MILE

Free, fast, secure stablecoin

August 28, 2018

Tech Paper v.1.2

By Lotus Mile

Short version: mile.global

1 Introduction

There is still no tool for measuring, storing and transferring a value that would have the following simultaneous properties:

- a sustainable cost;
- a transparent emission algorithm;
- a free, fast and value transfer without charge to any party in any place of the world and with no volume limit;
- a secure value storage in a long term timespan;
- non-blocking non-returning transactions.

The existing basic currencies (USD, EUR, CNY and etc.) do not solve the matter:

- it takes several documents and a series of reconciliation for a legitimate transfer of more than 10 000 USD in fiat currency between different countries. The transfer itself takes more than a day with a risk of additional reconciliations and transfer withdrawal;
- national debt trust is decreasing year after year, a number of defaults on government stocks is about 0.25 tn USD on average per year, national debt is getting bigger;
- principles and reports of fiat money emissions are not transparent;
- most fiat currencies are fluctuating greatly every year. Even in sustained economies like in Norway, EU and Japan the value of local currency fluctuates within 15-25 % per year. In such circumstances people automatically consider alternative means of offsetting;
- central bank as a main contractor, takes more risks than ever and the US withdraws from 10 to 150 banking licenses, in the EU almost a trillion EUR have banks with high default risks, a half of banks have been revoked for the past 7 years in Russia;
- it might take between a month or a half a year in order to open a bank account in Europe;
- in any country of the world a bank can block finances until the legal clarification or the government establishes new laws or resolves the issue post factum that the finances were obtained illegally and impose a fine of up to 100% of Deposit amount as happened in Cyprus.

Today's digital currencies also do not solve these problems:

- BTC is decentralized, but is too volatile;
- Integrating Lighting Network the price transaction in BTC decreased down to 1.2 USD, but it is still expensive for such a "coffee tip" and taking into an account the limits of this technology, such fee is fine only for the significant money transfers;
- existing stablecoins are tied to the centralized fiat storages, i.e. are 100 % dependent on one of the parties;
- existing stablecoins have non-transparent emission mechanisms;
- Market Pegged Asset in BitShares are tied to the BTS pledge cryptocurrency which is more volatile than BTC.

That is why there's a strong demand for a new space with the following set of features

1. Means of payment with a stable price that is tied to the XDR.
2. Transparent emission, based on open source code with mathematically proven concept.
3. Free transactions for XDR and 0.2 % commission for MILE transactions.
4. Fast transactions with a delay of less than a minute.
5. Decentralized on 10 000 nodes all over the world and owned by different people and organizations.

This solution would allow people:

- to be sure in the reliability of their assets;
- to sent any amount of value to any place in the world at no extra charge, freely, fast and securely.

2 Price stability

There are two levels of consensus in social resource systems - social and technical.

Take the BTC example:

- social consensus is a community-driven discussion of new bitcoin network protocol versions;
- technical onchain-consensus is a miners' voting on installing or not installing software on their devices that support new bitcoin network protocol versions.

No matter how technical consensus is formed, social level is always more powerful:

- there are instances of technically modern and formally transparent consensuses where the centralized elite has corrupted the voting by bribery (LISK, developed democratic governments);
- the opposite is also true: sane and moral people can negotiate verbally without using any sophisticated technologies.

Network members of MILE have come to an agreement on a social level that 1 XDR in MILE system equals to 1 XDR (currency rate is calculated and published by IMF).

The main area of XDR application is real commodities and services exchange. That is why stock trading and stock price for a definite currency cannot have any significant influence on XDR value.

For instance, the total daily volume of stock trading of the most popular BTC cryptocurrency on the world exchange is about 5 billion US dollars by the end of March 2018. The total volume of transactions in bitcoin network is only 1 billion USD. Stock volume of Ethereum is 1.5 billion and network transaction volume is 0.7 billion USD. Bitcoin Cash is 0.4 billion versus 0.2 billion USD.

