MILE
Stablecoin libre, rapide et sécurisé

19 juillet 2018

Tech Paper v.1.2
By Lotus Mile
Short version: mile.global

1 Introduction

Pour le moment, il n'y a pas d'instrument pour mesurer, stocker et transférer de la valeur, qui possède les attributs suivants:

- prix stable
- algorithme d'émission transparent
- transfert gratuit, libre et rapide de la valeur à tout contractant se trouvant à n'importe quel coin du monde
- possibilité de stocker de la valeur à long terme
- transactions non-bloquées et non-remboursables

Les instruments de base existants tels que : USD, EUR, CNY etc. n'arrivent pas à résoudre le problème car:

- pour effectuer un transfert légal de plus de 10 000 USD en fiat à un autre état il est obligatoire d'obtenir plusieurs documents ainsi que d'attendre plus d'un jour l'accomplissement de la transaction. N'oubliez pas que cette transaction peut être bloquée;
- Le niveau de la confiance envers la dette souveraine ne cesse pas de baisser, les défauts de paiements sont de plus en plus fréquents ayant le total de 0,25 billard USD par an ; les dettes nationales sont en train d'augmenter;
- les principes de l'émission des monnaies-fiat ne sont guère transparents;
- la plupart des monnaies-fiat oscillent chaque année, c'est le cas même pour la Norvège, l'UE et le Japon qui semblent stables mais où les monnaies nationales fluctuent de 15-25% par an, ce qui mène à l'apparition de moyens de paiement alternatifs;
- vu que les banques sont les contractants principaux, elles font face à de nombreux risques. 10-150 agréments bancaires sont annulés aux Etats-Unis chaque année ; presque 1 billard de dollars se trouve dans des banques européennes qui menacent d'être en défaut de paiement ; quelque 50% de banques russes ont fermé leurs portes lors des 7 dernières années;
- ouvrir un compte dans une banque européenne vous demande 1-6 mois;
- dans n'importe quel pays la banque peut bloquer vos fonds, il se peut que les autorités introduisent

et infligent une amende allant jusqu'à 100% de la somme, comme nous l'avons vu à la Chypre.

Les monnaies numériques ne parviennent non plus à résoudre les problèmes cités ci-dessus car:

- le BTC est décentralisé mais trop volatile;
- grâce à Lightning Network le prix d'une transaction en BTC est désormais 1,2 USD, ce qui est tout de même trop cher pour « payer son café ». D'ailleurs, le champ d'application de cette technologie est limité, elle ne peut être appliquée que lors des acomptes;
- les "stablecoins" existants sont accrochés aux stocks-fiat centralisés et donc complètement dépendants de l'un des contractants;
- les "stablecoins" existants sont émis d'une manière non-transparente;
- Market Pegged Asset au sein de BitShares est accroché à la caution en BTS qui est encore plus instable que le BTC.

Voilà pourquoi nous créons un espace qui possède les attributs suivants:

1. Moyen de paiement stable dont le prix est lié à celui du XDR.
2. Emission transparente basée sur un code ouvert réalisé dans un algorithme mathématique clair et valide.
3. Transactions sans commission.
4. Transactions rapides en une seule minute.
5. Décentralisation grâce à 10 000 nœuds se trouvant dans les quatre coins et qui appartiennent à de divers gens et organisations.

Cet instrument permettra aux gens de:

- être sûr de la sécurité et de l’intégrité de la valeur;
- transférer de la valeur à n'importe quel endroit de la carte de manière libre, rapide, sécurisé et sans aucune commission.

2 Prix stable

Les systèmes que l'homme crée pour gérer les ressources ont deux niveaux de consensus qui sont social et technique.

Par exemple, prenons le BTC:

- le consensus social, c'est la discussion sur la nouvelle version du protocole du réseau BTC;
- le consensus technique onchain, c'est le vote des miners par l'installation (ou bien par la non-installation) du logiciel qui répond à la configuration du nouvel protocole BTC.

