MILE　マイル

無料で速く安全で分散した安定しているコイン

2018 年 5 月 30日

技術報告書 v.1.5

作成者：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、値を転送できるツールはありません

- 安定した価格；
- 高速取引；
- 自由と無料な取引；
- 無制限のボリューム
- ブロック及びキャンセル不可能な取引
- エミッションの透明なアルゴリズム；

既存の決済通貨（USD や EUR や CNY など）は上記の問題を解決しません:

- 価格が安定してない。ほとんどの決済通貨は揮発性です。スイスや日本などの先進国であっても、現地通貨の価値は急速に上昇または下降する可能性があります：2016年10月〜12月に日本円が15%低下し[1]、2015年1月にCHFが1週間で20%上昇しました[2]。
- 遅い取引。様々な国間で決済通貨で10万米ドル以上場合の送金を行うためには面倒な一連の交渉を行うべきで多くの書類を準備も必要です。海外振り込みには数日かかりますし、追加的な調整や資金の後退のリスクがあります。 また、ヨーロッパで銀行口座開設に数ヶ月かかることもあります。
- 高価な取引。 決済システムのウェブサイトによると、平均為替相場は約3〜5%です。
- 検閲レベルの成長。 2018年に制裁と貿易戦争に関与した数十の国々が、SWIFT制度からブロックされたり、重大な制限を受けています。その中には、中国、インド、ロシア、イラン、トルコ、ベネズエラなどがあります。そのうち5カ国はGDP上位30カ国にある[3]
- トランザクションの可逆性

---

[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)

- エミッションの不透明なアルゴリズムで個人の少数が制御する。それは超インフレと経済危機をもたらす[4]。正式には先進国の中央銀行が「M0」などの指標を公表しているが、社会はその数値を監査していない。

既存のデジタル通貨も上記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；
- 既存の安定したコインの多くは、集中化されたフラットストレージに結びついており、取引相手に100%依存しており、これも腐敗集団に可能性があります（USDT、サークルなど）；
- 既存の安定したコインの多くは、貴金属、労働力価格、または他の資産に付いていますが、安定していません。例えば金商品は米ドルで1ヶ月以内に15%上昇または下落することができます[5]；
- ERC20ベースの安定したコインは、Ethereumメインネットに依存します。各人気アプリケーションが表示されているときにそのメインネットが詰まる[6]；
- アルゴリズムな安定したコインはソロス（Soros）によって攻撃される可能性があります[7]
- 高速で安価な取引できる安定したコインはビットシェアーズ市場のBTSです。しかし、大きな問題があります：Dan Larimer氏がビットシェアーズのコミュニティを離れ、それが崩壊につながりました。BTSの日次取引量は数百万ドル前後で変動している[8]。主なBitSharesフォーラムには、毎のアクティブトピックがほとんどありません[9]。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[10]。非常に少数の人々が実際にネットワークを支配する。
- 初期のホワイトペーパー段階には、分散型の安定したコインを記述しようとするプロジェクトがいくつかありますが、現在は動作していないので、こちらの説明の範囲外です。

上記のすべてに従って、オールインワンの製品には以下の品質が必要です：

1.安定した価格。

2.無修正。

3.自由と無料な取引。

4.高速取引。

5.誰でもコインを発行することを許可する。

このソリューションは、人々、企業、

•制裁や貿易戦争やSWIFTの問題にもかかわらず、世界中のどの国にも価値があるものを即座に無料で送ること。

•長期間にわたり価値のあるものを無料で保管すること。

2 価格の安定性

お金は社会的合意です

エンティティのお金を定義する唯一のものは、このエンティティを貿易、融資、投資、送金および引当金のためのお金として何人が使用しているかです。**ニクソン・ショック（ドル・ショック**、1971年）以来、米ドルは金に固定されておらず、常に発行されています。しかし、それはまだ多くの人々が実体経済のためにそれを使用するため、他の通貨にはまだ使用され、比較的安定しています。 経済が成長しているよりはるかに早く金が印刷されると、危機が起こっている。

---

[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

そのため、MILEのネットワークの安定した価格の安定性は、次の2つに基づいています。

- 実体経済の幅広い利用：貿易、融資、投資、送金、貯蓄。
- マネーサプライを経済成長よりも速くならないアルゴリズム。

実体経済の利用は技術的なものよりも外交上の仕事です。とにかく、オールインワンの品質（安定した価格、迅速かつ自由な取引、検閲の抵抗と透明性）の組み合わせは、既存の金銭や暗号通貨に比べて非常に競争力があります。

