MILE

免费，快速，安全，稳定的数字货币

2018 年 3 月 30 日

技术文件 v.1.2

Lotus Mile 编

精简版：mile.global

1 概述

目前世界上还没有一个同时具有以下属性，且能够衡量、储存和转移价值的工具。这些属性包括：

- 成本稳定；
- 发行公式透明；
- 免费、快速、自由的价值转移，可向全球任何地点的任何交易房转账；
- 贵重品安全长期储存；
- 交易不冻结、不可撤销。

现有的主流支付工具（美元、欧元、人民币、卢布等）都无法解决这个问题：

- 跨国合法转账价值超过 10000 美元的法定货币，需要数份文件和一系列批准，转账时间超过 24 小时，并可能遭遇额外的审批环节，或被阻止转账；
- 民众对国家主权债务的信心逐年下降，政府债券违约金额平均每年 0.25 亿美元，国债持续增长；
- 法定货币发行规则和发行报告不透明；
- 大多数法定货币的价值每年都会大幅波动，即使是在挪威、欧盟和日本这类经济相对稳定的国家，当地货币价值每年波动范围为 15-25％，在这种情况下，人们自然会使用某些替代结算方式；
- 银行作为核心交易者，承担着越来越高的风险。美国每年吊销 10～150 个银行牌，欧盟银行约 1 万亿欧元的资金具有高违约风险高，俄罗斯银行七年内关闭了一半；
- 在欧洲银行开户可能需要一到六个月的时间；
- 世界上任何国家的银行都能在可疑情况明确前冻结资金。国家机关有权发布新法令，事后认定这部分资金为非法获取，并处高达 100％存款金额的罚金。这种情况正发生在塞浦路斯。

当今的数字货币也无法解决这些问题：

- BTC 实现了去中心化，但波动太大；
- 闪电网络的引入使 BTC 的交易费用下降到 1.2 美元，但“这杯咖啡”的成本仍然很高。并且由于该技术应用范围有限，这样的手续费率只能在相互结算的情况下才能实现；
- 现有的稳定币种均与中心化法币基金相关联，即 100％依赖于某个交易者；
- 现有稳定币种的发行机制并不透明；
- 比特股上的市场挂钩资产与抵押的数字货币 BTS 挂钩，这比 BTC 更加不稳定。

为什么我们要搭建具有以下特性的平台

1. 与 XDR 挂钩的价格稳定的结算方式。
2. 发行过程开源，使用被数学计算严格证实的算法代码，保证透明度。
3. XDR 交易免手续费，MILE 交易手续费 0.2％。
4. 一分钟快速交易。
5. 去中心化，全球 10,000 个节点，基于不同的人和组织。

这一工具使人们：

- 能够确认自身财物安全；
- 自由、快捷、可靠、无需手续费地将资产转移到世界各地。

2 价格稳定

人为制造的公共资源管理系统中有两种共识水平——社会共识和技术共识。
以 BTC 为例：

- 社会共识——关于比特币协议新版本的公开讨论；
- 技术性 onchain 共识——矿工投票决定是否在自己的设备上安装或卸载比特币网络协议新版本。

不管达成怎样的技术共识，社会共识总起到决定性作用：

- 某些技术层面先进且看似公开透明的共识，其实都某些中心化精英集团通过贿赂操纵了投票结果（LISK，发达民主国家）；
- 反之亦然：即使没有使用复杂的技术，有良心的人们也可以仅用口头方式就达成协议。

MILE 网络参与者在社会层面上商定 MILE 系统中的 1 XDR 永远等于 1 XDR（其汇率由国际货币基金组织计算并公布。）

XDR 的主要应用领域是作为实际商品和服务交易的结算方式，因此交易所交易和特定货币的交易价格不会对 XDR 价格产生重大影响。
例如，2018 年 3 月底全球所有交易所最主流币种 BTC 的每日总交易量为 50 亿美元，而比特币网络中的总交易量仅为 10 亿美元。 以太坊交易所交易量为 1.5B，网络内交易量为 0.7 亿美元。 Bitcoin Cash 交易量则为 0.4 亿美元和 0.2 亿美元。
需注意：

- 研究数字货币交易所成交量图
- 大多数数字货币交易都是交易所钱包间转账，或大型钱包合并和转移，例如：
  - BTC 日交易量的 40%仅由一百笔交易贡献，平均每笔交易 3000 万美元；
  - ETH100 笔交易的交易额相当于总交易额的四分之一；
  - BCH 则接近 40%；
  - LTC 则为 61%。

也就是说，货币的实际周转量是该数字的 1.5-3 倍。

Coinmarketcap 上绝大多数币种的实际交易量为零，但交易所交易量却不断增长。因此，如今数字货币币价完全取决于投机炒作和新闻消息，数字货币本身具有巨大的波动性。

MILE 拥有独特的交易机制：

- 投资者不愿意将 XDR 转到交易所并人为地增加交易量；
- XDR 的主要目的是成为：
  - 存储和转移价值的一种方式
  - 实体经济中商品和服务交换的一种方式

