MILE

無料で速く安全で分散したステーブルコイン

2018 年 5 月 30 日

技術報告書　v.1.2

ロータスマイルで

短縮版: mile.global

1 はじめに

世界には、以下の特性を同時に保有する価値を測定し、保管し、移転する手段はまだありません。

- 安定したコスト;
- 透明なエミッションのアルゴリズム;
- 世界各地のあらゆる取引先に無料で迅速かつ自由に価値を移;
- 長時間にわたる価値の確実な保管;
- ノンブロッキングで取消不能な取引;

既存の基本的な楽器（USD や EUR や CNY など）はこの問題を解決しません:

- 様々な国間通貨で 10,000 米ドルを法的に引き出すためには、複数の書類と複数の承認が必要です。移転には、追加の承認と移転の阻止のリスクを伴い 24 時間以上かかります;
- 毎年国家の主権債務の信頼が低下し、国債の債務不履行の数は平均 0.25 兆/年であり、国家債務は絶えず増加しています;
- 不換紙幣の発行に関する原則と報告書は透明ではありません;

- 毎年大勢の不換紙幣が価値を変化して、ノルウェ･EU･日本との安定していても、現地通貨の価値は 15～25%/年です。そのような時に、人々は自動的にネッティングの代替手段を考え出します;
- 中央のカウンターパーティーとしての銀行は、もっと多くのリスクを負っています。米国では年間 10～150 ライセンスを撤回し、EU では約 1 兆ユーロがデフォルトのリスクの高い銀行にあります。ロシアでは、7 年間にわたって銀行の半数が閉鎖した;
- 欧州銀行の口座開設は 1 ヶ月から 6 ヶ月かかります;
- どの国でも、銀行は状況を明らかにする前に資金をブロックすることができ、政府は新しい法律を導入し、資金が不法に受け取られることを遡及的に決定し、キプロスの状態のように預金金額の 100%までの罰金を課すことができます。

今日のデジタル通貨もこれらの問題を解決しません:

- ビットコインは分散化されていますが、ボラティリティが高いです;
- ライトニングネットワークを導入したのは、BTC の取引価格は 1.2　米ドルまで引き下げられましたが「コーヒーを払う」ように高価であり、この技術の限られた適用を考えると、このような手数料は相互の和解のみで可能です;
- 既存のステブルコインは集中化したファイトストレージに結びつけられています。すなわち、取引相手の 1 つに依存しています;
- •既存のステブルコインは不透明なエミッション機構があります;
- ビットシェアーズの市場の固定資産は BTS よりも不安定な BTS 暗号通貨の担保に縛られています;

それで次のプロパティセットを持つ新しいスペースが強く求められています:

1. XDR に結びついた安定した価格の決済手段;

2. 数学的に厳密な証明があるアルゴリズムのコードで実施されたオープンソースに基づく透明なエミッション;

3. XDR にとって無料トランザクションと MILE を送信するための料金は 0.2%です;

4. 1 分以内に実行される速いトランザクション;

5. 様々な人々や組織に属している世界中の 10,000 のノードに基づく分散化;

このツールを使用すると、次のことが可能になります:

- 価値の安全を確かめます;
- 自由に、迅速に、信頼性高く、手数料なしで世界中どこでも価値を持ちます;

2 価格の安定性

人によって作成された公共資源管理のシステムには社会的および技術的という 2 つのコンセンサスがあります。

ビットコインの例について:

- 社会的コンセンサスはビットコインの通信プロトコルの新しいバージョンの一般的な議論です。
- 技術的なオンチェインコンセンサスはビットコインの通信プロトコルの新しいバージョンをサポートするデバイスにソフトウェアをインストールまたはアンインストールするかことによって鉱夫の投票です。

技術コンセンサスがどのように構成されていても、社会レベルはいつも決定的です。

- 技術的に現代的かつ透明なコンセンサスの例があり、その上に中央のエリートが賄賂による投票を腐敗させる（LISK(リスク)と先進国）;
- 逆も正しいでしょう：良心的な人々は複雑な技術を使わずに口頭でさえ合意することができます。