次の章では、マネーサプライ管理のアルゴリズムについて説明します。

3 エミッションアルゴリズム

MILEプラットフォームには、XDR（安定したコイン）とMILE（XDRの要求インデックス）の2つのコインがあります。

3.1 XDR

- XDRは、支払いの単位と価値の記憶として使用される安定したコインです。
- これは、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マスタノードによって発行されます。
- 社会的コンセンサスおよびマネーサプライ管理アルゴリズムを通じて、国際通貨基金(IMF)のSDR[11]と同等である傾向がある。
- XDRは、マスタノードを起動するブロックチェーン内にロックされるデポジットとして使用されます。
- XDRには12の整数と2つの小数があります。つまり、XDRの最大供給量は999 999 999 999.99（ほぼ1兆）です。最大量は、マスターノード間のコンセンサスおよびソフトフォークを介して更新することができる。

3.2 MILE

- MILEはXDRの需要の指標です。
- MILE / XDRレートは、ブロックチェーンネットワークのノード投票によって1日に1回設定されます。
- 証券取引所、OTC取引、オフライン経済のデータを使用するノード所有者は、考慮して公正な通貨レートを公表します。
- MILE / XDRレートは、排出センタを介して印刷できるXDRの数を示します。
- MILEは、エミッションセンターを立ち上げるためにブロックチェーン内にロックされるためのデポジットとして使用されます。
- MILEは9つの整数と5つの小数を持ちます。つまり、MILEの最大供給量は999 999 999.999 99（約10億）です。

3.3 一次のエミッション

- 当初は、創世記のブロックに300,000のXDRがあり、合意を開始するためにマスターノードの預金としてロックされます。
- 最初に、999 999 999.999 99 MILEが起源ブロックにあり、将来新しいMILEが放出されることはありません。
- 最初の値段は 1 MILE＝ 1 XDR になります。
- MILEの初期出荷および価格は、以下のステートメントに基づいています。14億米ドル相当の資本金がMILEエコシステムに組み込まれ、MILEの10億を108財布に広げました。財務会計では、銀行口座の決済通貨の金額ではありません。

---

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

さまざまな資産のポートフォリオ全体です：フラット通貨、暗号通貨、生産要素、知的財産、人的資源、ブランド価値、不動産、営業権、その他の有形無形資産、企業（上記のすべての資産の組み合わせ）。

3.4 二次のエミッション

3.4.1 ブロック閉止のためのマスターノード排出（鋳造）

- ノードになり、ブロックサインのコンセンサスに参加するには、MILEアプリケーションをインストールし、ブロックチェーンに10 000〜100 000 XDRを入金する必要があります。
- 稼動マスターノードは、預託金額に応じてXDRでの預金の年間ブロックチェーンから8-13％を受け取っている。依存関係は放物線で100 000のデポジットが近ければ近いほど、プロットが速くなります。
- 誰でも公開ドッカーからマスターノードを実行できます
- ブロック型の操作を続けているネットワーク参加者にとって、このタイプの排出は動機付けです。
- 任意の数のマスターノードが存在する可能性がありますが、コンセンサスはそれらの10,000ノード（アクティブノード）からのみ構築されます。残りのノードは待機モードで動作している。 彼らはブロックチェーンを格納することができますが、彼らは署名のためのブロックを受け取っていないし、鋳造（ミンティング）プレミアムを受け取っていません。
- いくつかのアクティブノードがブロックに署名できなかった場合、コンセンサスから追い出され、最も近い待ちノードが代わりにアクティブになります。
- 10,000ノードのアクティブノードの制限により、8-13％の鋳造プレミアムのためのマネタリーベースは10億XDRに制限されています。このシステムが、例えば100億XDRにまで拡大すれば、全体のインフレ率は0.8-1.3％と非常に小さくなります。
- すべての1兆XDRが作成されると、マスターノードはミンティングプレミアムの受信を停止します。おそらく、XDRの最大供給量をアップグレードしたソフトフォークにつながるでしょう。

