Freeman Family

2019年7月4日

EPIC CASH

エピックプライベートインターネットキャッシュ

ピアツーピア電子現金システム

価値の保存＋交換の媒体＋会計の単位

成人のうち 17億人が金融システムにアクセスできず、加えて 13億の人々は十分なサービスを受けられません。エピックキャッシュは、個人を世界市場につなげることによって、人間の可能性を引き出します。迅速で、事実上自由に使用でき、そして誰にでもオープンなものです。

Version 7.1b Japanese

コンテンツ

I. アブストラクト

エピックキャッシュは、真のP2Pインターネットキャッシュ、個人金融システムの礎となる、いわば旅の最後、集大成とも言えます。エピックキャッシュは、世界で最も効果的なプライバシー保護のためのデジタルマネーを目指しています。その目標を達成するために、お金の3つの主要な機能を満たします。

1. **価値の保存 - 後で保存、検索、交換することができ、予測可能な値です。**
2. **交換の媒体 - 価値基準を表すものとして認められ、商品またはサービスと交換可能なものです。**
3. **会計の 単位 - 物の価値とされ、比較される単位となります。**

	$ USD	BTC	EPIC
価値の保存	✗	✓	✓
交換の媒体	✓	✗	✓
会計の単位	✓	✗	✓

2009年に、Bitcoinが最初のブロックチェーンベースのデジタル通貨として登場しました。それにあたって、以下の3つの軸で暗号資産は評価されます

- **信用不要** – ネットワークが機能するために、あらゆる集中化された事業体または取引相手を信頼することは必要ありません。
- **不変性** – 取引は 元に戻せません。
  a.歴史を書き換えるのは、非常に困難です。
  b.秘密鍵 の所有者以外の誰かが、その秘密鍵 に関連する資金を移動する ことは不可能です。
  c.すべてのトランザクションはブロックチェーンに記録されます。
- **分散化** – 「ブロックチェーンは 政治的に分散化されている（誰もそれらをコントロールすることはできない）し、そしてアーキテクチャとしても分散化されている（インフラストラクチャーの障害ポイントの観点）...」

Bitcoinは、その金融のアーキテクチャの中でファンダメンタルズに固執しながら、技術的に新しい道を切り拓いた。Bitcoinの成功は、信頼が要らず、不変で、分散したブロックチェーンと組み合わせた上で、その限られた供給に強く関係しています。エピックキャッシュは、Epic通貨を効果的な価値のある保管場所として使用するために、インフレを抑え供給を制限するというBitcoinの金融ポリシーをエミュレートします。

Bitcoinの成功にもかかわらず、10年前のローンチ以来、いくつかの欠点が明らかにされてきました。他のプロジェクトはこれらの欠点を克服することを試みてきました。そして、我々は出発点として、これらのうち最良のものを調査しました。私達が苦労して達成した成果を完璧にするため、Grinコードベースと他のいくつかのプロジェクトの素晴らしい仕事を利用して、そしてエピックキャッシュの前回の欠点を発見しました。エピックキャッシュは、理想的な通貨であるための重要な資質を持っています。

- **ファンジビリティ** – 与えられたエピックユニットの価値は常に 1円または元が常に他の円または元と等しく置き換え可能であるように、別のエピック単位に等しいものとします。代替可能性の達成は、大部分がプライバシーにかかっています。
- **プライバシー** – エピックキャッシュブロックチェーンは匿名性を保護します。第三者から取引の詳細を保護することによって、トークン保有者とユーザーは、追跡できず監視にも見えないように設計されています。
- **スケーラビリティ** – エピックキャッシュはスペース効率の良いブロックチェーンを維持しています、リソース集約型の仕組みなし で、新しい ノードを簡単に用意できます。エピックキャッシュブロックチェーンは 、Bitcoinの少なくとも2倍の スループット が可能です 。
- **スピード** – エピックキャッシュの取引はスムーズで継続的です。 以前の世代のブロックチェーンテクノロジよりもはるかに高速に実行されます。Bitcoinは完全なトランザクション確認を達成するために6つのブロック（10分）を必要としますが、Epicトランザクションは1分でブロックが採掘され、1つのブロック確認ですぐに確認できます。

[1] Buterin, Vitalik, *The Meaning of Decentralization*, 6 February, 2017, https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

II. プライバシー

現代のお金の使用は、人々と機関との間の会計単位の集合的な移転として理解することができます。次の質問に答えることで、任意の時点でのお金の状況をマッピングすることができます。

1. 誰がそれを持っていますか、そしてどのくらい持っていますか？
2. 誰が誰と取引していますか？

伝統的なフィアット通貨、そして実際にはBitcoinについても、これらの質問に答えることができます。そうすることで、消費パターン、所有権、取引相手など、人々の生活について多くのことが明らかになります。価値の移転を追跡することによって、個人の興味や意図についてかなり正確な結論を引き出すことができます。プライバシーがないと、取引データは悪意ある第三者の手に渡り、危険な情報となる可能性があります。

過去10年間の暗号資産の使用は、さまざまなブロックチェーンの実装における「プライバシー」の連続性を示しています。プライバシーのスケール範囲は、片方の端ではオープンで悪用されやすいもの、もう一方は匿名です。プライバシーが侵食されるにつれて、暗号資産における信頼性の欠如という1つの重要な基礎が悪化します。Bitcoinブロックチェーン分析サービスの成功によって証明されているように、Bitcoinは、プライバシースペクトラムが悪用されやすい透明な部分に向かっています。ユーザーは、誤って不正なBitcoinで取引しないようにするための対策を講じる必要があります。エピックキャッシュソリューションは、個人のプライバシーと取引のプライバシーの両方が基本的なレベルでシステムに組み込まれるようにすることで、匿名への針を揺り動かし、この重要な特性を復元します。