社会レベルで MILE ネットワークの参加者は MILE システムの 1 XDR が常に 1 XDR に等しいことに同意した（国際通貨基金はレートを計算して公表します）

XDR の主な適用範囲が実際の商品とサービスの交換のための計算なので為替取引と特定通貨の為替価格は XDR のコストに重要な影響を与えません。

たとえば、2018 年 3 月末には世界のすべての取引所で最も人気のある暗号通貨の（ビットコイン）1 日平均出来高は 50 億米ドルで、ビットコインネットワークの総取引量は 10 億ドルです。 **イーサリアムの**為替取引は 15 億で、ネットワーク内の取引量は 7 億ドルです。 **ビットコインキャッシュ**は 2 億米ドルに対して 4 億です。

考慮すべき点:

• 描かれた暗号取引所の量に関する研究;

• 暗号通貨の支払いの大部分は暗号取引所の財布間の振替や大規模な財布の合併や動きなどです。例えば、

- ビットコインの 1 日のボリュームの 40%が 100 トランザクションだけ転送され、トランザクションあたり平均 3000 万米ドル
- ETH は 100 トランザクションに瞬間
- BCH はあまり 40%;
- LTC は 61%

すなわち、実際の資金繰りは 1.5-3 倍以下になります。

コインマーケットキャップのコインの大部分は実質商品交換においてゼロ回転を持ち、同時に株式取引の量を増やす予定です。それで、今日、暗号通貨のコストは投機とニュースのバックグラウンドに完全に依存しており、暗号通貨は大きなボラティリティを持っています。

MILE には独自のアプローチがあります:

• 参加者は仮想通貨取引所へ XDR を引き出し、人為的に取引量を増やそうとはしません。

• 重要な XDR の目的は：

－貴重品を保管し移動する手段;

－ 実体経済における商品とサービスの交換手段

そのため誰かが XDR 為替レートを省略しようとしても、日常生活で XDR を使用する人はこの贈り物を利用します。現実世界での XDR の購買力はこの交換の傾向から変わらないので、誰でも取引所では 0.8 XDR の価格で 1 XDR を購入したいと思うでしょう。

XDR の利用については、次のセクションで見って見よう。

3 エミッションアルゴリズム

MILE プラットフォームは放出や計算のため利用しているものが二つあります。これは Coin (XDR) や Token (MILE)になります。

3.1 XDR

- プラットフォームでの価値の保管や為替のための計算単位です。
- 透過型ブリッジを通じて MILE トークン保有者やブロックチェーンのノードで放出されています。
- 計算単位はずっと国際通貨基金の 1 XDR です（現為替：XDR/USD）
- 全体部分の数：１２
- コンマ後部分の数：２

- つまり、XDR の限界：999.999.999.999.99（１兆）
- この XDR はブロックチェーンのノードが「燃料」として使われているし、MILE を支援したり資源を費やしたりする着実なメンバーを明らかにするノードのデポジットということです。

3.2 MILE

- XDR の放出アルゴリズムでの主なことです。
- 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などの販売部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。

- コンセンサス中、現実、MILE/XDR の最終の為替レートが定義されています。このレートは放出センターで放出の限界を計算するために利用しています。

- MILE/XDR を計算するアルゴリズムは移動平均を計算するアルゴリズムに似ています。つまり、ブロックチェーンにある史的な為替レートが使われています。これによって可能な現地操作の振幅を少なくなることができます。

- 全体部分の数： 9
- コンマ後部分の数： 5
- つまり、MILE の限界：999.999.999.999.99（十億）

3.3 一次の放出

- 最初はシステムが 0 XDR[1]あります。
- 最初はシステムが 1　000　000　000 MILE あり、これ以降新 MILE が放出していません。
- 最初の値段は 1 MILE＝１XDR になります。

