）将被销毁。每个万物魔坊（AMFC）系列的详细描述将在网站文档中提供。最终，万物魔坊（AMFC）将被引入加密货币交易所，要购买这些代币，用户将需要一个兼容ERC-20的钱包。

万物魔坊（AMFC）和资产区块链币的含义相同。

一、万物魔坊（AMFC）对区块链的理解

随着比特币进入大众视线，区块链技术的魅力也被越来越多的人发现和认可。其突出的去中心化、去信任化和数据不可篡改特性，将会颠覆许多传统行业， 目前区块链技术处于初级阶段，其应用范围还十分狭窄，万物魔坊（AMFC）致力于打破这种局面。

区块链的本质是一个一致的分布式数据账簿，万物魔坊（AMFC）在项目开发过程中，对区块链技术有了更深层次的理解。结合 p2p 技术和共识机制，基于万物魔坊（AMFC）公有链的应用开发，就像在传统数据库上面开发一样简单，结果就是万物魔坊（AMFC）能为各种应用尤其是商业应用提供底层协议支持。万物魔坊（AMFC）的技术和业务，将会为区块链行业带来突破性的发展。

二、什么是万物魔坊（AMFC）？

万物魔坊（AMFC）是一个定位于区块链商业应用底层平台的公有链项目，其深层应用基于区块链技术的分布式数据存储协议。开发团队力图打造一个安全稳定的股权行业区块权益资产平台，以满足金融、股票、投资、公共服务等传统领域快速步入区块链+智能股权投资时代，是在 MIT 许可协议内进行开发的项目，技术和代码全部开源。

它提供了一系列的 SDK 和 api 来帮助开发者构建基于 Javascript 和侧链技术的去中心化应用。万物魔坊（AMFC）通过提供定制侧链、智能合约、应用托管等一体化的行业解决方案，致力于打造一个易于使用、功能完备、即插即用的系统。

利用万物魔坊（AMFC）生态系统，开发者可以快速迭代他们的 Javascript 应用，并发布到系统内置的应用商店中，这些应用可以被平台中的分布式节点下载并执行，并服务于普通用户，整个过程都由诚实安全的万物魔坊（AMFC） 侧链共识网络提供安全保证。

万物魔坊（AMFC）系统本身也是一个完全开放的、去中心化的应用，内置有代币，单位为万物魔坊（AMFC），中文名叫万物魔坊（AMFC）。万物魔坊（AMFC）可以通过双向楔入的方式与侧链或 DAPP 进行交互，作为所有 DAPP 之间资产转换的桥梁和媒介，这些代币将在系统发布之前以 ICO 的方式预售给投资人。系统一旦发布，万物魔坊（AMFC）最初的核心团队将不再掌控系统的走向，只有持有的权益人拥有者决定系统将来的发展。

三、万物魔坊（AMFC）为什么更适合发展股票机制应用?

区块链人才短缺，底层技术门槛高，多数应用需要建立在某一个已经搭建好的底层平台上，万物魔坊（AMFC）为这些应用提供了另一个选择。

比特币和以太坊、lisk 等平台没有考虑实际的通用股市交易场景的需求，股市交易需求契合底层困难，应用与股市交易产生业务逻辑同样困难。还有很重要的一点，不符合商业监管的需求。

万物魔坊（AMFC）是第一个专业的股市交易区块链应用生态平台，从底层架构身份认证管理分级系统，签订双私钥的多重签名注册绑定管理。这一系统结合管理股市交易和万物魔坊（AMFC）拟订开发的高级仲裁系统一起，满足去中心网络的去中心监管和政府准入性商业级监管要求。

能够直接从您的加密货币卡参与全球金融市场。

代币价格与相应的股票或债券指数保持联系。

透明的投资组合。

投资者运营成本低。

流动性高。 万物魔坊（AMFC）可以保证无条件地直接从投资者或从加密交易回购代币。

四、万物魔坊（AMFC）的受众

1、股权用户

万物魔坊（AMFC）平台提供的工具可以非常容易地创建一个完整的区块链，更重要的是可以楔入到万物魔坊（AMFC）平台的主链或者比特币的区块链中，实现与成熟电子货币的对接，这对中小型投资者， 特别是初级投资者和传统投资者是非常有吸引力的。

中小型投资者可以通过区块链技术提供原本封闭在股市交易、互联网内部的信息和数据，甚至与监管机构的相关系统数据相互链接，增强透明度，以此树立良好的形象，赢得投资者、金融机构的信任度，顺利拿到更高的股市融资等。

中小型投资者主动公开和开放资料，已成无法阻挡的趋势。因为现在有很多企业的公开渠道来获取数据，各类上市企业已经越来越难隐瞒它们不想让外界知道的信息。我们可以大胆预测，在未来区块链将是帮助中小型投资者的重要武器。

2、开发者

开发者可以根据万物魔坊（AMFC）平台的应用开发规则和商业行为准则，并按照相关的规范进行开发和提交 dapp,Dapp 的商业模式或免费，或定价销售，或按增值服务付费。采用何种股权交易模式完全由开发者决定。

五、万物魔坊（AMFC）的创新之举

1、共识创新

万物魔坊（AMFC）独创了创新的 POC-Proof of Credit 信用共识机制（下文有详细介绍）。

2、账户系统创新

为适合商用，万物魔坊（AMFC）在底层接入了独家认证分级管理体系，为不同角色配备不同的权限和功能，使股权企业和其他角色账户可以自然的形成模式组合，实现多种交易模式。

3、系统代币信用双价值中介

除了代币 AMFC，节点还可以在共识中积累和获得另一个数据流：信用值。万物魔坊（AMFC）首次创造性的把信用值作为管理中介引入区块链，构成万物魔坊（AMFC）的双中介机制。

4、交易模型创新

不同于其他区块链项目只有转账、双重签名等简单交易类型，万物魔坊（AMFC）创造性的在底层的基础上嵌入了很多交易模型，这些模型自助完成更复杂的交易活动。如： 验证返币交易模型，悬赏合约模型，信用保证金模型以及拍卖竞价模型等。

5、模式创新

万物魔坊（AMFC）将采用全局资产白名单和应用白名单支持架构，使发行资产可以在协议合约、应用、底层网络多个层面管理和监管资产。从而实现了类似现实企业资产的发行、破产清算、应用上线，资产安全等全面功能。