アイデンティティのプライバシー

取引のプライバシー

アイデンティティのプライバシー

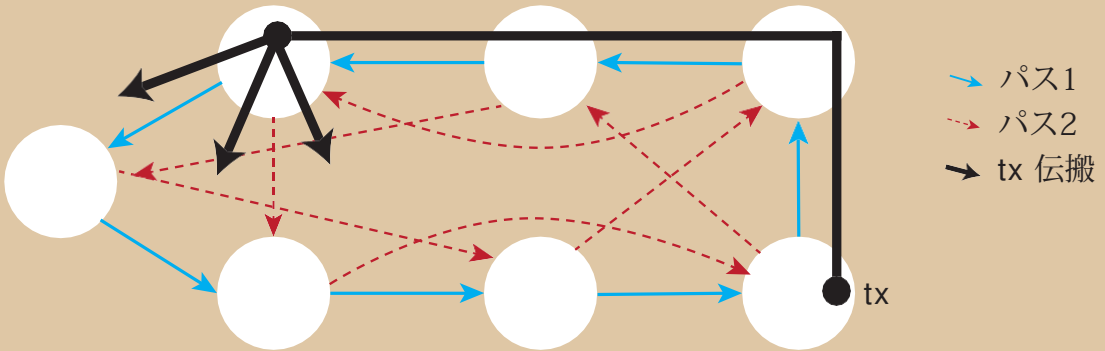
ビットコインのような暗号資産では、アドレスの ウォレットの秘密鍵から派生した公開鍵 でウォレットに格納されています 。これらのアドレスは、デジタルの世界での個人用格納域のロケータとして考えることができます。エピックキャッシュのブロックチェーンは完全にアドレスを排除し、代わりに、すべての公開鍵と秘密鍵が、シングルユースに基づいて生成され、ひとつの多重署名を生成 します 。

Bitcoinウォレットアドレスはデジタルの世界ではボールトのロケータなので、そのウォレットは所有者のインターネットプロトコル（IP）アドレスをたどることができます。これは、特定の時点における所有者を特定の場所にあるコンピュータに固定します。簡単に説明すると、Bitcoinトランザクションが発生すると、そのトランザクションは「ノード」と呼ばれる通信ハブからブロードキャストされ、次に「ピア」と呼ばれる他のノードに伝播されます。その情報は、その後、ネットワーク全体にわたって連続的にそれらのノードのピアのそれぞれに迅速に広がります。このプロセスは「ゴシッププロトコル」と呼ばれています。非常に簡単に言うと、各Bitcoinは目に見えるオンライン上の位置、つまりBitcoinの所有者を見つけることができる物理的な場所を持っています。ジャーナリストのGrace Caffynが述べたように、ビットコインは「家庭のインターネット接続から行うグーグル検索よりも秘密というわけではない」。[2]

ウォレットアドレスを排除することに加えて、エピックキャッシュブロックチェーンは、IPアドレスを追跡できないようにすることで、IDのプライバシーを保護します。これは Dandelion++ プロトコルの 統合を通じて行います。エピックキャッシュの前身において、Dandelion++プロトコルは研究者の継続の結果であり、ブロックチェーンに対する非匿銘化攻撃に対抗するために努力した結果です。Dandelion++ を通じて 、トランザクションがランダムに絡み合ったパス上を通過し、茎から吹き飛ばされた綿毛のように、ノードの大きなネットワークに突然広がります（図1）。これにより、トランザクションをその発信元、つまり発信元IPアドレスを追跡することはほぼ不可能になります。

図1：Dandelion++プロトコルによるトランザクションの匿名化

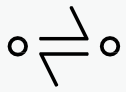
***?Dandelion++** は、4正則グラフ上で絡み合った2つのパスのうちの1つを介してメッセージを転送し、次に拡散を使用してブロードキャストします。図では、トランザクションは青い実線で伝搬します[3]。このプロセスはトランザクションをそれらのソースにトレースバックすることを非常に難しくし、それによってプライバシーを保護します。*



[2] F2Caffyn, Grace, *Chainalysis CEO Denies 'Sybil Attack' on Bitcoin's Network,* 14 March, 2015, https://www.coindesk.com/chainalysis-ceo-denies-launching-sybil-attack-on-bitcoin-network

[3] Fanti, G, Venkatakrishnan, SB, Bakshi, S, Denby, B, Bhargava, S, Miller, A & Viswanath, P 2018, 'Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees', *Proc. ACM Meas. Anal. Comput. Sys.*, Vol. 2, Article 29, pg. 8, https://www.readkong.com/page/dandelion-lightweight-cryptocurrency-networking-with4805755-?p=1

取引のプライバシー



エピックキャッシュブロックチェーンは、取引の金額と送信者と受信者の関係を不明瞭にすることで、取引のプライバシーを保護します。これは、機密取引（CT）4 と CoinJoin 5 といったお馴染みのアイデアを適用することによって達成され 、大部分の方法はGregory Maxwell 、（ビットコインコア開発者、Blockstream共同創設者兼CTO）によって開発されました。

CTは 、元々は Adam Back、そして 後にマクスウェルによって洗練されました。これは準同型暗号を通じて小さく取引を分割することで暗号化し 、暗号化計算を実行する方法として、プライバシーを保護するため、復号する必要なしに情報を保護します。分割後は 観察者は実際の取引金額を見ることができません。ブラインディングファクター のため、それらの断片的な値を隠すために、トランザクション・フラグメントのミックスに乱数を投げます。最終的には、取引の当事者だけが交換された価値を知っています。取引は、出力値の合計が入力値の合計と等しく、出力ブラインドファクタの合計が入力の総合計と等しいことを確認することによって検証されます。 詮索をさらに複雑にするために、すべてのエピックキャッシュ取引は CT で 隠されて 、それから取引当事者間の関係を隠すために一緒に混合されます。これはマクスウェルの2番目のコンセプトを通して行われ 、CoinJoin されます。

A、B及びCが送信していることを想像し、簡略化し CoinJoinを 説明するために それぞれX、Y、Zに Epic を送るとします。CoinJoin 媒体 を通して送られるとして、わかっているのは、A、B、Cが送信中で、X、Y、Zが受信中で、取引金額は見えないままであるということだけです。CoinJoin システム は、一方向性集約署名 (OWAS), を通じ、エピックキャッシュの基本として、単一ブロック内にすべてのトランザクションを組み合わせる（OWAS）トランザクションを生成します。

