Bitcoin Vault ホワイトペーパー

Eyal Avramovich, Kacper Wiśniewski, Piotr Kozłowski, Radek Popiel et Anon

ホワイトペーパー v1.0

概要

2009年に、匿名の個人または開発者チームが、匿名のハッシュアドレス間での資金移動を可能にするブロックチェーンテクノロジーに基づいた、初めてのpeer-to-peerネットワークを作成しました。これがBitcoin革命の始まりです。その結果、原点であるコンセプトから一連のフォークが生まれました。

そのうちの一つが、Bitcoin Valtのコンセプトへと導きました。

私たち開発者の目的は、ウォレットアドレスの管理、個人キーと公開キーの保管、そして、個人間の資産移動を、ユーザーがさらに制御し、安全レベルをさらに引き上げることができる独自の機能で、既存のブロックチェーンをアップグレードすることでした。

分散型Ledgerの背後に存在する重要機能であるブロックチェーンの不変性は、利点だけでなく資金の紛失、誤送金、または盗難に関する危険性も伴っている事を、私たち自身の経験も踏まえて認識しました。そこで私たちは、コードと、ブロックチェーンのエコシステムにおける個人キーと公開キーの使用方法をいくつか変更することで、ブロックチェーンの不変性を損なうことなく、不可逆的取引を可逆的にするという事を思いつきました。

目次

はじめに

Bitcoin Vault（BTCV）は2019年にアルファチェーンとしてローンチされました。2019年12月から2020年11月の間に大規模な開発が行われ、ブロックチェーン上で可逆的取引を可能にするキー機能がリリースされました。

Bitcoin Vaultは、ユーザーがブロックチェーン上で作成したトランザクションをキャンセルできる世界初の暗号通貨です。この革新的な取り組みは、144のブロック（または約24時間）以内の支払いを確認するカスタマイズされたブロックチェーン・プロトコルによって可能となります。この機能は、一般的なキーの盗難、ユーザーの誤操作やエラー、バグによる資金の紛失を防ぎます。

Bitcoin VaultはBitcoinRoyaleのハードフォークで、1つの個人キーをプロセスに追加し、合計を3つにします。2019年後半にローンチして以来、2020年とそれ以降に向けて野心的なロードマップに沿い、技術的基盤とマーケットの基盤を拡大してきました。

問題提起

CipherTraceによる2020年春の暗号通貨犯罪とアンチマネーロンダリング報告書によると、2020年の最初の5ヶ月間の暗号の盗難、ハッキング、そして詐欺の合計額は13億6000万ドルにのぼりました。

暗号通貨取引所は日常的に誤ったアドレスに送金されたユーザーの資金を回復処理しなければなりません。これには多大な費用と時間を要しますが、ユーザーの資金が回復される保証はありません。

有名な詐欺アドレス、ハッカーまたは中間者攻撃型のハッカーに毎日送られている暗号資産、コイン、トークの量に関して信頼できる情報源はありません。

ユーザーの誤操作、資産の盗難、または暗号資産ウォレットに誰かが不正にアクセスをした事が発覚した直後、簡単に送信取引をキャンセルし取り消すことが可能であれば、上記の大半を回避することができると信じています。

ミッションとビジョン

BTCVはブロックチェーン上の特定のタイプのトランザクションを取り消すことができる3キー・ソリューションに基づいた、安全性の高いセキュリティを提供するために開発されました。これは、ユーザーに透明性と自由を付与する重要な機能を追加した上で、Bitcoinのすべての利便性を備えています。Bitcoin Vaultは、暗号通貨コミュニティが過去10年間直面してきた次の課題に対する答えなのです。

1. ハッキングまたはユーザーの個人キーへのアクセスによる、ウォレットへの不正アクセス
2. 暗号資産を誤ったウォレットアドレスに振り込む、振込金額の誤入力、または振込額と手数料を間違える等の人為的ミス
3. エラー、バグやその他暗号通貨のソフトウェアに関する問題

BTCVの開発は、セキュリティと安全機能、ユーザーコンビニエンスとユーザーエクスペリエンスに重点をおいています。これらは、社会の大半がグローバルな暗号コミュニティの一部になることを防ぐための重要な挑戦であると信じています。

BTCVのアプローチ

暗号通貨はユーザーに対し、P2Pネットワーク全体で資金を保管、管理、移動する方法について自由と責任を付与しました。このホワイトペーパーでは、暗号通貨ユーザー全員が個人キーと公開キーのコンセプトについて理解し、それらのキーを安全に保管し保証する方法を知っている必要があることを前提としています。

