



ハイブリッド コンセンサス アルゴリズムを使用した最初の汎用暗号通貨、 ダイナミック Zerocoin プルーフ・オブ・ステーク、 プルーフ・オブ・トランザクションと 期間ベースの報酬の燃焼のためのマスターノード投票

## ホワイトペーパー V1.11

Maik Broemme<sup>1</sup>, 2019 霜月



## 目次

事業計画概要 .....	3
はじめに .....	3
Galileel コイン .....	3
問題とソリューション .....	4
動的 Zerocoin プルーフ・オブ・ステーク (dzPoS) .....	4
プルーフ・オブ・トランザクション (ghPoT) .....	6
ハイブリッド プルーフ・オブ・ステーク (ghPoS) .....	7
定期預金 (gTD) .....	9
マネーサプライコントロール (gMSC) .....	10
マスターノードでインスタント (gIOMN) .....	12
機能と仕様 .....	14
競合製品分析 .....	18
開発ロードマップ (行程表) .....	20
ヘルプ .....	22
重要なリンク .....	23
付録 .....	24



## 事業計画概要

フィアットマネーはすでに何百年もの間経済標準を定義し証明してきましたが、デジタルマネーの状況は異なります。デジタルマネーは、予測不可能な価値と孤立したブロックチェーンを残す開発チームの消滅を伴う高リスクの投資です。政府はこの問題を特定し、ICO（Initial Coin Offering）規制により今後数年間でそれを解決する予定です。さらに、独自のブロックチェーン機能を実装するデジタルマネーは、デジタルマネーの将来の標準を定義する可能性が高いです。Galileelは、このホワイトペーパーで概説した独自の機能を実装することで、このプロセスの一部になります。

## はじめに

Galileel コインは、完全な透明性と公共開発手法を利用した、コミュニティ主導の暗号通貨です。投資家とプロジェクトチーム間の信頼関係は成功への鍵です。そのため、私たちは *Galileel-Project*<sup>2</sup> という名前の GitHub 組織を作成しました。これは、私たちのすべてのバックエンドコードを含む公共リポジトリでのすべての開発活動を追跡し、*Know Your Developer (KYD)*<sup>3</sup> 公開検証に合格しました。プロジェクトは主に MIT<sup>4</sup>、GPLv3<sup>5</sup> と CC-BY-NC 4.0<sup>6</sup> オープンソースとオープンコンテンツライセンスを使用します。翻訳とローカライゼーションは Transifex<sup>7</sup> プラットフォームを使用します。

## GALILEL コイン

Galileel コイン (GALI および zGALI) は、高速 (SwiftX を使用)、非公開 (ZeroCoin<sup>8</sup> プロトコル)、および安全なミクロ取引のための、オープンソースのパブリックおよびプライベートのプルーフオブステークデジタル暗号通貨です。私たちの主な目標は、アプリケーションを実行するための分散型の完全に安全で匿名のネットワー-



クを作成することです。分散システムを使用することで、何千ものユーザーがアプリケーションとデータの保守を担当し、单一障害点がなくなります。

## 問題とソリューション

ブロックチェーン技術の宣伝は大きな関心を生み、世界中で人気を集めており、デジタルマネー以外のさまざまな目的で多くの企業で使用されています。 ただし、支払いサービスの基盤として使用するには、検証するための特定の機能が必要です。何千ものトランザクションを保管および検証します。これは既存の合意アルゴリズムを使用してチェーン内にブロックを生成することすでに解決されていますが、現在のブロックチェーンの実装には、デジタルマネーの主流採用を達成するための弱点がいくつかあります。

## 動的 ZEROCOIN プルーフ・オブ・ステーク (dzPoS)

Zerocoin プルーフ・オブ・ステーク (zPoS) は、PIVX開発チームによって2018年に導入された最も革新的なブロックチェーン機能です。 ただし、技術的な実装はブロックチェーンに対して特定の方法で行われ、その報酬構造はソースコードに静的に含まれているため、他の人に簡単に採用することはできません。