プライバシー：まとめ

エピックキャッシュブロックチェーンは、以下によって個人とその取引のプライバシーを保護します。

- **ウォレットアドレスの削除 - ブロックチェーン内にデジタルポールトの位置識別子はありません。トランザクションは、ウォレット-ウォレットベースで直接の個人間で作成されます。**
- **Dandelion++プロトコル - デジタル経路が不明瞭になる。トランザクション送信者のIPアドレス、トランザクションなどが対象。**
- **機密トランザクション - トランザクションを複数に分割し、 断片の値および他のトランザクションパラメータを知ることができないように、断片を収集し、それらの断片のコレクションにブラインドファクタを導入する。**
- **CoinJoin - 取引当事者間の関係、トランザクションをバンドルにまとめます。**

[4] Maxwell, Gregory, ***Confidential Transactions,*** Technical Report (2015), https://people.xiph.org/~greg/confidential_values.txt

[5] Maxwell, Gregory, ***CoinJoin: Bitcoin Privacy for the Real World***, 22 August, 2013, post on Bitcoin Forum, https://bitcointalk.org/index.php?topic=279249.0

III.ファンジビリティ

Charlie Lee 、ライトコインの作成者は、代替性が不足しているため、健全なお金が唯一の財産であると述べました 。BitcoinとLitecoinは、プライバシーと代替性がこれらのコインの次の戦場であることを認めました[6]。Andreas Antonopoulos は世界有数のブロックチェーン専門家の一人であり、次のように述べています。「コインは破壊可能です。もし あなたが代替性とプライバシーを破った場合、それは通貨を破壊したということです。」[7]

ファンジビリティは、そのセットの個々の単位が同等の価値を持ち、交換可能であることを保証する一連の商品または資産の特性です。それは、最も初期の形の通貨と、それまでの物々交換のシステムとを区別するものです。お金の代替性に強みが無い場合、そのお金は急速にその有用性を失います。以下に説明するように、ほとんどの暗号資産の代替可能性は不確かですが、エピックキャッシュのプライバシーアーキテクチャはそれが同じ脅威に対し不透過であることを保証します。

Bitcoinに似たほとんどの暗号資産は、透明なブロックチェーンの性質により、それらが保管されていたすべてのウォレットを通して検証可能で追跡できます。民間の第三者や政府も同様で、以前の活動で使用されたコインを迅速に識別するため、ますます洗練された手段でBitcoinブロックチェーンを監視しています。これは当然のことながら、汚染された硬貨がいつの日か取引から禁止され、その後の誠実な保有者が損失を被る可能性という懸念につながります。
2018年3月19日に、米国外貨管理局（ OFAC ）は 、米国の個人または企業が取引を禁止されている団体である特別指定国民（ SDN ）のリストにデジタル通貨アドレスを含めることを検討していると発表しました。

さらに厄介なことに、OFACはアドレスを含める可能性を除外していません。
現在、汚染されたコインをSDNリストに載せています。これにより、ニューヨーク大学の法定教授、Andrew Hinkesは、「代替性にさよならのキスを」という内容を発表し、国民は「新たに刻まれた硬貨にプレミアムを払う、またはきれいな硬貨だけを扱えるよう」期待すべきであると語った[8]。

これらの動向を念頭に置いて、暗号市場の混乱と多くの確立された暗号資産の苦しみ、あるいは絶滅さえも想像するのは難しくありません。ただし、Epicは、このホワイトペーパーで前述した強力なプライバシー機能により、この問題を完全に回避できる数少ない暗号資産の1つです。アイデンティティと所有権、そして取引当事者間の関係の間のリンクを取り除くことによって、人または活動に決して所属することはありません。そのため、Epicの価値はユーザーから独立したままであり、刑事、金融、または政治の分野で悪意のある行為者が容易に操作することができない高度なプライバシーとセキュリティを提供します。

> **“…コインは破壊可能です。もしあなたが信頼性とプライバシーを破ったら、それは通貨を破壊したということです。”**
>
> **ANDREAS ANTONOPOULOS**

[6] Njui, John P, ***Charlie Lee: Litecoin (LTC) To Soon Have Confidential Transactions for Fungibility***, 29 January, 2019, https://ethereumworldnews.com/charlie-lee-litecoin-ltc-to-soon-have-confidential-transactions-for-fungibility/

[7] Carl T, ***Andreas Antonopoulos Says If Fungibility Is Not Fixed Bitcoin Could Be Attacked,*** 9 April, 2019, https://bitcoinexchangeguide.com/andreas-antonopoulos-says-if-fungibility-is-not-fixed-bitcoin-could-be-attacked/

[8] Hinkes, Andrew, Ciccolo, Joe, ***OFAC's Crypto Blacklist Could Change Crypto***, 24 March, 2018, https://www.coindesk.com/goodbye-fungibility-ofacs-bitcoin-blacklist-remake-crypto

IV. スケーラビリティ

エピックキャッシュは 冗長なトランザクションデータを投げかけ、スペース効率的な設計の結果として、拡張性の進歩をもたらす MimbleWimble ブロックチェーン実装 です 。カットスルー 機能 はブロックチェーンに関して、ビットコインを含むほとんどの暗号資産とは異なり、時間をかけてより多くのスペースを効率的に使い成長することを保証し、その新しいノードがメモリ内の最小限の投資とコンピューティングパワーを使用して作成することができます。スペース効率を維持することで、広く分散したネットワークをキャパシティ化し、分散化を促進します。さらに、各Bitcoinノードはチェーン全体を格納する必要がありますが、エピックキャッシュノードは小さなブロックのサブセットに基づいてネットワークセキュリティに貢献することができます。

ほとんどの暗号資産では、すべてのトランザクションデータをブロックチェーンに無期限に保存する必要があります。現在、Bitcoinチェーンは毎日0.1353 GBだけメモリが増え続けていますが、Ethereumのチェーンは1日0.2719 GBというさらに速い速度で増加し続けています。ビットコインのチェーンが現在の速度で成長し続ける場合、2140年に最後の報酬ブロックが採掘されるまでに、最終的にサイズは約6 TBに達するでしょう。そして、その日までにEthereumは10TBを超えるでしょう [9]。MimbleWimbleのないほとんどのブロックチェーンでは、トランザクションは世界中のノードによって検証されなければなりません。データが増えるにつれて、各ノードの負担も増えます。たった200 GB（現在のBitcoinチェーンのおおよそのサイズ）であっても、データを同期させるには安定したネットワークと高速なディスク読み書き能力が必要です。