正因如此，即使有人试图压低 XDR 的交易所价格，对那些在日常生活中使用 XDR 的人，这反而是件好事。

现实世界中 XDR 的购买力不会因交易趋势而改变，因此任何人都会希望以 0.8 倍的价格在交易所购买 1XDR。

下节将介绍 XDR 的实际应用。

3 发行公式

MILE 平台有两个用于结算和发行的实体 Coin (XDR)和 Token (MILE)：

3.1 XDR

- 平台内价值存储和交换的结算单位。
- 由 MILE 代币持有者和区块链系统节点发行，发行公式公开透明。
- 价格永远等于国际货币基金组织的 1XDR（XDR / USD 当前汇率）。
- 整数位数：12。
- 小数点后位数：2。
- 因此 XDR 发行上限为 999,999,999,999.99（1 万亿）。
- 此外，该结算单位也用作区块链节点的“燃料”，即节点存款。这能帮助区分出那些花费自身资源支持 MILE 网络的优质用户。

3.2 MILE

- XDR 发行算法的主要参数。
- MILE / XDR 汇率通过区块链节点投票决定，每昼夜更新一次。
  - 节点使用者参考各交易平台数据，发布他们认为公平的价格。
  - 在共识基础上确定当日最终 MILE / XDR 汇率。发行中心根据此汇率计算出最大发行量。
  - MILE / XDR 的计算方法与移动平均值计算方法相似，即应用存储在区块链中的历史汇率值进行计算。这样能够最大程度减少局部人为操控的可能。
- 整数部分位数：9。
- 小数点后位数：5。
- 可得出 MILE 最大发行量：999 999 999.999 99（10 亿）。

3.3 首次发行

- 最初，系统 0 XDR[1]。

1 初始区块将包含 300 000 XDR，这 300 000 XDR 将完全存入参与投票的节点作为存款。 这些节点归 MILE 团队所有，并将尽可能长时间地保持其活跃状态

- 最初，系统中有 1,000,000,000 MILE，且不计划发行新 MILE。
- 初始价格 1 MILE = 1 XDR。

3.4 二次发行

3.4.1 区块关闭后的节点发行（造币）

- 区块封闭后的节点发行（造币）
- 根据 MILE 算法，活跃节点根据账户余额规模，从区块链中获得 8-13％的 XDR 年利息。
- 依照该算法，约每天每个账户钱都能收到随机金额的年利息。但整体而言，年利息可达到 8-13％。
- 为获得成为节点并参与区块签署的权利，您需要安装 MILE 应用程序，并且在您的钱包里存入$ 10 000 $ - $ 100 000 $ XDR 的保证金。
- 区块关闭的奖金金额与账户存款金额非线性相关。
- 开发团队将公开项目源代码，任何人都可以部署和启动节点。
- 节点操作仅需使用一台 4TB 硬盘和稳定互联网的计算机即可。
- 这种发行方式有利于维持网络参与者的积极性，从而保障区块链正常运作。

3.4.2 发行中心的发行}

- MILE 代币位于区块链用户的钱包里。
- MILE 代币持有者可以将自己拥有的任意数量 MILE 转到某个地址。
- 用户须转账最少 10～000MILE，才能成为发行中心。
- 成为发行中心后，用户可按实时 MILE / XDR 汇率即时获得某一数量的 XDR。实时汇率由前一个节点共识决定并记录在区块链中。
- 如果在 t_2时刻 MILE/XDR 价格上涨，用户可使用钱包的“释放 XDR”功能，系统将为该用户额外发放 MILE ·(XDR(t_2)-XDR(t_1)). 。
- 为解锁 MILE 代币，用户应向特定地址转账 XDR，并按实时 MILE/XDR 汇率获取 MILE，手续费 0.2%。收取手续费是为降低区块链拥堵。收取的手续费将被分配给各个节点，用于社区网络的维护。

- 基于系统的合理架构，随着大众购买 XDR 量的增长，MILE/XDR 价格也将增长。因此 MILE 持有者将倾向于长期持有代币。
- 假设 XDR 以 MILE/XDR = N, 的汇率发行，则只有当 MILE/XDR 变为 ≥ N 时，MILE 才有可能解锁。

3.5 发行的经济基础

- 用于维持节点和/或发行中心的用户存款越多，需要 XDR 的人就越多，MILE 价格就越高。
- 用户使用 XDR 进行的实际商品交易越多，XDR 需求量就越高，MILE 价格就越高。
- MILE 的价格越高，您可以发行的 XDR 就越多。

3.6 反射点

- 由于 XDR 转账零手续费，系统允许您进行小额交易，因此，为保证区块链的长期稳定运行，我们将对其进行定期截断。
- 一旦区块链大小达到 4 Tb，截断算法就会被激活：系统从区块链上删除所有存款为零（空）的钱包，和所有存款少于 1XDR 的钱包。清洗后的区块链状态将被写进新的创世区块里。之前的区块链状态将只在特定节点中保存。
- 区块链截断后将使用假定为空钱包（余额少于 1XDR 的钱包）中应被销毁的余额支付节点手续费。
- 此外，将资金存储在自己钱包中的死节点也将被删除。

4 快速免费转账

MILE 网络中的交易是免费的（XDR - 0%, MILE - 0.2%），区块在 20 秒内关闭，预计吞吐量高达每秒 10,000 个交易。 由于我们不存储输入输出相关信息（与 BTC 类系统中的 UTXO 模型相比），因此我们的区块链更加优化。
最小化机制和反射点函数的应用使得免费交易成为可能（参见“区块关闭时的节点发行（minting）”一节和反射点的作用）。