3.4 二次性放出

[1] コンセンサスに参加するノードのデポジットへ向かう 300,000 の放出がジェネシス・ブロックに定義されています。このノードは MILE チームの部分であり、なうべく長く活発的に維持されます。

3.4.1　ブロック閉止の際ノード放出（鋳造）

- ブロックをサインする際ブロックチェーンのノードの放出
- MILE アルゴリズムに応じて作動しているノードが 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。
- そのアルゴリズムのしかたは年収の利率がランダムの部分でワォレットに入金されているということです。一般的に一年にわたって利率は 8-13%になります。
- ノードになる権利またブロックをサインするコンセンサスに参加する権利を受けるため MILE アップを開くし、ワォレットで 10,000 – 100,000 XDR のデポジットを保有すべきです。
- ブロック閉止の報酬がデポジットに依存するのは非線形です。
- 開発チームがソースコードを公開にして、誰でもノードが着手できます。
- ノードが安固に作動するため、４Tb のハードディスクがある普通のコンピューターや安固なインターネット･コネクションがずいぶんです。
- この放出の方法は、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。

3.4.2　エミッションセンターでの放出

- MILE トークンはブロックチェーンのユーザーのワォレットにあります。
- MILE トークン保有者は特別なアドレスに MILE トークンが何でも預金できます。
- 放出センターになるため、保有者は 10,000 MILE 以上を預金すべきです。
- これによって、前にノードコンセンサスで定義されてブロックチェーンに記録した XDR/MILE の現為替レートに応じる XDR をすぐに受けます。
- もし、時間にわたって、t_2 という点に、MILE/XDR の為替レートが高くなれば、ユーザーがワォレットから「XDR を離す」というコマンドが利用できます。そしてシスタムが、「$MILE(XDR(t_2) - XDR(t_1))$」という定式を利用して、XDR を自動的に加えることができます。
- MILE トークンのブロックを解除するため、ユーザーが特別なアドレスへ XDR を送るべきです。返事としてユーザーは 0,2%ぬき現 MILE/XDR 為替レートで MILE を受けます。口銭はブロックチェーンにおける殺到を減少するために必要で、ネットを維持するコミュニティー、つまりノーソのなかで配分されています。

- システム構成から推して、時間がたつとともにコミュニティーは XDR の必要性が高ければ、MILE/XDR の為替レートも高くなるようです。それから MILE 保有者がトークンを預金することに関心があるようです。

MILE/XDR=N というレベルでの XDR 放出の場合、「MILE/XDR≥N」という定式が事実になるときだけに、MILE のブロック解除が可能になります。

3.5 放出の経済的な論拠

- ノードまたは放出センターを支援するためのデポジットを保有しているユーザーが多ければ多いほど XDR が重要になり、MILE の為替レートが高くなります。
- 交易の事実取引のために XDR を利用するユーザーが多ければ多いほど XDR の重要性が高くなり、MILE の為替レートが高くなります。
- MILE の価値が高ければ高いほど XDR を放出する可能性も高くなります。

3.6 反省点

- 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 4 Tb 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 1 XDR 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。
- ブロックチェーンの切頭の際、ノードで口銭を払うため、仮定的に空ろなワォレット(1 XDR 以降があったワォレット)からしている残部が使われる予定です。
- 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.

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 – ½ D ½ – 1,5[1 – 4*D*2)n – 1]0,5,0,5 + ½ D ½ + 1,5[1 – 4*D*2)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	½ D ½ = 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:

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

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 c^2 値：c^2= 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 c^2 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:
- ソフト:
- * 計算（取引）をして、バランスをチェックします。
  * 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。
- 標準:
- * ブロックチェーン全体を保管します。
  * ノードとして登録することができます。
- マルチサイン:
- * 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。
- ポイントウォレット:
- * 開発者ウォレットを通じて、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。
  * 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。
- システムウォレット:
- * 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。
  * 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することができます。

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。