6、技术整合创新

万物魔坊（AMFC）努力将区块链与本行业及其他行业先进技术进行整合，会陆续添加虚拟机，高级智能合约，高级仲裁， 隔离验证等新技术。

六、万物魔坊（AMFC）的技术架构

万物魔坊（AMFC）完全基于 nodejs 平台研发，后台使用 Express.js 框架，前端使用 Angular.js 框架， 客户端使用 Electron 框架，数据库使用 sqlite，前后端统一采用 Javascript 脚本语言，界面使用 HTML5 和 CSS3. Nodejs 其天生的异步处理机制和强大的网络开发能力，非常适合基于时间的实时交互的加密货币应用，为万物魔坊（AMFC）高性能的即时通讯提供了坚实的技术保障。

1、侧链

通过比特币套完备脚本引擎，不但可以实现普通的转账功能，还可以实现多方签名、抵押担保、博彩等智能合约应用。但是出于安全和实现难度的考虑，比特币的脚本系统设计的较为简陋，做了非常多的限制，比如它不支持循环、脚本长度受限、只支持几种标准的的交易类型。

以太坊的最大特色就是极大地扩展了这个脚本引擎的功能，加入了读取区块链、计费、跳转等新指令，还解除了栈内存、函数调用深度以及脚本长度限制等。

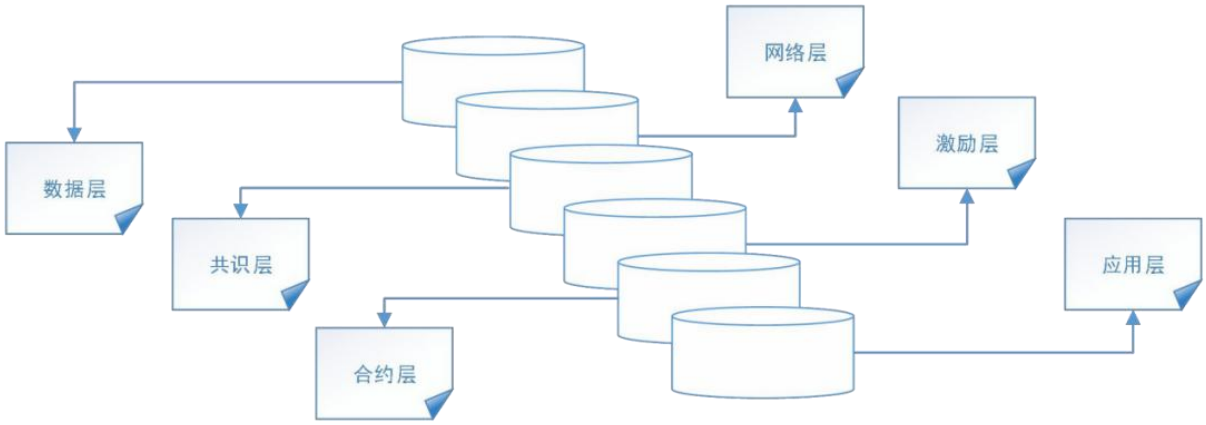
自以太坊以来，扩展脚本成为了一种实现去中心化开发平台的流行方式，但这种方式有一个很大的缺点就是，应用代码本身及应用产生的数据都存在同一个区块链中，造成了区块链的快速膨胀。以太坊试图通过优化和压缩区块和交易本身来延缓这种膨胀，也只是一种治标不治本的方法。此外，基于脚本实现的应用之间是共享同一个账本的，像区块产生时间等参数是无法被定制的，这无疑限制了应用的个性化。

侧链机制是通过另一个维度实现扩展性的，每个侧链运行在不同的分布式节点网络中， 有独立的受众、投资人和开发团队。这种天然的分片解决方案，不但解决了区块链的膨胀问题，而且每个应用都拥有一套个性化的账本，其共识机制、区块参数、交易类型都是可以被定制的，所以我们认为侧链

与完备交易脚本相比，是一种成本更低、更加灵活、也更加易用的解决方案。

开发者也可以通过万物魔坊（AMFC）侧链深度定制自己的去中心化应用 DAPP，侧链可以托管在独立的委托人节点集群中，这就自然形成了一种分片的机制，延缓了主区块链的膨胀。每一个DAPP 对应一个侧链，侧链的核心逻辑使用nodejs 开发，前端与后端之间一般通过 json rpc 协议通讯。

万物魔坊（AMFC）包括了数据层、网络层、共识层、激励层、合约层、应用层共六层基础。



2、数据层

万物魔坊（AMFC）的区块数据采用链式结构进行存储，所有区块都带有上一区块的指针引用，保证数据不被篡改。万物魔坊（AMFC）采用 sha256 函数对数据进行哈希散列，采用 ecc 非对称加密算法进行身份认证，采用 aes 加密算法加密私钥，采用 Merkle 数验证和存储交易。

3、网络层

万物魔坊（AMFC）的节点交互用的是 nio socket，用 dns 方法和程序内置方式加载种子节点。所有节点启动后会进行自检，处于公网下的节点会主动上报自己的 ip 和端口到网络中，其它节点会对其上报的信息进行验证，如果验证通过，所有节点会将可用节点的 ip 地址和端口存储到本地，下次启动会直接连接无需再次探测； 若验证多次不通过（会有一个规则，每 10 分钟探测一次，当失败

次数超过曾经成功连接次数的 10 时，会触发），该节点可能已经下线，将从存储队列里面删除。当连接节点数量过少时，会主动向已连接节点询问获取更多可用节点。

万物魔坊（AMFC）通过打洞穿透方式，让处于内网的节点间能进行互联互通，

利用已验证通过的节点作为连接桥梁，帮助处于 nat 背后的节点握手并完成连接。

4、共识层

万物魔坊（AMFC）没有采用现有的共识机制，是因为万物魔坊（AMFC）的商业定位，会成为用户流量和tps 最大的公有链，同时在商业环境中找到一个价值纽带，poc 就此而生。这也算是万物魔坊（AMFC）的一种"硬创新"，在兼顾性能的同时，兼顾维护效率。

5、激励层

万物魔坊（AMFC）的代币将保留一部分用于共识奖励，因为万物魔坊（AMFC）独特的共识机制，性能不受节点数量的影响，所以万物魔坊（AMFC）的共识节点没有设置上限，并且是动态变化的，任何人都可以随时加入赚取奖励。