5 区块链

5.1 选择理由

使用 MILE 大片的目标需要达成一致，以达到该区块的以下特征。

1. 创建新区块所需时间为 20 秒。
2. 有资格参与共识的节点总数为 10^3 到 10^4 不等。
3. 交易速度高 - 每秒至少 10 美元的交易额。
4. 与 PoW 相比，区块链算法运行对算力要求并不高。

使用 sdBFT 算法，相较 BFT 算法具有更高的速度。潜在共识参与者数量多，从而使有组织的操控投票结果变得困难，投票节点群无法创建新区块并控制该内容为自己所用，而在下一共识产生时，系统会自动选取另一个多数节点群。多数投票节点伪随机抽样法将禁止其在下次投票中占据多大权重。

该算法具体描述请参阅文章 consensus sdBFT。

5.2 新区块产生算法

- 在某个时间点让用户创建了一笔交易 *I*。
- 该交易被转交到与客户关联的最近一个节点。
- 节点可能处于以下三种：被动节点、护送节点和主节点。
- 如果节点是被动节点，它会核对交易并将其发送到对等网络，直到交易到达护送节点为止。
- 护送节点将交易转发给主节点。
- 主节点核对交易，如果交易正确，则将其发送给护送节点，并将交易I写入正在生成的区块中。
- 护送节点接收交易 *I* 后，核对信息并将它写入已生成区块。
- 这一系列操作不断重复，直到区块生成完毕，全程不超过 20 秒。
- 在此之后，主节点发送消息通知区块关闭。
- 各个护送节点计算交易区块的 Hash，电子签名 Hash，并将接收到的 Hash 发送给主节点。

- 主节点计算正确的电子签名数量。如果有效签名数超过参与投票的护送节点数的 2/3，则认定该区块声称。反义该区块不生成。
- 区块链没有时间概念，不检查区块中交易发生的具体时间。
- 区块链上层系统默认以区块平均生成时间为准（约 20 秒）。

5.3 伪随机数发生器

通常内置于操作系统中的标准伪随机数发生器具有许多严重漏洞，其中最危险的是：

- 作为 seed，timestamp 用于创建伪随机数。如果非法用户知道用于生成伪随机数的算法及其生成的近似时间，结果就是，他可以大概率地选择由该算法生成的私钥（密码）。
- 即使除 timestamp 之外还使用其他数据，标准的伪随机数生成器也会生成足以具有预测性的序列，这使得攻击者可以通过测算法选择密码（散列）。

在 Mile 平台里，从电子签名中的密钥生成到“随机数字”，任何地方都可以使用随机数字。对此，平台对随机数的质量施加了特殊的要求。 从随机数发生器获得的序列要经过大测试。以下是测试发生器的结果。

5.3.1 测试目的

测试的目的在于验证生成的随机数序列的动态控制的事实，确认生成序列的均匀分布的统计学假设。

5.3.2 测试条件和顺序

测试要检查由伪随机数发生器产生的随机数序列。为了执行检查，需要进行下列操作 ：

1. 创建站点以验证加密模块中生成和测试随机序列功能的实现，该模块由 APM 程序设计构成（安装有 Visual Studio 2017 开发环境和 PO MILE 软件的自动化工作站）组成。
2. 在 AWP 上编程附加的免费分发软件进行测试
   a) NIST Statistical test Suite (NIST-STS);
   b) Test-U01.
3. 在伪随机序列发生器的帮助下，在长度测试的性能和持续时间的自然限制条件下尽可能地产生随机数序列，但不小于 1024 GB。复制到 APM 编程的永久存储器中的指定随机变量序列是在二进制文件 StatMessTime（1000 字节）和 StatCurrent（2000 字节）中执行的。

4. 在自动化工作站上，使用上面列出的统计测试包对执行基本统计标准的随机变量序列进行分析。
5. 为了评估解释为二进制随机序列的质量，我们使用 3s 准则来计算二进制数字的相对频率

(0,5 – ½ D ½ – 1,5[1 – 4*D*2)n – 1]0,5,0,5 + ½ D ½ + 1,5[1 – 4*D*2)n – 1]0,5

为了评估被解释为二进制序列的随机序列的质量，我们使用 3s 标准来计算二进制符号的相对频率，其中 $p = 0,5 + D$, $q = 0,5 - D$

表 1. 我们运用了以下 3s 标准间隔

	3s 标准间隔:	
N	D=0	½ D ½ = 0,01
2^{13}	(0.4835„0.5165)	(0.4734„0.5265)
2^{15}	(0.4918„0.5082)	(0.4818„0.5182)
2^{16}	(0.4941„0.5058)	(0.4841„0.5158)
2^{17}	(0.4959„0.5041)	(0.4859„0.5141)
2^{18}	(0.4971„0.5029)	(0.4871„0.5129)

6. 为了评估用字节序列解释的随机序列的质量，这里使用了自由度标准：

$$c^2_{0,5} = 295, \quad c^2_{0,01} = 313$$

7. 为了验证动态测试程序，要测试结果进行处理，分析和评估。
8. 如果所使用的统计标准不拒绝第 5 章中所列分析的随机数序列的均匀分布的假设，则该检查被认为是成功的。