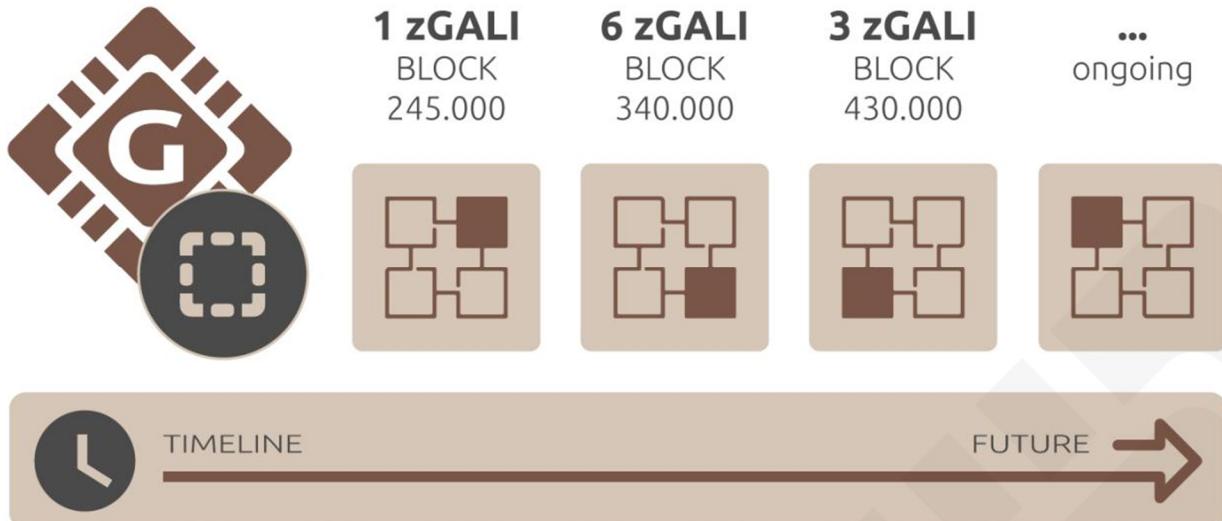


図1. ブロックチェーンのフェーズに基づく動的Zerocoin プルーフ・オブ・ステーク報酬。

Galileelでは、動的バージョンの Zerocoin ステーキングを実装しています。 Zerocoin ステークは整数値を表す宗派で報酬を生み出します。最小の額面金額は1です。最初のバージョン（ウォームアップフェーズ）では、テスト目的で常に最小の額面金額を使用します。このアプローチの欠点は、 Zerocoin ステークが非常にCPU集約的であり、公共のコインステークが後でブロックを解決するが、それをチェーンに早く分配できるため、孤立ブロックを生成する可能性が高いことです。 2番目のバージョン - フルフェーズ - では、ブロックの報酬額に基づいて最適な額面金額構造が自動的に決定されます。 これにより、孤立ブロックが生成される可能性が大幅に減少します。



## プルーフ・オブ・トランザクション (ghPoT)

銀行口座間の送金を伴う従来の経済学では、受取人が特定の請求書に金額を割り当てるようになります。件名を指定することができる。現在のウォレットの実装では不可能です。これは、トランザクションの一部ではなく、ローカルにのみ格納されているコメントまたはコメントへの値を指定することができます。特定の受取人に請求書を割り当てるには、両方の利害関係者の間に1対1のマッピングでウォレットアドレスを作成する必要があります。