Quelle que soit la structure du consensus technique, c'est toujours le niveau social qui est déterminant:

- il y a des exemples de consensus officiellement transparents et modernes du point de vue technique mais qui sont corrompus par des élites centralisées via des concussions (LISK, démocraties développées);
- et vice versa: ceux qui sont consciencieux et adéquats sont capables de tout arranger sans technologie complexe.

Ainsi, les participants du MILE sont tombés d'accord que 1 XDR au sein du MILE est toujours égal à 1 XDR dont le cours boursier est calculé et publié par le FMI.

Le champ d'application principal du XDR - les acomptes pour acheter/vendre des services et des marchandises, c'est pourquoi les marchés d'échanges ainsi que le cours boursier de monnaies n'ont pas d'impact significatif sur le prix du XDR.

On voit, par exemple, que le total boursier quotidien du BTC, cryptomonnaie la plus populaire, est de 5 milliards USD pour la fin mars 2018, lorsque le volume total de transactions en BTC ne fait que 1 milliard USD. Le volume de transactions boursières pour l'Ethereum est de 1,5 milliards USD ; son volume de transactions au sein du réseau - 0,7 milliard seulement. Bitcoin Cash - 0,4 milliard USD contre 0,2 milliard.

A noter:

- étude sur les volumes faux des bourses crypto;
- La plupart des paiements en crypto, ce sont des transferts entre les marchés d'échanges, ainsi que des fusions et des délocalisations des porte-monnaie de taille, par exemple :
  - 40% du volume total quotidien en BTC est transféré par quelque cent transactions dont chacune fait 30 millions USD en moyenne;
  - 100 transactions transfèrent 25% du total quotidien de l'Ethereum; presque 40% de celui du BCH ; et 61% de celui du LTC.

Le volume de transactions réels est donc 1,5-3 fois moins.

La plupart des monnaies du « coinmarketcap » ont une circulation insuffisante dans les échanges réels de marchandises et essaient en même temps d'accroitre leur volume de transactions boursières. Voilà pourquoi les cryptomonnaies sont si volatiles aujourd'hui, leurs prix étant encore influencés par des spéculations et par les médias.

Chez MILE, on a une autre approche:

- les participants ne visent pas à introduire le XDR en bourse pour faire gonfler le volume de transactions boursières;
- le XDR est destiné d'abord à:
  - stocker et transférer de la valeur;
  - acheter/vendre des services et des marchandises dans l'économie réelle.

Autrement dire, même si quelqu'un essaie de faire baisser le cours boursier du XDR, ce serait une occasion parfaite pour ceux qui en utilisent quotidiennement. Tout le monde achèterait 1 XDR comme si c'était 0,8 XDR, puisque cette tendance boursière ne changera point son pouvoir d'achat réel.

Vous trouverez des détails plus pratiques dans le chapitre suivant.

3 Algorithme de l'émission

Il y a deux entités au sein du MILE utilisés pour les acomptes et pour l'émission: Coin (XDR) et Token/jeton (MILE).

3.1 XDR

- Unité de compte pour stocker de la valeur et en échanger au sein de la plate-forme.
- Est émis conformément à un algorithme transparent par les détenteurs de MILE et par les nœuds du réseau blockchain.

- Est toujours égal à 1 XDR du FMI.
- Nombre des ordres de la partie entière: 12.
- Nombre des ordres après la virgule: 2.
- La quantité maximale de XDR fait donc : 999 999 999 999,99 (1 billard).
- Cette unité de compte est également utilisée comme un « fuel (carburant) » pour les nœuds, c'est aussi un « node deposit », c'est-à-dire un dépôt du nœud qui permet d'identifier un participant bienveillant qui dépense ses ressources pour supporter le système MILE.

3.2 MILE

- Paramètre principal dans l'algorithme de l'émission de XDR.
- Le taux MILE/XDR est défini quotidiennement, une fois par jour, via le vote du réseau de nœuds.
  - Les propriétaires des nœuds publient leurs taux en tenant compte des données de bourses et d'autres plateformes d'échange.
  - Cela est suivi par la procédure de consensus, pendant laquelle on choisit le taux définitif MILE/XDR qui sera utilisé lors de la journée pour établir les limites de l'émission.
  - Les algorithmes sont pareils à ceux employés pour calculer la moyenne mobile. Les taux précédents enregistrés par la blockchain seront pris en compte, ce qui minimisera l'effet de machinations possibles.
- Nombre des ordres de la partie entière: 9.
- Nombre des ordres après la virgule: 5.
- La quantité maximale de MILE fait donc : 999 999 999,999 99 (1 milliard).