5.3.3 统计研究结果

StatMessTime 材料处理结果

1 在 16 段 1024 字节中的频率

4075 4129 4206 4148 4098 4180 4042 4021

4092 4134 4202 4226 4064 4052 4070 4112

1 在 16 段 1024 字节中的相对频率

0.4974 0.5040 0.5134 0.5063 0.5002 0.5103 0.4934 0.4908

0.4995 0.5046 0.5129 0.5159 0.4961 0.4946 0.4968 0.5020

1 在位移量为 1-512 中的相对频率

0 0.4976 0.5003 0.4997 0.4993 0.4994 0.4985 0.5017 0.5009

8 0.4985 0.5001 0.4989 0.4990 0.5015 0.5005 0.4994 0.5000

16 0.4990 0.5015 0.4998 0.4994 0.5000 0.4987 0.5019 0.5007

24 0.5012 0.4990 0.5017 0.5007 0.5006 0.5005 0.5001 0.5009

32 0.5011 0.5019 0.4985 0.5026 0.4997 0.5002 0.5011 0.5014

40 0.4983 0.5017 0.4995 0.4997 0.5000 0.5000 0.4989 0.5030

48 0.4983 0.5030 0.4985 0.4994 0.4995 0.5000 0.5012 0.5006

56 0.4996 0.5010 0.5003 0.5015 0.5006 0.5006 0.4994 0.5010

64 0.4980 0.4998 0.5001 0.4985 0.5030 0.5010 0.4990 0.5023

72 0.4984 0.4971 0.5004 0.4981 0.4989 0.5016 0.5000 0.5024

80 0.5027 0.5002 0.5022 0.4973 0.5025 0.5004 0.5022 0.4971

88 0.5000 0.4984 0.5025 0.5004 0.4972 0.5025 0.5006 0.4975

96 0.5007 0.5025 0.5009 0.5018 0.4997 0.5023 0.5015 0.4998

104 0.4980 0.4973 0.5026 0.4986 0.4976 0.5005 0.5024 0.5038

112 0.5012 0.4989 0.5024 0.5010 0.5011 0.4984 0.4998 0.4998

120 0.5008 0.4970 0.4969 0.4975 0.5013 0.5005 0.4972 0.5006

128 0.4976 0.5005 0.5021 0.5021 0.5007 0.5029 0.5002 0.4980

136 0.4993 0.5004 0.5015 0.4991 0.4970 0.4993 0.5019 0.4970

144 0.4994 0.4977 0.4990 0.5015 0.5001 0.5006 0.4970 0.5011

152 0.5033 0.5027 0.5029 0.5008 0.5004 0.5007 0.5031 0.5012

160 0.4984 0.5003 0.4967 0.4980 0.5011 0.4995 0.4998 0.5002

168 0.5022 0.5008 0.5001 0.4982 0.4996 0.4990 0.4995 0.5009

176 0.4978 0.5030 0.4999 0.4995 0.5013 0.4993 0.4975 0.5004

184 0.4963 0.4974 0.4962 0.4995 0.4988 0.5001 0.5017 0.4999

192 0.5036 0.5001 0.5000 0.5017 0.5026 0.4998 0.5033 0.4994

200 0.5022 0.5005 0.5020 0.4976 0.4987 0.5009 0.4974 0.5017

208 0.4998 0.5028 0.5001 0.4998 0.4996 0.5018 0.4980 0.4995

216 0.5003 0.4993 0.4979 0.5013 0.5035 0.5005 0.4992 0.4976

224 0.5025 0.5003 0.4998 0.5007 0.4982 0.4994 0.5024 0.5004

232 0.4978 0.4991 0.5007 0.4998 0.4981 0.5017 0.4990 0.5025

240 0.4972 0.4998 0.4978 0.4982 0.5042 0.4983 0.4994 0.5005

248 0.4980 0.5031 0.5035 0.5008 0.4969 0.5023 0.4981 0.4990

256 0.4997 0.4992 0.5021 0.5036 0.5004 0.4973 0.5025 0.5012

264 0.4986 0.5009 0.5001 0.4997 0.5029 0.5028 0.4976 0.4984

272 0.4999 0.4995 0.5002 0.5005 0.5012 0.5015 0.5023 0.5017

280 0.4988 0.4996 0.4996 0.4971 0.4969 0.4996 0.5029 0.4998

288 0.4995 0.4985 0.4977 0.4970 0.4984 0.4999 0.4988 0.5025

296 0.4973 0.5005 0.4979 0.5006 0.4977 0.4997 0.4983 0.4998

304 0.4998 0.5008 0.4978 0.5025 0.5015 0.4996 0.5025 0.4996

312 0.5023 0.4985 0.5023 0.4991 0.4995 0.5003 0.5020 0.4974

320 0.4994 0.5001 0.5008 0.5012 0.4997 0.5003 0.4967 0.5008

328 0.4982 0.5026 0.5003 0.5029 0.5000 0.4971 0.4981 0.4997

