MILE

Stablecoin libre, rapide et sécurisé

8 octobre 2018

Tech Paper v.1.5
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 va-leur, qui possède les attributs suivants :

- prix stable ;
- algorithme d'émission transparent ;
- transactions libres et gratuits ;
- transactions rapides ;
- absence de limites ;
- transactions non-bloquées et non-remboursables.

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

- Prix instable. La plupart des monnaies-fiat oscillent chaque année, c'est le cas même pour des pays développés tels que la Suisse ou le Japon où JPY a connu une baisse de 15 % en octobre-décembre 2016 [1] et CHF s'est accru de 20 % en une semaine en janvier 2015 [2] ;
- Transactions lentes. 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 de tout négocier pour ensuite attendre plusieurs jours l'accomplissement de la transaction. N'oubliez pas que cette transaction peut être bloquée. L'ouverture d'un compte bancaire en Europe et, elle aussi, un processus très long ;
- Transactions chères. Selon les sites Web de plusieurs systèmes de paiement, la commission moyenne est de 3-5 %. ;
- Censure en hausse. Il n'est pas rare aujourd'hui qu'un pays soit sous le joug de sanctions ou participe à une des guerres commerciales, étant privé de l'accès au SWIFT ou d'autres systèmes. Parmi ces pays : la Chine, l'Inde, la Russie, l'Iran, la Turquie, la Venezuela. 5 d'entre eux font partie du top-30 des pays du monde selon leur PIB [3] ;

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)

— Possibilité de voir sa transaction bloquée ;
— Les principes de l'émission des monnaies-fiat ne sont point transparents, ce qui provoqu l'hyperinflation et des crises économiques [4]. De-jure, les Banques Centrales de pays développés publient M0 et d'autres indices, sauf que personne n'a jamais fait de l'audit de ces chiffres-ci ;

Les monnaies numériques déjà existantes ne parviennent non plus à résoudre les pro-blèmes cités ci-dessus car :

— BTC est décentralisé mais trop volatile ;
— Les "stablecoins" existants ont des liens forts avec des stocks-fiat centralisés et donc complètement dépendants de l'un des contractants ;
— Nombreux sont les stablecoins dépendant de métaux précieux, de main d'œuvre ou d'autres actifs, qui ne sont pas stables. Les oscillations du taux or-USD peuvent atteindre 15 % par mois [5] ;
— Les stablecoins basés sur ERC-20 dépendent du marché de l'Ethereum, qui, lui aussi, connait des fluctuations lorsqu'une nouvelle application populaire appa-rait [6] ;
— Les "stablecoins" algorithmiques font souvent l'objet d'attaques Soros [7]
— La seule famille stablecoin qui donne accès aux transactons rapides et pas chères, c'est BitShares BitAssets. Cependant, Dan Larimer ayant quitté la communauté, la dernière a connu ses bas. Le volume de trading fait quelques millions de dollars seulement [8], et le forum principal n'a que dix branches ac-tives par semaine à peu près [9]. De surcroît, la communauté devient de plus en plus centralisée avec très peu de gens qui dirigent le réseau en réalité [10].

Voilà pourquoi le produit ayant les caractéristiques suivantes peut être mis en place :

1. Prix stable ;
2. Absence de censure ;
3. Transactions libres et gratuites ;
4. Transactions rapides ;
5. Permettre à chacun d'émettre des jetons.

Cet instrument permettra aux gens de :

— Effectuer des transactions à tout coin du monde d'une manière libre et gratuite malgré guerres commerciales ou accès au SWIFT rejeté ;
— Stocker de la valeur à long terme et sans commission.

2 Prix stable

L'argent représente une construction sociale. Le seul aspect pouvant définir l'unité de compte, c'est le nombre des gens qui l'utilisent pour faire du commerce, des investissements, des réserves, pour obtenir des crédits etc. USD ne dépend plus d'or à partir de Nixon Shock et est émis sans cesse. Cependant, on l'utilise beaucoup dans l'économie réelle, et le dollar reste rela-tivement stable par rapport à d'autres monnaies. Lorsque on émet trop d'argent en même tempe que l'économie stagne, on vit des crises.

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

Voilà pourquoi le réseau MILE a pour base les deux principes :

— Usage des jetons dans l'économie réelle : commerce, crédits, investissements, réserves.

— Mécanismes pour équilibrer l'émission et la croissance économique.

Il est moins trivial de mettre en place l'aspect technique que d'intégrer quelque chose à l'économie réelle. Et quand même, un système possédant les caractéristiques précisées ci-dessus est un système très compétitif par rapport à d'autres systèmes crypto ou fiat. Vous trouverez la description détaillée de l'algorithme d'émission 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 : XDR (stablecoin) et MILE (indice de demande pour XDR).

3.1 XDR

— XDR est un stablecoin utilisé en tant que moyen de paiement et moyen de stockage de la valeur.

— Emit par les détenteurs de jetons MILE et par les nœuds master via l'algorithme code ouverte.

— Egal à 1 FMI SDR [11] grâce au consensus sociale et aux algorithmes employés.

— Dépôt à garder dans la blockchain pour lancer un nœud master.

— Le nombre des ordres de la partie entière faisant 12, le nombre des ordres après la virgule faisant 2, le nombre maximal de XDR fait donc : 999 999 999 999,99. Ce nombre maximum peut être modifié suite au consensus des nœuds master et suite au soft fork [12]

3.2 MILE

— Indice de demande pour 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.

— Le taux MILE/XDR montre le nombre de XDR que l'on peut émettre via le centre d'émission.

— Dépôt à garder dans la blockchain pour lancer un nœud master.

— Le nombre des ordres de la partie entière faisant 9 et le nombre des ordres après la virgule faisant 5, le nombre maximal de MILE fait donc : 999 999 999,999 99.

3.3 Emission initiale

— D'abord, il y a 300 000 XDR dans le Genesis Block. Ils seront bloqués en tant que dépôt de nœuds master pour lancer la procédure du consensus.

— Il y a 1 000 000 000 de MILE sans la possibilité d'en émettre plus.

— Le taux initial est 1 MILE = 1 XDR.

— La distribution et le prix initiaux de MILE sont basés sur les déclarations sui-vantes. L'écosystème MILE résulte d'un capital de 1,4 milliard de dollars, composé de monnaies fiat, d'actifs cryptographiques, de facteurs de produc-tion, de la propriété intellectuelle, de ressources humaines,

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

12. https://www.investopedia.com/terms/s/soft-fork.asp

de la valeur de la marque, de l'immobilier, ainsi que d'autres actifs corporels et incorporels réu-nis. Cela a eu pour effet la distribution de 1 milliard de MILE à 108 porte-feuilles.

3.4 Emission secondaire

3.4.1 Emission effectuée par les nœuds master après la fermeture du bloc (minting)

- Pour acquérir le droit de devenir un nœud et pour pouvoir participer au con-sensus 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.
- Un nœud master en service reçoit 8-13 % de plus par an avec les versements en XDR vers son dépôt. Le pourcentage varie en fonction de la du nœud. Les ver-sements sont envoyés de manière plus ou moins quotidienne. Avec l'agrandissement du dépôt le pourcentage s'agrandit en dépendance parabo-lique.
- Chacun-e peut lancer un nœud master via le paquet d'installation (docker).
- 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 maintien-nent en condition la blockchain.
- Le nombre de nœuds master n'est pas limité, mais 10 000 seulement partici-pent au consensus (active nœuds). D'autres nœuds (waiting) ne reçoivent pas de blocs à signer ni reçoivent le prime minting.
- Au cas où un des nœuds actifs ne signe pas le bloc, il est exclu du consensus et le nœud « waiting » le plus proche devient actif.
- Comme le nombre maximal de nœuds actifs est de 10 000, le prime est limité par 1 milliard de XDR. Si l'écosystème atteint 10 milliards de XDR, par exemple, l'inflation fera 0,8-1,3 % seulement.
- Au cas où le total de XDR sera émis, les nœuds master ne recevront plus de primes. Il est très possible, que ceci mène au soft fork avec le nombre de XDR plus grand qu'autrefois.

3.4.2 Centres d'émission

- Il est obligatoire de déposer 10 000 MILE ou plus pour devenir un centre d'émission.
- La blockchain enverra de nouveaux XDR au porte-monnaie du centre d'émission. Le nombre est défini par le taux interne MILE/XDR.
- Au cas où le taux MILE/XDR a connu une hausse au fil du temps, chaque centre d'émission peut émettre plus de XDR grâce à l'augmentation de la li-mite.
- 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 socié-té qui supporte le réseau.
- Si la demande pour XDR augmente, le taux MILE/XDR fait le même. Sinon, le taux reste stable ou baisse.
- En cas d'émission de XDR où $MILE/XDR = N$, le déblocage de MILE ne sera possible que si le $MILE/XDR$ est $\geq N$.
- Le système utilise des algorithmes ayant pour but de filtrer des taux MILE/XDR trop hauts ou trop bas pour le rendre moins volatile.

— Le principe de calculation du taux ressemble celui d'une moyenne mobile ; on recourt par exemple à des taux précédents stockés par la blockchain, pour pré-venir des manipulations et l'hyperinflation.

3.5 Reflection point

— Grâce à l'absence de commission pour les transactions en XDR, le système permet les micro-transactions ; pour assurer que la blockchain fonctionne lors d'une longue période, on introduit la procédure de "truncation" soit du con-trôle de la croissance de la blockchain pour l'optimiser.
— Dès que la blockchain atteint 4 To, l'algorithme se déclenche : Le système va effacer de la blockchain tous les porte-monnaie vides ou ceux ayant 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.
— Les XDR seront distribués parmi les nœuds master.
— Les nœuds "morts" seront également effacés, leurs fonds étant sauvegardés dans les porte-monnaie.

4 Transactions rapides et gratuites

Les transactions XDR sont gratuites, pour celles MILE la commission est de 0.01 MILE, le bloc se ferme en 20 secondes. Le système assure jusqu'à 10 000 transactions par se-conde. L'optimisation de la blockchain est due au fait que nous ne gardons pas les in-formations sur input-output contrairement au modèle UTXO au sein de systèmes proches du BTC. Les transactions sont gratuites grâce au mécanisme de "minting".

5 Blockchain

5.1 Possibilité de choisir

Les buts demandent un consensus qui relève les défis suivants :

1. Temps requis pour générer un nouveau bloc – 20 secondes.
2. Nombre total de nœuds pouvant participer à l'élaboration du consensus – de 10^3 à 10^4.
3. La vitesse de transactions élevée, 10^3 transactions par seconde au moins.
4. Réalisation de l'algorithme ne doit pas demander des puissances de calcul ex-trêmes par rapport aux blockchains Proof-of-Work comme Bitcoin, Ethereum etc.

Nous avons choisi l'algorithme sdBFT qui est plus rapide en comparaison aux algo-rithmes BFT. Le nombre potentiellement grand de participants rend plus difficile et complexe un concert préalable lorsqu'un groupe de nœuds qui votent forme un nou-veau 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 des-cription 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.
— Le nœud master 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 se-condes..
— Ensuite le nœud master distribue le message de fermeture du bloc.
— Chaque nœud escorte calcule le hash du bloc de transactions, la signature nu-mérique 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 du-rée 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 sé-rie de vulnérabilités importantes dont les plus dangereuses sont les suivantes :

— 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 gé-nération, 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 soigneusement 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. 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. 2 Le logiciel libre GNU suivant est également installé :
   a) a) NIST Statistical test Suite (NIST-STS) ;
   b) b) Test-U01.
3. 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 séqu-ence 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. 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. 5 Pour évaluer la séquence interprétée comme binaire on utilise le critère $3s$ pour les fréquences relatives de symboles binaires avec un intervalle

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

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

TABLE 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. 6 Pour évaluer la qualité de la séquence aléatoire, interprétée comme une séqu-ence d'octets, on utilisait le critère c^2 avec 255 degrés de liberté.

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

7. 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 bien passée si les critères statistiques utilisés obéissent à l'hypothèse statistique sur "steady coverage" (distribution uniforme) des séquences générées (voir le pa-ragraphe 5).

5.3.3 Les résultats des études statistiques

Résultats du traitement des données StatMessTime

TABLE 2. **Fréquences de 1 en 16 sections de 1024 octets**

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

TABLE 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

TABLE 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

TABLE 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

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

Résultats du traitement des données StatCarrent

TABLE 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

TABLE 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

TABLE 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

Table 8 Continuation

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. **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

TABLE 9. **Fréquences d'octets à la base de 32768 octets**

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

Déterminer 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 sous condition que $|D| < 0.01$, 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'ab-sence de commission.
- Pas de somme maximale d'une transaction.

— La blockchain s'optimise régulièrement elle-même pour contrôler sa crois-sance.
— Les porte-monnaies ayant moins de 1 XDR se vident, leurs XDR envoyés vers les nœuds qui ont participé au truncation.

5.3.7 Types de transactions

— Envoi de XDR.
— Envoi de MILE.
— Annonce à l'inscription du nœud (Announcement on a node registration).
— Annonce à l'élimination du nœud (Announcement on a node dismissal).
— Nouvel Genesis Block (truncation).
— 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 truncation.
— Intervalle de blocs qui répète le truncation si le truncation 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.
  — Standard :
    — 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 gé-rer le système d'une manière très précise.
    — Point Wallet ne fonctionne que lors de la première année, en-suite il sera enregistré dans la blockchain
  — System wallet :

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

6 Champ d'application

Comme le présent document couvre plutôt l'aspect technique, relativement peu d'attention sera prêtée à celui économique.

— Instrument et réseau multilatéral d'acomptes pour ceux auxquels le SWIFT n'est pas toujours accessible et qui ne font pas partie de Bank of International Settlements (3 milliard de gens, toute une série de pays et de territoires d'Afrique [13], la Chine, la Russie, la Turquie, la Venezuela, l'Iran, le Soudan etc. [14]
— Transactions libres, gratuites et rapides sans limite ni censure.
— Moyen stable et indépendant de stocker de la valeur.
— Moyen d'échange entre les communautés qui se considéraient pauvres n'ayant pas de USD. Si elles possèdent des ressources naturelles ou produisent des produits, elles peuvent bien recourir aux XDR pour assurer les acomptes, le comptable, les déclarations etc.

7 Lois appliquées

Les actifs crypto est un phénomène relativement nouveau, et les législations sont en train de formation partout dans le monde. Tout de même, plusieurs états assez riches et développés ont déjà introduit quelques règlements concernant le Bitcoin [15] tels que la Suisse, le Japon, les Etats-Unis, le Canada, la Corée du Sud, l'Allemagne etc.

Il n'y avait pas de Token Sale (ICO) pour XDR ou MILE. XDR sont émis par tout un réseau décentralisé, ils ne possèdent pas de caractéristiques principales d'un titre. Selon la législation du pays, XDR peuvent être considérés comme un moyen d'échange ou un actif incorporel numérique.

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