



JMT

基于抗量子共识算法（FRMH1.0）
增强区块链安全性的积分公链系统

2020.7 JMT 团队

目录

一. 概述.....	3
1. 综述.....	3
2. 区块链技术.....	3
二. JMT 的使命、目标与创新.....	4
1. 问题总览.....	4
2. 什么是 FRMH1.0 共识算法?	4
3. JMT 的优势.....	4
3.1. JMT 大幅度地提高了区块链的安全性能.....	4
3.2. JMT 可抵抗量子计算机的攻击.....	4
3.3. JMT 具有广泛群众性.....	5
3.4. JMT 是具有多种奖励分配模式（两挖）的积分公链.....	5
3.5. JMT 有抗量子攻击的安全智能合约开发平台.....	5
3.6. JMT 实行的叔块奖励具有公平性.....	5
三. 前期平台模型.....	7
1. 前期边缘计算层级.....	7
2. 前期 JMT 技术架构.....	8
3. 前期应用架构.....	9
四. 前期生态场景.....	10
1. 前期生态概述.....	10
2. 生态场景一-智能硬件.....	10
2.1. JMTime 成就.....	10
3. 生态场景二-JMT 即时支付.....	10
五 JMT 发行计划.....	12
5.1. 出块速度.....	12
5.2. 奖励机制.....	12
六 JMT 路线图.....	13
1. 第一阶段.....	13
2. 第二阶段.....	13
3. 第三阶段.....	13
七 JMT 的治理结构.....	14
1. 新加坡海外基金会主体.....	14
2. 海外基金会人事架构.....	14
八 团队介绍.....	15
九 结语.....	16
十 风险警示.....	17

一. 概述

1. 综述

过去，我们区块链的挖矿常常被高算力所苦恼，人们为获得打包权，不断地对挖矿设备进行更新换代，从 CPU,GPU 到芯片一代，二代，三代.....等专业“矿机”不断被研发出来投向市场；这让依据算力公平分配奖励的机制，演变为了对矿机算力的大举投入，扭曲了中本聪的设计初衷，浪费了大量的人力和物力。

现在，JMT 通过 FRMH1.0 共识算法，对高算力进行双重调节处理，对算力猛增的风险具有控制能力，可抵抗量子计算机的攻击；同时大幅度地提高了区块链的安全性，缩短了区块链达成共识的时间，加快了区块链上交易速度，拓展了区块链的应用边界，从根本上解决信任和安全问题。

2. 区块链技术

2008 年，中本聪第一次提出了区块链的概念。广义来讲，区块链技术是利用块链式数据结构来验证与存储数据、利用分布式节点共识算法来生成和更新数据、利用密码学的方式保证数据传输和访问的安全、利用由自动化脚本代码组成的智能合约来编程和操作数据的一种全新的分布式基础架构与计算范式。

区块链的特点是去中心化、系统开放、自治性、信息不可篡改、匿名性，这些特性使得区块链得到了广泛的应用。

二. JMT 的使命、目标与创新

1. 问题总览

如前所述，随着区块链应用的落地，信任和安全问题日益突出。通过 JMT 的独特区块链技术，赋能抗量子计算机和快速交易，从而为区块链应用的大面积推广提供保障。

2. 什么是 FRMH1.0 共识算法？

FRMH1.0 共识算法即模糊随机碰撞工作量证明 (fuzzy random proof of work) 共识算法，它是基于 n 阶模糊伪随机矩阵的模糊传递闭包阵加密后再进行哈希二次加密的双重加密共识算法。其中模糊矩阵的阶数 n 和 hash 值前 0 的个数 p 是随算力的大小自动调节，分为线性调节和几何调节，具有双重智能调节机制。

3. JMT 的优势

3.1. JMT 大幅度地提高了区块链的安全性能

众所周知哈希加密算法的解空间为 2^{256} ，而 jmt 的双重加密算法解空间为 $n^4 \times 2^{256}$ ，当 $n=10$ 时 则解空间为比特币（包括以太坊）共识算法的 10000 倍，大幅度提高了安全保障性，且随着 n 的增大，其安全性能呈几何级数的增长。