この前提に基づき、キーの管理と多様なタイプの取引の使用方法に対して、新しいアプローチを開発しました。

3キーセキュリティ・ソリューション

Bitcoin Vaultはユーザーが3つの楕円曲線DSA（ECDSA）キーを生成する必要がある3キーセキュリティ・ソリューションを開発しました。1つはアプリ内で自動的に保存され、他の2つはユーザによって管理される必要があります。Bitcoin Vaultによりユーザーは、開始されたトランザクションのキャンセルと、それを既存または新しいウォレットアドレスに戻すことができます。

ソリューションは、エコシステム内で異なる役割を担う3つのECDSAキーをサポートします。:

- スタンダード取引キーは、バックグラウンドで自動的に生成され、機能します。すべての取引の開始と、技術的問題が発生した際にウォレットの回復に必要となります。
- キャンセル取引キーによりユーザーは、144ブロックの生成後、24時間以内に取引のキャンセルを実行することができます。
- クイック取引キーを使用することでユーザーは、保安クイック取引を実行し、BTCVを数分で移動させることができます。

Bitcoin Vault エコシステム

Bitcoin Vaultのエコシステムは、BTCVの保存と管理のために社内で作成された3つのアプリで構成されています。これらを合わせることで、ハイスタンダードな安全性、透明性、自由を保証する強力なツールとなります。

Gold Wallet

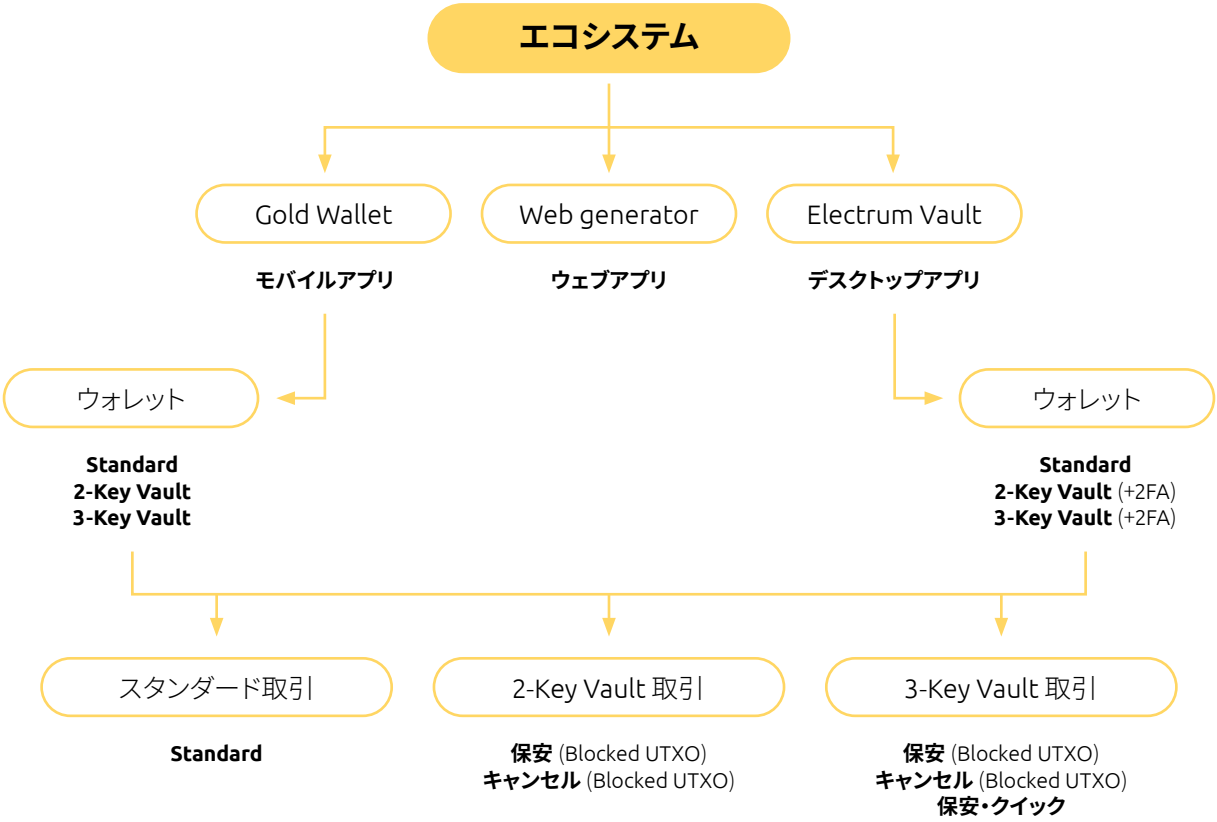
Gold WalletはBTCVを保存、送金、受取のために設計されたモバイルデバイス用アプリです。これを使いユーザーは3種類のウォレットを作成し、保安、クイック、キャンセル取引を含む多様な取引を実行することができます。Gold WalletはElectrum Vaultデスクトップアプリの2段階認証（2FA）の認証システムとしても使用できます。