その結果、マイニングは、高価なコンピューティングリソースを活用する大規模プール間でますます集中化されてきました。ブロックチェーン全体としての Bitcoinの歴史が、代わりにエピックキャッシュブロックチェーンに保存されることになった場合、90%少ないスペースに収まるでしょう。小さいほど速いので、各トランザクションは送信と保護にかかる時間が短くて済みます。

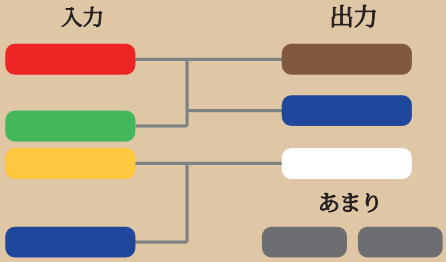
MimbleWimbleは、「カットスルー」と呼ばれる革新的なブロック剪定方法を使用して、このストレージのジレンマを解決します。カットスルーがどのように機能するのかを理解するためには、最初にトランザクションとブロックがMimbleWimbleブロックチェーン内でどのように構成されているかを調べるのが最善です。

インプット:
古い出力への参照

アウトプット:
機密取引の 出力と範囲補償

あまり:
出力と入力の間の違い、それと 署名（認証とインフレの非証明）

図 2:
MimbleWimbleトランザクションパーツ



[9] Li, Crypto, *Blockchain's Big Data Problem*, 27 January, 2019, https://www.longhash.com/news/blockchains-big-data-problem

すべてのエピックキャッシュブロックには以下が含まれます。

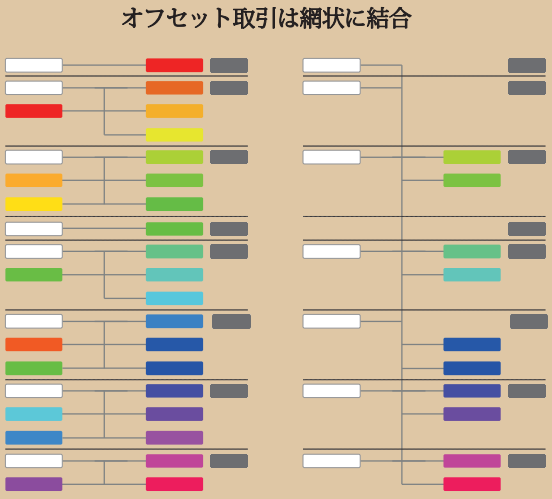
Andrew Poelstraのプレゼンテーション 10 から引用した図2と図3では、新しく入力されたEpicが白い入力セルとして表示されています。同じ色のセルは、対応する使用済み入力を含む出力を表します。カットスループロセスでは、入力とそれに対応する使用済み出力が削除され、ブロック内のスペースが解放されます。これにより、ブロックチェーンに格納する必要があるデータ量が削減されます。トランザクションが元帳から除外されている間、残りの余分なカーネル（わずか100バイト）は、トランザクションを永続的に文書化します。

ブロックが作成され続けると、MimbleWimbleはブロック全体にカットスルーを適用するので、長期的に見ればブロックヘッダー（約250バイト）、未使用のトランザクション、およびトランザクションカーネル（約100バイト）だけが残ります。2回目のMimbleWimbleの実装であるGrinは、Bitcoinチェーンと同数のトランザクションを持つMimbleWimbleチェーンがBitcoinのチェーンのサイズの10%近くになることを示しました 11 。さらに、ノードのサイズは「Bitcoinサイズのチェーンでは数GB程度であり、潜在的には数百メガバイトに最適化可能」です。[12]

これは、ブロックチェーン全体を各ノードに格納する必要があるBitcoinとは著しく対照的です。時間の経過とともに、エピックキャッシュブロックチェーンのスペース効率がBitcoinブロックチェーンに比べて大きくなるにつれて、ノードの参加に関連するコスト効率も高くなります。参加障壁を低くすることは、ネットワーク設計のノード層における大切な回復力の確保に役立ちます。

MimbleWimbleの実装とカットスループロセスによるチェーンプルーニングの適用により、エピックキャッシュブロックチェーンは、暗号資産業界では見過ごされがちな方法でスケーラビリティを提供します。それがBitcoinと志を同じくするというプロジェクトの本質を捉えたものです。1秒間にコインで処理できるトランザクションの数にかかわらず、広範で多様なネットワークで処理できない場合はどうなるでしょうか。メモリの要件が、検証のために最終的に強力なマイニングコングロマリットに引き寄せられるようなものである場合、分散型エコシステムを作成するための暗号資産コミュニティの取り組みはすべて不要になります。追加のスループットを提供するために、Lightningスタイルのレイヤ2実装は、エピックキャッシュ開発ロードマップの短期的な目標として計画されています。

図 3:
MimbleWimble
前後のトランザクションとカットスルー



[10] SFBitcoin Developers, *MimbleWimble with Andrew Poelstra,* 24 November, 2016, https://www.youtube.com/watch?v=aHTRIbCaUyM&t=940s

[11] Grin Forum, *Grin Blockchain Size,* December, 2018, https://www.grin-forum.org/t/grin-blockchain-size/1334

[12] GandalfThePink, *Introduction to Mimblewimble and Grin,* 28 March, 2019, https://github.com/mimblewimble/grin/blob/master/doc/intro.md

V.金融政策

エピックキャッシュとBitcoinの金融政策はよく似ています。エピックキャッシュの 循環供給 は最初に急速に拡大し、次に2028年にBitcoinの循環供給と同期します。その後、最大供給量 に達するまで減少率が増加します。2140年で2100万エピックとなります。エピックキャッシュには、長期的な価値のある安全な保存先になるための資質があります。 循環供給は、その 排出ライフサイクルに 沿った任意の時点でわかっていて、一定の最大供給に達します。エピックキャッシュの金融政策は、次の4つを特徴としています。