336 0.5003 0.4980 0.4982 0.5022 0.5018 0.4975 0.4993 0.5026

344 0.5018 0.5031 0.4994 0.4968 0.5034 0.5032 0.5001 0.5020

352 0.5025 0.4987 0.4977 0.4966 0.4977 0.5000 0.4961 0.5004

360 0.4995 0.5018 0.4979 0.4974 0.5009 0.4970 0.4999 0.5008

368 0.4974 0.4998 0.5007 0.5003 0.4998 0.4999 0.4972 0.4995

376 0.4968 0.4996 0.5004 0.5024 0.5021 0.4974 0.5032 0.4991

384 0.4998 0.4995 0.5015 0.4982 0.5004 0.4993 0.5025 0.4972

392 0.5024 0.4996 0.5000 0.4996 0.5017 0.4993 0.4974 0.5003

400 0.5008 0.4982 0.5031 0.4985 0.5008 0.5030 0.5005 0.5015

408 0.4985 0.5000 0.4981 0.5008 0.5021 0.5021 0.5004 0.4977

416 0.4999 0.4995 0.5001 0.4969 0.5031 0.5001 0.4970 0.5012

424 0.5000 0.5012 0.5000 0.4999 0.5006 0.4988 0.4966 0.5006

432 0.5023 0.4994 0.4978 0.4973 0.5011 0.4971 0.5009 0.4979

440 0.4968 0.4994 0.5004 0.4991 0.4997 0.4971 0.5002 0.5010

448 0.4994 0.5033 0.4988 0.4993 0.5021 0.5034 0.5010 0.4963

456 0.5016 0.4989 0.5003 0.4971 0.5020 0.4978 0.5000 0.4974

464 0.5008 0.5015 0.5007 0.4994 0.4967 0.5009 0.4994 0.4996

472 0.5010 0.4977 0.5007 0.4979 0.4979 0.4997 0.4973 0.4966

480 0.4998 0.4988 0.5026 0.4990 0.4985 0.5017 0.4979 0.5029

488 0.4997 0.5013 0.5038 0.4994 0.5006 0.4998 0.4991 0.4992

496 0.5003 0.4963 0.4993 0.5012 0.4994 0.4979 0.5001 0.4979

504 0.4982 0.5028 0.5022 0.5033 0.5003 0.5032 0.4995 0.4997

最小结果：0.4961，最大结果 0.5042

16384 字节上的字节频率

0 70 58 72 71 73 67 58

60 8 58 83 50 74 57 66

57 62 16 49 73 60 55

71 73 62 64 24 61 74

66 74 63 62 73 65 32

54 62 69 60 68 65 64

50 40 66 60 68 57 49

56 52 60 48 64 68 64

59 56 65 61 67 56 50

80 63 68 69 45 61 57

64 63 55 73 76 79 59

48 68 72 64 62 65 62
51 49 62 69 80 69 66
46 55 64 77 61 67 88
63 64 62 54 59 82 56
70 96 56 72 60 65 58
61 71 57
104 60 63 61 60 55 75
65 61 112 72 68 77 75
56 65 62 73 120 61 76
58 68 59 78 70 64 128
67 72 59 72 67 68 59 65
136 60 61 54 77 55 67
41 75 144 57 61 66 65
62 78 56 68 152 72 68
55 61 73 59 51 75 160
54 67 66 57 74 53 81 66
168 64 49 58 59 64 61
74 50 176 66 61 70 70
59 54 69 69 184 61 68
74 57 68 61 64 82 192
82 69 47 70 63 58 60 61
200 68 57 60 76 69 61
45 65 208 76 61 55 58
60 70 53 67 216 72 78
67 62 62 78 73 68 224
62 64 52 65 62 80 75 56
232 55 62 61 66 53 51
72 58 240 51 60 69 73
77 60 56 71 240 51 60
69 73 77 60 56 71 248
80 56 66 86 73 61 77 67

最小：41，最大：86

在 16384 字节（自由度为 255）材料上的值: c2 = 268.5

StatCurrent 的处理结果

1 在 32 段 1024 字节中的相对频率

4047 3991 4189 4072 4068 4177 4113 4036
4043 4041 4102 4044 4101 4064 4098 4087
4090 4131 4092 4105 4117 4100 4145 4069
4112 4117 4094 4068 4110 4097 4099 4077

1 在 32 段 1024 字节中的相对频率

0.4940 0.4872 0.5114 0.4971 0.4966 0.5099 0.5021 0.4927
0.4935 0.4933 0.5007 0.4937 0.5006 0.4961 0.5002 0.4989
0.4993 0.5043 0.4995 0.5011 0.5026 0.5005 0.5060 0.4967
0.5020 0.5026 0.4998 0.4966 0.5017 0.5001 0.5004 0.4977