Key Generator

Key Generatorはウォレットの設定と取引実行に必要な個別の公開キーと個人キーを生成するウェブベースのアプリです。ローカルリソースのみを使用するので、キー生成プロセスもキー自体と同様にユーザーのデバイスから離れることはありません。これらはどこにも保存されず、オンラインでアクセスすることはできません。キーはオフラインで保存されるため、最高レベルの安全性を提供します。

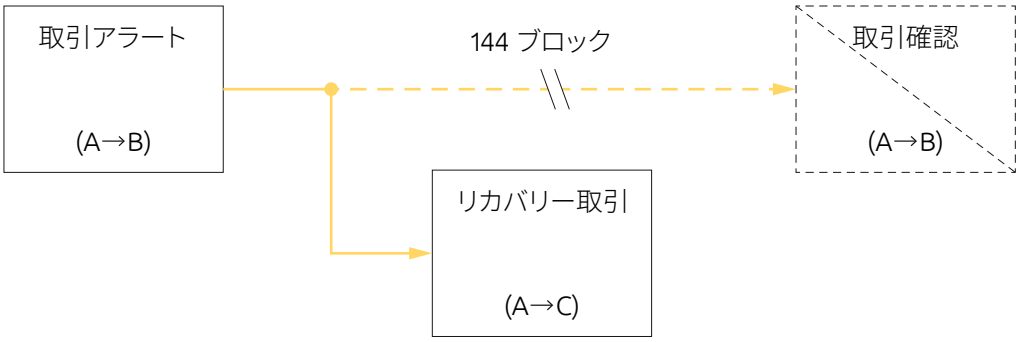
Electrum Vault

Electrum VaultはElectrumWalletをベースとしたデスクトップアプリです。Gold Walletのすべての機能を備えているので、BTCVの保存、送金、受取、ウォレットの作成および保安クイック、保安、キャンセル取引を含む取引を実行できます。

