MILE
免费、快速、安全、稳定的数字货币

2018年10月8日

技术手册 v.1.5

Lotus Mile 编
精简版: mile.global

1. 概述

目前在世界上还没有一个同时具有下列属性，并且能够衡量、存储和转移价值的工具。这些属性括：

- 成本稳定;
- 快速交易;
- 自由交易;
- 不限交易额度;
- 审查不受阻以及交易不可撤销;
- 发行运算公式透明

现有的主流支付工具（美元，欧元，人民币等）不能解决如下问题：

- 价值不够稳定，大多数法定货币的价值会出现大幅波动。即使是在像瑞士和日本这样的发达国家，本土货币价值也会出现段时期内快速升降：日元在2016年10月到12月间贬值了15%[1],瑞士法郎在2015年1月一个星期的时间内贬值了20%[2]。
- 交易缓慢，如果想在不同国家间跨境交易价值超过10000美元的法定货币，那么需要准备数份文件和获得一系列批准。转账需要数天时间，而且有可能会遭遇附加审批环节拖后转账进度甚至被阻止转账。此外，如需在欧洲开设银行账户还需要几个月的时间。
- 价格不菲的转账费用，根据交易系统的网站说明，平均货币兑换率约为 3-5%。
- 不断严格的审查制度，有数个国家被卷入了2018年的制裁和贸易战中，他们被制裁不能使用SWIFT转账，或是转账需要被严格限制，被制裁的国家有：中国、印度、俄罗斯、伊朗、土耳其、委内瑞拉。他们中的五个国家GDP总量居于全球前30位[3] 。
- 交易的可逆性

[1]https://www.bloomberg.com/quote/USDJPY:CUR
[2]https://www.bloomberg.com/quote/USDCHF:CUR
[3]https://en.wikipedia.org/wiki List_of_countries_by_GDP_(nominal)

- 交易运算公式不透明，交易的运算公式往往被少数个人所控制。这往往会导致恶性通货膨胀和经济危机的产生[4]。有发达国家的中央银行推行过M0和其他指数，但是没有人对这些数字进行过审计。

现有的数字货币也无一可以解决这些问题：

- BTC实现了去中心化，但是它的波动太大。
- 现有的绝大多数稳定币种都与中心法币基金相关联，即 100 %依赖于交易的其中一方，但其中一方有暴跌的可能 (如USDT, Circle等)。
- 许多现存的稳定币种都与贵金属、劳动力价格或其他因素相挂钩。但是这些因素是不稳定的。金价与美元的汇率可以在一个月内产生上下 15%的浮动[5] 。
- 基于ERC20的稳定币种一般依赖于以太坊（ Ethereum）的主网络,当有新的应用程序出现的时候，主网络往往会发生堵塞[6] 。
- 稳定币种的交易运算公式会受到索罗斯攻击[7] 。
- 现存于稳定币种体系中，唯一既快速又实惠的转账方式是比特股和比特资产（BitShares BitAssets）但是它们存在一个主要的问题：丹· 拉里莫离开比特股后，导致了比特股的衰落。BTS如今的日成交量浮动在几百万美元左右[8]，而比特股的主要论坛上如今每周只有数十个活跃话题[9] 。而主要的问题在于比特股委员会成员过度集中，决策权集中在数十个人手中 ,所以网络交易实际上也是掌握于数十个人手中的。
- 在早期白皮书中有一些项目，白皮书中当时描述的正尝试着去建立一些分散管理的稳定币种。它们超出了此文件的范畴[10]，因为当时他们还并未生效。

这就意味着如今的市场需要集以下特点于一体的产品：

1. 价格稳定;
2. 不受审查;
3. 自由交易;
4. 快速转账;
5. 允许任何人持有货币.

持有货币的主体包括个人、企业和国家。

- 任何金额的资产快速转移到世界上的任何地方，不受贸易战或SWIFT的影响与限制;
- 长期免费地存储任何数额的资产

2. 价格稳定

金钱是一种社会构造的产物。唯一能够定义货币体价值的是多少人使用该货币进行交易、借贷、投资、汇款和储蓄。自尼克松新经济政策以来，美元就不再与黄金挂钩了，并且一直在持续不断地发行。但它现在仍在使用并且比其他的流通货币更加稳定可靠。因为很多人在实体经济中选择使用美元进行交易。经济危机的产生是基于货币发行速度快于经济增长速度的情况才会出现。

