MILE

Free, fast, secure stablecoin

October 17, 2018

Tech Paper v.1.5

By Lotus Mile

Short version: mile.global

1 Introduction

There's no tool for measuring, storing and transferring value having all these properties at once:

- stable price;
- fast transactions;
- free transactions;
- no volume limits;
- censorship-resistant and irreversible transactions;
- transparent emission algorithm.

Existing fiat currencies (USD, EUR, CNY etc.) don't fit:

- Not a stable price. Most fiat currencies are volatile. Even in developed economies like Switzerland and Japan, the value of local currency can rise or fall very fast: JPY has fallen 15% in October-December 2016[1], CHF has been pumped 20% in one week in January 2015[2];
- Slow transactions. One should prepare a lot of documents and pass an exhausting series of negotiations to perform a money transfer of more than 10 000 USD in fiat currency between different countries. The transfer itself takes a few days with a risk of additional reconciliations and moving money backwards. Plus, it might take a few month to open a bank account in Europe;
- Expensive transactions. According to the websites of the payment systems, average currency exchange spread is roughly 3-5%.
- Growing censorship level. There are dozens of countries involved in sanctions and trading wars in 2018, being blocked from SWIFT transfers or having some serious limitations. Among them are: China, India, Russia, Iran, Turkey, Venezuela. 5 of them are in top-30 countries by GDP[3].
- Transaction reversibility.

[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)

- Nontransparent emission algorithm, controlled by limited amount of private persons. That leads to hyperinflation and economic crises[4]. Formally Central Banks of the developed countries publish M0 and other indicators, but nobody has audited those numbers.

Existing digital currencies also don't have those qualities in one entity:

- BTC is uncensored, but is too volatile;
- Lot of existing stablecoins are tied to the centralized fiat storages, i.e. are 100 % dependent on one of the parties, which could be corrupted (USDT, Circle etc.);
- Lot of existing stablecoins are attached to the precious metals, labour force price or another assets, but those are not stable. Gold can rise or fall to USD at 15% a month[5].
- ERC20-based stablecoins depend from the Ethereum mainnet, which is being clogged when each popular application is showing up[6];
- Algorithmic stablecoins are subject to Soros Attack[7];
- The only working stablecoin family with fast and cheap transactions is BitShares BitAssets. But there's a major issue: Dan Larimer has left the BitShares community and that lead to the downfall. BTS daily trading volume is floating around few millions of dollars[8] and the main BitShares forum has only dozen of active topics weekly[9]. And the main issue is the excessive centralization of the BitShares delegates and committee members: there's only dozen of them[10], so a very few people actually rule the network.
- There are some projects at the early whitepaper stage, trying to describe a decentralized stablecoin. Those are out of this documents' scope, because they're not working at the time.

Thats means there's an market for the product with the following qualities all-in-one:

1. Stable price;
2. Uncensored;
3. Free transactions;
4. Fast transactions;
5. Allowing anyone to issue the coin.

This solution will allow people, enterprises and countries:

- To send any amount of value to any place in the world instantly and free, despite sanctions or trading wars or SWIFT issues;
- To store any amount of value for a long time for free.

2 Price stability

Money is a social construction.

The only thing defining moneyness of the entity is how many people are using this entity as a money for trade, loans, investments, remittance and reserves. USD is not pegged to gold since Nixon Shock, and is constantly issued. But it's still used and relatively stable to other currencies, because a lot of people use it for the real economy. Crises are happening when money are printed much faster than the economy is growing.

[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

That's why the stability of the MILE's network stablecoin price is based on two things:

- Wide usage for the real economy: trade, loans, investments, remittance and reserves.
- Algorithms for making money supply growing not faster than the economy growth.

Real economy usage is way more diplomatical task than a technical one. Anyway, the combination of all-in-one qualities (stable price, fast and free transactions, censorship resistance and transparency) is highly competitive comparing to the existing fiat and crypto currencies.

Algorithms of money supply management are described in the next chapter.

3 Emission algorithm

There are two coins in MILE network: XDR (stablecoin) and MILE (index of demand on XDR).