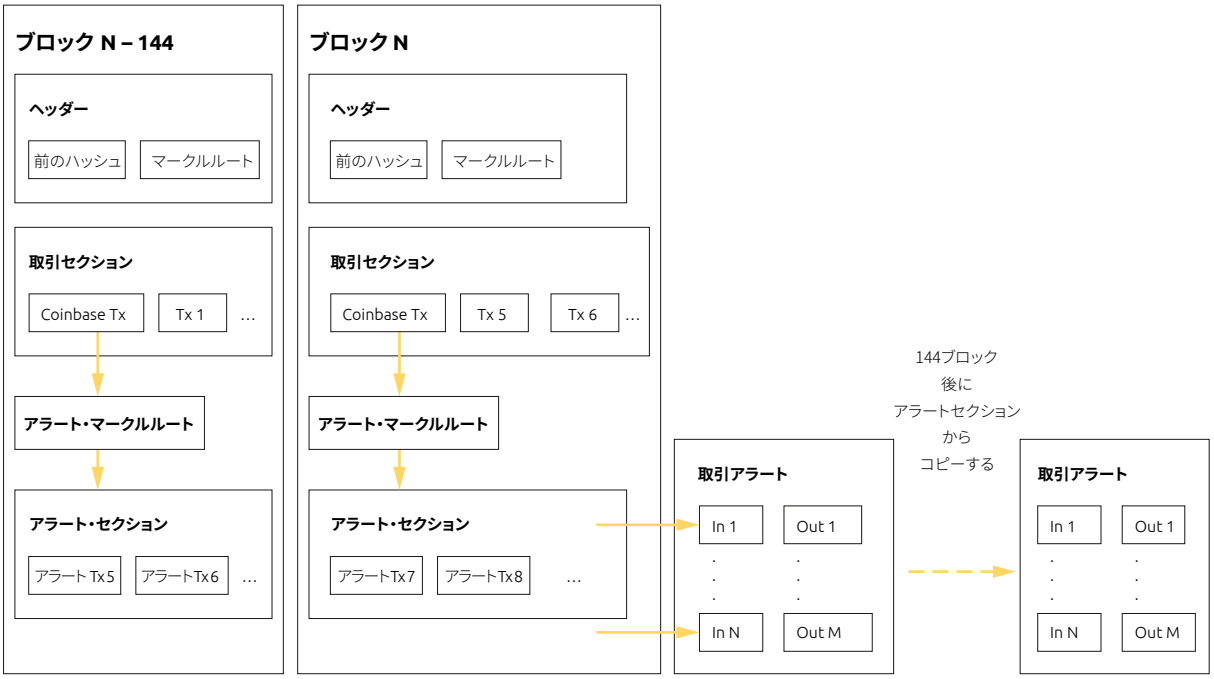


技術的概要

Locking script、144ブロックのデフォルト遅延、オンチェーンアラート取引：



BTCVブロック構造はアラートセクションを備えています（保存方法、取引のステータスがアラートから確認完了に変更された際の動作、取引のステータス変更時のマイナーによる検証方法）



取引アラートはUTXOのライフサイクルを変更します。

スタンダードバージョンでは、UTXOには未使用と使用済（基本的には移動したことを意味します）の2つの状態が存在します。Bitcoin Vaultの新しいバージョンでは新しい状態が導入されました。それは、確認完了です。これはUTXOのデータベースへの保存方法を変更します。これからは、「確認完了」の状態はUTXOがデータベースから移動され、、使用済の状態がUTXOをロックし、使用されたブロック高に関する情報を保存されている時間です。このようにして、システムは取引アラートがUTXOが移動される前に、確認完了になるのを待ちます。

確認完了を受領するまでの間に取引アラートはリカバリー取引によって回復される可能性があるため、これは必要なアプローチとなります（これはインプットとしてロックされたUTXOのみを使用します）。アプリケーション内でUTXOのライフサイクルを変更する最善の方法は、UTXOが消費された高さに関する情報を保存することです。この新しい情報によって、UTXOの状態が決まります：

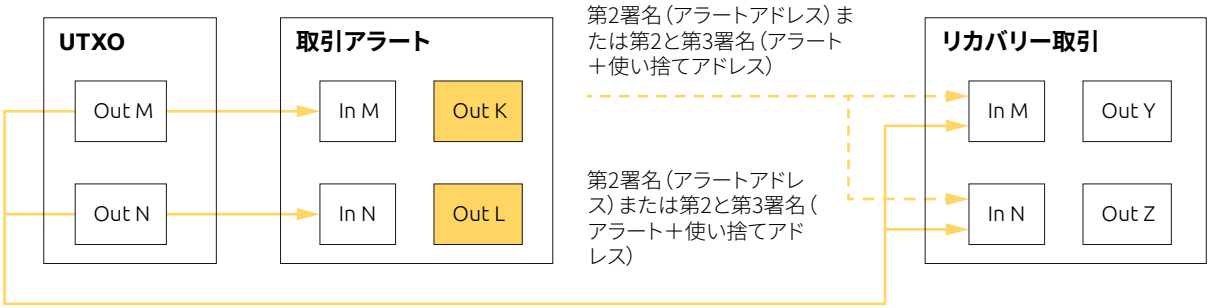
- 未使用の場合は0
- 使用済の場合は>0

また、取り消し構造でも同じ情報を考慮する必要があります。取り消しリストには様々な高さのUTXOの以前の状態の情報が保存され、チェーンの再編成が実行された際に、そのような情報が利用されます。

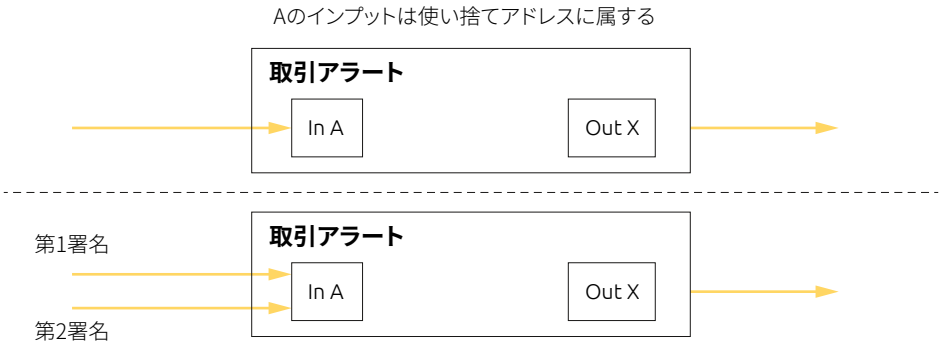
新しいUTXOの状態と取引の種類も、ユーザーに表示される残高に影響を与えます。使用済の状態のUTXOは、確認済残高に表示される新しい残高としてカウントされなければなりません。その残高は、未採掘で使用