It should be taken into an account:

- investigation on "imaginary" volumes of crypto exchanges;
- most of the cryptotransactions are transfers between exchange wallets, merges and transitions of bigger wallets as for example:

  - 40 % of daily volume is transferred with only a hundred of transactions in BTC, it's about 30 million US dollars per transaction;
  - it takes 100 transactions in ETH to make a fourth of the volume in total;
  - BCH — is almost 40 %;
  - LTC — 61 %.

so that the real coin exchange is less in 1.5-3 times.

Most of the coins on the coinmarketcap have a zero exchange in real economy, but they still strive to increase stock exchanges volumes. For this reason the value of cryptocurrencies is almost entirely dependent on speculation and news buzz and cryptocurrencies themselves have a high volatility risk.

There is a different approach in MILE:

- participants do not strive to pull XDR on stock exchanges and artificially increase the volume of trading;
- the main designation of XDR is:
  - means of keeping and transfer of assets;
  - means of commodity and service exchange in the real economy.

With a help of that even if someone tries to lower the stock price of XDR, then it will benefit those who use it in their daily lives. Anyone would like to buy 1 XDR on stock exchange for 0.8 XDR as its purchase power in the real world would not be affected of such stock exchange trend.

Let's take a look at the practical use of XDR in the next chapter.

3 Emission algorithm

There are two principles in the MILE platform that are used for payments and emissions: Coin (XDR) and Token (MILE).

3.1 XDR

- is a payment unit for storage and exchange of values within the platform..
- is emitted by the transparent algorithm by MILE token holders and blockchain network nodes.
- is always equals to 1 XDR from IMF (up-to-date currency exchange XDR/USD).
- has the number of units: 12.
- has the number of fraction units: 2.
- i.e. the limit quantity of XDR is 999 999 999 999.99 (1 trillion).
- is also a payment unit used as a "fuel" to blockchain nodes and it is so-called the "node deposit" which allows to classify bona fide participant of the system as he spends the resources on maintaining the MILE network.

3.2 MILE

- is the main parameter in the emission algorithm of XDR.
- Exchange rate MILE/XDR is set once a day by node voting of blockchain network.
  - Node owners that use data from stock exchange and other exchange sources publish a fair currency rate as they consider it.

  - The final exchange rate of MILE/XDR is considered for current day in terms of consensus procedure. It is used for maximum limits of emission by the emission centers.
  - 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.
- Number of whole units: 9.
- Number of fraction units: 5.
- i.e. the limit quantity MILE: 999 999 999.999 99 (1 billion).

3.3 Primary emission

- Initially there is 0 XDR[1].
- Initially there is 1 000 000 000 MILE in the system and new MILE will not be emitted in the future.
- Initial price is 1 MILE = 1 XDR.

3.4 Secondary emission

3.4.1 Node emission in block closure (minting)

- Blockchain node emission in block signing (minting)
- According to the MILE algorithm, an operating node receives from blockchain 8-13% per annum on its own deposit in XDR depending on its volume.
- The algorithm works as follows: % per annum is received on the wallet approximately everyday in fractions of random size, but annually there will be 8-13%.
- In order to get a right to become a node and take part in consensus for block signing you need to install MILE application and have a deposit of 10 000 — 100 000 XDR on your wallet.
- The prime for block closure depends on deposit sum non-linearly.
- Project source code will be available for public and anyone can set up and run the node.
- You need to have a modern PC with 4 TB hard drive and a reliable Internet connection.
- This way of emission is motivational for network participants that keep blockchain operation on.

3.4.2 Emission of emission centers

- MILE tokens are kept on the users' blockchain wallets.
- Owner of the MILE tokens may deposit any quantity of MILE on a special storage address.
- User need to deposit no less than 10 000 MILE in order to become an emission center.
- This will allow instantly receive the necessary quantity of XDR on his wallet by the current rate MILE/XDR that was determined previously by the node consensus and reported in blockchain.
- If over time at the t_2 moment, the rate of MILE/XDR had risen then the a user may call a wallet command "release XDR" and the system can additionally pay XDR in amount of $MILE \cdot (XDR(t_2) - XDR(t_1))$.

[1]There will be emission of 300 000 XDR in the genesis block which will be transferred on node deposit as part of consensus. These nodes belong to the MILE and will be supported in active state as long as possible.