[4] https://en.wikipedia.org/wiki/Nixon_shock
[5] https://www.bloomberg.com/quote/XAUUSD:CUR
[6] https://media.consensys.net/the-inside-story-of-the-cryptokitties-congestion-crisis-499b35d119cc
[7] https://en.wikipedia.org/wiki/Black_Wednesday
[8] https://coinmarketcap.com/currencies/bitshares/
[9] https://bitsharestalk.org
[10] https://cryptofresh.com

MILE平台及价格的稳定性主要基于以下两点:

- 实体经济中被广泛使用于交易、借贷、投资、汇款和储蓄;
- 交易运算公式使得货币供应速度不快于经济增长速度;

实体经济的使用与其说是一项技术任务不如说它是一项外交任务。总之，多合一的产品具有的特性（稳定的价格、快速自由地交易、审查不受阻和算法透明)与现有货币和加密货币相比有很强的竞争力。

交易算法公式将在下节中具体说明。

3. 发行公式

在MILE平台上有两个用于结算和发行的实体: XDR (稳定币种) 和 MILE (基于XDR的需求指数)。

3.1 XDR

- XDR是一种稳定币种, 是价值存储和交换的结算单位;
- 由MILE持有者和区块链节点发行，发行公式公开透明;
- 根据共识和货币供应管理算法，它大致等于 1 IMF SDR [11] ;
- XDR 会作为存款锁定在区块链内用以启动主节点;
- XDR有12个整数位数和2个小数点后位数，即XDR的最大供应量为 999 999 999 999.99 (近1万十五)，最大供应量可以通过考虑主节点共识和少量分歧的情况下进行更新;

3.2 MILE

- MILE是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；
- 节点使用者可以综合考虑股票交易所、场外交易和线下经济数据，发布一个他们认为合理的汇率；
- MILE/XDR 指数可以展示出通过发行中心可以发行多少XDR；
- MILE将会作为存款锁定在区块链内用于启动发行中心；
- MILE 整数部分有9位，小数点后有5位，即MILE的最大供应量为999 999 999.999 99 (近10亿)

3.3 首次发行

- 最初会有300 000 XDR在系统中，这些XDR会被锁定为区块链中的存款启动共识;
- 最初在系统中会有 999 999 999.999 99 MILE币，在此后MILE币将不会被投放 ;
- 初始价格1 MILE = 1 XDR;
- 最初MILE币的分配和价格基于下列情况说明。在MILE系统中相当于投入了14亿美元的资本，系统会将价值10亿美元的MILE分配到108个钱包账户中。在财务审计中，资本不是指银行账户中的法定货币数量。它是不同资产的整体组合：法定货币、加密数字货币、生产要素、知识产权、人力资源、品牌价值、不动产、商业信誉、其他有形及无形资产、企业（以及以上资产的组合）。

[11] https://www.imf.org/external/np/fin/data/rms_sdrv.aspx

3.4 二次发行

3.4.1 区块关闭后的节点发行（造币）

- 为了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，并且在区块链中投入 10 000 — 100 000 XDR。
- 操作主节点可以从区块链中获得8-13%的XDR年利息，这取决于存款数量、货币发行数量和已交付部分，平均1-2天一次。 这种利息以抛物线形发展，存款越接近100 000，利率增长得越快。
- 任何人都可以从公共坞中持有和启动节点。
- 节点操作只需要使用一台具有4TB硬盘和稳定互联网连接的电脑即可。
- 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。
- 主节点是不限数量的，但只有大约10 000个主节点（活跃节点）可以参与建立共识；其他的节点会在等待模式中工作。例如他们可以存储区块链，但是它们不能收到区块署名也不能参与造币。
- 如果有活跃节点参与区块署名失败，那么它会被共识淘汰，最近的等待区节点会取而代之被转化成活跃节点。
- 由于10 000活跃节点数量的限制，基于 8-13%造币溢价是有限的，限于10亿XDR。例如，生态池会不断扩大到100亿XDR，那么整体通胀率会被控制在 0.8-1.3% 之间，这是非常小的通胀率。
- 如果累计发行1万亿XDR ，那么主节点会停止接收附加造币任务。这也会导致少量分歧产生，也许会导致增加最大XDR供应量。