3.2. JMT 可抵抗量子计算机的攻击

一般的普通电脑要破解哈希加密算法的解空间几乎是完全不可能的，这就是比特币（包括以太坊）至今未被攻破的原因。但是 1 台量子计算机约相当于 10^5 台普通电脑的算力，如用量子计算机来破解哈希加密算法的解空间，那只是分分秒秒的事，一旦量子计算机出现，哈希加密算法毫无秘密可言，现今的比特币（包括以太坊）亦就荡然无成。而 JMT 使用的 FRMH1.0 共识算法是双重加密共识算法，且其中模糊矩阵的阶数 n 和 hash 值前 0 的个数 p 是随算力的大小自动调节，虽然 hash 值前 0 的个数 p 是有限的（最多 2^{256} 个），但模糊矩阵的阶数 n 却是变动调节且是可无限大的，量子计算机运算速度再快亦总是有限的，从理论上讲用无限抵抗有限总是可行的。事实上，经测算如果有 1 亿台量子计算机来挖 JMT，JMT 链对其仍调节有余。即是说 JMT 亦是一条可抗量子攻击的具有真正共识机制意义的公链。

3.3. JMT 具有广泛群众性

由于 JMT 的 pow 挖矿实行双重调节（线性调节与几何调节），对任何算力都具有智能控制和调节的能力，使其按 JMT 即定的平均出块速度出块和达成共识，即是说 JMT 不会被高算力所左右和俘获，普通电脑均可挖矿，具有广泛群众性。

3.4. JMT 是具有多种奖励分配模式（两挖）的积分公链

除 pow 挖矿分配奖励外，同时 JMT 还实行了特别的积分奖励分配模式：分布式存储和物联网边缘计算应用积分奖励分配，因此 JMT 是一条具有两种分配模式（两挖）的公链。实现了节约能源，充分地利用了设备的边缘计算能力。

3.5. JMT 有抗量子攻击的安全智能合约开发平台

Jmt 的智能信任合约作为一种通过信息化的方式传播、验证和执行的计算机协议。JNT 链作为图灵完备的智能合约系统加上 JMT 提供的安全信任保障，可以满足开发者编写任意复杂的，存在于 JMT 链上并且能在 JMT 链上传播的合约。开发者可以完全安全信任地在 JMT 链上实现定制货币，金融衍生品、身份系统和去中心化组织等功能。

且 JMT 链设定的交易与运行智能合约的费用较低（约为以太坊的三分之一），以此鼓励在 JMT 链上的交易和合约的运行。

3.6. JMT 实行的叔块奖励具有公平性

JMT 实行叔块节点奖励，用于鼓励勤劳的矿工，体现了区块链的公平性。

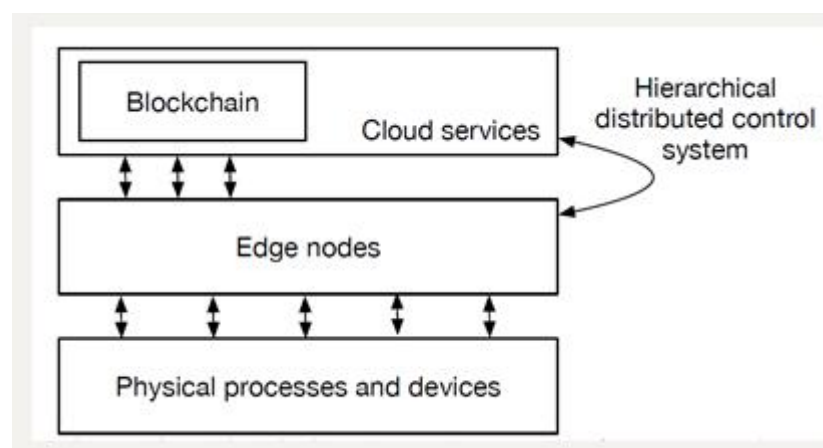
三. 前期平台模型

JMT 前期的任务是用区块链赋能边缘计算，打造安全的万物互联的去中心化网络，用边缘计算分配 JMT 通证。

JMT 会推动现有价值属性的物联网数据资产的交换，交互以及流动。通过合约和配置，从而产生新的比特资产。JMT 将区块链这项未来最重要的底层技术，与边缘计算这一最重要的社会资源结合在一起，一定会释放出极大的商业价值和社会价值。JMT 的使命和愿景，就是构建于此。我们已经开发了一系列基于区块链和边缘计算的应用产品。其中，最底层的就是我们的 JMT，前期 JMT= 区块链 + 边缘计算。