3.4.2 エミッション（放出）センター

- 放出センターになるためには、保有者は1万MILE以上を預金するのは必要。
- ブロックチェーンは、放出センターの財布にすぐに新しいXDRを発行します。発行されるXDRの量は、内部ブロックチェインのMILE / XDRレートによって定義されます。
- MILE / XDR率が時間とともに上昇した場合、各排出センターは制限が拡大したため、より多くのXDRを発行することができます。
- 排出ガスセンタからMILEのロックを解除したい場合は、現在のMILE / XDRレートに従って適切な量のXDRをブロックチェーンに送信する必要があります。XDRの0.2％は、その操作のために洪水を下げるために請求されます。この課金はアクティブなマスターノードの間で分割されます。
- XDRの需要が増加すると、MILE / XDRが成長します。 XDRの需要が増加しなくなるかマイナスになると、MILE / XDRレートは安定し、または低下します。
- MILE / XDR = NでXDRが発行された場合、MILE / XDR□Nの場合にのみMILEをブロック解除することができます。
- 特定のアルゴリズムを使用して、MILE / XDRを揮発性の低いものにするために、マスターノードからの不十分な低いまたは高いMILE / XDR投票のノイズを遮断します
- 移動平均計算と同様のMILE / XDRを計算するために、特定のアルゴリズムが使用される。すなわち、ブロックチェーン内に保持される歴史的な為替レートが使用される。

可能な限り局所的な操作を最小限に抑え、ハイパーインフレを避けるためにXDR供給の成長を遅らせる

3.5 反射点

- XDR送金のゼロ・コミッションのため、システムはマイクロ・トランザクションを行うことができます。そのため、長期ブロックチェーンのメンテナンスをサポートするには、定期的な切り捨ての手順があります。
- ブロックチェインサイズが4 TBサイズに達すると、切り捨てアルゴリズムが有効になります。
- システムは、すべてのゼロ（ダミー）又は1XDR以下のトランザクションをブロックチェーンから条件的に削除します。ブロックチェーンの状態は、解除後の新ジェネシス（起点）ブロックに記録されます。ブロックチェーンの以前の状態は、特別なアーカイブノードにのみ保存されます。アーカイブノードが自発的になります。
- これらのトランケートされたトランザクションからの残量は、トランケーション後にマスターノードに送信されます。
- また、デッド・ノード（長時間応答していないノード）は、ブロックチェーンが切り捨てられたときに資産をウォレットに保存する間に削除されます。
-

4 無料で高速なトランザクション

XDR取引のコミッションは0%、MILE取引のコミッションは0.2%です。 ブロックは20秒で閉じ、帯域幅は1秒あたり最大10,000取引ができます。ブロックチェインの最適化は、ビットコインのようなシステムのUTXOモデルとは異なり、誰も入出力情報を保持しないことによって実行されます。マスターノード作成メカニズムのおかげで、ユーザーの無料なトランザクションベースが可能になります。

5 ブロックチェーン

5.1 選択の説明

MILEアプリケーションの目標は、次のブロックチェーン機能を担当するコンセンサスが必要です。

1. 新しいブロックの総作成時間は20秒です
2. コンセンサス生産に参加できるノードの総数は、10,000～100,000,000まで変化する可能です。
3. 高速トランザクション：1 秒あたり少なくとも10,000取引
4. ブロックチェーンアルゴリズムのパフォーマンスは、PoWブロックチェーンと比較して十分なコンピュータ電力を必要とすべきではありません

sdBFTは、BFTアルゴリズムと比較してより高い演算能力を有するアルゴリズムとして選択された。議決権のあるホストグループが次のコンセンサスの議決権行使ホストとしてブロックコンテンツを管理することによって新しいブロックを形成するので、予備的な固定交渉を複雑にするコンセンサスの潜在的な参加者がたくさんあります。投票ホスト配列の疑似ランダムサンプリングは、次の投票によってホスト選択に大きな影響を与えることはできません。アルゴリズムの説明は個別の記事で提供されています[12]

---

[12] magnet:?xt=urn:btih:c5a3d2762bd1f10c18f51b2606b1a32549d79ed4&dn=Article20concensus20sdBFT. pdf&tr=udp3A2F2Ftracker.leechers-paradise.org 3A6969&tr=udp3A2F2 Ftracker.coppersurfer.tk □ 3A6969