- 最初の9年間にわたる急速な放出、その間に20,343,750エピック（総供給の96.875%）が採掘されることになっています。正確な排出量はドキュメントで 概説されている 排出スケジュールの通りです。
- Epicの循環供給および放出率 は、2028年5月24日頃に Epic の特異点 でビットコインと同期し ます。特異点に従って、排出量の増加率は減少し、循環供給量は減少率が増加します。
- 2140年には、最大2100万エピックの供給量に達する予定です。これは、ビットコインが最大2100万ユニットの供給量に達するのとほぼ同時です。
- Epicは8進数の除数アーキテクチャを持ちます。1Epicは100,000,000のフリーマンに相当します（1 Bitcoinが100,000,000のサトシに相当します）。

エピックキャッシュの金融政策は、以下の理由からBitcoinをモデルにしています。

- Bitcoinの経済的な基礎との一致、すなわち循環供給の不足と予測可能性、価値の強い保存が根底にあるということ。
- 一般の人々は、Bitcoinのモデルとその誕生以来の過去10年間の実績をすでに知っています。Bitcoinの循環供給とほぼ同期させ、Bitcoinの最大供給と分割可能性アーキテクチャを反映させることで、Epicは大量採用への抵抗を最小にする道をたどります。

VI. 排出スケジュール

エピックキャッシュは、33の時代、ブロック報酬の減少によって定義されたそれぞれの合計を有します 。Epicジェネシス、エピックブロック#1の採掘日は、2019年8月　に行われます。ブロックは毎分1回採掘されます。 最初の5つの時代はエピックの最大供給量の97%近くを生産し、約9年間で20年間分のビットコイン排出量に相当します。これは、Bitcoinの目覚ましい上昇を見逃した人々にとっては、「時計を戻す」チャンスと考えることができます。

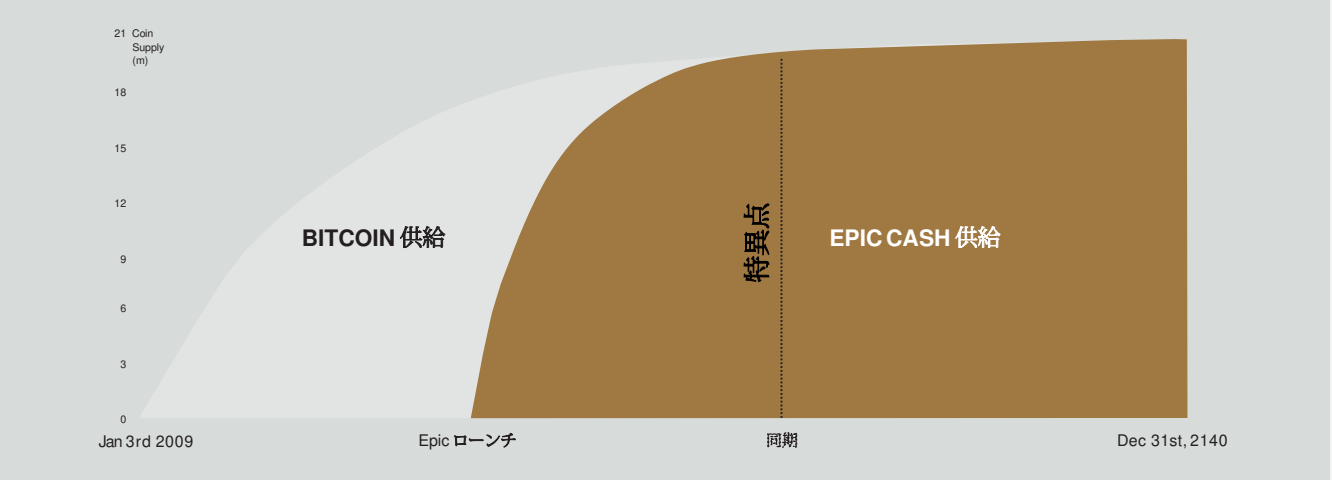
表1の排出スケジュールは、最初の7回の時代の開始日と終了日、それらに対応するブロック報酬、および各時代の次の循環供給の概要を示しています。簡潔にするために、8から33の時代は表に含まれていません。以降の各時代が、まさにBitcoinのように、前の時代の報酬の半分の量でブロック報酬を設定されるということが理解できていれば、十分でしょう。これらの各時代の間に発行されるエピックの量は、4年間のブロック報酬の合計になります（およそ1460日）。

Epic Singularity（2028）では、Epic循環供給量はBitcoinの循環供給量の数と交差します。その時点で、エピックキャッシュは 4年ごとに半分ずつ減少する Bitcoinブロック報酬および 半減 パターンを 採用し ます。唯一の例外は、Epicブロックが毎分1回の割合でマイニングされ続けるのに対して、Bitcoinの10分ごとの1ブロック、という割合である。これを行うことによって、エピックの循環供給は残りの間、ビットコインの循環供給とおおよその同等性を維持します。

表1：最初の7回の採掘時代の排出スケジュール日付は近似値です。

Era	1	2	3	4	5	特異点	6	7
ブロック報酬	16	8	4	2	1		0.15625	0.078125
開始日	Aug 1, 2019	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025		May 24, 2028	May 22, 2032
終了日	Jun 29, 2020	Oct 11, 2021	Jun 3, 2023	Aug 10, 2025	May 24, 2028		May 22, 2032	May 20, 2036
期間の日数	334	470	601	800	1019		1460	1460
開始供給	0	7,695,360	13,109,760	16,571,520	18,875,520		20,342,880	20,671,380
終了供給	7,695,360	13,109,760	16,571,520	18,875,520	20,342,880		20,671,380	20,835,630
最大供給に対する割合	36.6%	62.4%	78.9%	89.9%	96.9%		98.4%	99.2%

図4：EpicとBitcoinの排出スケジュール



VII. マイニング

エピックキャッシュブロックチェーンは、多種多様な計算ハードウェアを歓迎することによって分散化を追求していきます。Epicマイニングは 、RandomX、ProgPow、およびCuckATоo31 +の 3つの ハッシュアルゴリズム を使用して 、最初は CPU、GPU や ASIC で使用 できます 。チェーンの整合性を損なうことなく、アルゴリズムを簡単にホットスワップすることができます。 ハッシュアルゴリズム: RandomX、 ProgPow、CuckATоo31+