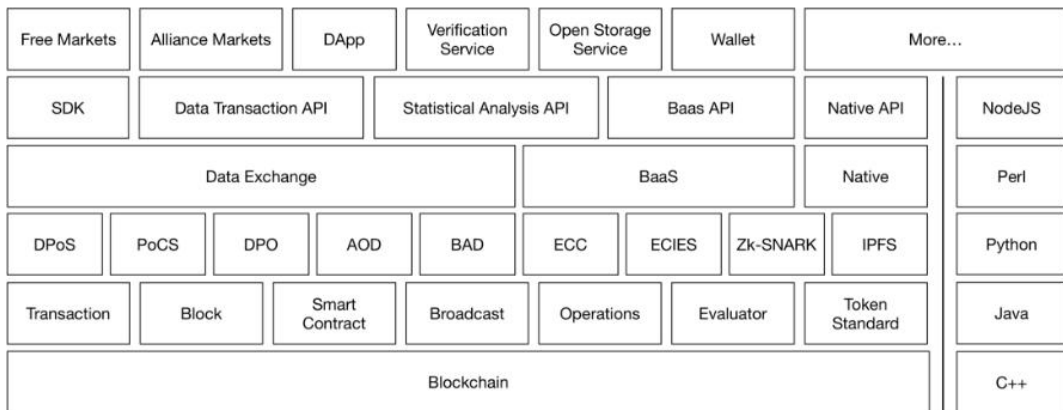
1. 前期边缘计算层级

边缘计算有四个领域：设备域（感知与控制层）、网络域（连接和网络层）、数据域（存储和服务层）、应用域（业务和智能层）。这四个“层域”就是边缘计算的计算对象。对于各层级独有的业务，只需在对应层级独立部署针对性的计算能力。JMT 使用区块链技术进行分布式层级控制。



