Salvium - ライトペーパー v1.0

2024 年 7 月 3 日

セージ **($SAL)** /ˈサルビアム/

名詞 (安全、確実、救済を意味するラテン語の salvus に由来) 収益生成、ステーキング、規制順守に重点を置いたプライベートのレイヤー 1 プロトコル。

導入

Salvium は、仮想通貨規制を乗り越えながら、ステーキング、プライバシー、DeFi 機能をシームレスに組み合わせる、最先端のプルーフ・オブ・ワーク・プライベート・ブロックチェーンです。Monero のフォーク上に構築されており、ステルス アドレスやリング署名などの Monero の高度なプライバシー機能を保持しています。ただし、Salvium はトランザクションの仕組みを大幅に変える画期的なイノベーションを導入し、DeFi 分野に独自のソリューションを生み出します。

革新

Salvium は、プライベート DeFi における CryptoNote の可能性を探る研究プロジェクトとして始まりました。チームは、スケーラビリティ、拡張性、マルチチェーンの相互運用性に焦点を当てて、Monero 研究者の研究成果を再検討し、プロトタイプを作成しました。この研究では、特に MiCA の下での世界的な規制の変更も考慮されており、Salvium が Cryptonote と Monero の本質的な進化として位置づけられています。

Salvium は「プライバシー第一」のアプローチを採用し、暗号資産市場 (MiCA) 規制に完全に準拠するよう努めています。最初のフェーズには、コンプライアンスをサポートするための返金可能な支払いや交換モードなどの機能が含まれます。過去 1 年間、当社は条件付き支払い (CP)、返金可能な支払い、ネイティブ利回り、ステーキングの分野で進歩を遂げてきました。これらの機能の一部はリリースの準備ができていますが、その他の機能は将来のアップデートに含まれる予定です。

Salvium は、トランザクション不均衡 (TI) や非同期トランザクション (AT) などの独自の技術的進歩を導入し、初のネイティブ暗号通貨ステーキングおよび利回りシステムを形成し、将来の開発を推進し、エコシステムの基盤を形成します。

プライベートDeFi

これらの技術の進歩に基づいて、Salvium は、準拠したプログラム可能なプライバシーに重点を置いた堅牢な分散型金融 (DeFi) 機能を提供する準備ができています。

プログラム可能なプライバシー: Salvium ベースレイヤーは、Monero から優れたレベルのプライバシーを継承しました。準拠した CEX インタラクションや DeFi アプリケーションなど、このレベルのプライバシーが不可能な場合、Salvium は DApp 開発者がさまざまなプライバシー層を備えた DApp を構築できるようにし、ユーザーが共有するデータの種類を選択できるようにします。これにより、従来のプライバシー コインにありがちな制限がなく、制御可能またはプログラム可能なプライバシーが実現します。

DeFiの未来

Salvium には、レイヤー 1 での DeFi アプリケーションの構築を数学的に可能にする機能がすでに含まれています。これはフェーズ 3 でさらに開発され、固有のパフォーマンスとスケーラビリティの利点を備えたレイヤー 2 ソリューションが組み込まれる可能性があります。いずれの場合でも、これらの中核となるイノベーションは、DeFiをよりプライベートなものにするのに役立ちます。

条件付き支払い: CP を使用すると、事前定義された基準に基づいて条件付きでトランザクションを実行できます。これにより、スマート コントラクト、潜在的なアプリケーションの奔流のロックを解除します。

ミドルウェア: Salvium は、他の暗号プラットフォームとのシームレスな統合のためのミドルウェアを提供します。これにより、開発者は、Solidity (イーサリアムの主要な DApp 言語) などの言語で書かれたアプリケーションを、Salvium で使用できるように簡単に適応させることができます。その結果、既存の DApp を Salvium ネットワーク上で迅速かつ効率的に起動できるようになります。

潜在的な DeFi アプリケーション

これらの機能が Salvium で利用可能になると、サードパーティはすぐに DAAP を構築し、Salvium をイーサリアムに代わるプライバシー重視の代替手段として位置づけることになります。

これには、分散型取引所 (DEX)、貸付および借入プロトコル、イールド ファーミング、ステーブルコイン、NFT、ミームコイン、ギャンブルが含まれます。

なぜ暗号通貨にはサルビアムが必要なのでしょうか?