- For MILE token unblocking a user need to send to a special XDR address and will receive the MILE for a current rate MILE/XDR with deducting 0.2%. Commission charge is needed for lowering the 'flood' in blockchain and it is spread between the nodes, i.e. participants that keep the network support.
- Over time if there would be an increased community demand in XDR the currency rate MILE/XDR will rise. That is why MILE holders will be interested in a long-term token deposits.
- 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 $\geq N$.

3.5 Economic feasibility of emission

- The more users keep deposits for node support and/or emission centers, the more people need XDR and the higher the MILE currency rate.
- The more users use XDR for real trading deals, the more XDR is needed and the higher the MILE currency rate.
- The higher rate for MILE the more XDR can be emitted.

3.6 Reflection point

- Due to zero commission 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 conditionally removes all the zero (dummy) or less 1 XDR wallets 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 nodes.
- Nodes will use destroyable leftovers from relatively empty wallets (with less 1 XDR) while the blockchain truncates in order to pay the commission fees.
- Also dead nodes will be deleted while saving their assets on wallets when the blockchain truncates.

4 Free fast transactions

Transactions in the MILE network are free of charge (commission for XDR transactions is 0 %, commission for MILE transactions is 0.2 %), block is closed in 20 seconds, projected 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 'minting' mechanism (see the part "Node emission in block closure (minting)") and the 'Reflection point' function.

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 PoW blockchains.

sdBFT was chosen as the algorithm that has a higher operation capacity in comparison to BFT algorithms. There are a lot of potential participants of consensus that complicate the preliminary fixed negotiation as the voting host group form a new block by managing block content by its own as by the next consensus another array of voting hosts. Quasi-random sampling of voting host array will not allow a significant influence on host choice by the next voting. Algorithm description is provided in the following article Article consensus sdBFT.

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.
- Node may be in 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 prevails 2/3 of the total escort-node quantity that participate in the consensus, 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 pseusorandom 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.

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 cryptomodule 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	$\frac{1}{2}D\frac{1}{2} = 0,01$

Table 1 continued from previous page

	criterion intervals $3s$:	
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

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

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

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

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
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 commission fees.
- Max sum of a transaction is not limited.
- Periodically blockchain 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

- Microtransactions support (a “coffee tip”) thanks to the zero commission fees.
- XDR sending.
- MILE sending.
- Announcement on a node registration.
- Announcement on a node dismissal.
- New genesis block (truncation).
- Currency rate MILE/XDR publication.
- Question submission on node voting.
- Node voting.
- XDR emission/reverse emission of the emission center.

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 receive 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 commission accumulation from removable wallets in blockchain truncation.
    - It can form an outgoing transaction only for commission fee payment to the nodes that participated in blockchain truncation.

6 Practical application

6.1 Free international payments

Cryptocurrency market has grown thanks largely to the demand on fast and cheap international payments. It is especially true to China where other currencies are largely limited by the government.

Following the results of the Money 2020 conference participants in Singapore, there is no payment system that can make international transactions more than 5 000 USD. The only way to transfer more than 5 000 - 10 000 USD between the countries is SWIFT. In order to make a transfer you need to fill in many documents and wait until a bank authorizes it and discuss the details with the currency control manager and then wait another few hours for the transfer completion. SWIFT commission fee is about 1%.

MILE allows to send any amount of payments in any place in the world within a few seconds and without any banker interference.

6.2 Independent storage

Keeping cash at your home is pretty dangerous. There is a contract clause about safety deposit box which states that the bank does not take any responsibility for keeping the deposit box safe. A lot of money is regularly stolen from safety deposit boxes as a result of this clause. Bank closing statistics is provided in the "Introduction". MILE allows to securely keep the money in the decentralized network with a zero-risk of central counterparty and with no account blocking.

6.3 International cooperative economy

One of the most important aspects for making the MILE worth is the real commodity and services turnover. MILE authors see the biggest potential of the MILE spreading in cooperative economy and especially in developing countries with unstable monetary system. Especially on those markets there a high deficit of fiat money and the disposition to the barter transactions and other ways of offsets.