可能な取引に関連するため、未確認の残高としてカウントすることはできません。使用はできないが、有益である残高を作成する事に意義があります。:

- 送信アラートは取引アラートによってロックされている使用済状態のUTXOがカウントされます
- 受信アラートは取引アラート確認後に利用可能となるUTXOがカウントされます



クイック取引の仕組み（それを可能にする24時間遅延の回路の説明 - マルチシグ）:



プルーフ・オブ・ワーク

Bitcoin VaultはBitcoinRoyaleのオープンソースコードに基づいたプルーフ・オブ・ワークコインです。2020年11月17日に実行されたハードフォークにより、Bitcoin（BTCV）とのマージマイニングが導入されました。

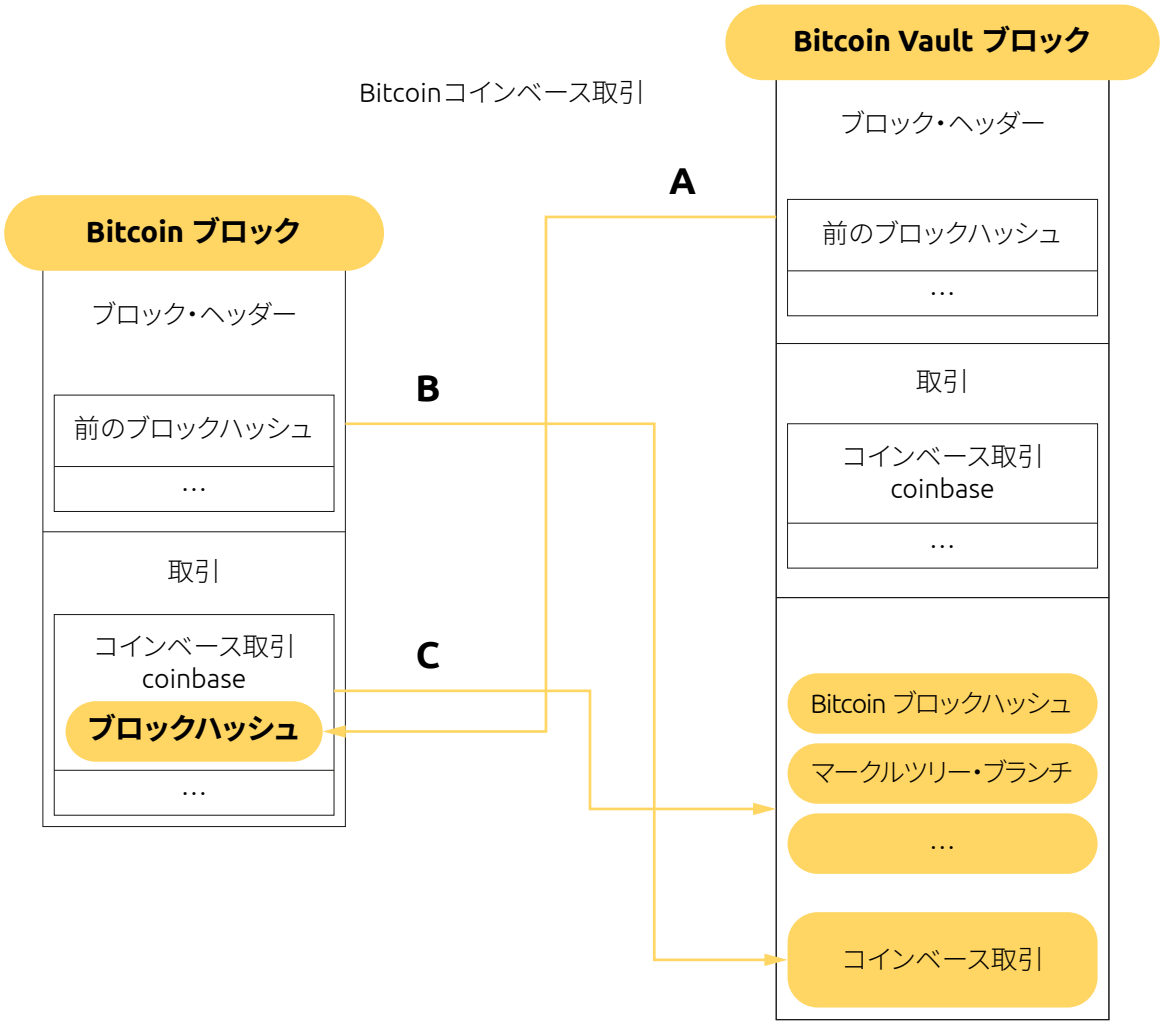
マージマイニング

ブロックナンバー58,420のBTCVプロトコルのメジャーアップデートに加え、Bitcoin Vaultもマージマイニングを承認するよう調整されました。マージマイニングは補助的プルーフ・オブ・ワークとしても知られ、マイナーが少なくとも同じ計算能力を持つ2つの異なる暗号通貨のPoWを同時に探すプロセスです。親と補助という関係をブロックチェーン間で構築するには、補助チェーンが変更のために準備されていると簡単です。

両方の暗号通貨でSHA-256ハッシュ関数を使用するため、Bitcoin VaultではBitcoinとのマージマイニングが導入されました。この場合の親チェーンはBTCで、BTCVは補助チェーンになります。

その結果、Bitcoin（親）のプルーフ・オブ・ワークソリューションがBitcoin Vault（補助チェーン）を検証するため補助的プルーフオブワーク（AuxPoW）コンセンサスメカニズムとして使用できます。

ブロック構造、BTCとBTCVブロック間の関係の図を用いた技術的説明：



プロトコルにマージマイニングを導入することにより、BTCとBTCVの両方のブロックチェーンから2つのブロック報酬を受け取れる可能性が、BTCVマイナーの動機付けとなります。より高いハッシュレートをもつBitcoinネットワークのピギーバックによって、ネットワークに追加されたハッシュパワーのおかげで、ネットワークの安全性を向上することが追加のインセンティブなのです。

ブロック報酬