5.2 新しいブロックを形成するためのアルゴリズム

- ある時点で、ユーザーがトランザクションIを作成すると仮定しましょう
- このクライアントがバインドされている最も近いノードにトランザクションが送信されます
- どのノードもパッシブ、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。
- ノードがパッシブの場合、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によってさらに送信します
- 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送信します。
- マスターノードはトランザクションをチェックし、正しい場合はそれをエスコートノードに送信し、トランザクションIもフォーミングブロックに書き込みます
- トランザクションIを受け取ることによって、エスコートノードは真正性をチェックし、それをフォーミングブロックに書き込む。
- この一連の動作は、ブロックが完了するまで繰り返されるが、20秒以上続くことはありません
- その後、マスタノードはブロック完了時にメッセージを送信します。
- 各エスコートノードは、トランザクションのブロックハッシュを計算し、デジタル署名をハッシュし、受信したハッシュをマスターノードに送信する
- マスターノードは、仮定可能な正しいデジタル署名の数を計算する。受け取った正しい署名の数がコンセンサスに参加する総エスコートノード数の2/3を超える場合、ブロックは完了したものとみなされます。それ以外の場合、ブロックは完了しません。
- ブロックチェーンは時間外であり、ブロックに配置されたトランザクションの時間をチェックしたり、合意したりしません。
- ブロックチェインを使い果たしたシステムは、ブロック完了の平均時間（約20秒）に向けられます。

5.3 擬似乱数ジェネレータ

組み込みのオペレーティングシステムである擬似乱数の標準的なジェネレータには、通常、深刻な脆弱性が存在します。それらの中で最も危険なものは次のとおりです。

- 疑似乱数生成のための「シード」の代わりに、「タイムスタンプ」が使用されます。 最終的に、攻撃者が擬似乱数生成と生成時間の推定を知っている場合、同じアルゴリズムを使用して生成された秘密鍵（パスワード）をブルートフォースできる可能性が非常に高いです。
- たとえ「タイムスタンプ」とは別のデータが使用されていても、擬似乱数の標準ジェネレータよりもかなり予測可能なシーケンスが生成され、攻撃者はパスワード（ハッシュデータ）を盗むことができます。

MILEブロックチェーンでは、電子署名の鍵生成から「塩」までの乱数が普遍的に使用されています。 これを念頭において、乱数の品質には特定の要件があります。 乱数ジェネレータではないシーケンスは完全にテストされています。 ジェネレータの作業の結果は次のとおりです。

5.3.1 テストの目的

テストの目的は、生成された乱数列の動的制御の事実を乱数でチェックすることです。 これは、生成された乱数列の安定したカバレッジに関する統計的仮説証明に使用されます。

5.3.2 条件とテスト順序

テストは、疑似乱数のプログラムジェネレータによって生成された乱数のシーケンスチェックから構成されます。制御処理のために、以下のアクションが実行されます。

１．暗号モジュールの生成関数の実装をチェックし、ワークステーションプログラミングからなるランダムシーケンスのテストを行うためのワークベンチがあります。Visual Studio 2017 IDEとMILEアプリケーションがインストールされたワークステーションです。
２．ワークステーションでテスト用にGNUソフトウェアがインストールされています。 これが下記になります：
a）NIST統計テストスイート「NIST Statistical test Suite」 (NIST-STS)；
b）テスト-U01（Test-U01）
３．擬似乱数シーケンスジェネレータの助けを借りて、パフォーマンスとテストの長さの持続時間が自然に制限される条件で最大1024 GB以上の乱数列が生成されます。バイナリファイルStatMessTime（1000バイト分）とStatCurrent（2000バイト分）にランダム変数の設定されたシーケンスをコピーします。
４．主要な統計的基準の実行をチェックするために、前述の統計的テストにおけるパケットの助けを借りて、ランダム変数の選択されたシーケンスについてワークステーション上で分析が実行される。
５．バイナリとして解釈されているランダムシーケンスの品質評価では、間隔を持つバイナリ符号の相対頻度について基準3 s を使用した

$$(0{,}5 - ½\,D\,½ - 1{,}5[1 - 4D2)n - 1]0{,}5{,}0{,}5 + ½\,D\,½ + 1{,}5[1 - 4D2)n - 1]0{,}5$$

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.　次の基準間隔3sを使用した：

	3s 基準間隔:	
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して解釈されるランダムシーケンスの品質を推定するために、基準c2が255自由度で使用された。

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

７．動的テストの検証手順には、以下の専門知識の方法があります。処理、分析、テスト結果の評価です。検証は、使用された統計的基準が、5ページに記載されている分析された乱数列の一様分布についての仮説を拒否しない場合に完了すると推定される。

5.3.3統計調査の結果

StatMessTime処理の結果

第 2 表．1024バイトの16セグメントで1の周波数

4075 4129 4206 4148 4098 4180 4042 4021

4092 4134 4202 4226 4064 4052 4070 4112

第 3 表．1024ビットの16セグメントに1の相対周波数

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．1-512のシフト合計で1の相対頻度

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

16384バイト（255自由度）の値c2：c2 = 268.5

StatCurrentマテリアル処理の結果

第 6 表. 1024バイトの32セグメントの1の周波数

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セグメントの1の相対周波数

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．1-512のシフト合計の相対周波数1

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

第 8 表．1-512のシフト合計の相対周波数1

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バイト時のバイト周波数

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

第 9 表．32768バイト時のバイト周波数

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バイトの値c2（255自由度） $c^2 = 239.8$