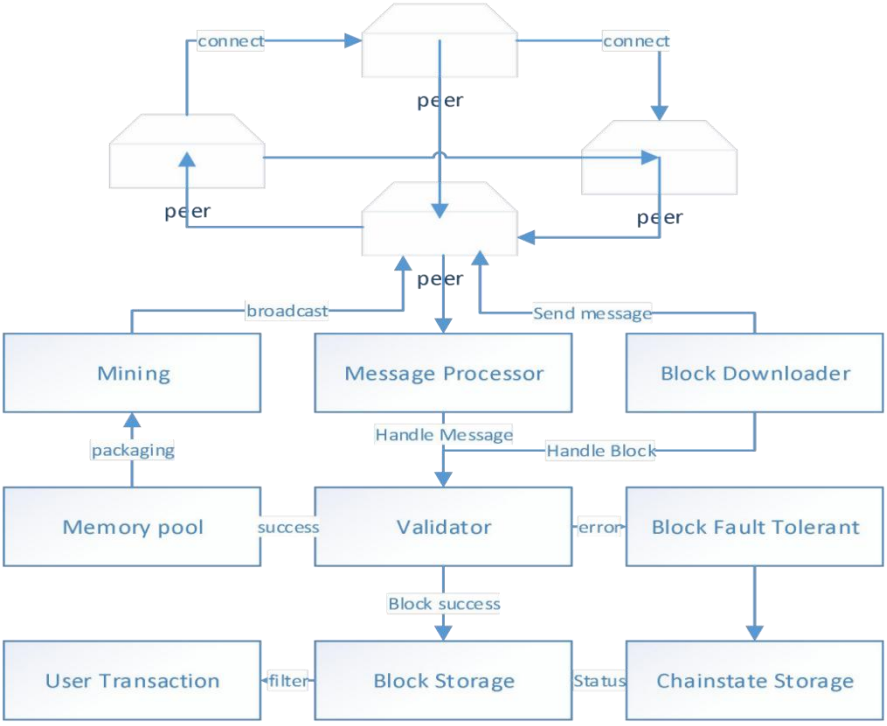
6、合约层

目前万物魔坊（AMFC）的合约层仅是简单的脚本代码，防伪码的验证脚本、共识保证金的赎回脚本，都是一个个小小的智能合约。万物魔坊（AMFC）的定位是商业应用平台，故万物魔坊（AMFC）会采取与其它智能合约平台不同的方式进行公有链生态整合和促进成型。万物魔坊（AMFC）会招募第三方团队基于万物魔坊（AMFC）打造更多接地气、具有实用性的落地应用项目，前端的受众人群将会是普通大众，进而为万物魔坊（AMFC）积累沉淀大批用户。万物魔坊（AMFC）计划于 2019 年开发

图灵完备的虚拟机，以提供更高的灵活性，前提是万物魔坊（AMFC）有一定庞大的用户基数之后，在这之前万物魔坊（AMFC）的目标和方向非常明确。

7、应用层

万物魔坊（AMFC）前期会在底层提供通用的应用协议，以开发不同的落地项目，尽快让区块链普惠大众。目前已开发完成通用的股权对等区协链协议，实际上这套业务协议的适用范围远远不止股权交易，后面有详细的介绍。



万物魔坊（AMFC）框架图

七、万物魔坊（AMFC）的分解

1、万物魔坊（AMFC） 是美国市场上五大表现最好的科技公司，名称为Facebook，苹果，亚马逊，Netflix和Alphabet的谷歌的组合，截至2017年年中，这些公司的市值约为2.4万亿美元，仍在增长。

公司:	比例:
Facebook	22%
亚马逊	22%
苹果	17%
Netflix	21%
谷歌 (Alphabet)	18%

2、2016年大型多人在线角色扮演游戏(MMORPG)和移动市场，总市值为1010亿

美元。2017年这个市值为1,090亿，预计2018年为1160亿。亚洲游戏市场增长最快。NetEase是中国最大，最成功的出版商之一。

公司:	比例:
Take-Two Interactive Software	27%
Activision Blizzard	24%
Electronic Arts	24%
Zynga	7%
NetEase Inc ADS	18%

3、由15个发展中国家的债券组成。这些是具有高收益潜力的流动主权债务。它们包括多种不同的货币，以及不同的到期期限。每个国家的 份额不会超过10%，虽然这个代币可能不会显示出令人难以置信的增长，但它可以是一个非常稳定的投资，因为它的波动最小。

Countries:	比例:
墨西哥	10.4%
俄罗斯	9.2%
巴西	9.1%
希腊	8.5%
土耳其	7.7%
南非	7.0%
中国	6.0%
波兰	5.7%
匈牙利	5.5%
罗马尼亚	5.2%
马来西亚	5.2%
菲律宾	4.9%
其他	15.6%

八、万物魔坊AMFC账户

在比特币及其衍生系统中，是没有一个所谓的账户来存储用户的余额的，用户的余额是通过整个系统的交易状态转换来实现的。这里要引入一个术语，UTXO（unspent transactionoutputs），即未花费的交易输出。每个 UTXO 都有一个面值和所有者，一笔交易包括一个或多个输入和一个或多个输出。每个输入包含一个对现有 UTXO 的引用和由与所有者地址相对应的私钥创建的密码学签名，如果一个用户拥有这个私钥，那么他就可以消费这个 UTXO 对应的币值，也就是说一个用户的余额就是他所有拥有的所有私钥对应的 UTXO 的币值总和。

UTXO 主要优点是高度的私密性，用户可以为每一笔交易生成一个新的地址，从而使得用户无法被追踪，这对于货币来说是好事，但对于各式各样的 DAPP 来说，就未必了。账户相对于 UTXO 来说，有以下几个优点：

- 节省空间。举例来说，如果某个用户有 5 个 UTXO，需要的存储空间是（20 + 32 + 8）
- 5 = 300 字节（其中 20 字节为地址，32 字节为交易号，8 字节为交易额），而账户需要 20+8+2=30 字节（20 字节位地址，8 字节位余额，2 字节为随机数）；

- 利于监督。账户存在使得电子货币很容易被区分，因为我们只要知道这些币来自哪些账户即可；
- 简单、易于编码和理解；
- 常量级引用。轻客户端能以常数时间访问一个用户的账户任意数据，而在 UTXO 系统中，每当有交易发生时，数据引用将发生变化。

万物魔坊（AMFC）本身并不是一个纯粹的货币系统，要容纳各种各样的应用，综合比较起来，账户对于我们来说是一种更好的选择。

和比特币不同，万物魔坊（AMFC）每个账户由一个口令、一对公私钥、一个地址组成，用户可以额外设置一个二级密码。为了更好的助记，我们将 128bit 长度的熵转换成 12 个单词。口令由用户保管，不对外公开，一单失去用户将失去对应账户的所有权。

九、信用体系

1、什么是信用体系?