Pプライバシーは基本的人権ですが、これはそれが邪悪な目的に使用されるべきであるという意味ではありません。救い は、倫理的な使用を推進し、適用される法律や規制を遵守しながらユーザーの機密性を保護する分散型プラットフォームの作成に努めています。

の 影響を与える新しい規制 既存のプライベート暗号通貨により、プライバシーとコンプライアンスを保証する新しいプライバシー コインが緊急に必要とされています。 ほとんど DeFi トークンはパブリック ブロックチェーン上で動作し、機密性の高いユーザー データを公開します。 救い は、ユーザーがプライバシーと規制遵守のバランスを取ることを可能にすることで、この問題に対処します。

達成する 準拠したプライバシー

EU の MiCA 規制ではプライバシー コインの適応が求められており、これが Salvium プロジェクトの中心的な焦点です。最初のステップとして、規制により、Monero や ZCash などのプライバシー コインを含む取引の隠蔽を明らかにすることが集中型取引所に義務付けられます。 Pこれらの規制に準拠していないプライバシーコインにはリスクがあります デリもの。

欧州議会規則 2023/1114 では次のように規定されています。

「 暗号資産取引プラットフォームの運用ルールでは、匿名化機能が組み込まれた暗号資産については、暗号資産の保有者及び取引履歴を運営する暗号資産サービス提供者が識別できない限り、取引を認めることができないものとします。暗号資産の取引プラットフォーム。」

ソース: https://eur-lex.europa.eu/eli/reg/2023/1114/oj 第76条第3項

主な機能 Cコンプライアンス

この特定の規制に準拠するには、プロトコルには以下が必要です。

1. ～する能力 拒否する そして戻る トランザクション: 準拠したプロトコルでは、取引所が未承認のウォレットからの未承認のトランザクションを拒否できるようにする必要があります。この機能は、従来のプライバシー コインでは通常不可能です。

2. 承認されたウォレットの可視性: 取引所は、プラットフォームに資金を入金するために使用される承認されたウォレット内のトランザクションを監視する機能を必要とします。

Salvium はこの要件を満たします による：-

1. 匿名さんr資金提供可能なトランザクション: 他のプライバシーコインでは珍しい機能です。
2. 見える財布 (またはサブアドレス) 歴史。ユーザーは交換を可能にする完全表示キーを提供できます。現在提供されている限られたビューだけでなく、規制当局の要求に応じた完全な履歴を表示する「ビューウォレットメカニズム」。

Salvium のアプローチは選択的な透明性を可能にし、ユーザーが自分のプライバシーを制御できるようにします。たとえば、ユーザーは自分の取引を非公開に保ちながら、コンプライアンスのために必要な場合に取引履歴を確認するために取引所と「ビューキー」を共有できます。これにより、税務上の目的で銀行取引明細を公開するなど、プライバシーと規制上のニーズのバランスがとれます。

目標は、コミュニティが世界中のさまざまな法域にわたる規制の動向を積極的に監視および分析する中で、特に米国と EU の暗号資産市場 (MiCA) 規制を重視し、プライバシー準拠のリーダー的地位を維持することです。

プロジェクト フェーズ

フェーズ 1: レスキューを起動する

ステーキングと利回り 世代:

Salvium の進化したプライバシーによって提供される強化された機能のデモンストレーションとして、また、Salvium コンセプトの基礎として、発売からユーザーは SAL トークンを賭けて報酬を獲得し、安全で魅力的なネットワークを促進できます。