3.4.2 发行中心

- 想要变成发行中心需要用戶投入 10 000 以上MILE到区块链中。
- 区块链会直接向用户发行中心的钱包中发放新的XDR。发放XDR的数量会根据内部区块链中MILE/XDR的汇率来决定。
- 如果MILE/XDR汇率增长超时，那么每一个发行中心都可以发行更多的XDR，因为发行限额也在增长。
- 如果用户想要在发行中心中解锁 MILE, 用户必须向区块链中转账一定数量的XDR，区块链根据实时MILE/XDR汇率进行计算。XDR中的0.1% 用于防止资金溢出。这部分钱会用被用于分配给活跃节点。
- 如果XDR的需求增加，那么MILE/XDR也会增长。如果对 XDR的需求停止增长或需求转为负面，那么 MILE/XDR汇率也会不变或下跌。
- 假设 XDR以 M ILE/XDR = N 的汇率发行，则只有当MILE/XDR ⩾ N时，MILE才有可能被解锁。
- 某些特定的算法用于解决MILE/XDR 公认主节点中过高或过低的情况，以此来减少MILE/XDR的不稳定性。
- 用于计算 MILE/XDR的特定算法与计算平均移动值的算法类似。例如，运算时会把历史交换汇率保存在区块链中。
- 发行中心会使得操作尽可能控制在小范围内，以此供应XDR的缓慢增长从而避免恶性通货膨胀的发生。

3.5 反射点

- 由于XDR转账是零手续费，系统允许用户进行小额交易。因此，为了保证区块链的长期稳定运行，我们将定期对其进行截断。

- 一旦区块链大小达到4TB，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。清洗后区块链状态将被写进新创设的区块内。之前的区块链状态将只在特定节点中予以保存，成为归档节点被视为自愿选择。
- 截断操作后剩余的部分会被发送到主节点中。
- 此外，将资金存储在自己钱包中的死节点（长时间无操作无反应的节点）也会区块链截断删除。

4. 免费快速转账

MILE网络中的交易是免费的（XDR——0 %；MILE——0.2 %），区块一般会在20秒内关闭，预计吞吐量高达每秒10 000个交易。由于我们不像BTC类系统中的UTXO模型那样，我们不存储输入输出的相关信息，因此基于用户主节点的造币机制使得我们的免费快速转账成为了可能。

要每秒处理10,000个事务，机器必须每分钟处理大约600,000个事务。由于电子签名验证，3 GHz的单处理器核心可以处理大约80,000 ts / min。这意味着网络要求互联网的每个大部分（欧盟，美国，中国，俄罗斯，拉丁美洲，非洲，澳大利亚，东盟）至少有1个主节点，并且至少有8个频率为3 GHz的核心用于处理10 000吨/秒。

5. 区块链

5.1选择理由

MILE应用程序的区块链拥有以下特征：

1. 创建新区块的时间是20秒。
2. 有资格参与共识的节点总数为 103 to 104不等。
3. 交易速度快，每秒至少103次交易。
4. 与 PoW区块链算法相比，MILE的区块链算法运行对计算机算力要求并不高。

使用sdBFT算法，比BFT算法速度更快。 潜在共识参与者数量众多，从而使得有组织的操控投票结果变得极其困难。投票节点群无法创建新区块并控制该内容为自己所用。而在下一次共识产生时，系统会自动选取一个多数节点群。多数投票节点为随机抽样，这样可以禁止下次投票中个体对投票选择的特定影响。该算法的具体描述请参阅备注文章。[12]

5.2 关于新区块产生的算法

- 假设在某个时间点用户创建了一笔交易I。
- 该交易被转交到与客戶相关联的最近一个节点。
- 节点可能处于下面三种情况：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。
  护送节点会将交易发送给主节点。
- 主节点会核对交易，如果交易正确则将其发送到护送节点，并将交易I写入正在生成的区块中。
- 护送节点接收到交易I后,会核对信息并将它写入已生成的区块内。

[12]magnet:?xt=urn:btih:c5a3d2762bd1f10c18f51b2606b1a32549d79ed4&dn=Article%20concensus%20sdBFT. pdf&tr=udp3A%2F%2Ftracker.leechers-paradise.org%3A6969&tr=udp%3A%2F%2Ftracker.coppersurfer.tk%3A6969

- 上述一系列操作会被不断重复，直到区块生成完毕，但全程不会超过20秒。
- 在此之后，主节点会发送消息通知区块关闭。
- 各个护送节点计算交易区块的散列、电子签名散列然后把收到的散列发送给主节点。
- 主节点会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的 2/3，则会认定该区块生成。如有效签名数达不到要求，则区块生成失败。
- 区块链没有时间概念，不检查也不依据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都具有许多严重漏洞，其中最危险的是:

- 在伪随机数的创建过程中，用“timestamp”作为“seed”的替代品，最终，如果非法攻击者知道用于生成伪随机数的算法及其生成的大致时间，他可以大概率地选择由该算法生成的私钥（密码）。
- 即使除了“timestamp”外，使用其他的数据，标准的伪随机数生成器也会生成足以具有预测性的序列，这很可能会使得攻击者可以通过测算法破解密码（散列）。

在MILE平台里，从密钥生成到电子签名到区块链的数字都是随机使用的。对此，平台对随机数的质量增加了特殊要求。从随机数发生器获得的序列都应该经过完全测试。测试发生器的结果如下所示。

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，为了进行检查需要执行以下操作:

1. 在加密模块中有一个用于检查生成函数实现和随机序列测试的工作台，由工作站编程组成。工作站安装了 Visual Studio 2017 IDE和MILE 应用程序。
2. 有一些 GNU软件被安装在工作站上用于测试，他们是:
   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1024GB。复制到存储器中的制定随机量变序列是在二进制文件(1000字节)和StatCurrent (2000字节)中执行的。
4. 在自动化工作站上，利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，以检查主要统计标准的执行情况。
5. 为了评估解释被二进制随机数列的质量，我们使用3s准则来计算二进制数字的相对频率

$$(0,5-\frac{1}{2}D\frac{1}{2}-1,5[1-4D2)n-1]0,5,0,5+\frac{1}{2}D\frac{1}{2}+1,5[1-4D2)n-1]0,5$$

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	$\frac{1}{2}D\frac{1}{2} = 0,01$
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，我们使用了255个自由度的判断标准c2:

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

7. 为了验证动态测试程序，要对测试结果进行处理、分析和评估。如果所使用的统计标准不排斥第五小节所列分析的随机数序列均匀分布的假设，则该检验被认为是成功的。

5.3.3 统计研究结果

StatMessTime 材料处理结果

表2. 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

表 3.1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

表4. 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

最小结果: 0.4961 : 最大结果: 0.5042

表 5. 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

在StatCurrent 上的处理结果

表6.1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

表7. 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

表8. 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

表8. 1在位移量为1-512中的相对频率

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

表 9. 32768 字节材料中的字节频率

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

min: 99 max: 154

材料上的 c2 值为 32768 字节 (255个自由度)

$$c^2 = 239.8$$

5.3.4 结果

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，伪随机数列生成器生成的随机数列质量不低于0.5 + D，这满足了随机数序列均匀分布的假设。

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”）
- 不限交易最大数额
- 区块链定期会进行自我优化，支持额度设定
- 钱包中被标有“垃圾”设定的账户会被归零，参与区块链截断的节点将会接收其内容。

5.3.7 交易类型

- 发送XDR
- 发送MILE
- 节点注册声明
- 节点删除声明

- 新创世区块(截断)
- MILE/XDR 汇率投票
- 提交问题由节点投票
- 节点投票
- XDR 发行中心

5.3.8 控制参数

- 通过区块中的间隔可以开始阶段区块链的过程
- 如果前一个截断失败，则重复执行阶段区块链的过程
- 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，写入了区块链中事务处理的字符中
- 您可以在钱包中接收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:
    - 它保存整个区块
    - 可以作为节点注册
  - 多重签名:
    - 系统只接收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.
    - 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

这份手册主要是一篇关于算法的技术论文，因此这里简短介绍一下经济用例。

- 为使用SWIFT有问题且不属于国际清算银行的用户提供网络工具。这样的用户大约有30亿，数十个国家和地区：数十个非洲国家[13]、中国、俄罗斯、土耳其、委内瑞拉、伊朗、苏丹等等
- 快速自由地交易任何数额，并且可以不受审查

[13]https://www.bis.org/about/member_cb.htm?m=1 7C2 7C601

- 稳定独立地存储价值
- 为那些自认经济不发达的、没有美元的社区提供交换媒介，如果他们有自然资源或者任何有价产品，他们就可以使用XDR来进行审计、结算、监理和报告[14]。

7. 法律信息

加密资产属于近年出现的新的经济现象，所以世界范围内的立法还在进程中，无论如何，已经有几十个国家加密资产进行了规定[15] ，很多经济持续稳定发达、在全球享有高声誉的国家也在其中例如：瑞士、日本、美国、加拿大、韩国、德国等等。

鉴于XDR或MILE没有进行首次公开发行（ICO） 。XDR是由分散的网络组成的。它不具备证券的属性，这就是为什么根据不同国家的不同法律，XDR可以扮演下列角色之一：交换媒介或者无形数字资产。

[14]https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
[15]https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory