MILE

無料で速く安全で分散したステーブルコイン

２０１８年１０月１７日

技術報告書:　v.1.5

ロータス・マイル
短縮版： mile.global

1. はじめに

同時に下記の特徴を持つ測定値、保存値、値が転送できるシールはありません。

- 安定的な値段；
- 速い取引；
- 無料の取引；
- ウォリュームが無限；
- 検閲に強て逆にできない取引；
- 透明な放出アルゴリズム。

いまである通貨（例えば、USD, EUR, CNYなど）が　合いません。理由は：

- 値段が安定ではありません。多くの不換紙幣の通貨が変わりやすいものです。スイスや日本のような発展国々でも通貨の価値が速く上昇し、減少できます。例えば、２０１６[1]年１０－１２月にかけてJPYが１５％で減少し、２０１５ 年1月一週間にかけてCHFが２０％で上昇しました。

- 取引は時間がかかります。あらゆる国々の間で10.000 USD以上の不換紙幣の通貨を振り替えるために、多くの書類の準備や疲れさせる交渉の連続が必要になってしまいます。振り替えが数日かかり、加えた調停または返金という恐れもあります。これ以上、欧州で銀行預金口座を開設するのは時間がかかれます。

- 取引が高価です。支払システムのサイトによって、評価して売買為替の開きがやく3-5%になります。

- 検閲が強くなります。２０１８年には制裁または商戦で影響が与えられている国々が数十になりました。その国家はSWIFTの振り替えが限定させられるし、他の限界で悩まされています。中国、インド、ロシア、イラン、トルコ、ベネズエラがその例です。そのうち　つが国内総　産額 によってトップ　　に入ります。

- 取引の可逆性。限界された個人で管理している不透明な放出アルゴリズムが超インフレーションや経済の危機の原因になります。正式に発展国の中央銀行がM0などのインジケーターを出版するが、誰でもその数字を確認しませんでした。

---

[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)
[4]https://en.wikipedia.org/wiki/Nixon_shock

電子通貨も以上のような測定を同時に持ちません。

- BTCが検閲に強て大変不安定です。
- 多くのステーブルコインが中心にした不換紙幣の保管につけますから、曲げられる参加者に依存しています（USDT, Circleなど）。
- 多くのステーブルコインが貴金属、労働力の価値などにつけていますが、安定ではありません。金がUSDに当たって1カ月にかけて15%で上昇したり、減少したりできます。[5]
- ERC20に踏まえているステーブルコインが、人気なアップが出すと制動されるEthereumのメインネトに依存しています。[6]
- アルゴリズムステーブルコインがSoros Attackに左右されます。[7]
- BitSharesやBitAssetsが安くて速い取引を施す唯一の作動しているステーブルコイン系統です。しかし、大事な問題があります。ダン・ラリマーがBitSharesを捨てて、機器がきました。BTSの毎日の商売規模が数百万ドール[8]で、BitSharesのファーラムでは能動的なトピックが毎週数十だけあります。[9] BitSharesの代表や委員会のメンバーが集中すぎるのは問題になります。十人だけいるから、実にネットワークの管理官はすくないです。[10]
- 分散ステーブルコインを教えてくれるプロジェクトが以前の白書の段階にあります。今作動しませんからその文書で。

それから、そのような特徴を持つ商品が市場では望ましいです：

- 安定的な値段；
- 無検閲の取引；
- 速い取引；
- 無料の取引；
- コインの発行が誰でもできる。
- その解決が人間、企業や国々にとって、
- 姿勢、商戦、SWIFT問題にもかかわらず、どこでも、どんな価値でも、速くて無料で送るようになり；
- **無料で長い時間で価値をいくらでも保管する可能になります。**

2. 安定的な値段

貨幣が社会で作ったものです。

企業の通貨性を明確する唯一のは、売買、貸付、投資、送金、積立金を目的にして、その企業を利用している人間の数です。ニクソンショックの時代からUSD が金につけなくて、いつも発行されます。しかし、事実の経済におけるUSDは利用されているから、他の通貨と比較していえば、今でも安定的です。経済が発展するに比べて金がより速く発行すると、危機が出ます。

---

[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

それから、MILEネットワークのステーブルコインの値段の安定が次のようなことに踏まえています

- 売買、貸付、投資、送金、積立金などの事実の経済における利用；
- 貨幣供給量のアルゴリズムが経済成長より速くないです。事実の利用は技術的な利用より円転滑脱なものです。とにかく、同時に作動している安定的な値段、速くて無料の取引、検閲に強い取引、透明性という特徴の結合は、不換紙幣や電子通貨に比べてとても競争てきです。

貨幣供給量のアルゴリズムの管理について次の章に読んでください。放出アルゴリズムMILEネットワークにはコインが二つがあります：XDR（ステーブルコイン）やMILE（XDRの要求索引）です。

3.1　XDR

- XDRは払うユニットや価値の保管として利用されるステーブルコインです。
- オープンソース・アルゴリズムを通じてMILEトークン保有者やブロックチェーン・マスターノードで放出されています。
- 社会コンセンサスや貨幣供給量のアルゴリズムで決まってXDR＝ 1 IMFSDR [11] 1 1 と思われています。
- ブロックチェーンの中でマスターノードをスタートさせるためにXDRが預金として利用されます。
- XDRは全体部分が１２あり、コンマ後部分が２つあり、つまり、MILEの限界は999.999.999.999.99 (1 兆) です。その限界はマスターノードコンセンサスやソフトフォークを通じて昇格させることができます。 [12]

3.2　MILE

- MILEはXDRの要求索引です。
- MILE/XDR 為替はブロックチェーン・ノードの投票で２４時間に一度定義されています。
- ノードの保有者は取引所、OTC取引、オフライン経済などからの情報を利用して、適正だと思っている為替レートを出版します。
- MILE/XDRの為替レートは放出センターでXDR発行の限界に指摘します。
- ブロックチェーンの中で放出センターをスタートさせるためにMILEが預金として利用されます。
- MILEは全体部分が９つあり、コンマ後部分が５つあり、つまり、MILEの限界は999.999.999.999.99 (約十億)です。

3.3　一次の放出

- 最初はXDRが、コンセンサスをスタートさせるマスター・ノードのデポジットとして締めこまれたジェネシス・ブロックに３００．０００あります。
- 最初はジェネシス・ブロックにはMILEが999 999 999.999 99あり、これ以降新MILEが放出されません。
- 最初の値段は 1 MILE＝ 1 XDRです。
- MILE の配分や最初値段は次のような条規に踏まえてうます。MILEのエコシステムが現金の1.4B USDの結果になります。それは不換紙幣の通過と電子資産、生産要素、知的財産、人的資源、ブランド価値、不動産、好意などの実体的または実体のない資産という結合から編成されています。その結果、最初の1B MILEが１０８ウォレットに配分されてきました。

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

3.4　二次性放出

3.4.1　ブロック閉止のマスター・ノード放出（鋳造）

- ノードになるまたブロックをサインするコンセンサスに参加するためにMILEアップを取り付けて、10,000 – 100,000 XDRのデポジットを保有すべきです。

- 作動しているマスター・ノードがXDRの規模によってそのXDRのデポジットにブロックチェーンから年収の8-13%を受けています。受取りがいつも鋳造されているし、１－２日に一度配分されています。依存は放物線です。つまり、100,000デポジットに近ければ近いほど%が速く成長しています。

- パブリック・インストール・パッケージ（ドック）から誰でもマスター・ノードが着手できます。

- ４TBのハードドライブがある最近のコンピューターや安固なインターネット・コネクションが必要です。

- その放出のタイプはブロックチェーンがよく作動しているころを確認するネットの参加者にとって動機づけのものです。

- マスター・ノードがいくらでも存在できますが、コンセンサスがその中の１００００から編成されています（活発なノード）。他のノードが待機モードに作動しています。例えば、ブロックチェーンが保管できます。しかし、サインのためのブロックもプレミア鋳造も受け取りません。

- もし活発なノードはブロックがサインできなければ、コンセンサスから捨てられて、待機モードからの次のノードが活発になります。

- 活発なノードは限界がありますから、8-13%のプレミア鋳造のための貨幣的ベースも限界されます。つまり、最高のXDRは十億になります。例えば、エコシステムが百億XDRに成長すれば、インフレーションがただ0.8-1.3%になります。

- 一兆のXDRが鋳造されると、マスターノードがプレミア鋳造を受け止めるようになります。最高に昇格した供給のソフトフォークがその結果になります。

3.4.2　放出センター

- 放出センターになるため、ブロックチェーンに10,000 MILE以上を預金すべきです。

- ブロックチェーンがすぐに放出センターワォレットへ新XDRを発行します。発行したXDRの数は内ブロックチェーンMILE/XDRレートに依存しています。

- もし、時間にわたってMILE/XDRレートが成長すれば、限界が増やしたから、各放出センターは多くのXDRが発行できます。

- 放出センターからMILEのブロックを解除したがれば、ユーザーが現実MILE/XDRレートを応じてブロックチェーンへXDRを送るべきです。XDRの0、2%がその費になります。悪意のあるユーザーが多くの無用な取引を通じてネットワークを制動してみろこと、つまり、殺到を避ける方法です。口銭が活発なノーソのなかで配分されています。

- XDRの要求が高ければ、MILE/XDRの為替レートも高くなるようです。XDRの要求が成長し止れば、または減少すれば、MILE/XDRの為替レートも安定になるまたは減少します。

- MILE/XDRの放出＝N の場合、MILEのブロックを解除することは MILE/XDR ≥ N の場合だけに可能になります。

- 不適切に高いまたは低いMILE/XDRのマスターノードからの投票を解除する数アルゴリズムが利用されています。目的はMILE/XDRをより安定的にすることです。

- MILE/XDRを計算するため数アルゴリズムが利用されています。そのアルゴリズムが平等計算に似ています。つまり、ブロックチェーンにある歴史的な為替レートが利用されています。その結果、地元の動きの可能性が低くなります。また、超インフレーションを避けるためにXDR供給の成長が時間がかかるようになります。

3.5　省点

• XDR送金の料金が０であるおかげで、マイクロペイメントができます。それから、ブロックチェーンが長い時間にわたって作動させるために、周期に切頭が起こります。

• ブロックチェーンが４Tbになると切頭のアルゴリズムが発動されます。つまり、システムは、ブロックチェーンの作動部分から空ろなワォレットまたは１XDR以降があるワォレットを仮定的に解除します。ブロックチェーンの解除後、情勢が新ジェネシス・ブロックに記録されています。ブロックチェーンの以前の情勢が特別なノードだけにあります。

• 断ち切った取引から残ったのは、断ち切りのあと、マスターノードへ送るようになります。

• また、ブロックチェーンの切頭の際、作動しないノードが解除されているし、そのノーソにある資金が守られています。

4. 無料で高速なトランザクション

MILEネットワークのトランザクションは無料で、ブロックは20秒で閉じられ、設計吐出し量は1秒あたり最大10,000トランザクションです。ブロックチェーンの最適化は（ビットコインのようなシステムのUTXOモデル（未使用トランザクションとは異なり）取引の壁付けに関する情報を格納しないという事実のために発生します。ユーザーのための無料トランザクションはミンチングのメカニズムと反射点のおかげで可能です。（「ブロック閉鎖時のノードエミッション（minting)」のセクションで詳しく説明）。

5.　ブロックチェーン

5.1　選択の説明

- MILEを使用する目的はブロックチェーンの以下の特性を満たすコンセンサスを必要とした。

  1. 新しいブロックを作成する時間20秒
  2. コンセンサスの発展に参加できるノードの総数は、103から104まで変化する可能性
  3. トランザクションの高い速度（1秒あたり少なくとも103トランザクション)
  4. ブロックチェーンアルゴリズムの実装は、PoWのブロックチェーンと比べ大きな計算能力を必要とすべきではありません

- 選択肢はBFTアルゴリズムと比べ高速であるアルゴリズムsdBFTになりました。投票ノードのグループはその裁量でブロックの構成を管理して新しいブロックを形成する時コンセンサスの多数の参加者は予備的陰謀を複雑にします。次のコンセンサスセットは他の投票ノードのセットを選択するからです。

- 複数の投票ノードの擬似ランダム選択は次の投票におけるノードの選択に大きな影響を与えません。アルゴリズムの説明は、Article concensus sdBFTの記事に記載されています。

5.2　新しいブロックを形成するためのアルゴリズム

- ユーザがある時点でトランザクションIを形成させます

- トランザクションはお客様が関連付けられている最も近いノードに渡されます

- ノードはパッシブ・エスコート・マスターの3つの状態のいずれかになります

- ノードがパッシブである場合ノードはトランザクションをチェックし、トランザクションがエスコートノードに到達するまでピアツーピアネットワーク上にそれを渡します

- エスコートノードは、トランザクションをマスターノードに転送します

- マスターノードはトランザクションをチェックし、トランザクションが正しければ、それをエスコートノードに転送し、生成されるブロックにトランザクションIを書き込みます。

- トランザクションIを受け入れたエスコートノードは、それををチェックし、形成されたブロックにそれを書き込見ます

- この一連のアクションはブロックの最後まで20秒以内に繰り返されます

- この後、マスターノードはブロックの完了に関するメッセージを送信します

- 各エスコートノードは、トランザクション・ブロックのハッシュやハッシュの電子署名などを計算し、受け取ったハッシュをマスター・ノードに転送します

- マスターノードは、正しい電子署名の数を計算します。受け取った正しい署名の数がコンセンサスに参加しているエスコートノードの合計値の2/3を超える場合、ブロックは形成されたとみなされます。さもなければ、ブロックは形成されません

- ブロックチェーンは時間外であり、チェックしないで、ブロック内に置かれたトランザクションの時間と一致しません

- ブロックチェーンの上で動作するシステムは平均ブロック終了時間（約20秒）に焦点を当てます

5.3　擬似乱数ジェネレータ

- オペレーティングシステムに組み込まれている標準の擬似乱数ジェネレータは多くの重大な脆弱性がありますが、最も危険なものは次です。

- シードとして、タイムスタンプを使用して疑似乱数を生成します。その結果、攻撃者が擬似乱数を生成するアルゴリズムとその生成の近似時間を知っていれば、そのアルゴリズムによって生成された秘密鍵（パスワード）を高い確率で選択することができます。

- タイムスタンプに加えて他のデータが使用されても、標準の擬似乱数ジェネレータはかなり予測可能なシーケンスを生成します。攻撃者は無差別にパスワード（ハッシュ）を選択します。

- MILEでは乱数は鍵の生成から電子署名の「塩」まで使用されています。

- これに関連して、乱数の品質には特別な要件が課せられます。擬似乱数ジェネレータから得られた順は広範なテストを受けます。以下は結果です。

5.3.1　テストの目的

このテストの目的は生成された乱数列の動的制御の事実を検証することです。その検証は配列の一様分布に関する統計的仮説を確認するために実施されます。

5.3.2　テストの条件と注文

テストは、疑似乱数ジェネレータによって生成された乱数のシーケンスをチェックすることから成ります。制御を実行するために、以下の動作が実行されます。

1. APMプログラミング7（開発環境「Visual Studio 2017」およびMILEソフトウェアがインストールされた自動化されたワークステーション）で構成される暗号モジュールで、世代およびランダムシーケンステスト機能の実装をチェックするためのスタンドが作成されます。

2. APMプログラムにはテストするようにフリーソフトウェアがインストールされています。
   a) NIST Statistical test Suite (NIST-STS);
   b) Test-U01.波数ため料理されました

3. 擬似乱数ジェネレータは生産性と長さ試験の持続時間に自然な制限がある条件で乱数列を生成します（少なくとも1024ギガバイト)。擬似乱数列をAPMプログラムのStatMessTimeバイナリファイル（1000バイト）やStatCurrent（2000バイト）などのバイナリファイルにコピーします。

4. APMプログラムは上記の統計的テストパッケージを使用して基本的な統計的基準することによって擬似乱数を分析します。

5　バイナリという擬似乱数列の品質を評価するには、3sという基準は間隔を有するバイナリシンボルの相対周波数ため料理されました.

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

ここは $p = 0,5 + D, q = 0,5 - D$ 場合nバイナリシンボル：

第1表. 3sという基準の以下の間隔を使用しました

	3sという基準の間隔:	
n	D=0	$\frac{1}{2}D\frac{1}{2} = 0,01$
2^{13}	(0.4835„0.5165)	(0.4734„0.5265)
2^{15}	(0.4918„0.5082)	(0.4818„0.5182)
2^{16}	(0.4941„0.5058)	(0.4841„0.5158)
2^{17}	(0.4959„0.5041)	(0.4859„0.5141)
2^{18}	(0.4971„0.5029)	(0.4871„0.5129)

6.　バイトシーケンスという擬似乱数列の品質を評価するには、255自由度があるc 2という基準を使用されました:

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

7. 動的試験手順を検証するために、試験結果の処理、分析および評価が行われます。使用された統計的基準が、第5項に記載された擬似乱数列の一様分布の仮説を棄却しない場合、このチェックは成功したとみなされます。

5.3.3　テストの目的

StatMessTimeの処理結

第2表. 1024バイトの16セグメントに「1」の発生頻度

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

第3表. 1024バイトの16セグメントに「1」の相対発生頻度

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

第4表．シフト1-512の合計で「1」の相対発生頻度

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

最小結果：0.4961，最大結果0.5042

第5表.16384バイトのときバイト頻度

0	70	58	72	71	73	67	58	60
8	58	83	50	74	57	66	57	62
16	49	73	60	55	71	73	62	64
24	61	74	66	74	63	62	73	65
32	54	62	69	60	68	65	64	50
40	66	60	68	57	49	56	52	60
48	64	68	64	59	56	65	61	67
56	50	80	63	68	69	45	61	57
64	63	55	73	76	79	59	48	68
72	64	62	65	62	51	49	62	69
80	69	66	46	55	64	77	61	67

88	63	64	62	54	59	82	56	70
96	56	72	60	65	58	61	71	57
104	60	63	61	60	55	75	65	61
112	72	68	77	75	56	65	62	73
120	61	76	58	68	59	78	70	64
128	67	72	59	72	67	68	59	65
136	60	61	54	77	55	67	41	75
144	57	61	66	65	62	78	56	68
152	72	68	55	61	73	59	51	75
160	54	67	66	57	74	53	81	66
168	64	49	58	59	64	61	74	50
176	66	61	70	70	59	54	69	69
184	61	68	74	57	68	61	64	82
192	82	69	47	70	63	58	60	61
200	68	57	60	76	69	61	45	65
208	76	61	55	58	60	70	53	67
216	72	78	67	62	62	78	73	68
224	62	64	52	65	62	80	75	56
232	55	62	61	66	53	51	72	58
240	51	60	69	73	77	60	56	71
240	51	60	69	73	77	60	56	71
248	80	56	66	86	73	61	77	67

最小：41，最大：86

３ 16384バイト（255自由度）のc2値：c2=
268.5 StatCurrentの処理結果:

第6表. 1024バイトの32セグメントに「1」の発生頻度

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

第7表．1024バイトの32セグメントに「1」の相対発生頻度

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

第8表．シフト1-512の合計で「1」の相対発生頻度

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
320	0.4991	0.4986	0.4998	0.5003	0.4995	0.4994	0.4985	0.4994
328	0.4998	0.5014	0.5012	0.5006	0.5004	0.4984	0.4996	0.4984
336	0.4983	0.5007	0.4993	0.4992	0.5008	0.5012	0.5003	0.5024

344	0.4984	0.4993	0.4989	0.5006	0.4999	0.4986	0.4994	0.5002
352	0.5014	0.4991	0.5015	0.5002	0.5016	0.5004	0.5017	0.5006
360	0.4999	0.4985	0.4999	0.4983	0.4992	0.5004	0.5004	0.5005
368	0.5002	0.5004	0.5007	0.4996	0.5004	0.4999	0.4995	0.5016
376	0.4996	0.5006	0.4996	0.5007	0.5005	0.4995	0.5010	0.5006
384	0.5016	0.5012	0.4991	0.4994	0.5004	0.5002	0.5013	0.4994
392	0.5014	0.4996	0.4991	0.5019	0.4992	0.5021	0.5004	0.5018
400	0.5006	0.4991	0.4993	0.5009	0.5007	0.4999	0.5022	0.4995
408	0.4999	0.4973	0.4994	0.4997	0.4990	0.4982	0.4992	0.5008
416	0.4995	0.5004	0.5000	0.5005	0.5015	0.5008	0.5015	0.5003
424	0.5003	0.5005	0.5019	0.5009	0.4990	0.4994	0.4981	0.5008
432	0.4990	0.4988	0.5007	0.5020	0.5008	0.5003	0.5010	0.5000
440	0.4974	0.4993	0.4982	0.4994	0.5008	0.4994	0.5026	0.4984
448	0.5013	0.4995	0.4993	0.4996	0.5016	0.4985	0.4996	0.4991
456	0.5011	0.5012	0.5015	0.5018	0.5003	0.5004	0.4995	0.5017
464	0.4995	0.5004	0.5000	0.5024	0.4997	0.5027	0.4981	0.4987
472	0.5008	0.5006	0.5003	0.5007	0.5007	0.4990	0.4998	0.4992
480	0.5008	0.4996	0.5027	0.4996	0.5016	0.5012	0.4993	0.5004
488	0.5006	0.5008	0.5008	0.5026	0.5014	0.4993	0.4999	0.5012
496	0.4987	0.5018	0.4996	0.4998	0.5008	0.5009	0.4996	0.4988
504	0.5017	0.4993	0.5004	0.4980	0.5017	0.5014	0.4999	0.5011

最小：0.4970：最大：0.5030

第9表. 32768バイトのときバイト頻度

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

最小：99，最大：154

32768バイト（255自由度）のc2値：c^2= 239.8

5.3.4　結果

MILEでは初期状態の動的変化を伴うハッシュ関数の二重計算に基づく擬似乱数ジェネレータが実装されます。擬似乱数ジェネレータによって生成された擬似乱数の品質の方が|D| < 0.01のとき一つのバイナリシンボルに0.5 + D良くて、解析された乱数列の一様分布の仮説を満たします。

5.3.5　暗号法

- ECSDA デジタル署名(BTCで使用される).
- Ed25519 (使用されているBTCよりも速いだ)
- SHA-3 ハッシュアルゴリズム (BTCよりも速くて、安全だ)

5.3.6　ブロックチェーンの一般なプロパティ

- 手数料ゼロのおかげで、小口取引（「コーヒーを支払う」）をサポートします。
- 最大取引金額は制限がありません。
- ブロックチェーンは、定期的に自己最適化を実行し、指定された境界内でサイズを維持します。
- 「ごみ」バランスがあるウォレットはリセットされますが、ブロックチェーンの切り捨てに参加したノードにウォレットの内容が送られます。

5.3.7　取引タイプ

- 手数料ゼロのおかげで、小口取引（「コーヒーを支払う」）をサポートします。
- XDR
- MILEを送信しています。
- ノードの登録のアナウンスです。
- ノードの除外に関するアナウンスです。
- 新しいジェネシスブロック（切り捨て)です。
- MILE/XDRコースを出版します。

- ノードによる投票の問題を提出します。
- ノードによる投票です。
- XDR発行センターの発行またはバックエミッションです。

5.3.8 制御パラメータ

- ブロックを切り捨てる手順が開始されるブロック間隔です。
- 前のブロックが失敗した場合、切り捨て手順が繰り返されるブロック間隔です。
- ノードを作成できるデポジットの範囲です。
- ノード数が制限します。
- 制御パラメータの更新は、ノードの投票で行われます。

5.3.9 ウォレット

- ウォレット アドレスは、Base58checkerMod2でエンコードされた文字列で、ブロックチェーンでホストされているトランザクションに書き込まれます。
- ウォレットでは、XDRとMILEの両方を送受信できます。
- ウォレットタイプ:

ー ソフト:
ー 計算（取引）をして、バランスをチェックします。

ー 必要なブロックを取得し、ブロックチェーン全体ではなく、ハッシュ木のみをチェックできる特別なプロ トコルを使用します。

ー標準:
ー ブロックチェーン全体を保管します。ー ノードとして登録することができます。

ー マルチサイン:
ー システムは、複数の署名がある場合にトランザクションを受け入れることができます。

ー 署名者ウォレットは通じて、制御パラメータの変化によるシステムのポイント管理が行われます。
ー ウォレットは、ブロックチェーンの仕事の最初の1年間だけ必要です。その後、無効になります。

ー システムウォレット:
ー これは、ブロックチェーンの切り捨て時、削除されたウォレットから手数料を蓄積します。
することができます。
ー ウォレットは、ブロックを切り捨てることに参加したノードだけに手数料を支払う発信取引を作成

6 実用

6.1 無料国際支払い

暗号通貨の市場は、高速で安価な国際支払いの需要で大きく成長しました。これは、通貨の流通が国によって非常に制限されている中国に当てはまります。

シンガポールの開催されたMoney 2020会議の参加者を分析した結果によると、5000以上のUSDの国境を越える取引が可能な支払いシステムはありません。州間で5,000～10,000 USD以上を送金する唯一のツールはSWIFTです。しかし、送金には、多くの書類を記入し、書類が銀行によってチェックされるのを待つ必要があります。また、通貨制御マネージャーとの送金について話し合い、送金を行うまで数時間を待ちます。 SWIFTの費用は約1%です。

MILEを使用すると、銀行マネージャーと通信することなく、数秒間世界中のどこからでも無料で送金できます。

6.2　独立ストレージ

アパートや家にお金を保管するのは危険です。セーフボックスに財産を保管する銀行との契約では、銀行がセル内容物の安全性の責任を負わないという条項があります。その結果、大量の資金が定期的に銀行のセルから消えてしまいます。銀行閉鎖の統計情報は、「はじめに」に記載されています。MILEを使用すると、中央カウンターパーティーのリスクがゼロで、口座を閉鎖することなく、分散ネットワークに安全にお金を保管することができます。

6.3　国際協力経済

MILEの価値を保証する重要な側面の1つは、商品とサービスの本当の総売上高です。MILEの作成者は、MILEの普及の最大の可能性は協調経済だと見いだしています。これは、不安定な金融システムを有する途上国にとって特に当てはまります。これらの市場には、不換紙幣の不足があり、物々交換と他のネッティングの方法に対する素因があります。　　ほとんどの先進国は事実上経済成長を停止しており、世界経済の発展に最大の貢献をしているのは途上国です。同じことがビジネスにも適用されます。大企業は、いくつかの財政的保有を除いて、5％以下の収益性を有しています。危機時には、豊かな金融会社でも大きな損失を抱えています。

同時に、歴史的に協同組合は、特に危機の時代に市場に対抗して成長しています。例えば:

- Rabobankは、2008年に42％の増加を示し、創立メンバーは預金が20％増加しました。2008～2009年に、信用組合の会員数が大幅に増加しました。
- 3人のカナダ人にひとりは信用組合システムのメンバーです。小売預金および住宅ローン市場に信用組合のシェアは2010年に16％から19％に増加しました　[ムーディーズの投資家がグローバル・バンキングの報告書、2010年4月]。
- 2012年第1四半期から、Desjardins協同組合は、北米の7,500の預託金融機関のうち第16位で、第1順位の資本で2位（これは16.8％）です。

協調経済は膨大で、豊かな国や途上国では協同組合が共通しています:

- 協同組合には世界中、10億の株主がいます。
- インドでは、協同組合が農村人口の67％に商品を提供しています。
- アフリカの家主の40％が協同組合に参加しています。
- 2010年、1500の最大協同組合の収入は、2兆USD近くに達しました。
- 国際開発Desjardins（DID）はマイクロファイナンスのリーダーです。DIDは世界中の880万人の会員と顧客と協力していて、25億カナダドルのローン・キャピタルを有しています。
- 一部のアフリカ諸国では、Desjardinsはマイクロファイナンス市場の35％を占めています。
- 中国では、協同組合がマイクロクレジット市場の91％を占めています。
- 信用協同組合は、先進国に働く労働移民から途上国のその家族に手頃な価格の送金を提供しています。これはラテンアメリカとアフリカにとって特に重要です。

協調経済はより効率的に機能します:

- 協同組合の活動は、株式交換資本増強ではなくて、すべての株主のために資金を獲得することを目的としております。

- すべての株主が関与しており、モチベーションに費やす時間はかかりません。

- 企業では、トップマネジメントは通常の従業員の100倍稼得して、協同組合では10倍しか稼得しません。つまり、構造を維持するコストははるかに低くなります。

- 経済の内部輪郭と協同組合参加者間のネッティングにより、税金、取引と仲介者の支出を削減することができます。また、これにより、クレジットの必要性が減ります。

- その結果、協同組合内の商品やサービスの価格は、外市場よりも40％も低いです。これは、外部からの資本や人々の誘致のインセンティブであり、協同組合への長期的な参加のモチベーションをします。

MILEに基づいて協同組合用に作成されたツール:

- ネッティングの簿記、

- レシートとバランスを保管するための寄託、

- 外部からの出資の誘致、

- 税務当局への報告の準備、

- トークンで作業するための法的テンプレート、

- 大きな割引の商品とサービスの市場。

7　エコシステム参加者のモチベーション

ユーザーは:
• ユーザーは、高速無料取引を作成したり、暗号スペースに残ったまま価値を保管する機会を得ることができます。

投資家は:
• 投資を回収することに興味があります。

• 返品は、システムのサポートを通じてすることができます。 どんな参加者も、ブロックチェーンのノードと/または発行センターになることがあります。

発行センターは:
• MILEコースの増加に関心があります。これにより、資本と通常の収入が増えるでしょう。

ノードの所有者は:
• ブロックチェーンのブロックに署名するための手数料を受け取ることに興味があります。

• 所有者の所得範囲は、XDRで年率8～13％です。

8　法律カバー

毎日の使用

現地の法律は登録を必要としないであり、取引量が少ないことや、取引の規則性は欠けている場合は、MILEの使用は、法的に登録ないことができます。

他の場合には、地元の協同組合や消費者社会を創設したり、既存のに加入することが推奨されます。

協同組合の主なツールは「シェア」です。「シェア」寄付は、消費者社会のオープンエンド型ファンドに対する「シェア」がある参加者の寄付です。寄付は、金銭、有価証券、土地、その他の財産、または金銭的価値を有するその他の権利ですることができます。返寄付は、シェア」がある参加者が受け取った商品の金額または価格に関係なく課税されません。
協同組合内の「シェア」の交換は可能であり、課税されません。つまり、法的に、MILEを「シェア」の評価のためのツールとして使用することができます。

協同組合のメンバーではない外部の人々には、MILEとの協力をロイヤルティ プログラムとしてすることができます：

- トークンは、ボーナスポイントを請求する権利です。この権利は法人と個人に販売することができます。また、簿記で考慮してます。
- トークンが製品またはサービスのために交換されると、トークン所有者はボーナスポイントを請求する権利を認識します。ポイントを取得し、商品を受け取ります。
- スーパーマーケットのボーナスポイントと航空会社のボーナスマイルの同じスキームです。