万物魔坊（AMFC）的信用体系是系统对参与系统者的反馈过程。因为万物魔坊（AMFC）团队认为，获得系统嘉许的不该是既得利益者的不劳而获（pos），也不该是弱肉强食的强者恒强（pow），系统的朋友是活跃于系统，真心为系统贡献的劳动人民。因此,万物魔坊（AMFC）引入信用体系，实现这一理念。

2、万物魔坊（AMFC）为什么需要信用体系?

这里只分析一个最重要的原因，万物魔坊（AMFC）是一个商用的区块链底层平台。既然商用，节点的行为类型会比以往的其他区块链公链多很多。因此，需要用有效的办法规范节点的行为，形成稳

定的秩序，适合商用的同时可以避免链上的权限被人滥用，造成垃圾数据膨胀。

万物魔坊（AMFC）的代币需要流通，因此不适合作为规范节点行为的中介。因此万物魔坊（AMFC）提出代币与信用的双中介体系。顺应万物魔坊（AMFC）的商业落地和用户流量路线，设计信用体系作为规范用户行为一种管理和价值纽带。

3、万物魔坊（AMFC）的信用体系

基于区块链的信用体系，有可能会掀起大的浪潮。万物魔坊（AMFC）的信用体系结合商业性质，已有初级雏形。信用作为规范用户端行为的准则，不能变现和流通，是用户良好行为习惯的一种体现。

信用的用途包括但不限于参与共识、转账手续费打折、修改别名、转让商品、申请高级仲裁、参与股权企业有针对性的活动等等。万物魔坊（AMFC）目前已实现利用信用参与共识、共识违规信用处罚、修改别名消耗信用、转让二手商品消耗信用。信用作为整个系统的价值中介之一，会陆续利用其纽带作用开发更多用户行为准则。

信用的获得：信用作为和代币平行的价值中介，其获得不需要实际利益上的代价，

仅仅是遵守系统规则，保持良好的用户习惯，即可获得。

十、关系型数据库

目前大多数的区块链系统都选择使用模型较简单的非关系数据库来存储数据，

比如berkeley db，leveldb 等，这些数据库一般都提供一些简单的数据结构，比如 btree、hashtable、queue 等，它们一般不支持 SQL 对数据进行操作，虽然这些数据库对于一般的电子货币系统来说足够了，但对于应用平台来说是远远不够的，特别是对于金融、银行、电子商务等领域， 目前主流的存

储系统都是采用了关系数据库，因为关系数据有以下几个优点：

- 事务处理；
- 数据更新开销非常小；
- 可以进行 join 等复杂查询。

万物魔坊（AMFC）选择的 sqlite 是一种性能极佳的轻量级嵌入式关系数据库，容量最高支持 2T，数据文件可在不同字节序机器之间自由共享，特别是对 SQL的支持，将为 dapp 开发者提供极大的便利。

十一、POC 共识机制

任何区块链项目，都需要共识机制使分布在全球各地的对等节点、对数据的状态达成一致性。万物魔坊（AMFC）旨在开发一套高效、可自我维护的共识系统以适应万物魔坊（AMFC）的商业定位，POC 共识由此而生。

POC 的全称 Proof of Credit，中文名信用共识机制，简称 POC。

万物魔坊（AMFC）的 POC 共识机制解决了POW 的性能问题，解决了 POS 的权益不均问题，解决了 DPOS 的违规处理效率问题。

那么 POC 到底是什么样的呢?

POC 是基于万物魔坊（AMFC）信用体系基础上，使用信用准入，利用现有区块链账簿唯一性和确定性，协调各节点进行单点广播权限确定和可验证的系统。

1、共识准入

作为一条公链，共识节点涵盖了用户端，必须规范用户行为，才能使整个网络按照协议稳定安全的运行。POW 利用算力竞争规范节点，POS 利用持有代币数量和币龄规范节点行为，DPOS 利用投票选举受托人；这几种目前流行的共识，原理上除了 POW（其实 pow 的难度调节也是利用的已有账簿）之外都是利用账簿的确定性进而选出具有单点广播权限的节点。所以只要根据链上账簿数据确定性，进行共识集合顺序出块即可。

万物魔坊（AMFC）的共识门槛是信用达到一定值，即可参与。这种准入方式有一定的难度需要时间累积信用，作为开源公链，攻击者很有可能利用很长的时间做准备，发起一次对网络共识的攻击。

所以万物魔坊（AMFC）引入经济制裁机制杜绝这种情况的出现，因为攻击者发起攻击获得的收益并不会比损失大，这就是在信用准入的基础上增加保证金机制作为辅助。有人说：直接提交保证金不就行了，信用准入是多余的！原因是共识的情况极其复杂，有的情况是不适于经济制裁的，比如共识节点电脑死机，网络掉线， 若没有信用准入，那么系统无法甄别并排除这类节点，若统一采用经济制裁的方式，势必将大批用户拒之门外。另外，信用保证系统的权力不被大量持币者垄断。信用作为底层的价值中介之一，日后会有更加广阔和重要的用途。

2、浮动保证金机制

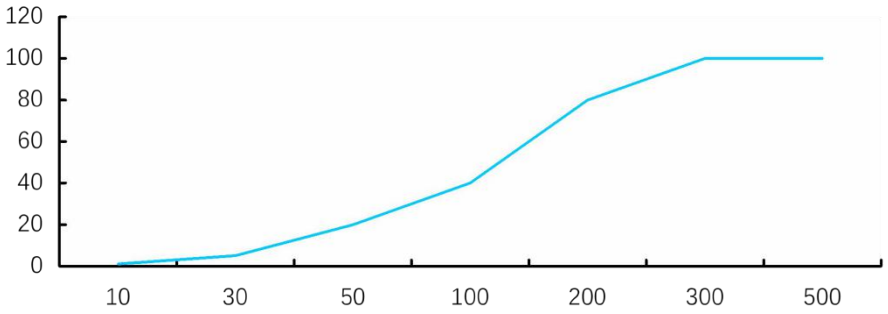
因为万物魔坊（AMFC）的共识无需节点之间频繁来回的通讯即可达成共识（下面有介绍）， 所以万物魔坊 (AMFC) 的性能是不受共识节点多少影响的，100 个节点和 1000 个节点的性能几乎一样。故万物魔坊（AMFC）采用创新的浮动保证金机制来平衡共识节点的收益。