3.1 XDR

- XDR is a stablecoin, used as unit of payment and storage of value.
- It's issued by MILE token holders and blockchain masternodes via the open source algorithm.
- It's tended to be equal to 1 IMF SDR [11] via the social consensus and money supply management algorithms.
- XDR is used as a deposit to be locked inside the blockchain to launch a masternode.
- XDR has 12 integer and 2 fractional digits, i.e. the maximum supply of XDR is 999 999 999 999.99 (almost 1 trillion). Maximum amount could be updated via the masternodes consensus and soft fork[12].

3.2 MILE

- MILE is an index of demand on XDR.
- MILE/XDR rate is set once a day by node voting of blockchain network.
- Node owners that use data from stock exchange, OTC deals and offline economy publish a fair currency rate as they consider it.
- MILE/XDR rate shows how many XDRs one can print via the emission center.
- MILE is used as a deposit to be locked inside the blockchain to launch an emission centre.
- MILE has 9 integer and 5 fractional digits, i.e. the maximum supply of MILE is 999 999 999.999 99 (almost 1 billion).

3.3 Primary emission

- Initially there are 300 000 XDR in the genesis block which will be locked as a masternode deposit to launch the consensus.
- Initially there are 999 999 999.999 99 MILE in the genesis block and new MILE will not be emitted in the future.
- Initial price is 1 MILE = 1 XDR.
- Initial MILE distribution and price are based on the following statements. The MILE ecosystem is the result of 1.4B USD in capital, consisting of the combination of fiat currencies; crypto assets, factors of production, intellectual property, human resources, brand value, real

[11] `https://www.imf.org/external/np/fin/data/rms_sdrv.aspx`
[12] `https://www.investopedia.com/terms/s/soft-fork.asp`

estate, and goodwill, as well as other tangible and intangible assets put together. This has resulted in the spreading of the initial 1B MILE to 108 wallets.

3.4 Secondary emission

3.4.1 Masternode emission for the block closure (minting)

- To become a node and take part in consensus for block signing one need to install MILE application and deposit 10 000 — 100 000 XDR to the blockchain.
- An operating masternode receives 8-13% from the blockchain per annum on its deposit in XDR depending on deposit volume. Those receivables are minted constantly and delivered once in 1-2 days. The dependence is parabolic — the closer the 100 000 deposit, the faster the % is growing.
- Anyone can run a masternode from the public installation package (docker).
- One need to have a modern PC with 4 TB hard drive and a reliable Internet connection.
- This emission type is motivational for network participants that keep blockchain operation on.
- There could be any number of masternodes, but consensus is build only from 10 000 of them (active nodes). The rest of the nodes are working in waiting mode, e.g. they can store the blockchain, but they don't receive the block for signature and don't receive the minting premium.
- If some of the active nodes failed to sign the block, it's kicked out of consensus, and the closest waiting node is turned active instead.
- Due to the limit of 10 000 active nodes, the monetary base for the 8-13% minting premium is limited with 1 billion XDR. E.g. if the ecosystem will grow, for example, to 10 billion XDR, the overall inflation will be 0.8-1.3% which is very small.
- If all 1 trillion XDR will be minted, masternodes will stop receiving minting premium. Most likely, that will lead to the soft fork with upgraded maximum supply of XDR.

3.4.2 Emission centres

- To become an emission centre one needs to deposit 10 000 MILE or more to the blockchain.
- The blockchain will instantly issue new XDR to the emission centre's wallet. The amount of issued XDR is defined by the internal blockchain MILE/XDR rate.
- If MILE/XDR rate had risen over time, then every emission centre can issue more XDR, because the limit has grown.
- If one wants to unlock the MILE from the emission centre, he must send a proper amount of XDR to the blockchain according to the current MILE/XDR rate. 0.2% in XDR is charged for that operation. It's a tool to prevent the flood: millions of useless transactions from malicious users trying to clog the network. The commission is spread between the active masternodes.
- If the demand on XDR will grow, the MILE/XDR will rise. If the demand on XDR stop growing or turned negative, the MILE/XDR rate will be stable or will fall.
- In case of XDR emission on $MILE/XDR = N$, an opportunity to unblock the MILE will be possible only in case of $MILE/XDR$ that would become $\geq N$.
- Certain algorithms are used to cut off the noise of inadequate low or high MILE/XDR votes from the masternodes, to make the MILE/XDR less volatile.
- Certain algorithms are used in order to calculate MILE/XDR that are similar as moving average calculation, i.e. there will be used historic exchange rates that are kept in blockchain.