1 在位移量为 1-512 中的相对频率

0 0.4976 0.5003 0.4997 0.4993 0.4994 0.4985 0.5017
0.5009 8 0.4985 0.5001 0.4989 0.4990 0.5015 0.5005
0.4994 0.5000 16 0.4990 0.5015 0.4998 0.4994 0.5000
0.4987 0.5019 0.5007 24 0.5012 0.4990 0.5017 0.5007
0.5006 0.5005 0.5001 0.5009 32 0.5011 0.5019 0.4985
0.5026 0.4997 0.5002 0.5011 0.5014 40 0.4983 0.5017
0.4995 0.4997 0.5000 0.5000 0.4989 0.5030 48 0.4983
0.5030 0.4985 0.4994 0.4995 0.5000 0.5012 0.5006 56
0.4996 0.5010 0.5003 0.5015 0.5006 0.5006 0.4994
0.5010 64 0.4993 0.5002 0.4994 0.5004 0.4994 0.4996
0.4996 0.5003 72 0.5014 0.5003 0.5017 0.5000 0.4984
0.4982 0.4990 0.4998 80 0.4994 0.5007 0.4970 0.4995
0.4991 0.4992 0.4990 0.5020 88 0.5005 0.5018 0.5010
0.4995 0.4974 0.5018 0.4997 0.5000 96 0.4999 0.5017
0.5024 0.5002 0.4999 0.4992 0.4993 0.5015
104 0.4996 0.5006 0.4976 0.4997 0.4993 0.4983
0.4996 0.5019 112 0.4980 0.4992 0.5015 0.4991
0.4989 0.5005 0.4994 0.5000 120 0.4981 0.5003
0.4996 0.4992 0.4995 0.4985 0.4990 0.4985 128
0.5001 0.5015 0.4994 0.5003 0.4994 0.4996 0.5015
0.5001 136 0.4992 0.5009 0.4974 0.5015 0.4979
0.4991 0.5030 0.5013 144 0.5010 0.4990 0.5030
0.5006 0.5021 0.4994 0.5004 0.5003 152 0.5008
0.4987 0.4992 0.4991 0.4999 0.5015 0.4994 0.4972
160 0.5005 0.4991 0.4972 0.4990 0.5001 0.4999
0.5006 0.4987 168 0.4987 0.4986 0.5003 0.5015

0.4992 0.4999 0.4998 0.4983 176 0.4994 0.5005
0.4993 0.4992 0.5007 0.5004 0.4987 0.4987 184
0.4995 0.5003 0.5012 0.4999 0.5010 0.4970 0.4991
0.5008 192 0.4993 0.5009 0.5008 0.5003 0.4985
0.5000 0.5019 0.4983 200 0.4995 0.5010 0.5006
0.4987 0.4994 0.5004 0.5006 0.4983 208 0.5000
0.4985 0.5004 0.5011 0.4994 0.4996 0.4985 0.4986
216 0.4983 0.5007 0.5009 0.5014 0.4998 0.5000
0.4997 0.5003 224 0.5000 0.5000 0.4981 0.5014
0.5017 0.5013 0.5019 0.5014 232 0.4996 0.5004
0.5024 0.4999 0.5017 0.5006 0.4984 0.5028 240
0.5002 0.5009 0.5004 0.5003 0.5010 0.5004 0.5018
0.5011 248 0.5017 0.4991 0.4990 0.5002 0.5000
0.4994 0.5003 0.5010 256 0.4995 0.4988 0.4989
0.4993 0.5002 0.5015 0.4983 0.4995 264 0.4985
0.5004 0.5003 0.4976 0.5024 0.5015 0.5013 0.5001
272 0.5024 0.4995 0.5002 0.4999 0.5015 0.5017
0.5015 0.4990 280 0.4998 0.5016 0.5005 0.4985
0.4990 0.5024 0.4998 0.4993 288 0.5004 0.4994
0.4981 0.5003 0.4981 0.5016 0.5012 0.5021 296
0.5012 0.4980 0.5005 0.5007 0.4993 0.4993 0.4988
0.4983 304 0.4981 0.4995 0.4995 0.5003 0.5008
0.5000 0.4998 0.5000 312 0.5012 0.5010 0.4996
0.4973 0.4994 0.5008 0.5005 0.5006 320 0.4991
0.4986 0.4998 0.5003 0.4995 0.4994 0.4985 0.4994
328 0.4998 0.5014 0.5012 0.5006 0.5004 0.4984
0.4996 0.4984 336 0.4983 0.5007 0.4993 0.4992
0.5008 0.5012 0.5003 0.5024 344 0.4984 0.4993
0.4989 0.5006 0.4999 0.4986 0.4994 0.5002 352
0.5014 0.4991 0.5015 0.5002 0.5016 0.5004 0.5017
0.5006 360 0.4999 0.4985 0.4999 0.4983 0.4992
0.5004 0.5004 0.5005 368 0.5002 0.5004 0.5007
0.4996 0.5004 0.4999 0.4995 0.5016 376 0.4996
0.5006 0.4996 0.5007 0.5005 0.4995 0.5010 0.5006
384 0.5016 0.5012 0.4991 0.4994 0.5004 0.5002
0.5013 0.4994 392 0.5014 0.4996 0.4991 0.5019
0.4992 0.5021 0.5004 0.5018 400 0.5006 0.4991
0.4993 0.5009 0.5007 0.4999 0.5022 0.4995 408
0.4999 0.4973 0.4994 0.4997 0.4990 0.4982 0.4992