万物魔坊（AMFC）网络通过当前共识节点数和一个线性增长算法，来动态计算当前参与共识所需

保证金。

recognizance = maxRecognizance * ((Math.log(size/Math.log(2)) * size)

/Math.log(maxSize/Math.log(2))



从上面的保证金计算公式可以看出，参与共识所需保证金，随着共识节点数量的增加成线性增长，当共识节点数量达到最大数量时，保证金也达到最大值。

3、全网效验

任何节点的共识申请和退出，都会被全网进行严格的效验。

3-1、信用的效验

当任何节点申请成为共识节点时，其它节点都会首先验证该节点的信用值， 若发现信用值低于准入门槛，那么该节点的该次请求会被丢弃。

3-2、保证金的效验

任何申请共识的请求，都必须提交相对应的保证金。和转账的不同之处在于， 提交的保证金接收方是一个智能合约脚本，该脚本对保证金的赎回进行了强制的规范。全网不止会对申请共识请求的信

用和保证金做效验，对保证金安全作了最高级别定义。

3-3、保证金的赎回效验

万物魔坊（AMFC）的共识协议有经济制裁制度，故节点提交的保证金，并没有采用传统冻结的方式；系统运行过程中，一旦发现有严重违规的节点，任何诚信节点可罚没该违规节点的保证金。节点的保证金实际上提交到了一个智能合约脚本，处于无主状态，为保证这部分资金的安全，任何退出共识或者处罚请求，都会被严格的效验，效验规则里面包含了严格的效验协议，任何人想领走别人的保证金，那是不可能的事，任何人想罚随意没别人的保证金，那也是不可能的事。

3-4、制裁效验

万物魔坊（AMFC）的每一个区块头部，都有出块人的签名，所以当有人试图作恶，必然会留下密码学证据，以便追责。

当共识节点超时出块，或者由于死机掉线等非人为因素不能出块时，全网能监控感知，并在第一时间将该节点降级为普通节点。这种情况虽然没有密码学证据，但依然需要提供全网其它节点能对其效验的证据。

任何节点要对其它节点实行制裁，必须提供合理的或者带有密码学的证据， 这样才会被全网其它节点效验并接受。

4、确定单点广播权限

结合前面几小节提到的理论知识，本小节将提供更全面 POC 运行原理和细节。

名词解释：

共识节点：达到信用准入门槛并成功申请共识的节点

共识轮次：所有共识节点轮流出块的完整时间段，称为一个共识轮次。每个共识轮次都有开始时间戳和结束时间戳，上一轮次的结束时间为当前轮次的开始时间，所以节点必须按照这个时间规则进行下去，否则任何的改动都会被全网排斥。在每个共识轮次中，所有共识节点有且只有一次广播区块的权力。

共识顺序：在一个共识轮次中，每个共识节点出块的顺序，叫做共识顺序。在万物魔坊（AMFC）的共识中，每轮的顺序都是随机变化的，根据当前轮次的开始时间戳（也就是上一轮的结束时间戳）与共识节点账户、通过算法排序决定。所有节点（包含非共识节点）必须遵守这个规则，才能正常运行，任何哪怕是细微的改动，都会导致改动的节点被全网排斥。

共识时段：在确定了共识顺序之后，每个节点都被映射到一个时间段上面， 这样自然就确定了单点广播权限，这个时间段也有开始时间和结束时间，间隔是区块出块时间，称为共识时段。

区块权限验证：每个区块头部，都有当前轮次的开始时间、共识节点的时段信息、共识节点的签名，通过这些信息对区块的合法性进行验证。

POC 完整的运行流程：

1. 申请共识
2. 效验信用和保证金
3. 申请包含进区块，被确认

4. 等待当前共识轮次结束

5. 当前共识轮次结束，下一轮共识开始，下一轮变当前轮

6. 确定当前轮次共识人数

7. 初始化当前轮次共识顺序，各自节点计算出自己的共识时段

8. 接收新块，并进行区块权限验证和容错监控，等待自己共识时段的到来

9. 到了自己的共识时段开始时间，开始打包区块

10. 打包程序从内存池中获取新交易并验证

11. 预估到了自己的共识时段结束时间，停止打包

12. 询问容错监控器是否有违规需要处理，发放信用

13. 验证区块交易数据

14. 广播区块到全网

15. 继续接收新块，并进行区块权限验证和容错监控，等待下一轮开始

5、容错监控与处罚机制

区块链系统是非常复杂的系统，不单因为底层技术的复杂，更因为其运行的环境极其复杂，尤其是公有链。使用习惯、网络环境、人为破坏等都有可能影响系统的正常运转。区块链的共识机制，能有效的解决这些因素带来的影响。

对于万物魔坊（AMFC）的 POC 共识机制来说，节点的任何动作，都会被全网其它节点监督。万物

魔坊（AMFC）创新的共识会对以下这些情况做出相应的处罚，整个系统会自身调节、维护稳定。

1. 不出块，扣除一定的信用值，并降级为普通节点。

2. 不按时出块或者网络同步延迟等非人为因素，会根据全网其它节点的选择作决定，若下一区块引用了这个块，那么正常相安无事；若下一区块丢弃了该块，那这个块将会成为孤块，其面临的结果是信用处罚并降级为普通节点。

3. 非共识节点胡乱广播区块，验证不通过，直接丢弃。

4. 同一时间段广播多个块，属于严重违规，会被没收保证金并信用拉黑。

5. 打包双花交易，属于严重违规类型，会被没收保证金并信用拉黑。

6. 从链上的旧块处尝试分叉系统，所谓的双花攻击，属于严重违规类型，会被没收保证金并信用拉黑。

7. （4）、（5）、（6） 这三类严重违规类型，全网可监控，并有密码学证据，任何诚信节点只需提交包含其签名的一个或多个区块头信息即可行驶处罚权力，没收该节点的保证金到社区基金账户，并扣除该节点 999999 点的信用值，被处罚的节点永久无法再次作恶。