5.3.4 結果

MILEブロックチェーンソフトウェア乱数生成器は、主状態の動的変化を伴うハッシュ関数の二重計算に基づいている。擬似ランダムシーケンスの生成器によって生成されるランダムシーケンスの品質は、バイナリ符号で0.5 + Dより悪くない、| D | <0.01であり、分析された乱数列の一様分布の仮説にとって満足できるものである。

5.3.5 暗号化

- 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的な機能

- 手数料ゼロのおかげで小口取引サポート（「コーヒーチップ」）をできます。
- 取引の最大金額には制限がありません。
- 定期的にブロックチェーンを使用すると、自己最適化が行われ、設定された範囲内でボリュームがサポートされます
- 「ジャンク」残高を持つ財布はゼロに縮小され、その内容はブロックチェーントランケーションに参加するノードによって受信されます。

5.3.7 取引タイプ

- XDR送信。
- MILE送信。
- ノード登録に関するアナウンス。
- ノード解雇に関するアナウンス。
- 新しいジェネシスブロック（切り捨て）。
- MILE / XDRレート投票。
- ノード投票の質問送信。
- 任意の代替案に対するノード投票。
- XDRエミッション（排出）

5.3.8 パラメータの管理

- ブロックチェイン切り捨て手順を開始するブロック内の間隔。
- 直前の試行が成功しなかった場合、切り捨て手順を再実行するブロック内の間隔。
- ノードを作成できるデポジットの（入金）範囲。
- ノードの最大数。
- パラメータの管理に関する更新は、ノードの投票

5.3.9 ウォレット

- ウォレットアドレスはBase58checkerMod2文字セットのシンボルシーケンスでブロックチェーン内のトランザクションに記録する。

ウォレットでXDRとMILEの両方を受信して取得できます。

ウォレットの種類：

□ライト：

□ 相互相殺（取引）と残高確認。

□ 必要なブロックを取得し、Merkleツリーのみをチェックすることができるが、ブロックチェーン全体をチェックすることができない特別なプロトコルを使用する

- スタンダード：

* すべてのブロックチェーンを保持します。
* ノードとして登録することができます。

□マルティシグ（Multisig）

* バーチャルウォレットは、複数の署名が利用可能な場合にのみ、トランザクションが受け入れられる場所です

□ポイントウォレット：

＊ 管理パラメータの変更に基づくシステムポイント制御が実行される開発者のウォレット（財布）。
＊ ブロックチェイン作業の最初の年だけが必要です。それからブロックチェーンで電源を切って書きます。

- システムウォレット

＊ このウォレットは、リムーバブルウォレットから手数料を累積してブロックチェーンを切り捨てるためのものです。

＊ ブロックチェーンの切り捨てに参加したノードに手数料を支払うためにのみ、発信トランザクションを形成することができます。

6. ユースケース（使用事例）

このドキュメントは、ほとんどがアルゴリズムそのものに関する技術論文です。そのため、経済的な使用例について簡単に説明します

- SWIFTを使用して問題を抱え、国際決済銀行の一部ではない人のための決済および多国間取引ツール。それは約3億です。 アフリカ諸国[13]、中国、ロシア、トルコ、ベネズエラ、イラン、スーダンなど数多くの国や地域があります[14]。
- 任意のボリュームの無償の高速かつ自由な取引オプション。
- 安定した独立した価値の記憶
- USDを持っていないために貧しい人々のための交換の媒体。天然資源を所有しているか、または実行可能な製品を生産できる場合は、XDRを使用してオフセット会計、決済、カストディアンおよび報告を設定します。

7. 法的枠組み

暗号資産は比較的新しい経済現象であるため、世界中の法律が進行中です。 とにかく、何十もの国がすでに暗号[15]に関するいくつかの規制を導入しています。スイス、日本、アメリカ、カナダ、韓国、ドイツなど多くの裕福で評判の高い国がたくさんあります。

XDRまたはMILEのトークンセール（ICO）がなかったため。 XDRは、分散型ネットワークによって作成されます。 有価証券の属性はありません。
そのため、異なる国の法律によって、XDRは交換の媒体または無形のデジタル資産としての役割を果たすことができます。

---

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