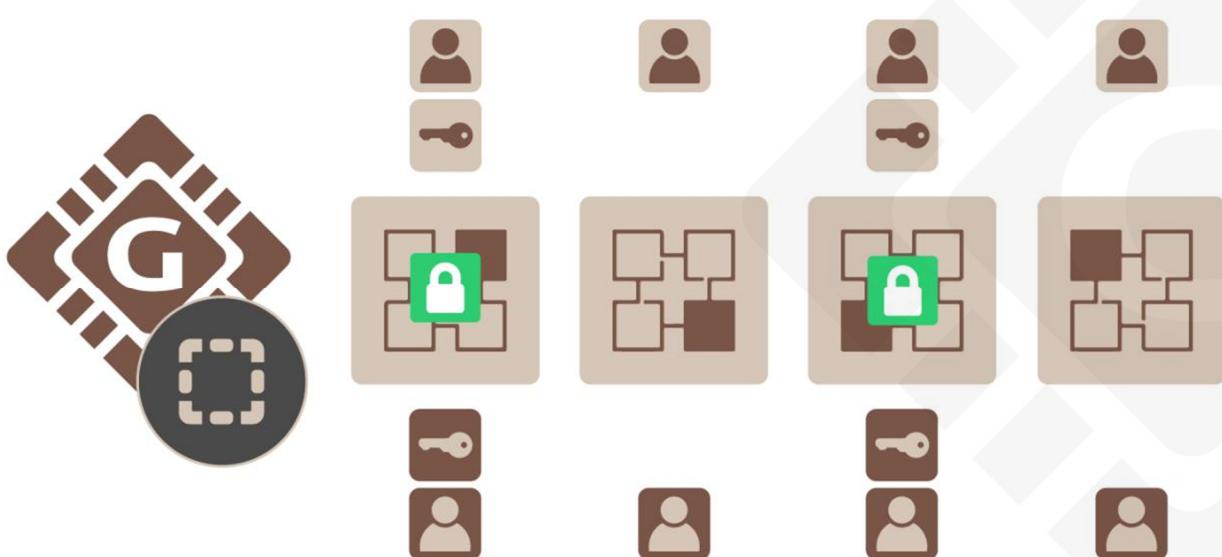


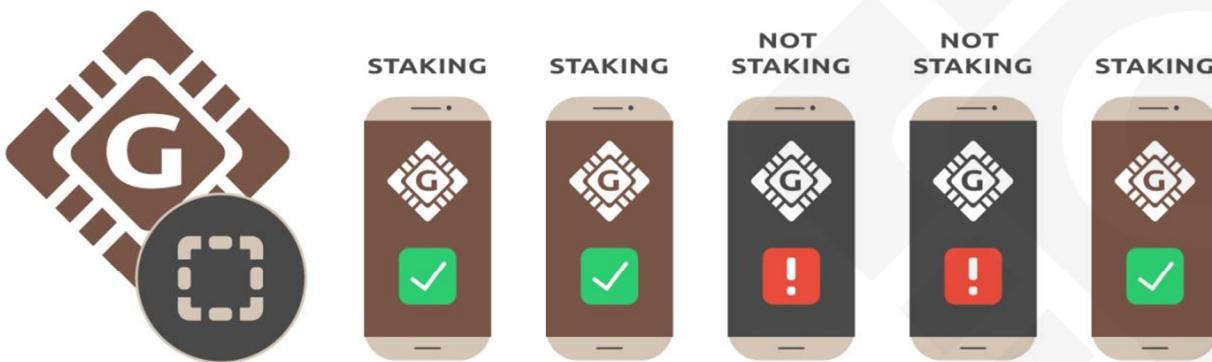
図2.暗号化されたサブジェクトを持つトランザクションの証明。

Galilelでは、追加のデータフィールドを含め、それをブロックに格納されているトランザクションに添付します。これは暗号化されたフィールドであり、復号化はトランザクションをネゴシエートしたウォレットによってのみ可能です。これは、トランザクション割り当ての問題を解決し、支払い処理ゲートウェイが従来のフィアット請求書と同様に請求書の受取人を識別できるようにします。



## ハイブリッド プルーフ・オブ・ステーク (ghPoS)

プルーフ・オブ・ステーク (PoS) は環境に優しいコンセンサスアルゴリズムですが、デスクトップウォレットが実行されている限りのみ報酬を生み出します。この問題を解決する1つの方法は、共有の プルーフ・オブ・ステーク プールにサインアップしてクラウドに参加することです。ただし、デメリットは、ユーザーがステーキプールを信頼し、特定の量のコインをそこに転送する必要があることです。大量のコインがいくつかのウォレットに収納されているという状況につながる可能性があります。これは分散型ネットワークアプローチにとって弱い状況です。



**IMPORTANT:** THE WALLET CAN RUN IN THE BACKGROUND BUT A CONNECTION MUST BE ACTIVE TO STAKE.

図3. Galilelネットワークから報酬を得るための方法。

Galilelでは、この問題の解決策は Galilel ハイブリッド プルーフ・オブ・ステーク (ghPoS) という名前の完全なハイブリッド合意アルゴリズムです。私たちは、パブリックとプライベートの両方のステーキングのために、モバイルステーキング機能を使ってプルーフ・オブ・ステークを拡張します。モバイルウォレットがロックを見つけた場合、モバイルステークは常にロック報酬の 10% で支払われます。こ



の場合 90 % がマスターノード保有者に支払われます。モバイルウォレットは、再編成の深さに等しい最小ブロック数で、ブロックチェーンのライトノードとして機能します。

#### ハイブリッド プルーフ・オブ・ス 酬の構造

ステーキングタイプ <sup>1</sup>	ステーキング	マスターノード
オンライン (GALI)	30%	70%
オンライン (zGALI)	60%	40%
モバイル (GALI)	10%	90%
モバイル (zGALI)	20%	80%