1 RandomX と CPU

RandomXは、 汎用CPUのために最適化された プルーフ オブワーク (POW)アルゴリズム です 。ランダムなプログラム実行を使用します。次の目標を達成するため 、いくつかの メモリハード 技術を用います:

- シングルチップASICの開発防止
- 汎用CPUよりも特殊なハードウェアの効率上の利点を最小限に抑えます。

CPUを使用してEpicをマイニングするには、マイニングスレッドあたり 2 GBの物理 RAM 、16 KBのL1 キャッシュ 、256 KBのL2キャッシュ、および2 MBのL3キャッシュを 連続して割り当てる必要があり ます [13] 。Windows 10デバイスには8 GB以上のRAMが必要です。それほど遠くない将来の携帯電話が、実行可能なマイニングノードになる可能性があることは考えられません。エピックキャッシュマイニングネットワークへの早期のCPU統合は、エピックキャッシュネットワークのセキュリティを保護することでブロック報酬を得るための 、ごく控えめなコンピューティング手段しかない多くの人にとって素晴らしい機会です。

2 ProgPow と GPU

プログラムによる作業証明書(ProgPow)は、メモリ帯域幅とランダム化された数学シーケンスのコア計算に依存するアルゴリズムで、GPUの多くの計算機能を利用してハードウェアの総エネルギーコストを効率的に取得します。ProgPowはコモディティGPUを最大限に活用するように特別に設計されているため、特殊なハードウェアを使用して大幅に高い効率を達成することは困難であり、かつ高価です。そのため、Bitcoinの SHA-256 など、他の多くのPoWアルゴリズムでよく見られるように、ProgPowアルゴリズムは、大規模なASICプールがGPUを上回るというインセンティブを緩和します 。GPUは、CPUほど普及していませんが、まだ一般的に利用可能です。NvidiaとAMDの大手によって推進される技術開発により、GPUはCPUを超える単位で、多数のマイニングソリューションを並列処理することができます。表2に示すように、GPUが初期の時代にマイニング活動の大部分にバックボーンを提供するのは、ユビキタスと高い処理能力のこの組み合わせによるものです。

3 CuckATоo31+ と ASIC

CuckATоo31+は、オランダのコンピュータ科学者John Trompによって開発された、Cuckoo CycleアルゴリズムのASICにやさしい順列計算です。ASIC耐性の相対 CuckARoo29は 、CuckATоo31 +は、ランダム 二部グラフを 生成 し、所定の長さのループを見つけるタスクをマイナーに提示し、「N」はグラフの頂点を通過します。

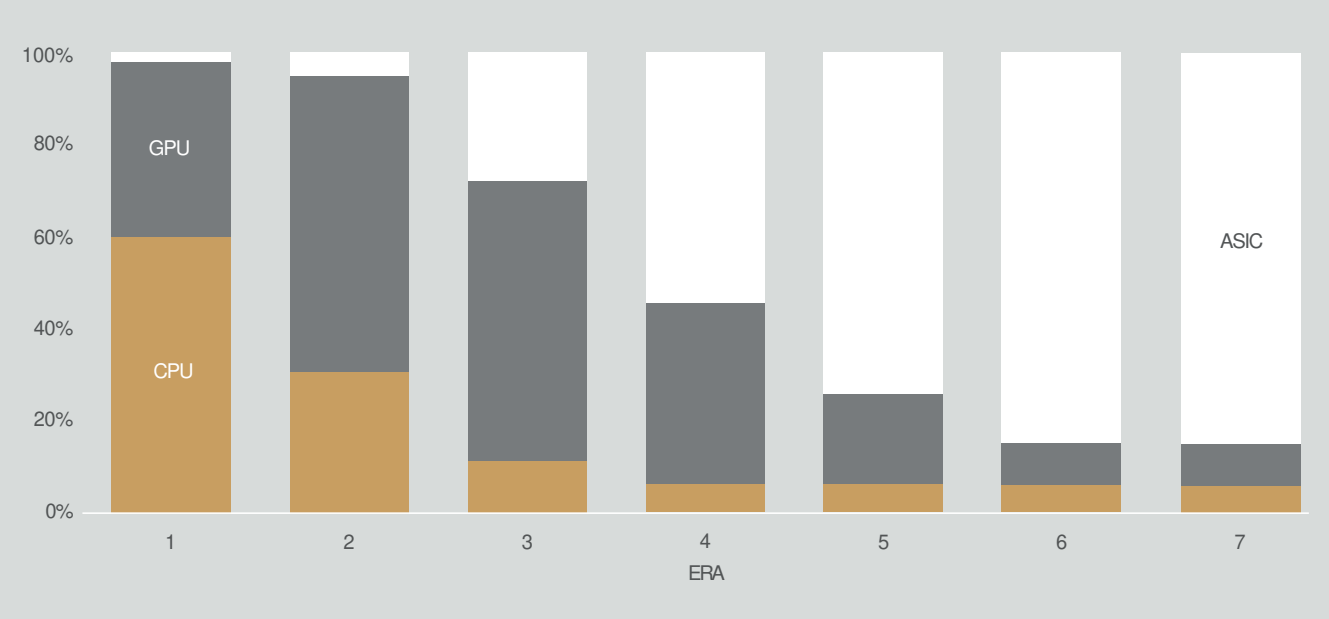
[13] Tevador, *RandomX*, 28 March, 2019, https://github.com/tevador/RandomX

これはメモリに縛られたタスクです。つまり、解決時間は、ロープロセッサやGPUの速度ではなく、メモリ帯域幅によって制限されます。結果として、Cuckoo サイクルアルゴリズムは、従来のPoWアルゴリズムよりも少ない熱を、著しく少ないエネルギーを消費するだけです。ASICフレンドリーCuckATOO31 +は、メモリ I / O 14 がボトルネックのまま SRAM の数百MBを使用して、GPUを超える効率を改善することができます 。最終的には、ASICは3つの採掘オプションの中で最大の潜在的規模の経済を提供します。包含性の観点から、初期段階ではCPUやGPUと比較してマイニング報酬のほんの一部しか割り当てられていませんが、最終的にはASICがマイニングブロック報酬の大部分を占めることになります。