Bitcoin Vaultは合計2100万コインを供給し、推定マイニング時間は10分です。

Bitcoin Vaultのブロック報酬は暗号通貨開発の初期段階で発生する特定の問題を取り除くために設計されました。特定された主な2つの問題は次の通りです：

新しい参加者を獲得するための初期段階が短すぎるため、プロジェクトの開発に必要なコミュニティメンバーに到達できない

初期段階後のブロック報酬が大幅に減少することで、マイナーがマイニング過程に参加することを妨げ、ハッシュパワーが大きく低下する可能性がある

このような脅威を抑制するために、Bitcoin Vaultは次のソリューションを提案します。

- Bitcoin Vaultのブロック報酬が高い期間を46か月に延長
- この期間をさらに9つの、6カ月毎のサブ・ピリオドに分割し、ブロック報酬の縮小を段階的に実施していく

これにより、プロジェクトの背後にいるチームは開発のための時間を十分にとることができます。コミュニティもメンバーを大幅に増やす機会があり、マイナーには初期の段階からより長期間ネットワークに参加する動機付けとなり、コインの枚数がBitcoinに追いつくために十分な時間がある一方で、ブロック報酬の大幅な減少は発生しません。

その期間中、ブロック報酬の減少は次のように予定されています：

日付	BTCV報酬縮小	サブ・ピリオド 11月	ブロック報酬	サブ・ピリオド 期間	サブ・ピリオド ブロック
2020年5月1日	175から150	1	175	6 ヶ月	29850
2020年11月1日	150から125	2	150	6 ヶ月	26600
2021年5月1日	125から100	3	125	6 ヶ月	26600
2021年11月1日	100から75	4	100	6 ヶ月	26600
2022年5月1日	75から50	5	75	6 ヶ月	26600
2022年11月1日	50から25	6	50	6 ヶ月	26600
2023年5月1日	25から12.5	7	25	6 ヶ月	26600
2023年11月1日	12.5から6.25	8	12.5	6 ヶ月	26600
2024年5月1日	6.25から3.125	9	6.25	6 ヶ月	26600

その結果、この期間中に19,687,500枚のコインが配布され、Bitcoinの4度目の半減期（推定2024年3月11日）でその枚数に到達する予定です。その後、BTCVブロック報酬は Bitcoinの半減期スケジュールに従います。