<sup>1</sup> 計算は5 GALI報酬に基づいています リワード > ブロック 430,000



## 定期預金 (gTD)

モバイルステーキングはネットワークの難しさやコインの量に左右されますが、*Term Deposit*<sup>9</sup> 機能では一定期間コインをロックして報酬を生み出すことができます。

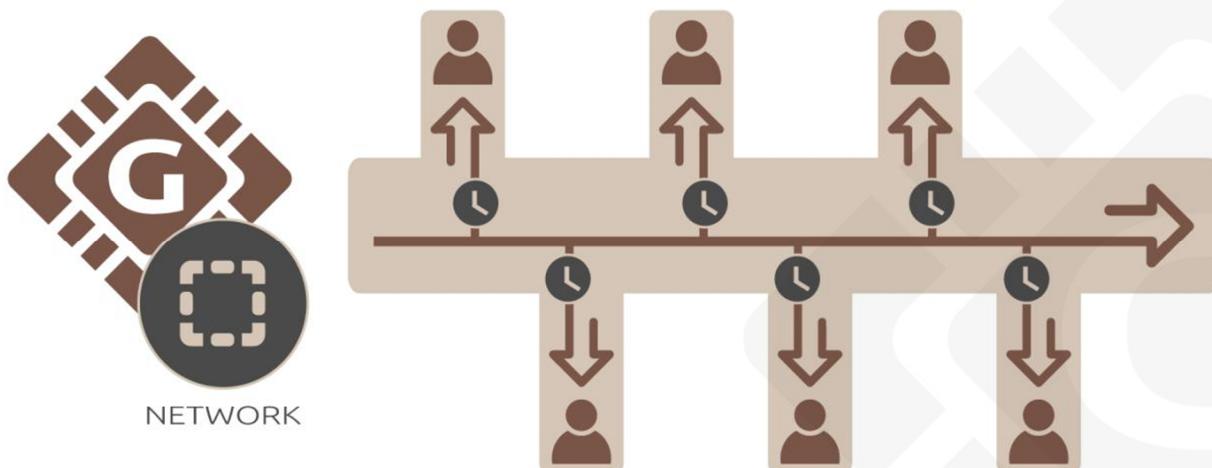


図 4. オフラインウォレットにカレンダーベースの定期預金。

Galilel定期預金 (gTD) を使用するためには最低限必要なコインの量は、5,000 GALIです。ロック期間は1年です。ブロック報酬は10%で、異なるウォレットのロックコインは加重されます。ロックされたコインでネットワークウォレットの新しいブロックで、彼らの重さに従って量を得てください。定期預金期間が終了するまで、この報酬はロックされています。ロックされると、購入のためにコインを移動または支出することは不可能になり、有効期限前に定期預金をキャンセルすることは不可能になります。これにより、ロック期間中のコインの供給が効果的に減少します。



## マネーサプライコントロール (gMSC)

インフレ抑制は、デジタルマネーが平等なお金に代わるものとして認識され受け入れられるための最も困難な部分です。いかなる管理メカニズムもなければ、どんなデジタルマネーの価値も予測不可能です。これは投資家が価値に賭け始めたときに状況を導き、そしてこれは数時間以内に市場に深刻なダメージを与え、そして即座に受け入れられた支払いオプションとして市場にデジタルマネーを押し込む可能性を排除します。インフレ制御により、私たちはデジタルマネーの分野以外の人々がそれを使用することに惹かれていると信じています。毎日ポートフォリオを見る必要はないからです。平等なお金の場合の中央銀行とは異なり、マネーサプライを監視し維持するための中心的な場所はありません。 Galileelでは、コインを焼くための分散型アプローチ、いわゆる個人用および公共用のステークコイン用の*Proof-of-Burn<sup>10</sup>* メカニズムを実装しています。これはお金の循環を制御するために必要な1つのステップですが、マスターノードの所有者はコインの生成を減らすために特定の期間の報酬の減少または完全な燃焼に投票する可能性を得ます。