3.3 Emission initiale

- D'abord, il n'y a pas de XDR[1] au sein du système.
- Il y a 1 000 000 000 de MILE sans la possibilité d'en émettre plus tard.
- Le taux initial est 1 MILE = 1 XDR.

3.4 Emission secondaire

3.4.1 Emission effectuée par les nœuds après la fermeture d'un bloc (minting)

- Emission effectuée par les nœuds après la signature d'un bloc (minting).
- L'algorithme MILE assure que le nœud en service reçoit un taux d'intérêt annuel de 8-13% avec les versements en XDR vers son dépôt. Le pourcentage varie en fonction de la taille du nœud.
- Les versements sont envoyés de manière plus ou moins quotidienne. Les sommes varient aléatoirement, mais le total des versements fera tout de même 8-13% en une année.
- Pour acquérir le droit de devenir un nœud et pour pouvoir participer au consensus sur la signature de blocs, il est nécessaire d'installer l'application MILE et d'avoir dans son porte-monnaie un dépôt de 10 000 — 100 000 de XDR.
- Le bonus pour la fermeture d'un bloc est en dépendance non linéaire de la taille du bloc.

[1] L'émission de 300 000 de XDR sera prédéfinie par Genesis Block; ces XDR seront versés vers le dépôt des nœuds qui participent au consensus. Ces nœuds-ci appartiennent à l'équipe MILE et seront actifs au plus long possible.

- Le code source du projet sera publié par l'équipe de développeurs, toute personne ayant donc la possibilité de déployer et déclencher un nœud.
- Il suffit d'avoir un ordinateur moderne ordinaire avec un HDD de 4 To et une connexion Internet stable.
- Ce type d'émission est conçu plutôt pour motiver les participants qui maintiennent en condition la blockchain.

3.4.2 Emission effectuée par les centres d'émission

- Les jetons MILE se stockent dans les porte-monnaie des utilisateurs de la blockchain.
- Le propriétaire peut déposer n'importe quelle quantité de ses MILE sur une adresse spéciale.
- Il est obligatoire de déposer 10 000 MILE ou plus pour devenir un centre d'émission.
- Cela lui permettra de recevoir tout de suite dans son porte-monnaie une quantité de XDR conforme au taux MILE/XDR actuel prédéfini par le consensus et enregistré sur la blockchain.
- Au cas où le taux MILE/XDR a connu une hausse au fil du temps dans le moment t_2, l'utilisateur peut appeler le commande "émettre XDR" de son porte-monnaie pour que le système lui envoie des XDR additionnels conformément à la formule : $MILE \cdot (XDR(t_2) — XDR(t_1))$.
- Afin de débloquer les jetons MILE il est nécessaire d'envoyer vers une adresse spéciale des XDR ; l'utilisateur va recevoir des MILE conformément au taux MILE/XDR moins 0,2%. La commission est destinée à faire baisser le "flood" sur la blockchain et distribuée parmi les nœuds, c'est-à-dire au sein de la société qui supporte le réseau.
- En tenant compte de l'architecture du système, si la communauté a besoin de XDR, le taux MILE/XDR augmentera. C'est pourquoi les détenteurs du MILE s'intéresseront aux dépôts à long terme.
- En cas d'émission du XDR où $MILE/XDR = N$, le déblocage du MILE ne sera possible que lorsque le $MILE/XDR$ sera $\geq N$.

3.5 Raisons économiques de l'émission

- Plus d'utilisateurs détiennent des dépôts pour supporter les nœuds et/ou centres d'émission, plus les gens auront besoin de XDR, plus le taux du MILE sera haut.
- Plus d'utilisateurs utilisent des XDR pour les transactions réelles, plus on aura besoin de XDR, plus le taux MILE sera haut.
- Plus le MILE coûte, plus de XDR on peut émettre.

3.6 Reflection point

- Grâce à l'absence de commission pour les transactions en XDR, le système permet les microtransactions ; pour assurer que la blockchain fonctionne lors d'une longue période, on introduit la procédure de "trimming" soit du contrôle de la croissance de la blockchain pour l'optimiser.
- Si la blockchain atteint 4 To, l'algorithme se déclenche : Le système va effacer de la blockchain tous les porte-monnaie vides ou ceux de moins de 1 XDR. Il y aura un nouveau Genesis Block après le nettoyage. L'état de l'avant-nettoyage ne sera sauvegardé que sur les nœuds spécialisés.
- Pour payer la commission lors du trimming, les nœuds utiliseront le contenu de tous les porte-monnaie relativement vides à effacer (ceux où on stocke moins de 1 XDR).
- Les nœuds "morts" seront également effacés, leurs fonds étant sauvegardés dans les porte-monnaie.

4 Transactions rapides et gratuites

Les transactions au sein du réseau MILE sont gratuites, le bloc se ferme en 20 secondes. Le système est destiné d'assurer jusqu'à 10 000 transactions par seconde. L'optimisation de la blockchain est due au fait que nous ne gardons pas les informations sur input-output contrairement au modèle UTXO au sein de systèmes proches du BTC.

Les transactions sont gratuites grâce au mécanisme de "minting". Pour plus de détails veuillez voir la chapitre « Emission effectuée par les nœuds après la fermeture du bloc (minting) » et « Reflection point ».

5 Blockchain

5.1 Nos raisons

Les buts demandent un consensus qui réponde aux caractéristiques suivantes:

1. Temps requis pour générer un nouveau bloc - 20 secondes.
2. Nombre total de nœuds pouvant participer à l'élaboration du consensus variable de 10^3 à 10^4.
3. La vitesse des transactions élevée - 10^3 transactions par seconde au moins.
4. Réalisation de l'algorithme ne doit pas demander des puissances de calcul extrêmes comparées aux blockchains PoW.

Nous avons choisi l'algorithme sdBFT qui est plus rapide en comparaison aux algorithmes BFT. Le nombre potentiellement grand de participants rend plus difficile et complexe un concert préalable lorsqu'un groupe de nœuds qui votent forme un nouveau bloc en le gérant à son gré, puisque le consensus suivant sera élaboré par un autre groupe de nœuds-votants. La sélection pseudo-aléatoire de votants ne permettra pas un impact significatif sur le choix des nœuds lors du vote suivant. Pour la description détaillée de l'algorithme veuillez voir l'article Article consensus sdBFT.

5.2 Algorithme de formation d'un nouveau bloc

- Prenons un point temporel où un utilisateur forme un transaction I.
- La transaction est transmise au nœud le plus proche relatif à ce client.
- Le nœud peut être : passif, escorte ou master.
- Si le nœud est passif, il vérifie la transaction pour la transférer plus loin via le réseau peer-to-peer jusqu'à ce qu'elle ne soit reçue par le nœud escorte.
- Ce dernier l'envoie vers le nœud master, qui vérifie la transaction. Si la transaction est correcte, il l'envoie vers les nœuds escorte et enregistre la transaction I dans le bloc en formation.
- Les nœuds escorte reçoivent la transaction I, la vérifient et l'enregistrent dans le bloc en formation.
- Cette séquence se répète jusqu'à la fermeture du bloc et pas plus de 20 secondes.
- Ensuite le nœud master distribue le message de fermeture du bloc.
- Chaque nœud escorte calcule le hash du bloc de transactions, la signature numérique du hash avant d'envoyer le hash calculé au nœud master.
- Le nœud master calcule la quantité des signatures qu'il considère correctes. Si la quantité totale des signatures correctes excède 2/3 du total des nœuds qui participent au consensus, le bloc est considéré comme formé. Dans d'autres cas, le bloc ne se forme pas.
- La blockchain est hors de temps, elle ne vérifie pas ni coordonne la durée des transactions mises dans le bloc.

- Les systèmes qui fonctionnent à la base de la blockchain s'orientent vers la durée moyenne qui est près de 20 secondes.

5.3 Générateur de nombres pseudo-aléatoires

Les générateurs de base qui sont implémentés aux systèmes opérationnels ont une série de vulnérabilités importantes dont les plus dangereuses sont:

- Pour créer un nombre pseudo-aléatoire ils utilisent timestamp en tant que seed. Résultat : au cas où une personne malveillante connaît l'algorithme de génération du nombre pseudo-aléatoire et la durée approximative de la génération, il se peut qu'elle ait la clé privée par la voie du balayage d'accès.
- Au cas où timestamp est combiné à d'autres données, les générateurs de base génèrent des séquences assez prédictibles, ce qui permet aux personnes malveillantes d'avoir le mot de passe (le hash) via le balayage d'accès.

La blockchain MILE utilise les nombres aléatoires partout, allant de la génération des clés jusqu'à la signature numérique. Voilà pourquoi il y a des exigences particulières que la qualité des nombres aléatoires doit satisfaire. La séquence issue du générateur de nombres aléatoires est toujours testée. Vous trouverez ci-dessous les résultats de la vérification du générateur.

5.3.1 Objectifs lors des essais

Les essais visent à vérifier les faits du contrôle dynamique de la séquence générée. Cela sert d'une preuve de l'hypothèse statistique sur "steady coverage" (distribution uniforme) des séquences générées.

5.3.2 Ordre et conditions des essais

Les essais représentent une vérification de la séquence des nombres aléatoires définis par le générateur de nombres aléatoires de logiciel. Pour effectuer le contrôle on procède aux activités suivantes :

1. On crée un workbench pour vérifier la réalisation de la fonction de génération dans le module cryptographique et pour tester la séquence aléatoire. C’est une workstation (un lieu de travail avec Visual Studio 2017 et le logiciel MILE installés).
2. Le logiciel libre GNU suivant est également installé:
   a) NIST Statistical test Suite (NIST-STS);
   b) Test-U01.
3. Grâce au générateur de séquences pseudo-aléatoires on obtient une séquence composée de nombres aléatoires la plus longue possible (1024 Go et plus) qui n'est limitée que par la puissance de calcul et par la durée de l'essai. La séquence composée de nombres aléatoires est copiée dans le mémoire permanent de la logicierie dans les fichiers binaires StatMessTime (paquets de 1000 octets) et StatCarrent (paquets de 2000 octets).
4. On procède à l'analyse de la la séquence composée de nombres aléatoires avec l'aide des paquets des tests statistiques cités ci-dessus pour comprendre si elle est conforme aux critères principaux.
5. Pour évaluer la séquence interprétée comme binaire on utilise le critère 3s pour les fréquences relatives de symboles binaires avec un intervalle

$$(0,5 - 1D1 - 1,5[1 - 4D2)n - 1]0,5, 0,5 + 1D1 + 1,5[1 - 4D2)n - 1]0,5$$

à la base de n symboles binaires; $p = 0,5 + D, q = 0,5 - D$.

Tableau 1. Les intervalles suivants du critère 3s:

	Les intervalles du critère 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. Pour évaluer la qualité de la séquence aléatoire, interprétée comme une séquence d'octets, on utilisait le critère c^2 avec 255 degrés de liberté.

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

7. Pour vérifier les tests dynamiques on procède au traitement, à l'analyse et à l'évaluation des résultats obtenus. La vérification est considérée comme succès si les critères statistiques utilisés obéissent à l'hypothèse statistique sur "steady coverage" (distribution uniforme) des séquences générées (voir le paragraphe 5).

5.3.3 Les résultats des études statistiques

Résultats du traitement des données StatMessTime

Tableau 2. Fréquences de 1 en 16 sections de 1024 octets

4075	41294206	4148	4098	4180	4042	4021
4092	41344202	4226	4064	4052	4070	4112

Tableau 3. Fréquences relatives de 1 en 16 sections de 1024 octets

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

Tableau 4. Fréquences relatives de 1 dans les sommes des décalages 1-512 (shift sums)

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

Résultat min: 0.4961, max: 0.5042

Tableau 5. Fréquences d'octets à la base de 16384 octets

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

Valeur de c^2 à la base de 16384 octets (255 degrés de liberté) c^2 = 268.5

Résultats du traitement des données StatCarrent

Tableau 6. Fréquences de 1 en 32 sections de 1024 octets

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

Tableau 7. Fréquences relatives de 1 en 32 sections de 1024 octets

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

Tableau 8. Fréquences relatives de 1 dans les sommes des décalages 1-512 (shift sums)

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

Tableau 8 Fréquences relatives de 1 dans les sommes des décalages 1-512 (shift sums)

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

Tableau 9. Fréquences d'octets à la base de 32768 octets

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

Tableau 9. Fréquences d'octets à la base de 32768 octets

112	113	136	136	130	139	121	154	14
120	132	137	121	129	124	124	124	12
128	146	117	118	124	117	115	138	13
136	124	119	147	128	123	132	144	13
144	139	125	127	138	123	110	130	13
152	128	145	126	128	119	127	122	12
160	136	120	132	124	115	126	120	11
168	110	133	131	125	146	125	122	12
176	134	112	122	115	116	132	108	12
184	140	111	125	104	133	133	110	11
192	129	134	141	137	131	124	125	14
200	106	126	145	133	122	140	116	13
208	123	134	127	131	132	120	127	14
216	128	125	136	120	133	113	123	14
224	137	122	129	114	113	108	107	12
232	125	139	142	107	99	122	126	11
240	130	137	139	152	137	132	137	12
248	137	124	138	124	137	112	114	11

min: 99, max: 154

Valeur de c^2 à la base de 32768 octets (255 degrés de liberté)

$$c^2 = 239.8$$

5.3.4 Résultat

La blockchain MILE possède un générateur de nombres aléatoires de logiciel basé sur le double calcul des fonctions de hash avec la modification dynamique de l'état initial. La qualité de la séquence aléatoire générée par le générateur n'est pas pire que $0.5 + D$ pour un symbole binaire avec $|D| < 0.01$, ce qui obéit à l'hypothèse statistique sur "steady coverage" (distribution uniforme) des séquences générées.

5.3.5 Cryptographie

- Algorithme ECSDA Digital Signature (utilisé au BTC)
- Schème Ed25519 (plus rapide que celle du BTC)
- Algorithme de hash SHA-3 (plus rapide et plus sécurisé que celui du BTC)

5.3.6 Caractéristiques générales de la blockchain

- Possibilité d'effectuer des microtransactions ("payer son café") grâce à l'absence de commission.
- Pas de somme maximale d'une transaction.
- La blockchain s'optimise régulièrement elle-même pour contrôler sa croissance.

- Les porte-monnaies ayant moins de 1 XDR se vident, leurs XDR allant vers les nœuds qui ont participé au trimming.

5.3.7 Types de transactions

- Possibilité d'effectuer des microtransactions ("payer son café") grâce à l'absence de commission.
- Envoi de XDR.
- Envoi de MILE.
- Annonce de l'inscription du nœud.
- Annonce de l'élimination du nœud.
- Nouvel Genesis Block (trimming).
- Publication du taux MILE/XDR.
- Mise en vote d'une question par les nœuds.
- Vote par le nœud.
- Emission (ou émission inverse) de XDR par le centre d'émission.

5.3.8 Paramètres de commande

- Intervalle de blocs qui déclenche le trimming.
- Intervalle de blocs qui répète le trimming si le trimming précédent a échoué.
- Diapason du dépôt permettant de déclencher un nœud.
- Quantité maximale de nœuds.
- La mise à jour des paramètres de commande s'opère via le vote des nœuds.

5.3.9 Les porte-monnaie

- L'adresse du nœud est la séquence de symboles codée en Base58checkerMod2, qui est enregistrée dans la transaction sur la blockchain.
- Le porte-monnaie peut envoyer et recevoir des XDR comme des MILE.
- Types de porte-monnaie:
  - Light:
    * Pour les acomptes (transactions) et pour vérifier l'état du compte.
    * A pour base un protocole spécial permettant de recevoir les blocs nécessaires en vérifiant seulement l'arbre de Merkle et pas la blockchain en tout.
  - - Standart:
    * Stocke toute la blockchain.
    * Peut devenir un nœud.
  - Multisig:
    * Porte-monnaie virtuel dont les transactions ne sont acceptées par le système que s'il y a plusieurs signatures.
  - Point wallet:
    * Porte-monnaie du développeur, qui assure la possibilité de gérer le système d'une manière très précise.
    * Point Wallet ne fonctionne que lors de la première année, ce qui sera écrit dans la blockchain.

— System wallet:

* Porte-monnaie pour accumuler les commissions venant des porte-monnaie effacés lors du trimming.
* La seule transaction qu'il peut envoyer est celle destinée àverser la commission aux nœuds ayant participé au trimming.

6 Champ d'application

6.1 Paiements internationaux libres

Le succès du marché des cryptomonnaies est largement dû à la demande pour les paiements internationaux libres, rapides et bon marchés. C'est surtout le cas chinois, où la circulation des monnaies est contrôlée par l'Etat.

Les participants à la conférence Money 2020 au Singapour ont conclu qu'il n'y a pas encore de système permettant les paiements de plus de 5 000 USD entre états. SWIFT reste le seul instrument pour transférer plus de 5 000 - 10 000 USD d'un état à un autre. A nombreuses conditions : grand nombre de formulaires à remplir, vérification des papiers par la banque, entretien avec un responsable, plusieurs heures à attendre. La commission est à peu près 1%.

MILE permet de transférer n'importe quelle somme à n'importe quel coin du monde en quelques secondes sans intervention bancaire.

6.2 Stockage indépendant

Garder son argent en espèces chez soi s'avère dangereux. Les contrats que l'on conclut avec la banque pour avoir un coffre individuel contiennent une clause de non-responsabilité, la banque n'étant point responsable de l'intégrité du contenu du coffre. Résultat : de grandes sommes disparaissent de temps en temps des coffres bancaires. Pour des statistiques supplémentaires relatives à la fermeture de banques veuillez voir l'Introduction. MILE permet de stocker de l'argent dans un réseau décentralisé sans aucun risque relatif au contractant central et sans blocage du compte.

6.3 Economie coopérative internationale

L'un des aspects les plus importants qui garantie la valeur du MILE est le volume de transactions réelles. Les créateurs du MILE considèrent extrêmement prospectif l'emploi du MILE dans l'économie coopérative et surtout dans des pays dont les systèmes financiers sont instables. Là, on voit un déficit significatif des monnaies-fiat ainsi que le troc combiné à d'autres opérations pareilles en tant que moyen préféré de paiement.
La plupart des pays développés ont plus ou moins arrêté leur croissance économique. Ce sont les pays en voie de développement qui apportent le plus à l’économie mondiale. C'est également le cas pour le business : toutes les corporations sauf quelques holdings financiers ont une rentabilité de moins de 5%. Lors des crises, même les géants financiers voient leur chiffre d'affaires drastiquement chuter.

D'ailleurs, historiquement, les coopératives grandissent contre les tendances du marché en crise. Par exemple:

- Rabobank a connu une croissance de 42% en 2008 et ses fondateurs ont vu leurs dépôts hausser de 20%. Les années 2008 et 2009 ont vu le taux de participation aux coopératives de crédit augmenter.
- Un Canadien sur trois participe à de telles organisation ; la part des marchés de dépôts et de crédits logement appartenant aux coopératives de crédit a augmenté jusqu'à 19% en 2010 [Moody's investors service global banking report, april 2010].
- Dès le premier quartier 2012 la coopérative Desjardins occupe la 16-ième place parmi 7500 organisations de dépôt en Amérique du Nord et est le deuxième détenteur important des fonds propres de base dont le volume est de 16,8%.

Le volume de l'économie coopérative est extrêmement important, les coopératives étant présents dans des pays riches comme dans des pays en voie de développement.

- Les coopératives comptent 1 milliard d'associés dans le monde.
- En Inde, les besoins en marchandises de 67% de la population rurale sont satisfaits par les coopératives.
- 40% de propriétaires africains font partie de coopératives.
- Les profits reçus en 2010 par les 1500 organisations coopératives les plus grandes ont fait presque 2 billards de dollars.
- Development International Desjardins (DID) est le leader dans les microfinances : il a 8,8 millions de participants et de clients dans les quatre coins et un capital de prêt de 2,5 milliards de dollars canadiens.
- Dans quelques pays africains, 35% du marché de microfinances appartient à l'entreprise.
- En Chine, les coopératives tiennent 91% du marché de microcrédits.
- Les coopératives de crédit assurent l'envoi de fonds de milliards de dollars par des migrants qui travaillent dans des pays développés vers leurs familles, ce qui est particulièrement important pour l'Amérique Latine et pour l'Afrique.

L'économie coopérative est plus efficace puisque:

- Les coopératives visent à gagner de l'argent pour tous les participants et pas à faire gonfler la capitalisation en bourse.
- Les associés sont a priori motivés, on ne dépense rien pour les motiver.
- Les top-managers gagnent 100 fois plus que les employés ordinaires dans les corporations, et seulement 10 fois plus dans les coopératives car on dépense moins pour maintenir la structure.
- Grâce à l'économie intérieure et aux mécanisme d'acomptes entre les participants on peut réduire les dépenses d'impôts, de transactions, d'intermédiaires, ainsi que de réduire la demande pour les crédits en fiat.
- Cela mène au fait que le prix de marchandises et de services au sein de coopératives est 40% plus bas que sur le marché extérieur. Une telle situation contribue à l'attraction de gens et de capitaux extérieures et motive les gens à la participation à long terme.

Instruments que l'on crée à la base du MILE pour les coopératives:

- comptabilité des acomptes,
- dépôt pour stocker les acquits et les soldes,
- attraction du financement extérieur,

- préparation des comptes pour les institutions fiscales,
- modèles juridiques pour formaliser l'interaction avec les jetons,
- marché de marchandises et de services aux bon plans.

7 Motivation des participants

Utilisateurs:

- Obtiennent la possibilité d'effectuer des transactions gratuites et rapides ou de stocker de la valeur à long terme en un espace crypto.

Investisseurs:

- S'intéressent au retour des investissements.
- Le retour peut s'opérer via la participation active au système car tout participant est libre de devenir un nœud et/ou un centre d'émission.

Centres d'émission:

- S'intéressent à la croissance du cours boursier du MILE car cela augmentera leurs capitaux et leurs profits réguliers.

Propriétaires des nœuds:

- S'intéressent à recevoir la commission pour la signature de blocs sur la blockchain.
- Le propriétaire reçoit un taux d'intérêt annuel de 8-13% en XDR.

8 Lois appliquées

Transactions quotidiennes

On peut ne pas formaliser l'emploi du MILE à trois conditions: sommes peu importantes, transactions irrégulières, formalisation n'est pas requise par des institutions compétentes.

Dans d'autres cas et surtout si vous effectuez d’une façon active vos transactions dont les sommes sont significatives, il est fortement conseillé de fonder ou rejoindre une coopérative ou une société locales.

L'instrument principal dans une coopérative est la part (share). L’apport (first fee) est le versement effectué par l'associé vers le fonds commun de placement de la société. Le versement peut consister d'argent, de titres, d'un fonds de terre et d'une autre propriété immobilière ou d'un droit patrimonial ou autre possédant de la valeur. Le retour de l'apport n'est pas soumis à un impôt quels que soient la somme ou le prix de la marchandise obtenu par l'apporteur.

Tout échange des apports au sein de la coopérative est possible et n'est pas soumis à un impôt ; du point de vue juridique le MILE peut donc être utilisé comme un outil d'évaluation des apports.

Ceux qui ne participent pas à la coopérative et ne sont donc pas associés, peuvent bénéficier d'une offre similaire à un programme de fidélité.

Le Jeton (ou Token) représente le droit de bénéficier des points bonus. Ce droit peut être vendu à une personne morale ou physique ainsi que compté au sein du service comptable.

- Lors de l'échange jeton-marchandise ou jeton-service le propriétaire du jeton demande des points bonus, en reçoit et en échange pour recevoir des marchandises contre ces points.
- C'est un schème propre aux supermarchés ou bien aux compagnies aériennes.