表2：マイニング報酬の割り当ての対象となります。割り当ては最大限の分散化を達成し、ネットワークの長期的利益と一致するように向けられるでしょう。

時代	1	2	3	4	5	6	7
日	334	470	601	800	1019	1460	1460
CPU	60%	30%	10%	5%	5%	5%	5%
GPU	38%	65%	62%	40%	20%	10%	10%
ASIC	2%	5%	28%	55%	75%	85%	85%

図5：表2に従って各時代の報酬配分をマイニングしていきます。



[14] Le Sceller, Quentin, *An Introduction to Grin Proof-of-Work*, 16 November, 2018, https://blog.blockcypher.com/an-introduction-to-grin-proof-of-work-103aaa9f66ce

4 マイニング貢献

Epic Genesis（2019）から始まってEpic Singularity（2028）で終わると、マイニングプロセス中に、EPIC ブロックチェーン Foundationへのマイニングの貢献としてリダイレクトされるEpicの割り当てがあります。

EPIC ブロックチェーン Foundationは、マーケティング活動を創出し、金融テクノロジー業界内でパートナーシップを築くことにより、創業の初期の頃に技術開発とエピックキャッシュプロジェクトの認識と実用性の促進に尽力しています。

特異点の後、EPIC財団の役割は、ハンドオーバ前に財団によって開発されるEPIC分散自治公社（EDAC）によって引き継がれます。
EPIC ブロックチェーン Foundationは、ブロック報酬から差し引かれた、以下の年率によるマイニング報酬の割合によって資金を供給されています。

表3：財団へのマイニングの貢献に対する年間の割合。マイナーの報酬に対する割合。

年	2019	2020	2021	2022	2023	2024	2025	2026	2027	2028
マイニング報酬の率	8.88 %	7.77 %	6.66 %	5.55 %	4.44 %	3.33 %	2.22 %	1.11 %	1.11 %	0 %

VIII. まとめ

Epicは、「分散デジタルシルバー」として認識されることを目的としています。これは、Bitcoinが分散デジタルゴールドとして認識されているポジションの代替手段です。代替性の観点から、はるかにエネルギー効率がよく、環境に優しいハードウェアバックボーンを再導入することによって、エピックキャッシュは最近の集中化傾向とは著しく対照的に、個々のユーザーに有利になるようにパワーのバランスを取り戻します。Bitcoinの経済学、ゲーム理論、および実績のある作業証明と最新のブロックチェーンテクノロジの組み合わせにより、スケーラブルで代替可能で信頼性の高い、信頼の要らない不変の分散通貨（Epic）が得られます。エピックキャッシュブロックチェーンは、オープン、パブリック、ボーダレス、そして検閲に強いです。それはユーザーのプライバシーと富を保護し、マイニングによってネットワークをサポートするために彼らのハードウェアを展開する人々に報酬を与えます。すべてのEpicは仕事の証明を通してマイニングされます。供給はゼロから始まり、機能的なテストネットが現在 実行されている状態で、ネットワークは公平に立ち上げられ ます。

エピックキャッシュのキーとなる事実:

- **マイニングは2019年8月 に始まります。**
- **エピックキャッシュブロックチェーンはMimbleWimbleに基づいています。**

  プロトコルの機能を定義すると、次のとおりです。:

  1. **カットスルー -** スペース効率を促進するためにブロックチェーンから余分な情報を削除する。 ネットワーク検証への大規模な参加、およびスチュワード分散化などを促進。
  2. **CoinJoin -** Epic暗号資産の代替性を保証するためのブロック内のトランザクションのバンドル。
  3. **Dandelion++ プロトコル -** 絡み合ったチャンネルを越えて通信し、拡散することによるトランザクションの伝播。トランザクションとそれらの起源との間の接続を切断して、広範囲のノードネットワークにわたる。
  4. **ウォレットアドレスなし -** 取引当事者のための使い捨ての秘密鍵を生成するための多重署名の使用。 ウォレットアドレスの必要性を完全に排除します。

- **エピックキャッシュの金融政策** は、およそ9年で、Epicの循環供給をBitcoinの循環供給と同期させるように設計されています。2140年には、Bitcoinと同時に2100万台の同じ最大供給量に達する。この漸減するインフレ政策は、透明性、供給の予測可能性、および不足を保証し、長期的な価値の保存に関するセキュリティを促進します。

- 対応するRandomX、ProgPow、およびCuckATOO31 +アルゴリズムを介したCPU、GPU、およびASICを組み込んだ **マイニング**で、大量採用とネットワーク効果を促進する。

IX.技術仕様

プロジェクト名: EpicCash

通貨名: Epic

ブロック時間: 60 秒

ブロックサイズ: 1 MB

開始時の供給: 0

最終供給: 21,000,000

ジェネシスブロック2019年8月

コンセンサス: RandomX (CPUs), ProgPow (GPUs) および CuckAToo31+ (ASICs)

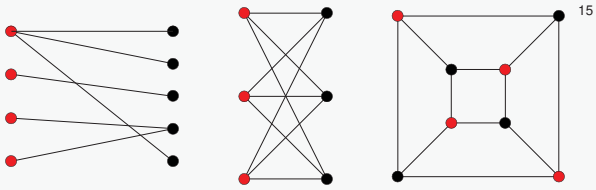
リンク:

www.epic.tech

t.me/EpicCash – Telegram

t.me/EpicCashJapanese

X. 用語集

ASIC	特定用途向け集積回路。単一目的のために設計されたチップ。
二部グラフ	二 個のグラフ頂点があるとき、二個の互いに素な集合に分解され、同じセット内では隣接した二個のグラフ頂点がないようにする  [15]
ブラインディングファクター	暗号化を容易にするためにデジタルメッセージに導入されるランダム要素。その特定の取引における入力および出力、ならびに取引当事者の公開鍵および秘密鍵を暗号化する2つの当事者間の共有秘密鍵
ブロック報酬	新しいブロック内のトランザクションを検証するために実行された計算に対する見返りとして、ネットワークによって配布された新しいエピック。
キャッシュ	データを格納するハードウェアまたはソフトウェアコンポーネント。これにより、そのデータに対する将来の要求に迅速に対応できるようになります。
循環供給	指定された時点で存在するエピックの量
CPU	中央処理装置：コンピュータの他のハードウェアおよびソフトウェアからのコマンドの大部分を解釈して実行する責任を負うコンピュータコンポーネント。
カットスルー	MimbleWimbleブロックチェーンプロセス。入力と一致する使用済み出力を削除してブロック内のスペースを解放し、ブロックチェーンに格納する必要があるデータ量を削減します。
分散化	ネットワークの運用とガバナンスの分散の状態
排出	マイナーがブロック報酬で獲得した新しいエピックの作成。トランザクションがブロックチェーンに確定されると、60秒ごとにEpicが作成されます。
特異点	Epicの循環供給がBitcoinの循環供給と同期する時点（2028年5月）。
あまり(MimbleWimble)	アウトプットとインプットの違い、署名（認証用と非インフレーション証明用）。
ファンジビリティ	個々の単位が本質的に交換可能であり、その各部分が他の部分と区別がつかないという商品または資産の特性
ジェネシス(イベント)	最初のエピックブロックのマイニングとブロックチェーンの正式な開始。
GPU	グラフィック処理装置：表示機能に特化したプログラマブルロジックチップ（プロセッサ）を含む装置。消費者向けGPUは、暗号資産マイニングに最適です。
半減期 (Bitcoin)	4年ごとに発生します。供給率は各イベントの後に50%減少します。.
ハッシュ	ハッシュ関数を使用して基本入力数から計算された値。
ハッシュ関数	任意のサイズのデータを、デジタル署名、メッセージ認証コード（MAC）、およびその他の形式の認証の生成と検証に使用される固定サイズのハッシュにマッピングする数学的アルゴリズム。
準同型暗号	暗号化された情報を最初に復号化せずに計算を実行する方法。
不変性	(不変性プログラミングにおいて)オブジェクトが作成後に変更できない状態。
入力 (MimbleWimble)	送信側を表すMimbleWimbleトランザクションのコンポーネント（Input（MimbleWimble））トランザクション;前のトランザクションの出力から作成されます。
I/O	入出力、コンピュータなどの情報処理システムと、外界、人間または他の情報処理システムとの間の通信。

[15] http://mathworld.wolfram.com/BipartiteGraph.html

[16] Macdonald, Andrew, *Grin Coin and MimbleWimble: An Introductory Guide*, 18 October, 2018, https://cryptobriefing.com/grin-coin-mimblewimble-introduction/

最大供給	循環供給、これ以上増加しないエピックの量(21,000,000 Epic).
メモリーハード	並列接続を試みる同時接続を排除するための大量のRAMの使用において、メモリハード関数は、主にメモリによって決定される計算時間を持つアルゴリズムです。データを保持するための利用可能なメモリに関してメモリバインド関数とも呼ばれます。
マークルツリー	コンピュータサイエンスアプリケーションで使用されるデータアーキテクチャ。ブロックチェーンでは、マークルツリーが大規模データアーキテクチャの効率的で安全な検証方法です。
MimbleWimble	プロトコルの一種。Bitcoin開発者チャットルームで匿名の寄稿者によって提案され、モニカのTom Elvis Jedusorによって実装された。
多重署名	ユーザーのグループが単一の文書に署名することを可能にするデジタル署名方式。通常、マルチ署名アルゴリズムは、すべてのユーザーからの個別の署名の組み合わせよりもコンパクトなジョイント署名を生成します。
ノード	ピアツーピアで、トランザクションおよびブロックに関する情報を配布するブロックチェーンネットワークに接続し、その中の他のノードに分岐するコンピュータ
一方向集約署名(OWAS)	暗号化されている多くの署名から成るトランザクション署名。集約された一部である個々の署名を計算することは非常に困難です。
出力 (MimbleWimble)	トランザクションの受領を表すMimbleWimbleトランザクションのコンポーネント。後続のトランザクションの入力として使用されます。
Pedersenコミットメントスキーム	証明者が値を公開したりコミットを取り消したりすることなしに、選択された値にコミットすることを可能にする暗号プリミティブ。
秘密鍵	秘密鍵は、テキストの暗号および復号アルゴリズムを設定するための公開鍵と対になっている小さなコードです。非対称暗号化中の公開鍵暗号化の一部として作成されます。メッセージを復号化して読み取り可能な形式に変換するために使用されます。
プルーフオブワーク (PoW)	作成するのが難しい(費用と時間がかかる)が、検証、および特定の要件を満たすことが簡単なもの。仕事の証明は、暗号資産ブロック生成によく使われます
公開鍵	公開鍵は、非対称鍵暗号化アルゴリズムを使用する公開鍵暗号化暗号方式で作成されます。公開鍵はメッセージを判読できないフォーマットにします。
RAM (ランダムアクセスメモリ)	オペレーティングシステム(OS)が存在するコンピューティングデバイス内の高速アクセスデータストレージチップ。現在使用されているアプリケーションプログラムとデータはデバイスのプロセッサを通じて保存される。
レンジプルーフ	トランザクション入力の合計が大きいことを検証するコミットメント検証。トランザクション出力の合計よりも大きく、すべてのトランザクション値が正となる。レンジプルーフは、通貨供給が改ざんされていないことを保証します。
デジタル署名	ブロックチェーンプロトコルの標準部分。主にトランザクションとブロックの保護、取引、情報の譲渡、契約管理、その他の場合に使用されます。外部からの改ざんを検出して防止することは重要です。それらはブロックチェーンへの情報の格納と転送において、3つの利点を提供します ・送信されているデータが改ざんされているかどうかを明らかにします。 ・取引への特定の当事者の参加を確認する。 ・法的拘束力を持つことができます。
SRAM (スタティックランダムアクセスメモリ)	電力が供給されている限り、メモリ内にデータビットを保持するランダムアクセスメモリ(RAM)
スループット	指定された暗号資産のプロトコルで実行できる1秒当たりのトランザクション数
信頼不要(トラストレス)	暗号資産ネットワークにおいて中央集権的な組織が不在であっても動作するプロトコル。

[17] Bellare, Mihir, Neven, Gregory, 2007, *Identity-based Multi-signatures from RSA*, Lecture Notes in Computer Science vol. 4377, https://link.springer.com/chapter/10.1007%2F11967668_10

EPIC CASH

エピックプライベートインターネット
キャッシュ