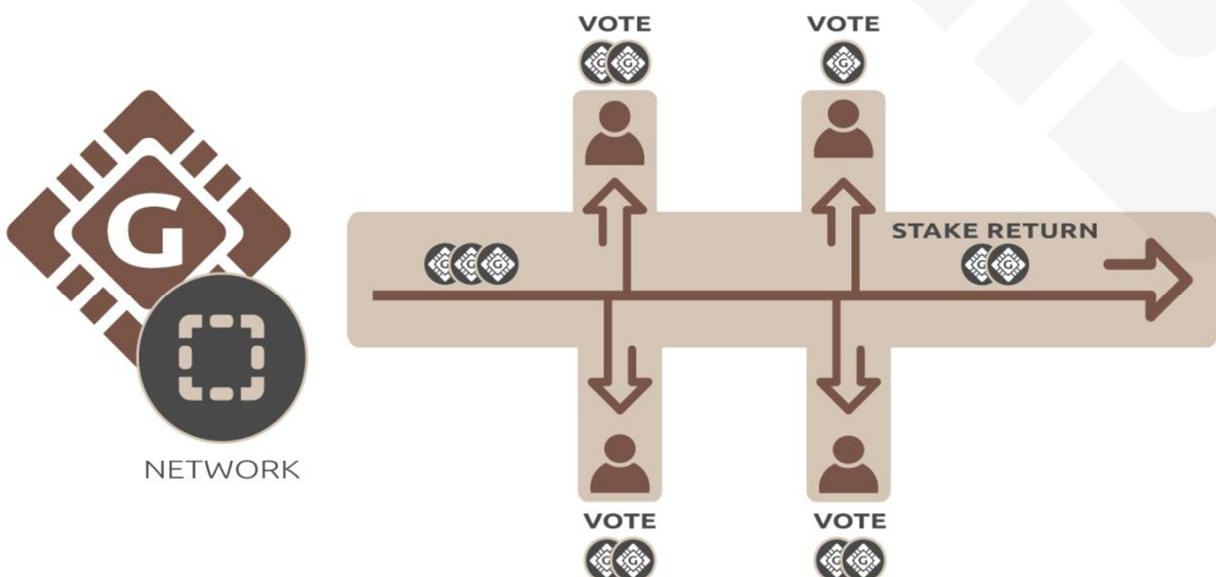


図 5.報酬生成を減らすためのマスターノード投票。



私たちは、Galileel マネーサプライコントロール (gMSC) と名付け、事実上 Proof-of-Burn v2 です。このメカニズムは報酬だけを燃やし、定期預金や開発予算は決してしません。コイン燃焼の期間は、報酬供給構造表に記載されているステップで1月になり、年間供給量が減少します。マスターノード保有者は毎月の投票に適用されます。この提案は月に一度、現在の報酬燃焼期間が終了する1週間前から開始することができます。ブロックチェーンは 1,000 GALIから始まるあらゆる提案を受け入れます。提案がブロックチェーンで配布されると、マスターノードの所有者は追加の1つ以上のGALIを使って投票することができます。提案期間が終了した後、最高額のコインを持ち、50%以上のマスターノード投票を持つ提案が勝ちます。プロポーザル期間が終了して受け入れられると、プロポーザルにロックされているコインが燃やされ、報酬燃焼期間が次の燃焼ブロックから始まります。プロポーザル承認の最低要件に達していない場合、ロックされているコインはロック解除されます。

#### 報酬燃焼構造

燃焼率	1か月あたりの燃焼 <sup>1</sup>
25%	54,750 GALI
50%	109,500 GALI
75%	164,250 GALI
100%	219,000 GALI

<sup>1</sup> 計算は5 GALI/報酬に基づいています> ブロック 430,000



## マスターノードでインスタント (gIOMN)

マスターノードはすでにデジタルマネー分野で多くの魅力を獲得しています。多くの新しいデジタル暗号通貨はばかりで高い投資収益率 (ROI) コインを作成しようとし、コインのインフレが始まると失敗し、マスターノードとステークウォレットの間に不均衡な報酬配分がある間、これはマスターノードを実行する主な目的ではありません。Galileelでは、マスターノードの主なユースケースは、コイン循環を維持するだけでなく、将来の開発側面に投票する機会を持ちながら、ネットワークを保護することです。ただし、利用可能なマスターノード実装の主な弱点は、マスターノードとして機能する各マシンでブロックチェーンを同期させてインデックスを付ける必要があることです。