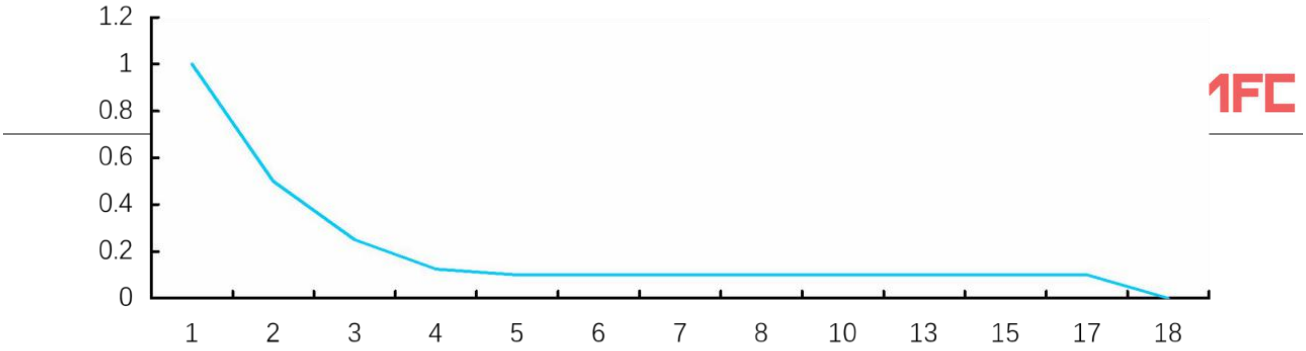
6、POC 总结

POC 的最大亮点是及时的处理作恶情况，系统自身高效的维护，虽然在技术实现上的难度非常大，但是万物魔坊（AMFC）团队做到了。

团队已有持续优化完善的方案，使 POC 不断完善以满足持续增长的商业需求。

1. 节点之间通讯，引入先进的压缩技术。

2. 优化新区块同步到全网的流程。



3. 实现隔离见证技术，减少新区块广播大小。

4. 通过以上 3 点优化改进，能大大提高整个网络的 TPS。

十二、激励机制

和其它公有链一样，万物魔坊（AMFC）对共识节点有奖励政策。奖励部分是总量的 10%， 通过新块的 coinbase 交易逐步分发。万物魔坊（AMFC）的区块出块间隔时间是 10 秒，第一年每个块产出 1AMFC，以后每年减半，直到达到每个块 0.1AMFC，以后保持这个值。万物魔坊（AMFC）的共识奖励部分，大概 17 年分发完，后面会逐步强制要求股权企业建立节点维护网络。

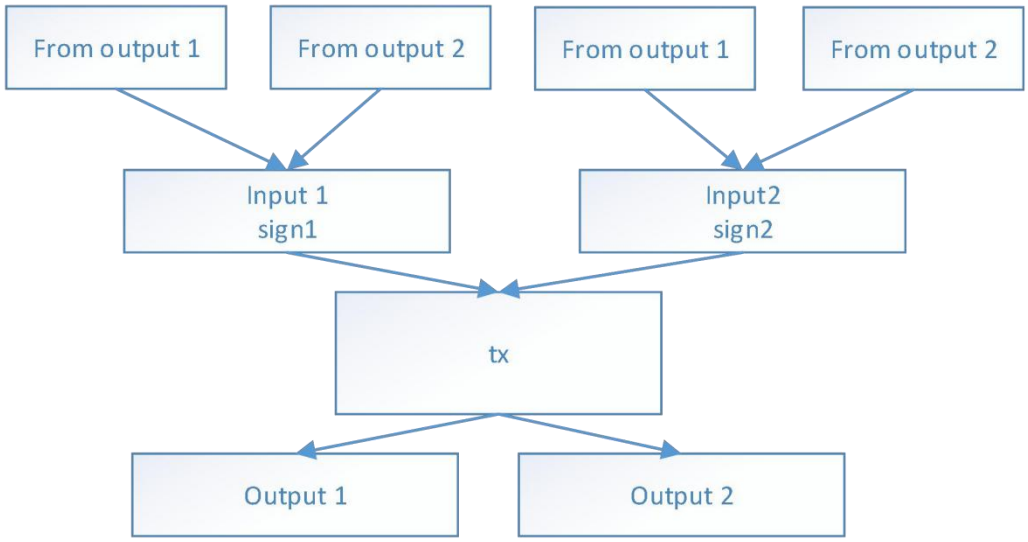
十三、账户分级认证系统

万物魔坊（AMFC）系统账户分为管理员账户、认证账户、普通账户、子账户。

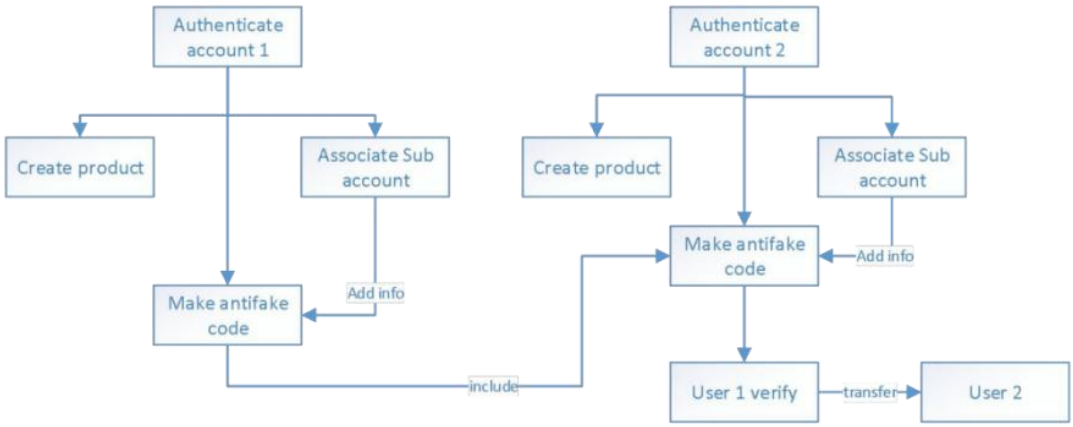
- 管理员账户：仅仅是多一个注册股权企业的权限，其它方面和认证账户没有区别。
- 认证账户：万物魔坊（AMFC）前期会充当股权企业接入审查者角色，后面适当的时候，与第三方机构合作，把这部分权限通过接口的方式移交出去。
- 所有认证账户，必须由管理员账户签名后，才会被万物魔坊（AMFC）接受。
- 普通账户：万物魔坊（AMFC）的广大用户群体，所使用的账户。包括万物魔坊（AMFC）客户端的基本功能、验证商品、转让商品等功能。