0.5008 416 0.4995 0.5004 0.5000 0.5005 0.5015
0.5008 0.5015 0.5003 424 0.5003 0.5005 0.5019
0.5009 0.4990 0.4994 0.4981 0.5008 432 0.4990
0.4988 0.5007 0.5020 0.5008 0.5003 0.5010 0.5000
440 0.4974 0.4993 0.4982 0.4994 0.5008 0.4994
0.5026 0.4984 448 0.5013 0.4995 0.4993 0.4996
0.5016 0.4985 0.4996 0.4991 456 0.5011 0.5012
0.5015 0.5018 0.5003 0.5004 0.4995 0.5017 464
0.4995 0.5004 0.5000 0.5024 0.4997 0.5027 0.4981
0.4987 472 0.5008 0.5006 0.5003 0.5007 0.5007
0.4990 0.4998 0.4992 480 0.5008 0.4996 0.5027
0.4996 0.5016 0.5012 0.4993 0.5004 488 0.5006
0.5008 0.5008 0.5026 0.5014 0.4993 0.4999 0.5012
496 0.4987 0.5018 0.4996 0.4998 0.5008 0.5009
0.4996 0.4988 504 0.5017 0.4993 0.5004 0.4980
0.5017 0.5014 0.4999 0.5011

最小：0.4970：最大：0.5030

32768 字节材料的字节频率

0 116 137 119 142 137 128 120
128 8 124 122 151 141 126 117
123 125 16 129 113 120 116 116
127 134 122 24 117 129 118 140
139 126 138 143 32 136 122 142
138 125 122 118 114 40 141 135
119 138 122 116 124 135 48 133
128 119 128 146 117 145 140 56
124 115 106 136 120 112 141 147
64 148 132 120 132 140 119 138
124 72 129 135 116 126 136 132
142 116 80 134 143 129 111 126
142 117 123 88 110 152 144 145
129 141 108 147 96 139 144 129
135 123 123 123 143
104 110 123 122 145 111 144 139
128 112 113 136 136 130 139 121
154 149 120 132 137 121 129 124
124 124 128 128 146 117 118 124
117 115 138 136 136 124 119 147

128 123 132 144 138 144 139 125
127 138 123 110 130 139 152 128
145 126 128 119 127 122 125 160
136 120 132 124 115 126 120 115
168 110 133 131 125 146 125 122
125 176 134 112 122 115 116 132
108 127 184 140 111 125 104 133
133 110 110 192 129 134 141 137
131 124 125 146 200 106 126 145
133 122 140 116 132 208 123 134
127 131 132 120 127 140 216 128
125 136 120 133 113 123 146 224
137 122 129 114 113 108 107 129
232 125 139 142 107 99 122 126
116 240 130 137 139 152 137 132
137 121 248 137 124 138 124 137
112 114 112

最小：99，最大：154

材料上的$ c^2 的值为 32768 字节（255 个自由度）

5.3.4 结果

在 MILE 区块链中，基于散列函数的双重计算和初始状态的动态变化，实现了随机数生成程序。在| D | <0.01 的情况下，伪随机序列生成器生成的随机序列的质量不低于 0.5+D，这满足了随机数序列的均匀分布的假设。

5.3.5 加密

- ECSDA 数字签名算法（在 BTC 中使用）。
- Ed25519 方案（比 BTC 更快）
- SHA-3 散列算法（比 BTC 更快，更可靠）

5.3.6 区块链的一般属性

- 零手续费支持微交易（“买咖啡”）。
- 不限制最大交易金额。

- 区块链会定期执行自我优化并将其大小保持在指定的范围内。
- 带有垃圾平衡收支的钱包清零，而其内容到达涉及的区块链的节点处。

5.3.7 交易类型

- 零手续费支持微交易（“买咖啡”）。
- 发送 XDR。
- 发送 MILE。
- 节点注册声明。
- 关于排除节点的声明。
- 新创世区块（截断）。
- 出版 MILE / XDR 课程。
- 提交问题由节点投票。
- 节点投票。
- XDR 发行中心发行/反向发行。

5.3.8 控制参数

- 通过区块中的间隔可以开始截断区块链的过程。
- 如果前一个截断失败，则重复执行截断区块链的过程。
- 允许您创建节点的存款范围。
- 限制节点数。
- 通过对节点进行投票来更新控制参数。

5.3.9 钱包

- 钱包地址是 Base58checkerMod2 中编码的一串字符，写入了在该隐私室中托管的交易。
- 在钱包上，您可以接收 XDR 和 MILE。
- 钱包类型：
  - 便捷：
    - 用于交易和检查余额

- 使用一个专门的协议来允许你获得需要的区块，并只检查默克尔树，而不是整个区块。

➢ 标准：

- 它保存整个块。
- 可以注册为节点。

➢ 多重签名

- 系统只接受虚拟钱包中有多重签名的交易。

➢ 点钱包：

- 开发者的钱包，可以通过改变控制参数来实现系统的点管理。
- 区块链只需要在第一年运行，然后会被分开，并在区块链中登记。

➢ 系统钱包：

- 该钱包用于在区块链截断情况下从可移动的钱包中积累佣金。
- 由此，发起的交易只能用于涉及到区块链截断节点的佣金的支付。

6 实际应用

6.1 国际自由支付

由于对免费、快速、廉价的国际支付的需求，电子货币的市场已经大幅增长。 中国的情况尤其如此，因为中国的货币流通受到国家的限制。

根据新加坡 Money 2020 会议的分析结果，没有任何支付系统允许 5,000 美元以上的跨境交易。 在各州之间转账超过 5000 - 10000 美元的唯一工具是 SWIFT。 但是为了转账，您需要填写大量文件，等待银行审理文件，与货币管理经理讨论转账，然后等待几个小时才能完成转账。 SWIFT 的成本约为 1％。
MILE 允许向世界任何地方免费转账，几秒钟就可以实现，并且不需要和任何银行管理者沟通。