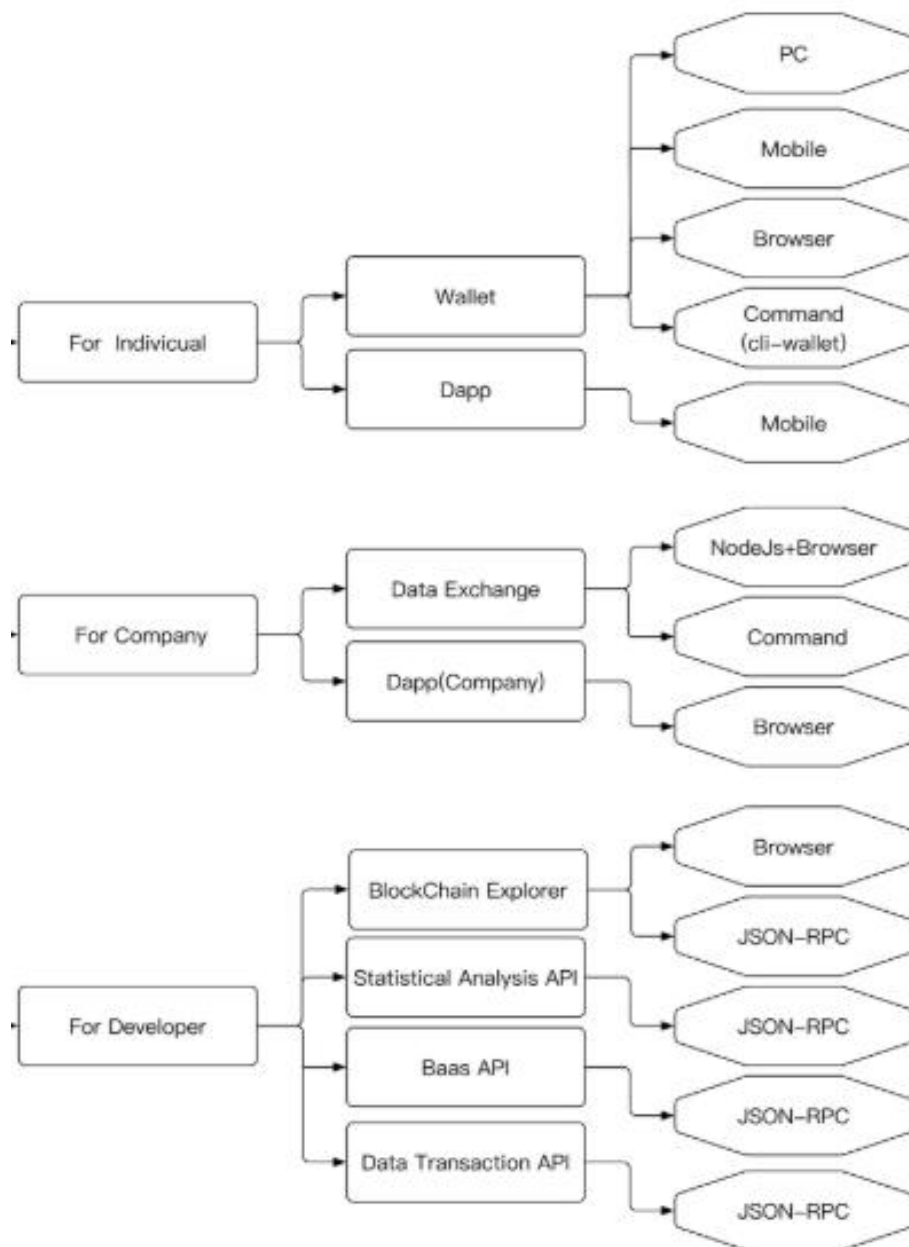
在边缘计算模型中，需要计算接近数据。但是，在某些使用情况下，需要为更复杂的算法提供更高的级别，需要对分布式控制系统的运营进行战略决策，并且该部分被提议在区块链上执行，通过智能合约在所有网络节点上实现的，这些合约是存储集合程序，只是等待事件发生才能执行。