また、完全なコンプライアンスに向けたステップ 1 も開始時に提供されます。返金可能な取引。未承認または誤った取引の返品を可能にします。返金可能なトランザクションにより、トランザクションの受信者は、アドレスを要求することなく、その正確な入力 (標準トランザクション手数料を差し引いたもの) を元の送信者に返すことができます。この機能はパブリック ブロックチェーンでは些細なものですが、Monero ベースのチェーンにとってはコンプライアンスへの大きな一歩となります。

フェーズ 2: 追加のコンプライアンス機能

コンプライアンス機能を備えたプライベート ブロックチェーン:

Salvium は、厳しい規制要件、特に EU の MiCA 規制を満たすために継続的に開発していきます。フェーズ 2 では、ユーザーは取引履歴を確認するためのビュー キーを取引所などの承認されたエンティティに提供しながら、取引を非公開に保つことができます。このアプローチにより、規制要求への準拠を維持しながら、ユーザーのプライバシーが確保されます。

Salvium の開発チームは、Monero と CryptoNote の基礎テクノロジーの進歩に専念しています。当社は、フルチェーンメンバーシッププルーフ、SERAPHIS、JAMTISなどのコンプライアンスへの取り組みに機会があれば貢献し、サポートすることに尽力しています。この取り組みは、Salvium エコシステム内でのプライバシー、セキュリティ、規制の互換性を強化するための当社の継続的な取り組みを反映しています。

フェーズ 3: DeFi サポート

スマートコントラクト機能 およびプライベートトークンの発行:

Salvium は、protocol_tx イノベーションを活用してスマート コントラクト機能を有効にし、複雑な DeFi アプリケーションがそのネットワーク上で安全かつプライベートに動作できるようにします。

Solidity 用のミドルウェア:

導入と開発を合理化するために、Salvium は、イーサリアム DApps の頼りになるプログラミング言語である Solidity で開発された DApps を迅速に調整してネットワーク上に展開できるようにするミドルウェアを提供します。この動きは、既存のイーサリアムプロジェクトからサルヴィウムへの移行を簡素化し、開発者の参入障壁を効果的に下げることを目的としています。

料金とインセンティブ

ステーキング報酬

トークンを賭ける Salvium (SAL) 保有者 意思 得る ある ステーキング報酬。参加するには、ユーザーは あらかじめ決められた期間、SAL をロックする必要がある 期間。ステーキング報酬はロック期間が終了すると分配されます解像度。報酬は、プロジェクトのフェーズに応じて 2 つのソースのいずれかから得られます。。

報酬の共有をブロックする

ストライカーズ ブロック報酬の 20% のシェアから恩恵を受けます プロジェクトの初期段階で。これらの報酬は配布されます 比例的に アクティブなステーカー全員の間で、奨励する ユーザーがネットワークに参加し、サポートする そのセキュリティ。

長期 - DeFi手数料

将来的には、ステーキング報酬はブロック報酬のシェアから、使用量に基づいた料金分配モデルに移行する予定です。ステーカーとマイナーは、他のブロックチェーンネットワークのガス料金と同様のシステム料金を受け取ります。

テクノロジー

Salvium は、返金アドレス、非同期トランザクション、ウォレット全体の残高を表示するビュー キーなど、いくつかの重要な革新によって Cryptonote プロトコルを拡張しています。これらの機能強化により、最高レベルの匿名性が保証されると同時に、利回りの生成と defi 機能の配信のための複雑なルールとトークンノミクスが可能になります。