6.2 独立存储

把现金存放在家里是很危险的。

在与银行保管箱中的财产保管合同中，有一条规定，银行不对保管箱中物品的安全负责。 结果，大量金钱经常从银行保管箱中遗失。 银行关闭的统计数字在“简介”中给出。

MILE 允许您安全地将资金存储在分散的网络中，不存在被中央监管的风险，无需账户封锁。

6.3 国际合作经济

确保 MILE 价值的最重要方面之一是商品和服务的真实周转。 MILE 作者认为，MILE 在合作经济中的传播潜力最大，特别是在金融体系不稳定的发展中国家。 正是在这些市场中，法定货币出现明显亏损，同时，在交易中有易货交易和其他净额结算方式的倾向性。

大多数发达国家实际上已经停止了经济增长，现在发展中国家对世界经济发展的贡献最大。这同样适用于企业：除了一些金融控股公司外，大公司的盈利能力低于 5%。 在经济危机期间，即使是富有的金融公司也出现了巨大的损失。

在这种情况下，**对抗市场的合作历史性地增长，尤其是在经济危机期间**

- 2008 年，荷兰合作银行的规模增加了 42%，它的创始成员的存款增加了的 20%。2008-09 年会员的信用水平已显著增长。
- 每隔三年，加拿大人是信用联盟系统的成员，信用联盟在零售市场上的份额从住宅抵押贷款和存款 16 \%增加到 2010 年的 19%[穆迪投资者服务公司全球银行业报告，2010 年 4 月。
- 从 2012 年第一季度，加鼎集团在 7500 个北美存款金融机构拍第 16 名，根据中占有资本的第一序列资本量，德信位列第二位，其比例为 16.8%。

合作经济的容量极大，合作公司团体在富裕国家和发展中国家是很普遍的：

- 合作公司团体在全球拥有 10 亿股东。
- 在印度，67%的农村商品需求由合作公司团体提供。
- 40%的非洲房主是合作公司团体的成员。
- 2010 年 1500 家最大的合作组织的收入达到近 2 万亿美元。
- 加鼎国际（DID）是小额信贷的领导者：它与世界各地的 880 万会员和客户合作，并拥有 25 亿加元的贷款资本。
- 在一些非洲国家，加鼎占据了小额信贷市场的 35%。
- 在中国，合作公司团体提供了 91%的小额信贷市场。
- 对于在发达国家工作的、家庭在发展中国家的劳务移民，信用合作社向他们提供了数十亿美元的汇款，这对拉美和非洲尤其重要。

合作经济效率更高，因为：

- 合作社的工作旨在为所有股东赚钱，
- 而不是夸大股票市值。
- 所有股东都参与其中，不需要花钱和时间来激励他们。
- 在企业中，高层管理人员的收入是普通员工的 100 倍，在合作社中只有 10 倍，即维护结构的成本要低得多。

- 由于经济的内部轮廓和合作社参与者之间的相互和解，有可能降低税收，交易和中介成本，同时也减少了对法定贷款的需求。
- 因此，合作社内商品和服务的价格比国外市场低 40%。 这为从外部吸引资本和人员提供了动力，也激励了人们长期参与合作社。

为基于 MILE 的合作社创建的工具：

- 会计结算，
- 收据和余额的存放处，
- 来自外部的融资吸引力，
- 准备向税务机关报告，
- 用令牌登记工作的法律模板，
- 商品和服务的市场有很大的折扣。

7 生态系统成员激励

用户：

- 用户能够快速、免费地进行交易或长期储存自己的数字货币资产

投资者：

- 具有吸引力的投资回报
- 回报可以通过系统的支持发生。任何参与者都可以成为区块链节点和 / 或发行中心。

发行中心：

- MILE 价格增长使他们的资本和固定收入随之增加。

节点所有者：

- 通过为区块链中的区块签名收取手续费。
- 节点所有者年受益为 8-13%（以 XDR 计算）。

8 法律信息

日常应用

如果当地法律无相关限制，或者交易量很小，或交易无规律性，则 MILE 的使用无法合法化。

在其他情况下，尤其大额交易频繁时，建议成立地区合作社或消费者社区，或加入现有社区。

社区的主要工具是股金。股份出资是指股东以货币、证券、土地或土地股份、其他财产或财产权等具有货币价值的权利向消费者协会股票基金提供的财产。股金退还不征税，无论股东收到货物数量及价格如何。
合作社内部允许各种形式的股份交换，且都不需缴税，也就是说，法律上讲 MILE 可以作为评估股份价值的工具。

非合作社成员的外部人员可以参与 MILE 忠诚度计划：

- 代币是获得奖励积分的权利。这项权利可以出售给法人和个人，或做会计核算。
- 代币交换为产品 / 服务时，代币持有者行使获得奖励积分的权利从而获得积分，并用积分兑换商品。
- 超市的会员积分和航空公司的里程奖励就是按此模式进行的。