It will lead to the minimum range of possible local manipulations, and will provide slow growth of the XDR supply to avoid hyperinflation.

3.5 Reflection point

- Due to zero comission for XDR transfer, the system allows making microtransactions and that is why in order to support the long-term blockchain maintenance there is a procedure for a periodical truncation.
- Truncating algorithm is getting enabled when the blockchain size is reaching a 4 TB size. The system condionally removes all the zero (dummy) or less 1 XDR transactions from the blockchain body. Blockchain status will be written in the new Genesis Block after a cleanup. Previous state of blockchain will be saved only on the special archive nodes. To be an archive node is a voluntary decision.
- The leftovers from those truncated transactions will be sent to the master nodes after the truncation.
- Also dead nodes (who are not responding for a long time) will be deleted while saving their assets on wallets when the blockchain truncates.

4 Free fast transactions

Commission for the XDR transactions is 0 %, commission for MILE transactions is 0.01 MILE. Block is closed in 20 seconds, bandwidth is up to 10 000 transactions per second. Blockchain optimization is performed by means that we don't keep input-output information unlike the UTXO-model in BTC-like systems. Free transaction basis for users is possible thanks to the masternode minting mechanism.

To process 10'000 transactions per second a machine needs to handle about 600'000 transactions per minute. A single 3Ghz processor core can process about 80'000 tx/min due to the e-signature checking. That means, the network needs at least 1 master node per each big internet segment (EU, US, China, Russia, Latin America, Africa, Australia, ASEAN) with at least 8 cores with 3Ghz per core onboard to process 10'000 tps.

5 Blockchain

5.1 Choice feasibility

Goals for the blockchain MILE application required the consensus that is responsible for the following blockchain features.

1. Total creation time of a new block is 20 seconds.
2. Total number of hosts that can take part in consensus production may vary from 10^3 to 10^4.
3. High speed of transactions – is no less than 10^3 transactions per second.
4. Blockchain algorithm performance should not require sufficient computer power in comparison to Proof-Of-Work blockchains (Bitcoin, Ethereum etc.).

sdBFT was chosen as the algorithm that has a higher operation capacity in comparison to BFT algorithms. There's a lot of potential participants of consensus in sdBFT, plus, it's a short timeframe between the blocks, so it's very complicated to corrupt the voting and push malicious transactions to the block content.

Quasi-random sampling of voting host array will not allow a significant influence on host choice by the next voting. Detailed algorithm description is provided in the separate article[13].

5.2 Algorithm of forming a new block

- Let's assume that at some time moment a user forms the transaction I.
- Transaction is sent to the nearest node which this client is bound to.
- Any node may be in one of three states: passive, escort and master.
- If node is passive then it checks the transaction and sends it further by peer-to-peer network until the transaction reaches an escort-node.
- The escort-node sends transaction to the master-node.
- Master-node checks the transaction and if it is correct then sends it to escort-nodes and also writes transaction I in a forming block.
- By receiving the transaction I, escort-nodes check it for authenticity and write it to the forming block.
- This sequence of operations is repeated until the block is completed but lasts no more than 20 seconds.
- After that the master-node sends a message on the block completion.
- Each escort-node calculates the block hash of transactions, hash digital signature and sends the received hash to the master-node.
- Master-node calculates the quantity of assumable correct digital signatures. If the received number of correct signatures is more than 2/3 of the total escort-node quantity, the block is assumed to be completed. Otherwise, the block is not completed.
- Blockchain is out of time and it doesn't check or accord the time of transactions that are placed into a block.
- Systems that work beyond blockchain will be oriented on some averaged time of block completion (about 20 seconds).