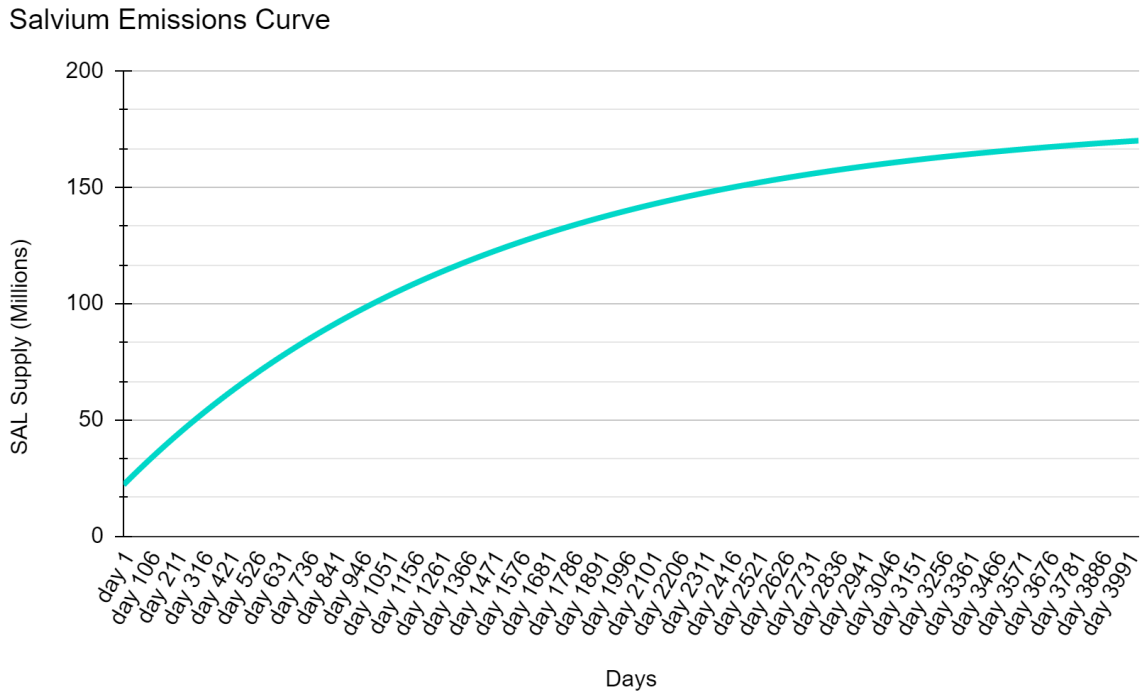
Salvium は、リング署名、ステルス アドレス、ゼロ知識証明などの高度なプライバシー テクノロジーを活用することで、プライバシーを維持しながら、コンプライアンスの目的で選択的な透明性を確保します。これらの機能は、DeFi 機能、トランザクションのプライバシー、分散化、責任ある規制の需要を総合的に満たし、Salvium をデジタル ファイナンスの先駆的なソリューションにしています。

マイニング

Salvium は、RandomX マイニング アルゴリズムを使用する Proof of Work コインです。DeFi機能が稼働すると、マイナーはシステム料金の一部も受け取ることになります。

排出スケジュール

排出スケジュールは、より広い流通を通じてより大きな流動性と採用を促進するために、Monero の修正バージョンに基づいています。ブロック時間は 120 秒のままですが、ブロックあたりの放出量は 5 倍に増加し、初期供給期間は 2 倍になりました。これにより、初期供給量は 1 億 8,440 万コインとなり、Monero と比較してより平坦で幅広い排出曲線を特徴としています。



テールエミッション

Monero と同様に、Salvium は長期的なマイニング インセンティブとネットワーク セキュリティを確保するためにテール エミッションを統合しています。最大供給量に達すると、プロトコルはブロックごとに 3 つの SAL を発行します。