Bitcoin Vaultの開発

BTCV 開発段階:

2019年5月～2019年12月	Pre-Alpha
2019年12月～2020年9月	Alpha
2020年9月～2020年11月	Beta
2020年11月1日	Mainnet

メインネット
メインネットは2020年11月17日、58,420のブロック高でのローンチに成功しました。

ロードマップ
2020年12月、BTCV開発チームは2021年から2022年までの新しいロードマップをローンチしました。さらなるBTCVの開発は、6つのワークストリームに分割されました。

ワークストリーム No.1 – 開発アップグレード
開発ワークストリームはBitcoin Vaultに追加される全てのブロックチェーンアップグレードに関連しています。このワークストリームの主な目標は2021年末までにWrapped Bitcoin（wBTCV）をもってEthereum 2.0 を中心としたDappエコシステムに参加することです。

- 2021年Q1
  - wBTCV ERC-20 トークン – wBTCV背後の分析 & トケノミクス
- 2021年Q2
  - Ledgerの統合
- 2021年Q3
  - wBTCV ERC-20 トークンデータのテストフェーズ
- 2021年Q4
  - wBTCV ローンチ
  - DeFI エコシステムとの統合開始
- 2022年Q1
  - DeFIエコシステムとの完全統合
  - Dapp開発
- 2022年Q2～
  - Dapp開発

ワークストリーム No.2 – 安全性アップグレード

Bitcoin Vaultは内部にブロックチェーンのセキュリティ専門家チームを持っています。メインネットのブロックチェーンの整合性は何度も検証されていて、2021年の主な目標はコードの強化と、外部パートナーのサポートを受けながら、どのようなバグやホールでも特定していくことです。内部と外部のペネトレーションテスト実施後、開発チーム向けのオープンバウンティプログラムを運用し、「ホワイトハット」コミュニティと連携していきます。

- 2021年 Q1
  - フルコード監査（内部&外部）
- 2021年Q2
  - ペネトレーションテスト（内部）
- 2021年Q3
  - ペネトレーションテスト（外部）
- 2021年Q4
  - セキュリティ監査CIS/20
  - Cloud Security Matrix
- 2022年～
  - 更なるセキュリティ向上と監査
  - ハッカソン
  - バウンティプログラム

ワークストリーム No.3 – ユーザーエクスペリエンスのアップグレード

ユーザーエクスペリエンスは、製品の使用やその普及の背後にある最も重要な要素の一つです。

- 2021年Q1 & Q2
  - GoldWallet モバイルアプリ UX 改善
  - Electric Vault モバイルアプリ簡易モードと専門モードスイッチ
- 2021年Q3
  - GoldWallet ユーザー通知
- 2021年Q4
  - GoldWallet サードパーティー・アプリと統合
- 2022年～
  - 更なるUXの改善

ワークストリーム No. 4 – 製品

ITの開発とともに、パイプライン内の新製品を市場に定着させることに重点を置いています。2021年にはBTCVパートナーのサポートでステーキング製品をローンチし、BTCVエコシステムをフィアットカランシーへと繋げたいと思っています。

- 2021年Q1
  - サードパーティを通した新しいステーキング製品
  - 新しいトレーティング製品

- 2021年Q2
  - 新しい決済ゲートウェイ
  - フィアット・インテグレーション
- 2021年Q3
  - データ分析プラットフォーム（ビッグデータ）
- 2021年Q4
  - wBTCVトークン関連製品
- 2022年～
  - 新3キー機能
  - dApps製品

ワークストリーム No.5 – マーケティング活動

2021年には、BTCVの既存および未来のユーザーだけでなく、世界中の暗号通貨コミュニティを対象としたグローバルな認知とエンゲージメントキャンペーンを進めていく予定です。私たちは、BTCVブロックチェーンのセキュリティを強化し、BTCVが量子研究の先駆けとなることを可能にする新しいパートナーシップを探していきます。

- 2021年Q1
  - 新ウェブサイトのローンチ
- 2021年Q2 & Q3
  - グローバル認知とエンゲージメントキャンペーン
- 2021年Q4
  - 戦略的セキュリティパートナーシップ
- 2022年～
  - 戦略的科学パートナーシップ