Most of the developed countries are almost stopped their economy growth and the most input in the development of the world economy are now doing the developing countries. The same applies to the business: big corporations except for some financial holdings have a profitability less than 5 %. In crisis years even the rich financial companies experience heavy losses.

Meanwhile **cooperatives are historically growing against the market scenario and especially in the crisis**. For example:

- Rabobank showed the growth for 42 % in 2008 and its founder members got 20 % depoist increase. For the years 2008-09 the level of participation in credit unions have grown significantly.
- Every 3rd Canadian is a member of credit union system and a share of credit unions on deposits of retail market and residential mortgage increased from 16 % to 19 % in 2010 [Moody's investors service global banking report, April 2010].
- Since the 1st quarter of 2012 the Desjardins cooperative has been ranked 16th place from 7500 deposit financial institutions in the North America and the 2nd place on the tier one capital index which is 16.8 %.

The volume of cooperative economy is high, cooperatives are popular in rich and developing countries:

- Cooperatives tally 1 billion shareholders around the world.
- Indian cooperatives cover 67 % of rural population in commodities demands.
- 40 % of African householders are involved in cooperatives.
- Income of the 1500 biggest cooperative organizations in 2010 made almost 2 trillion US dollars.
- Development International Desjardins (DID) is the leader in microfinance. They work with 8.8 million of members and clients all over the world and have lending capital for 2.5 billion Canadian dollars.
- In some African countries Desjardins makes 35 % of the microfinance market.
- In China cooperatives make 91 % of the microloan market.
- Credit cooperatives provide billions of US dollars for money transfers from migrant workers that have jobs in the developed countries to their families in the developing countries and that especially important for Latin America and Africa.

Cooperative economy works more effectively, because:

- Cooperative's work is directed on the income for all shareholders, but not on blowing the

stock capitalization.

- All shareholders are involved and there is no need to spend money and time for their motivational aspect.
- Corporations' top-management earns in 100 times more than regular workers, but in cooperatives it's in 10 times as expenses are way lower.
- Due to the new economy outline and offsets between the members of the cooperative it is possible to reduce expenses on taxes, transactions and intermediaries. It will also help to reduce the demand in fiat credits.
- In the end the price for commodities and services inside of the cooperatives will be on 40 % lower than on the international market. This will stimulate the capital and people from the outside and motivate for the long-term participation in cooperative.

Solutions that are created for cooperatives based on MILE:

- offset accountancy,
- depository for storing receipts and balance checks,
- external fundraising,
- financial reporting to the tax authorities,
- juridical templates for tokens' work procession,
- commodity and service marketplace with big discounts.

7 Ecosystem participant motivation

Users:

- Get a chance to make free and fast transactions or keep a value on a long-term basis in the cryptospace.

Investors:

- are interested in investment returns.
- Return might take place through the system support, i.e. any participant can become a blockchain node and/or emission center.

Emission centers:

- are interested in the MILE currency growth as it will increase their capital and regular income.

Node owners:

- are interested in receiving commission fees for block signing in blockchain.
- Income range of the node owner - 8-13 % per annum in XDR.

8 Legal framework

Daily usage

In case if that is not required local laws or transaction volumes are low, or transaction frequency is absent then there is no need for legal arrangements on MILE usage.

In other cases, especially in active transaction spree in big volumes, it is recommended to create local cooperatives or consumer societies, or enter the existing ones.

The main mean of cooperative is a share. First fee is the asset contribution of a shareholder in the share fund of consumer society of money, capital issues, land property of land share any other property, or any other right that has a money value. Return of the share contribution is not taxed and it does not depend on the sum or price of a commodity that received the shareholder.

Any share exchange inside of the cooperative is possible and not taxed, i.e. juridically MILE can be used as a tool for share price estimation.

For outsiders of the cooperative, MILE can be utilized as a loyalty program:

- Token is a right to use a bonus point. This right can be sold to a legal entity or an individual and it can be taken into accounting records.
- The token owner can have a right for bonus points, receive points and get a commodity for these points at the moment of token exchange on commodity/service.
- The same scheme is used in supermarkets for bonus points and air companies for bonus miles.