5.3 Generator of pseudorandom numbers

Standard generators of preusorandom numbers that are built-in operating systems usually have a range of severe vulnerabilities. The most dangerous of them are:

- In place of 'seed' for pseudorandom number creation is used a 'timestamp'. Eventually, if an attacker knows the algorithm of pseudorandom number generation and estimation of generation time then it's highly possible that he can bruteforce a private key (password) that was generated using the same algorithm.
- Even if apart from 'timestamp' there are some other data used, than the standard generators of pseudorandom numbers generate pretty predictable sequences that allows attackers a chance to bruteforce passwords (hash-data).

In the MILE blockchain random numbers are used universally: from key generation to the "salt" in electronic signature. Bearing this in mind, there are specific requirements to the quality of random numbers. The sequence that is not from the random number generator is thoroughly tested. The results of generator's work are below.

5.3.1 The goal of testing

The goal of testing is to check the facts of the dynamic control of the generated sequence by random numbers. It is used for a statistical hypothesis proof on a steady coverage of generated sequences.

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

5.3.2 Conditions and the testing order

Tests consist of the sequence check of random numbers that are generated by the program generator of the pseudorandom numbers. For the control handling there are following action steps:

1. There is a workbench for checking the implementation of generation function in the crypto-module and testing of random sequence which consists of the workstation programming. It is the workstation with installed Visual Studio 2017 IDE and MILE application.
2. There is some GNU software is installed for tests at the workstation. They are:
   a) NIST Statistical test Suite (NIST-STS);
   b) Test-U01.
3. With a help of pseudorandom sequence generator there is a sequence of random numbers generated that is a maximum on conditions of natural restrictions for performance and the testing length duration, but no less than 1024 GB. There is a copying of the set sequence of random variables into the binary files StatMessTime (portions by 1000 bytes) and StatCurrent (portions by 2000 byte).
4. Analysis is performed on the workstation for the chosen sequence of random variables with a help of the packets on statistical tests described above in order to check the execution of the main statistical criteria.
5. For the quality assessment of a random sequence, that is being interpreted as a binary, it was used the criterion $3s$ for the relative frequencies of binary signs with an interval

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

   on n material of binary signs by $p=0,5+D, q=0,5-D$.

Table 1. used the following criterion intervals $3s$:

	criterion intervals $3s$:	
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. In order to estimate the quality of the random sequence that is interpreted as a byte sequence, the criterion c^2 was used with 255 degrees of freedom:

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

7. For the verification procedure of dynamic testing there are the following methods of expertise: processing, analysis and test results assessment.
   Verification is presumed to be completed when the used statistical criteria do not refuse the hypothesis on the uniform distribution of analyzed random number sequence that was described in p.5.

5.3.3 The results of statistical research

The results of the StatMessTime processing

Table 2. **Frequencies of 1 in 16 segments for 1024 bytes**

4075	4129	4206	4148	4098	4180	4042	4021
4092	4134	4202	4226	4064	4052	4070	4112

Table 3. **Relative frequencies of 1 in 16 segments for 1024 bytes**

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

Table 4. **Relative frequencies of 1 in shift sums of 1-512**

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

The result is min: 0.4961: max: 0.5042

Table 5. **Byte frequencies on the 16384 byte material**

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

min: 41 max: 86

Value c^2 on the 16384 byte material (255 degrees of freedom): $c^2 = 268.5$

The results of StatCurrent material processing

Table 6. **Frequencies of 1 in 32 segments on 1024 bytes**

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

Table 7. **Relative frequencies of 1 in 32 segments on 1024 bytes**

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

Table 8. **Relative frequencies 1 in shift sums of 1-512**

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

Table 8 Relative frequencies 1 in shift sums of 1-512

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

min: 0.4970: max: 0.5030

Table 9. **Byte frequencies on 32768 bytes material**

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

Table 9. **Byte frequencies on 32768 bytes material**

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

Value c^2 on 32768 bytes material (255 degrees of freedom)

$$c^2 = 239.8$$

5.3.4 The result

MILE blockchain software random numbers generator is based on double calculation of hash functions with dynamic change of the primary state. The quality of random sequence that is produced by the generator of pseudorandom sequence is no worse $0.5 + D$ on the binary sign on condition of $|D| < 0.01$, that is satisfactory for the hypothesis of uniform distribution of the analyzed random number sequence.