- 子账户：认证账户可关联普通账户为其子账户，关联之后子账户可为认证账户生产的商品添加溯源流转信息。

十四、改进的UTXO 交易模型



万物魔坊（AMFC）的交易模型，大部分采用的是 UTXO 模型。结合万物魔坊（AMFC）的账户系统，改进了 UTXO 模型以提高效率和减少交易大小。



改进详情：合并同一账户的多个交易输入引用，采用一个签名。

十五、专为商业应用而设计的通用底层协议

万物魔坊（AMFC）的底层为商业应用而设计，目前已完成的一套应用协议，能适应众多业务场景。

- 认证账户资料和商品资料的灵活性，使用通用的 key value，能录入任何形式的资料信息。
- 认证账户创建商品。
- 认证账户生成指定商品的全网唯一身份 ID（在系统里面叫做防伪码）。
- 认证账户关联子账户。
- 认证账户关联的子账户对商品唯一 ID 关联流转信息（流转溯源信息）。
- 认证账户在生成商品唯一身份 ID 时，能引用其他商品的全网唯一身份 ID。
- 普通账户对商品唯一 ID 的验证。
- 普通账户对商品验证后的归属权进行转让。

以上业务流程协议，在万物魔坊（AMFC）客户端（钱包）里面已实现，并通过 PRC 的方式，对所有第三方开放。

十六、万物魔坊（AMFC）的商业应用及落地规划

1、令牌系统

使用万物魔坊（AMFC）工具创建的第一个 hello world 应用，就是一个最基本的令牌系统了。开发者可能不需要编写代码，只要在 genesis.json 文件里修改一些创世参数，就可以发布一个令牌系统了。万物魔坊（AMFC）系统中的令牌与以太坊的子货币一样，可以表示黄金、股票、抵押物、或任意

其他资产，这些令牌可以与转入侧链中的 XAS 通过去中心化的方式进行交易，从而实现流通，也可以在中心化的交易所与其他货币进行交易。

2、交易合约

假设一个买家想跟一个不认识的人进行交易，一般情况下如果交易顺利进行的话，双方都不希望有第三方介入，但是如果某个环节出了问题，比如买家对商品不满意时，他们就希望有一个中间人来做调解。这个中间人可能会要求买卖双方出示一些证据，然后做出判决， 比如把钱退还一部分给买家。这个业务流程如下：

- 买卖双方共同选择一个中间人；
- 买家使用三方的公钥创建一个 2-3 的多重签名账户，然后转账到这个账户，再以该账户为发起人，以卖家的账户为接收人，签署一个交易并发布出去。此时这个交易是不能立即被确认的，只有 3 个人中的 2 个人共同签名，才会生效；
- 卖家发货给买家；
- 如果买家收到货物后，检查没问题，使用自己的私钥对刚才的交易进行签名。然后卖家再次签名后，交易就顺利完成；
- 如果买家对货物不满意，可以向中间人发起申诉并出示证据，卖家也可以出示证据， 最终由中间人与买卖其中的一方达成一致，共同签署，完成交易，结束仲裁。

3、去中心化交易所

根据是否支持法币，可以分为两种程度的去中心化。如果不支持法币，可以实现完全的去中心化，如果支持法币，则只能实现半去中心化，即法币通过网关出入，但交易信息公开。完全的去中心化交

易所又分为两种，一种是点对点的交易，通过万物魔坊（AMFC）系统提供的“跨链交易 api”来实现。另一种是挂单交易，挂单交易要求卖方从其他区块链转入一定的资产到万物魔坊（AMFC）侧链中，这个转入操作通过父链冻结资产的 SPV 证明达成。此外，由于关系数据库的支持，利用联表查询和索引功能，可以很容易的实现一个效率不错的撮合引擎。

4、存在性证明

存在性证明可以用于登记文件版权、专利等，其基本原理是将要存储的文件的哈希值存入到万物魔坊（AMFC）的侧链中，以此来证明某个特定文件存在，还可以加上时间戳、当事人的数字签名等元数据，来证明他们是在何时持有这些文件的。这些信息无法伪造、无法篡改，不会暴露数据和隐私，在需要的时候随时可以验证且不依赖第三方机构。

5、物联网

物联网中存在海量的联网设备，很难有一个中央机构来管理所有的设备和各节点的身份。万物魔坊（AMFC）的侧链是一个很好的解决方案，首先，它解决了节点间信任问题，设备间彼此相连形 成分布式网络，通过共识算法来保证设备间交易的合法，并且可追踪、可审查、可分析。其 次，不同种类的设备可以接入不同的侧链，这是我们前面提到的天然分片机制，避免了总账 本的爆炸式增长。我们试想下，在一个基于区块链的物联网中，一个自动售货机不但可以监 控和报告它自身的存货，还可以通过分析历史交易数据智能地从分销商那里进行招标并自动 完成付款。

十七、万物魔坊（AMFC）后继规划

- 对应国家上市股票区块链发行。
- 纽约证交所、东京证交所、伦敦证交所和纳斯达克证交所平台，支持 AMFC支付购买。

- 结合万物魔坊（AMFC）代币，为股权企业开发更多营销工具。

- 打通产业链上下游，打造供应链金融中心。

十八、万物魔坊（AMFC）后继商业整合

1、万物魔坊（AMFC）为企业提供资产发行交易服务

万物魔坊（AMFC）为注册认证企业提供资产发行功能。说明资产的功能和承诺。经过万物魔坊（AMFC）委托的第三方公证公司公证后，通过审核即可发行自己的资产。企业可对资产设置白名单。只有在白名单内的账户可交易该资产。用户可设置自己的白名单资产。加入名单的即可接受其他账户该资产的转账。资产可申请在万物魔坊（AMFC）公链网络内置交易市场交易。万物魔坊（AMFC）交易市场具有特殊的公平交易机制。用户可尽享资产增值、自由交易的乐趣。

万物魔坊（AMFC）是创建在基于区块链的智能合约。 每个需求方需要使用兼容ERC-20的钱包。要购买万物魔坊（AMFC），买方需要将支持的加密货币转移到智能合约地址。 智能合约将万物魔坊（AMFC）转回买家的地址。 在ICO之前或之后发生的任何付款将被返回，而不会发布任何万物魔坊（AMFC）。

万物魔坊（AMFC）将参与公司的利润再分配，并可能是未来的被动收入的来源，我们认为，这个代币的价值将随着时间而增长，与已发出的加密货币的数量呈正相关。

它是基于目前最为领先的ICO的标准区块链协议的的区块链。

十九、万物魔坊（AMFC）的发展路线图

二十、风险

我们的加密货币与相应的指数和股票价格是相关联的。虽然价格在短期内可能会下降，但投资者的普遍共识是长期稳定增长。

美国股市的每年平均收益率约为6-7%。在复合增长理论下，您的资本预计在11-12年将翻一番。如果您购买万物魔坊（AMFC），您将投资于这一细分市场中最可靠的公司。这包括已被Warren Buffet, George Soros和David Einhorn等市场上最大的投资者投资的苹果股票（AAPL），他们依赖于稳定和可预测的增长，而比特币和并非如此，它们是高度挥发性的。

二十一、免责声明

该文文档只用于传达信息之用途，并不构成买卖 万物魔坊（AMFC） 的相关意见。以上信息或分析不构成投资决策。本文档不构成任何投资建议，投资意向或教唆投资。

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。

相关意向用户明确了解 万物魔坊（AMFC） 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。

万物魔坊（AMFC） 团队不承担任何参与 万物魔坊（AMFC） 项目造成的直接或间接的资产损失。

万物魔坊（AMFC）智能合约（发行代币）新定义函数类型

Name（名称）

```
function name() view returns (string name)
```

Symbol (符号)

```
function symbol() view returns (string symbol)
```

Decimal(小数点)

```
function decimals() view returns (uint8 decimals)
```

Total supply (总额)

```
function totalSupply() view returns (uint256 totalSupply)
```

Balanceof (余额)

```
function balanceOf(address owner) view returns (uint256 balance)
```

Transfer(转账)

```
function transfer(address to, uint256 value) returns (bool success)
```

Transferfrom(转出)

```
function transferFrom(address_from, address_to, uint256_value) returns
(bool success)
```

Allowance（批准额度）

```
function allowance(address_owner, address_spender) view returns (uint256
remaining)
```

Event 事件

Transfer (转账)

```
eventTransfer(address indexed from, address indexed to, uint256 value)
```

Approval(批复)

```
eventApproval(address indexed _owner, address indexed _spender, uint256
value)
```

万物魔坊（AMFC） MVM 对以太坊 EVM 的改变（指令集）

0s: Stop and Arithmetic Operations（停止和代数运算指令集）

指令代码	助记词	EVM 语义	MVM 语义
0x00	STOP	停止	相同
0x01	ADD	相加	相同
0x02	MUL	相乘	相同
0x03	SUB	减	相同
0x04	DIV	除	相同
0x05	SDIV	整除	相同
0x06	MOD	模(余)	相同
0x07	SMOD	代符号求模	相同
0x08	ADDMOD	相加后求模	相同
0x09	MULMOD	相乘后求横	相同
0x0a	EXP	幂去处	相同
0x0b	SIGNEXTEND	符号扩展	相同

10s: Comparison & Bitwise Logic Operations(比较和位运算指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x10	LT	小于比较	相同
0x11	GT	大于比较	相同
0x12	LGT	带符的大于比较	相同
0x12	SGT	带符的小于比较	相同
0x14	EQ	相等比较	相同
0x15	ISZERO	是否为零	相同
0x16	AND	并	相同

0x17	OR	与	相同
0x18	XOR	与或	相同
0x19	NOT	非	相同
0x1a	BYTE	取字节	相同

20s: SHA3 (SHA3	指令集)		
指令代码	助记词	EVM 语义	MVM 语义
0x20	SHA3	计算 SHA3	相同

30s: Environmental Information(环境信息指令集)			
指令代码	助记词	EVM 语义	MVM 语义
0x30	ADDRESS	获取账户地址	相同
0x31	BALANCE	获取余额	相同
0x32	ORIGIN	获取发送者地址	不同
0x33	CALLER	获取调用者地址	相同
0x34	CALLVALUE	获取转账金额	相同
0x35	CALLDATATOTAL	获取参数数据	相同
0x36	CALLDATASIZE	获取数据大小	相同
0x37	CALLDATACOPY	参数拷贝到内存	相同
0x38	CODESIZE	获取代码大小	相同
0x39	CODECOPY	代码拷贝到内存	相同
0x3a	GASPRICE	获取燃料价格	不同
0x3b	EXTCODESIZE	获取代码大小	相同
0x3c	EXTCODECOPY	代码拷贝到内存	相同

0x3d	RETURNDATASIZE	数据大小	相同
0x3e	RETURNDATACOPY	数据拷贝到内存	相同

40s: Block Information(区块信息指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x40	BLOCKHASH	获取区块的哈希	不同（不需要）
0x41	COINBASE	受益人地址	不同（不需要）
0x42	TIMESTAMP	时间戳	不同（不需要）
0x43	NUMBER	区块编号	不同（不需要）
0x44	DIFFICULTY	区块的难度	不同（不需要）
0x45	GASLIMIT	燃料限额	不同（不需要）

50s: Stack, Memory, Storage and Flow Operations(栈、内存、存储、控制流操作指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x50	POP	弹出数据	相同
0x51	MLOAD	内存加载 word(M)	相同
0x52	MSTORE	保存 word 到内存	相同
0x53	MSTORE8	保存字节到内存	相同
0x54	SLOAD	加载一个 word(S)	相同
0x55	SSTORE	保存 word 到存储	相同
0x56	JUMP	跳转指令	相同
0x57	JUMPI	条件跳转指令	相同
0x58	PC	计数器的值	相同
0x59	MSIZE	获取内存大小	相同

0x5a	GAS	获取可用燃料数	不同
0x5b	JUMPDEST	跳转目的地	相同

60s & 70s: Push Operations(压栈操作指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x60	PUSH1	1 字节压入栈顶	相同
...	...	...	...
0x7f	PUSH32	32 字节压入栈顶	相同

80s: Duplication Operations(复制操作指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x80	DUP1	1 对象复制	相同
...	...	...	...
0x8f	DUP16	32 对象复制	相同

90s: Exchange Operations(交换操作指令集)

指令代码	助记词	EVM 语义	MVM 语义
0x90	SWAP1	交换 1 和 2 对象	相同
...	...	...	...
0x9f	SWAP16	交换 1 和 17 对象	相同

a0s: Logging Operations(日志操作指令集)

指令代码	助记词	EVM 语义	EVM 语义
0xa0	LOG0	不设主题	相同

THE EHD

以顶尖区块链技术引领全球资产数字化进程

AMFC

版本：0.8.1

2018-07-01