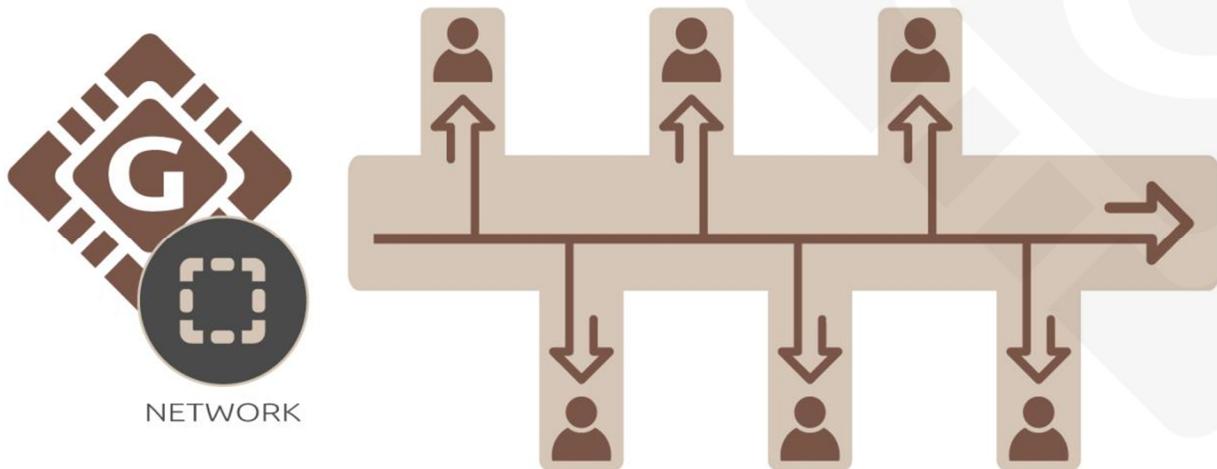


図6. クラウド内の単一のブロックチェーンに接続された複数のマスターノード。

Galileel マスターノードでインスタント (gIOMN) は、クライアントサーバーモデルで 1対多 (*one-to-many*<sup>1)</sup> 個のウォレットデータモンを実行するために共有ブロックチ



エーンを実装することで、この問題を解決します。これは *Electrum*<sup>12</sup> クライアントで利用可能な「インスタントオン」モデルに匹敵します。



## 機能と仕様

### コイン仕様

コイン名	Galileel
コインティッカー	GALI
ハッシュアルゴリズム	Quark
コンセンサスアルゴリズム	PoS + zPoS Hybrid
ブロックサイズ	2 MB
ブロックタイム	60秒（すべてのブロックを再ターゲティング）
RPC ポート	36002
P2P ポート	36001
タイプ	PoW / PoS / zPoS / MN
最小ステーキング年代	2 時間
成熟	120回の確認
適格性の送信	6の確認
報酬（ブロック1,500まで）	MN 60%, PoW 40%
報酬（ブロック205,000まで）	MN 60%, PoS 40%
報酬（ブロック205,001から）	MN 70%, PoS 30%
最後の PoW ブロック	1,500
マスターノード担保	15,000



最大コイン供給量（2020年1月）	19,035,999 GALI
最大コイン供給量（2030年1月）	45,315,999 GALI
最大コイン供給量（2040年1月）	71,595,999 GALI
最大コイン供給量（2050年1月）	97,875,999 GALI
動的なコイン供給	取引手数料とzGALIの採掘手数料が焼かれます
コミュニティ寄付アドレス	<u>UUr5nDmykhun1HWM7mJAqLVeLzoGtx19dX</u>
開発予算（ブロック250,001から）	毎月のスーパー ブロックで10%



## ZEROCOIN 仕様

ZeroCoin v1のアクティベーション	ブロック245,000
ZeroCoin v2のアクティベーション	ブロック245,000
zGALI 自動鋸造	10%
zGALIリワード（ブロック245,001から）	1 zGALI
zGALIリワード（ブロック340,001から）	MN 40%, zPoS 60%
zGALIリワード（ブロック430,001から）	MN 40%, zPoS 60%
zGALI デノミネータ	1, 5, 10, 50, 100, 500, 1000, 5000
蓄積モジュール	RSA-2048
成熟	240回の確認
成熟度送信の資格	20回の確認
手数料（鋸造）	0.01 GALI/鋸造 zGALI デノミネーション
手数料（費用）	手数料無料



### PROOF-OF-WORK 報酬の内訳

ブロックの高さ	報酬	MN	POW	供給	期間	ステージ終了
ブロック1	220,000	60%	40%	220,000	0 days	2018-05-25
ブロック2 - 1,500	1	60%	40%	221,499	1 days	2018-05-26