5.3.5 Cryptography

- ECSDA Digital Signature algorithm (used in BTC).
- Ed25519 scheme (faster than that one being used in BTC)
- SHA-3 hash algorithm (faster and more secure than in BTC)

5.3.6 General features of blockchain

- Microtransactions support (a “coffee tip”) thanks to the zero comission fees.
- Max sum of a transaction is not limited.
- Periodically blockain makes a self-optimization and supports its volume in the set limits
- Wallets with "junk" balance are reduced to zero and its content is received by nodes that participate blockchain truncation.

5.3.7 Transaction types

- XDR sending.
- MILE sending.
- Announcement on a node registration.
- Announcement on a node dismissal.
- New genesis block (truncation).
- MILE/XDR rate voting.
- Question submission on node voting.
- Node voting for one of the alternatives.
- XDR emission.

5.3.8 Managing parameters

- Interval in blocks that starts blockchain truncation procedure.
- Interval in blocks that reruns the truncation procedure if the previous attempt was not successful.
- Deposit range that allows to create the node.
- Maximum quantity of nodes.
- Update on managing parameters is performed through the node voting.

5.3.9 Wallets

- Wallet address is symbol sequence in the Base58checkerMod2 charset which writes in transactions that is in the blockchain.
- You can received and take both XDR and MILE on the wallet.
- Types of wallets:
  - Light:
    - For mutual offsetting (transactions) and balance check.
    - It uses a special protocol that allows to get the necessary blocks and check only the Merkle tree, but not the whole blockchain.
  - Standard:
    - it keeps all the blockchain.
    - It can be registered as a node.
  - Multisig:
    - Virtual wallet where only if several signatures available then the transaction would be accepted.
  - Point wallet:

    - Developer's wallet where the system point control is performed that is based on the change of managing parameters.
    - Only the first year of blockchain work is needed and then it will be turned off and written in the blockchain.
  - System wallet:
    - This wallet is for comission accumulation from removable wallets in blockchain truncation.
    - It can form an outgoing transaction only for comission fee payment to the nodes that participated in blockchain truncation.

6 Use Cases

This document is mostly a technical paper about the algorithm itself, that's why the economical use cases will be covered briefly.

- Settlement and multilateral netting tool for those who have issues using SWIFT and are not the part of the Bank of International Settlements. It's almost 3 bln. people, dozens of countries and territories: dozens of African countries[14], China, Russia, Turkey, Venezuela, Iran, Sudan and more[15].
- Free and fast transactions of any volume with an option to be uncensored.
- Stable and independent value storage.
- Medium of exchange for the communities who thought they're poor because they don't have USD. If they have a natural resources or can produce any viable products, they use XDR to establish an offset accounting, settlement, custodian and reporting.

7 Legal framework

Crypto assets are relatively new economic phenomena, so the legislation across the world is in progress. Anyway, dozens of countries have already installed some regulations on crypto[16], and there's a lot of wealthy and highly reputable countries among the list: Switzerland, Japan, US, Canada, South Korea, Germany and more.

Since there was no token sale (ICO) for the XDR or MILE. XDR is minted by the decentralized network, e.g. there are no attributes of securities. That's why, depending on different legislation in different countries, XDR could play one of the following roles: medium of exchange or an intangible digital asset.

[14] https://www.bis.org/about/member_cb.htm?m=1%7C2%7C601
[15] https://www.treasury.gov/resource-center/sanctions/Programs/Pages/Programs.aspx
[16] https://en.wikipedia.org/wiki/Legality_of_bitcoin_by_country_or_territory