取引手数料

Savrium の取引手数料は、Monero の手数料と同様に動的であり、いくつかの要因に依存します。 計算は次のように簡略化できます。

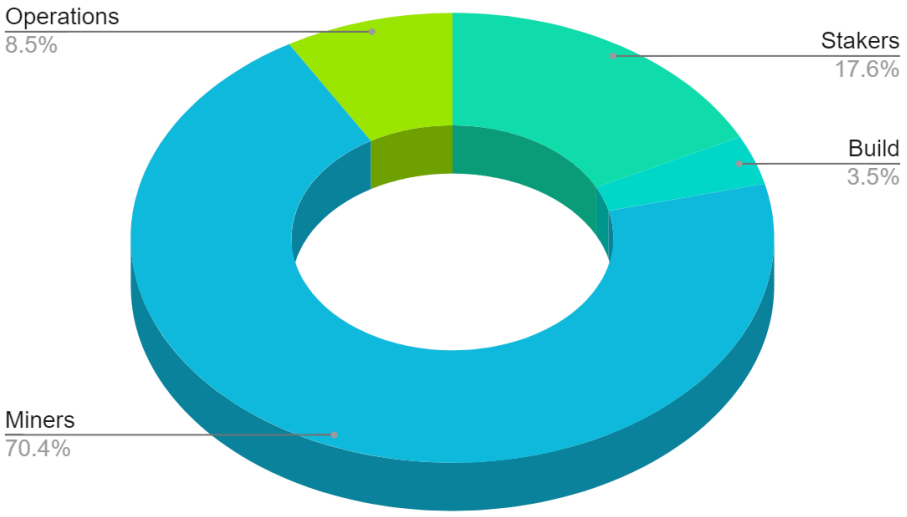
料金 = 基本料金 × トランザクション サイズ (KB)

通常の取引コストは非常に低くなります。

ブロック報酬の構造: Savlium ネットワーク上でマイニングされた各ブロックには、最後のブロック以降に送信されたすべてのトランザクションが含まれます。ブロックのマイニングに成功したマイナーは、新しく鋳造されたサブリウム コインとともに、そのブロックに含まれるトランザクションからのすべての手数料を受け取ります。

救い トークンの割り当て

このプロジェクトは、部分的にロックされている 12.01% のプレマイニングによって資金提供されています。これらの資金は建設と運営に割り当てられます。採掘者とステーカーは総供給量の 88% とテール排出量を獲得し



ます。
注: 表示されているパーセンテージは、テールエミッションを除いた、サルヴィウムの *1* 億 *8,400* 万コインの割合です。

1. ビルド - 3.5%

Salvium は、初期の開発者と貢献者のビジョンと献身のおかげで、2023 年初頭に現実になりました。プレマイニングの 3.53% は、プロジェクトの立ち上げをサポートするこれらのアクティブなチーム メンバーとサプライヤーへのインセンティブとして割り当てられます。

2. 操作 - 8.48% (ロック済み)

Salvium プロトコルの長期的な成功と持続可能性は、継続的な開発と革新にかかっています。これをサポートするために、初期供給量の 8.48% が、継続的な機能強化、スマート コントラクトの統合、報奨金および助成金プログラムによる新機能の実装のために確保されています。

これらのトークンはガバナンス ウォレット内で時間ロックされ、24 回の均等な月次分割払いでリリースされます。この期間の終わりまでに、エコシステム内で生成されるシステム料金 (ガス料金) を資金源として、プロジェクトが自立することを目指しています。

3。ブロック 報酬 - 87.99%

の ブロック報酬は最初にステーカー (20%) とマイナー (80%) に分割されます。 DeFi機能が稼働すると、ステーカーはシステム手数料の一部を受け取るため、マイナーはブロック報酬の100%を受け取ることになります。

独立した監査

Salvium は、主要なアップグレードの前に独立したセキュリティ監査を受けます。監査報告書は公開され、透明性とセキュリティに対する当社の取り組みを示します。コミュニティからのフィードバックと監査結果は、継続的なプロトコルの改善に役立ちます。

サイファースタックによる起動前監査

Salvium の起動前監査は、Salvium に特有の主要なテクノロジーの数学的妥当性とセキュリティをレビューすることに焦点を当てています。

1. 「トランザクションの不均衡」メカニズム。これはチームによって設計され、「protocol_tx」テクノロジーの実装に利用されました。

2. knacc によって元々提案された「リターン アドレス スキーム」。Salvium に含まれる「protocol_tx」テクノロジーによって実装された非同期トランザクションをサポートするための適応が含まれます。

Salvium の発売前監査は、Monero セキュリティの専門家である Cypher Stack によって実施されました。Cypher Stack の暗号研究、開発、コンサルティングにおける専門知識により、当社のプラットフォームはセキュリティとイノベーションの強固な基盤の上に構築されています。