### PROOF-OF-STAKE 報酬の内訳

ステージ	ブロックの高さ	報酬	MN	POS	供給	期間	ステージ終了
ステージ1	1,501-12,000	100	60%	40%	1,271,399	7 日	2018-06-02
ステージ2	12,001-22,000	90	60%	40%	2,171,309	7 日	2018-06-09
ステージ3	22,001-42,000	80	60%	40%	3,771,229	14 日	2018-06-23
ステージ4	42,001-100,000	70	60%	40%	7,831,159	40 日	2018-08-02
ステージ5	100,001-160,000	60	60%	40%	11,431,099	42 日	2018-09-13
ステージ6	160,001-205,000	50	60%	40%	13,681,049	31 日	2018-10-14
ステージ7	205,001-250,000	25	70%	30%	14,806,024	31 日	2018-11-14
ステージ8	250,001-340,000	13.5	70%	30%	16,156,009	62 日	2019-01-15
ステージ9	340,001-430,000	10	70%	30%	17,055,999	62 日	2019-03-18
ステージX	430,001-進行中	5	70%	30%	進行中	進行中	進行中



## 競合製品分析

毎日新しいデジタル暗号通貨プロジェクトが生まれ、主に特定の目的のために通貨を処理します。これは有効なシナリオですが、コインの使用例を特定の市場と規模に限定します。結局、それは通貨価値を制限します。同じ金額の機能を異なる金額のデジタルマネーと異なるブロック報酬で共有する暗号通貨の市場は過飽和です。過去には、ユニークなアイデアと明るい未来を持ついくつかのプロジェクトが生まれました。Galileelは、この傾向を継続し、デジタルマネーに使用されるブロックチェーンを改善しながら、市場での大量採用のために使いやすい汎用暗号通貨を構築します。



機能	GALILEL	DASH	PIVX	ROI COIN
公開ステーキング	✓	✗	✓	✗
プライベートステーキング	✓	✗	✓	✗
インスタント送信	✓	✓	✓	✗
プライベート送信	✓	✓	✓	✗
マスターノード	✓	✓	✓	✗
分散型ガバナンス投票	✓	✓	✓	✗
変動報酬分配 <sup>1</sup>	✗	✗	✓	✗
動的 ZeroCoin Proof-of-Stake	✓	✗	✗	✗
Proof-of-Transaction	✓	✗	✗	✗
変動報酬燃焼	✓	✗	✗	✗
切断されたブロックチェーン	✓	✗	✗	✗
モバイル Proof-of-Stake	✓	✗	✗	✗
定期預金	✓	✗	✗	✓

<sup>1</sup> Seesawアルゴリズムを使用してGalileelに実装することが可能



## 開発ロードマップ（行程表）

Galileelコインの開発は、将来のブロックチェーンにとって重要です。いくつかのコードはすでに書かれており、内部テスト中です。Galileelインスタントオンマスター／ノード（gIOMN）機能はほぼ完成していますが、Galileelハイブリッド プルーフ・オブ・ステーク（ghPoS）では、ブロック245,000でZerocoin v2をアクティブにした後に追加の開発およびテストサイクルが必要になります。ロードマップには主に開発項目のみが含まれています。私達はそれに細かく調整されたマーケティング項目を置くよりもむしろ適切な目標、期待および成果物を定義することが必要であると信じる。

- 2018 – PIVXコードベースをフォークしてMAINNETを起動します。BitcoinTalk<sup>13</sup> フォーラムでコミュニティ投票および事前発表のためのDiscord<sup>14</sup> チャンネルを作成します。
- 2018 – 最初の取引所とランキングサイトへの上場。報酬の配布、報酬構造の変更、およびマスター／ノードの担保に関するコミュニティ投票結果をv2.0に実装する。アプリケーション開発者向けのブランドカラー、ロゴ、およびブランドガイドを使用してGalileelブランドおよびWebサイトを作成するデザインチーム。開発とデザインの他に、私たちはKnow Your Developer (KYD) 公開検証に合格します。
- 2018 – TESTNETを有効にしてリリースすると、開発者は新しいブロックチェーンコードをテストでき、ユーザーは最先端の機能をテストできます。ブロックチェーンとネットワークの下位互換性を保ちながら、ブロック245,000でZerocoin v1およびv2をアクティブ化し、分散型自律組織（DAO）を機能させて、Galileelコードベースを最新のPIVX 3.1.1ソースおよびリリースv3.0にリファクタリングします。プライベートステークのためにZerocoin Proof of Stake (zPoS) を有効にし