2. 前期 JMT 技术架构



3. 前期应用架构

JMT 平台面向个人用户、企业用户、开发者三个方向上规划了丰富的应用和服务。



四. 生态场景

1. 生态概述

当前高清视频、VR/AR、大数据、物联网、人工智能的发展，传输需求剧增，仅通过集中式大型云计算中心，很难承担所有数据的存储、计算及交互，将给网络带宽带来极大压力，这要求 CDN 必须从传统的以缓存业务为中心的 IO 密集型系统演化为边缘计算系统，构架内容计算网络，以解决未来物联网带来的连接挑战。

2. 生态场景一-智能硬件

JMT 边缘计算生态

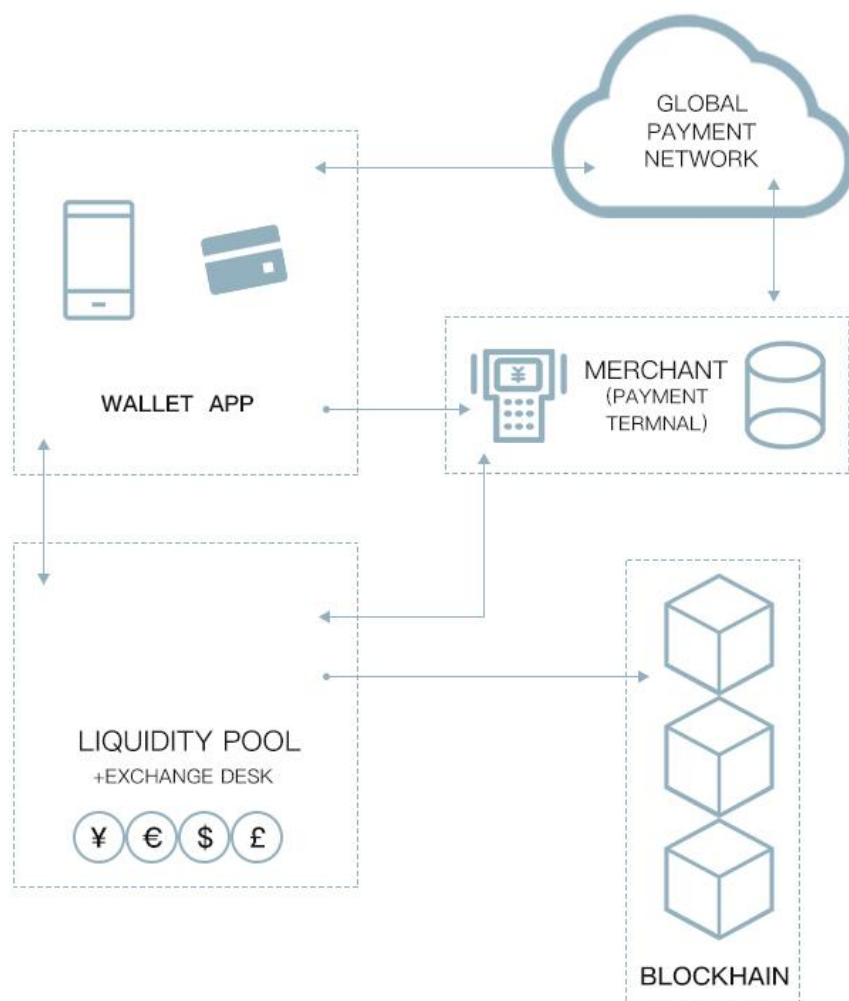
由 JMT 众多边缘计算硬件（智能物联网家居产品，移动智能终端，智能共享设备等）和应用区块链技术的 DAPP 奖励机制构成。生态用基于区块链技术的原生数字资产作为奖励，激励用户使用智能硬件进行获取奖励，推进边缘计算应用在物联网领域快速落地。

3. 生态场景二-JMT 即时支付

JMT 通证可直接通过用户私有的加密货币钱包进行实时线下（POS）交易，包括在店铺内或网上购物。其基于区块链的钱包，可以在线下交易的销售点进行即时付款。

在当前交易场景中，加密货币并没有被广泛使用。随着加密货币的用途和理念日益普及，相信在不久的将来，加密货币也会融入到我们的日常生活与消费中。

伴随着区块链支付技术的逐步成熟，JMT 也将成为全球范围内可使用的区块链支付方式。



五 JMT 发行计划

JMT 链是完全开放的积分区块链，全世界的人都可以参与系统维护工作。任何人都可以通过交易或挖矿（两挖）读取和写入数据，发行总量：15000000000，主网升级上线时全部用于公众挖矿（两挖：pow 挖矿 70%，pot 分布式存储和物联网边缘计算应用挖矿 30%，约可挖 30 余年）。在主网稳定后原物联网智能设备边缘计算所获得的 JMT 通证换成公链的 JMT 积分通证。

5.1. 出块速度

平均每约 20 秒出一个区块，主网升级上线后每个区块出 255 个 JMT 积分。

5.2. 奖励机制

获得记账打包权的节点主网升级上线后奖励 $g=175$ 个 JMT 积分，分布式存储和物联网智能设备边缘计算应用获得 75 个 JMT 积分，。另记账打包权的节点同时获得叔节点的记账权，最多可记 2 个叔节点。每个叔节点奖励 $\frac{1}{3}T$ ， T 为 5 个 JMT 积分。