チーム

チームは幅広いコミュニティと開発者で構成されています。すべての暗号通貨愛好家は、プロジェクトの最善の利益のために行動することに尽力し、奨励されています。それぞれが持ってくる 分散型金融とプライベート暗号通貨における豊富な経験と成功の実績。

連絡先

Webサイト: サルヴィウム.io

不和: discord.gg/YJmdGcdtDt

バツ: x.com/salvium_io

GitHub: github.com/somerandomcryptoguy/salvium

寄付する: https://salvium.io/donate/

付録1

トークンの配布と規制の姿勢

続いて、暗号資産に関する欧州連合の規制、特に「暗号資産ホワイトペーパー」の要件について、以下の情報を紹介します。

1. 発行者情報: Salvium は、プライバシー重視のブロックチェーン技術の進歩に尽力する暗号通貨愛好家と開発者の分散型チームによって開発されています。
2. プロジェクトの概要: Salvium は、Monero のプライバシー機能の利点と規制遵守および DeFi 機能を組み合わせたプライバシー中心のブロックチェーンの作成を目指しています。
3. 流通および規制状況:
    - サルヴィウム（SAL）は公募を行っていない。SAL トークンの最初の配布はマイニングによってのみ行われます。
    - 総供給量のごく一部は、開発と運用をサポートするために事前に採掘されています。
    - Salvium は一般公開 (ICO) を行っていないため、現在、公募に暗号資産ホワイトペーパーを要求する EU の暗号資産規制の範囲には該当しません。
    - 現在、当社はこれらの特定の規制の対象ではありませんが、透明性を維持し、暗号通貨分野におけるベストプラクティスを遵守することに尽力しています。
4. 権利、義務、および投票: a) 権利:
    - SAL マイナーはマイニングを通じてネットワーク コンセンサスに参加し、保有者は報酬を求めてステーキングに参加し、Salvium エコシステム内のトランザクションにトークンを使用できます。
5. 義務:
    - トークン所有者は、管轄区域で適用される法律および規制を遵守する義務があります。
6. 議決権:
    - SAL トークンを保有しても、Salvium プロジェクトに対する議決権やガバナンス制御は付与されません。
    - プロジェクトの開発と意思決定のプロセスはオープンかつ協力的であり、Salvium コミュニティ全体からの貢献が歓迎されています。開発者のコア グループがプロジェクトの特定の側面を指導する場合がありますが、私たちはテクノロジーとガバナンスの両方で分散化に努めています。
7. 基盤となるテクノロジー: Salvium は Monero コードベースのフォーク上に構築されており、CryptoNote プロトコルとトランザクション不均衡 (TI) や非同期トランザクション (AT) などの追加革新を利用しています。
8. 関連するリスク:
    - 規制リスク: 仮想通貨の規制状況は急速に進化しています。Salvium は規制順守に努めていますが、将来の規制要件をすべて満たせるという保証はありません。規制の変更は、Salvium の運営、SAL トークンの使用、またはその価値に影響を与える可能性があります。ユーザーは以下の点に注意する必要があります。a) Salvium の法的地位や運営モデルに影響を与える可能性のある新しい規制が導入される可能性があります。b) 既存の規制に対する当社の解釈は規制当局の解釈と異なる場合があります。c) 最善の努力を払っても、すべての規制変更に迅速に対応できない場合があります。d) Salvium の将来の製品は、異なる規制要件の対象となる可能性があります。
    - テクノロジーのリスク: すべてのブロックチェーン プロジェクトと同様に、コードまたは基礎となる暗号原理に未発見の脆弱性が存在するリスクがあります。
    - 市場リスク: SAL トークンの価値は変動し、市場の状況に影響される可能性があります。
    - 導入リスク: Salvium の成功は、コミュニティでの導入と開発にかかっています。

この情報は誠意を持って提供されており、当社の現在の理解と計画を表しています。これは財務上のアドバイスとして考慮されるべきではありません。参加予定者全員が独自に調査を行い、必要に応じて専門家のアドバイスを求めることをお勧めします。