てv3.1をリリースします。 BitcoinTalkフォーラムでの再発表とともに、Galileel Coinのホワイトペーパーの作成と公開。

- 2019 – Galileel Instant On Masternode (gIOMN) 機能の実装を終了し、v4.0の General Availability (GA) に進みます。このアップデートはチェーンをハードフォークするため、必須です。 Galileel Coreのリリース後、Q1後半にモバイルウォレットの開発が開始されます。
- 2019 – パブリックおよびプライベートステークのためのGalileel Hybrid Proof of Stake (ghPoS) の実装を完了します。リリース日がv5.0に近づいたら、アクティベーションブロックを公開します。このアップデートはチェーンをハードフォークするため、必須です。 v1.0のモバイルウォレットリリース第2四半期後半には、次世代のモバイルウォレットの開発に着手し、Galileel HybridのProof of Stake ( ghPoS) を導入しました。
- 2019 – Galileel Term Deposit (gTD) 機能は、wallet v5.1で一般公開される予定です。この機能はGalileel Hybrid Proof-of-Stake (ghPoS) に依存しており、その後開発されました。このアップデートはチェーンをハードフォークするため、必須です。リリース日が近づいたら、アクティベーションブロックを公開します。
- 2019 – Galileel Money Supply Control (gMSC) は生産準備が整っており、v6.0の General Availability (GA) を進めています。このアップデートはチェーンをハードフォークするため、必須です。リリース日が近づいたら、アクティベーションブロックを公開します。第4四半期後半、Galileel Term Deposit (gTD) 機能を搭載したモバイルウォレットv2.0を公開します。
- 2020 – Galileel Money Supply Control (gMSC) を備えたv3.0の本格的なモバイルウォレットのリリース。

上記のロードマップは明確でブロックチェーンに焦点を当てていますが、チームは、ウォレットの使用を単純化するためのさらなる技術の改善について、他にもいく



つかのアイデアを念頭に置いています。これらの弱点の1つは組み込みQtウォレットです。プラットフォームの相互運用性を高めるためには、フロントエンドフレームワークを使用して最高のユーザーエクスペリエンスを提供するシンビルトインWebサーバーに置き換える必要があります。

## ヘルプ

私たちが長期的な開発目標にコミットしていても、誰でもプロジェクトの目標を支援または支援することができます。開発は非常に重要な部分ですが、マーケティング、記事の執筆、技術者以外の人への機能の説明を手助けできる人は大歓迎です。



## 重要なリンク

### Website

<https://galilel.org/>

### Block Explorer (MAINNET)

<https://explorer.galilel.org/>

### Block Explorer (TESTNET)

<https://explorer.testnet.galilel.org/>

### Wallet

<https://github.com/Galilel-Project/galilel/releases>

### Discord

<https://discord.galilel.org>

### Twitter

<https://twitter.com/GalilelEN>

### Facebook

<https://facebook.com/GalilelEN>

### YouTube

<https://youtube.com/channel/UC26rKBciicXp33dK8NkALmg>

### BitcoinTalk

<https://bitcointalk.galilel.org>



## 付録

1. <https://www.linkedin.com/in/mbroemme/>  
<https://zuppy.pm/>
2. <https://github.com/Galilel-Project>
3. <https://review.kydcoin.io/galicoing/>
4. <https://opensource.org/licenses/MIT>
5. <https://www.gnu.org/licenses/gpl.txt>
6. <https://creativecommons.org/licenses/by-nc/4.0/legalcode.txt>
7. <https://www.transifex.com/galilel-project/galilel-project-translations/>
8. <http://zerocoin.org/media/pdf/ZerocoinOakland.pdf>
9. [https://en.wikipedia.org/wiki/Time\\_deposit](https://en.wikipedia.org/wiki/Time_deposit)
10. [https://en.bitcoin.it/wiki/Proof\\_of\\_burn](https://en.bitcoin.it/wiki/Proof_of_burn)
11. [https://en.wikipedia.org/wiki/One-to-many\\_\(data\\_model\)](https://en.wikipedia.org/wiki/One-to-many_(data_model))
12. <https://electrum.org/>
13. <https://bitcointalk.org/>
14. <https://discord.com/>



**galilel.org**