- a) 打包节点（记叔块奖励的节点）另获奖励为 $\frac{1}{3}T$ 。

六 JMT 路线图

1. 第一阶段

2018 年 1 月-2018 年 6 月

系统开发期，用区块链技术赋能边缘计算。

JMT 通证上线，并实现通证在应用系统内的方便流通；区块链技术重构产品形态，逐步落实合作引入方案；并在国内、东南亚、日韩等地区开展推广。

2. 第二阶段

2018 年 7 月-2018 年 12 月

生态建设期，深耕各个生态组成部分。

打造全球去中心化的区块链智能生态。

3. 第三阶段

2019 年-2020 年

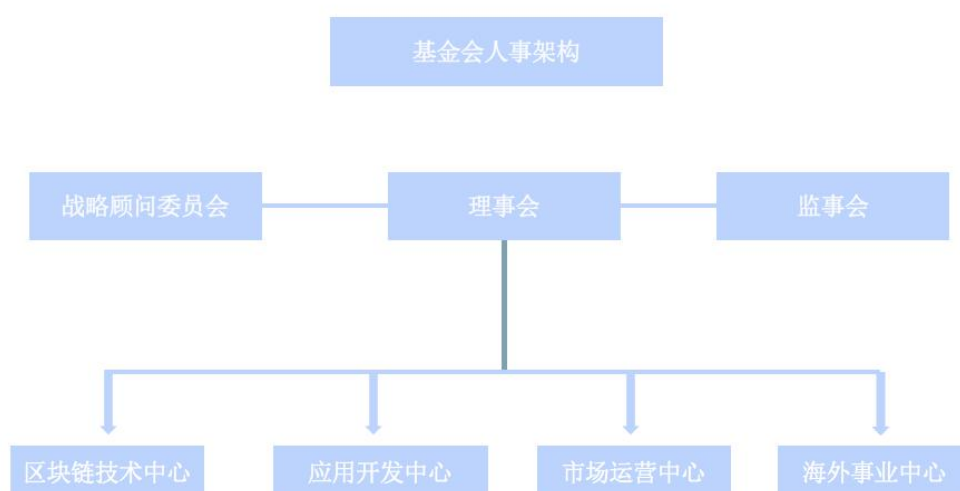
主网升级及公链上链期，全球生态开拓期。从应用搭建转到生态搭建，应用推广范围扩散至海外更多国家和地区。

七 JMT 的治理结构

1. 新加坡海外基金会主体

JMT 团队已在海外国家成立基金会，确保项目的合法合规运行。该基金会作为 JMT 治理的主体，全面负责执行 JMT 持有人大会决议，规范管理项目技术开发和应用开发，维护 JMT 通证持有人权益，宣传推广 JMT 品牌等。

2. 海外基金会人事架构



*战略顾问委员会：由多位投资领域、区块链技术领域、互联网领域的知名企业及专家担任，为项目提供战略性的意见指导和资源资金支持。

*理事会：理事会承担决策职能，通过由理事长召集并主持的定期理事会会议，对基金会战略规划、月季年度计划、预算等重大事项进行审议和审批。

*监事会：由社区成员代表构成，对项目运营提供及时的意见建议，督促项目重大事件推动，维护社区健康良好发展。

八 团队介绍

Morris

创始人

新加坡国立大学管理专业硕士，新加坡 ASTC 基金创始人，拥有丰富的公司管理经验和数据分析实践经验。

Devin

创始人

新加坡国立大学工程硕士，十五年以上半导体，智能硬件从业经验，着力于推动产品向区块链应用转型。

Fiona

社区负责人

北京外国语学院英语专业毕业，擅长于内容策划、用户运营等，实现用户增长、提升用户活跃度、提升 UGC 内容量。

Michael

运营负责人

加拿大渥太华大学通信专业硕士。具有丰富的大型技术团队和大型项目的架构管理运营经验。

Winstedt

运营负责人

新加坡理工大学商务专业毕业，曾任新加坡大型科技公司运营总监，负责全球生态拓展与项目运营推广管理。

John

技术负责人

从事研究、开发并实现区块链协议、运行机制、加密技术、共识算法和底层实现；负责基于区块链(blockchain)的互联网金融产品的设计和研发；组织制定和实施技术决策和技术方案，组织架构设计与升级优化。

九 结语

区块链项目的发展，体现它在技术性、应用性的迭代与革新，但也离不开它的市场创新和模式颠覆。JMT 代表了 JMT 生态服务的使用权，JMT 团队将继续深耕应用区块链技术升级，提供更有价值的服务。

十 风险警示

本文档为 JMT 团队对于平台业务和 JMT 功能的规划说明，JMTime 团队可能会根据行业发展和政策法规的要求调整实际业务发展的规划；

JMT 的参与者，请仔细阅读 JMT 技术白皮书，全面认识项目风险收益特征和技术特性，并充分考虑自身的风险承受能力，理性判断，审慎决策。

JMT 项目团队将按照所披露的白皮书内容，规范管理项目。尽管团队将恪尽职守，履行诚实、信用、勤勉尽责管理的义务，参与者也存在损失的风险，比如可能存在的政策风险、经济周期风险、网络黑客风险、管理风险、流动性风险、价值波动风险和其他风险。