ワークストリーム Np.6 – その他アップグレード

BTCVエコシステムへのいくつかの追加のアップデートによって、よりコミュニティと繋がり、絆を強め、2021年の第2四半期の初めに開始される新しいエアドロップメカニズムを通じて、Hodlerに新しいオプションを提供したいと考えています。長期的にはクウォンタム・コンピューティングと、それがブロックチェーンの暗号に与えうる影響力に重点をおきます。

- 2021年Q1
  - 新しいエアドロップメカニズムの開発とローンチ
  - Airdrops wallet のロック
- 2021年Q2
  - エアドロッププラットフォーム／アプリ
- 2021年Q3
  - ブロックチェーン分析プラットフォーム
- 2021年Q4～
  - 量子研究
  - 科学パートナーシップ助成プログラム

量子コンピューティングとDLT – 私たちのビジョン

私たちはブロックチェーンの開発チームとして、量子技術の進歩に非常に関心を持っています。ブロックチェーンのような分散型レジャーテクノロジー（DLT）に取り組んでいる研究者や開発者は、すべてのブロックチェーンのソリューションに不可欠な公開キー暗号とハッシュ関数に依存しています。

Bitcoin VaultブロックチェーンはECDSAやSHA-256などの強力な暗号化アルゴリズムによって保護されています。これらはBitcoinやその他多くの暗号通貨でも使用されています。現在使用されている暗号化アルゴリズムは、従来の計算方法に対しては十分強力です。

量子コンピューティングの脅威

理論上は、量子技術で計算能力を飛躍的に改善していくと、公開キーを解読して個人キーハッシュを計算したり、SHA-256アルゴリズムを破ってブロックチェーン上に必要なワンタイムハッシュ値ブロックを取得できるようになります。この分野の専門家によると、私たちは安定した量子コンピュータの開発からまだ数年しか経っていません。それでも、特定の暗号化アルゴリズムを解読するために、これらのコンピュータを適切に暗号化する必要があります。

量子コンピューティングの機会

脅威ではなく、機会に焦点を合わせたいと思います。

繰り返しになりますが、理論的には量子コンピュータが信頼できる計算を行うのに十分な安全性を確保できれば、それらを使用して暗号化アルゴリズムを改善することができます。これが、私たちが考えるブロックチェーンの未来です。

現在、量子プルーフコインの目標を達成するための様々なアプローチについて考えることができます：

- 格子ベース暗号システム
- マルチバリエイト・ベース公開キー暗号システム
- 超特異楕円曲線同種暗号システム
- ハッシュベース電子署名暗号システム
- Googleが実施したテストに似たハイブリッドソリューション（CECPQ1およびCECPQ2）
- その他

適切なアンチ量子ソリューションを見つけ、ポスト量子時代に向けてBTCVコインを準備するために、開発チームは必要なオン・キー圧縮技術と特定の型のコード及び暗号化技術に関してさらに調査を行う必要があります。

それにも関わらず、今日ではサイズの小さいキー、短い署名/ハッシュサイズ、高速実行、低い計算難易度、そして低いエネルギー消費を全て同時に提供できるポスト量子ブロックチェーンアルゴリズムは存在しません。これらの要素は、IoTで使用されているような資源制約付きデバイスにとって特に重要となります。

今後3〜5年間で私たちBTCV開発者は、特に多様な企業、新興企業、工科大学の専門家と新しいパートナーシップを通して、量子体耐性を運用できる準備をすることに重点を置いています。

Bitcoin Vault の創設者

Bitcoin Vaultはアジアとヨーロッパにある暗号通貨マイニング施設の世界有数のオペレータであるMinebestのCEO、Eyal Avramovichによって設立されました。

Minebestについての詳細はこちらからご覧いただけます: https://minebest.com/

公式ウェブサイトにてBitcoin Vaultのチームに関する詳細をご覧いただけます: https://bitcoinvault.global/

関連事業

Bitcoin Vaultの開発に繋がったコンセプトとアイディアに関して、BitcoinRoyaleの創設者に感謝いたします。

Bitcoin Royale ホワイトペーパー: https://bitcoinroyale.org/bitcoinroyale.pdf

BTCV 情報源:

プロジェクトに関する詳細はこちらからご覧いただけます:

https://bitcoinvault.global/
https://twitter.com/vaultbitcoin
https://medium.com/bitcoin-vault-btcv
https://t.me/Bitcoin_Vault
https://www.facebook.com/bitcoinvaultofficial
https://www.instagram.com/bitcoinvaultofficial
https://www.youtube.com/c/BitcoinVault

参考文献

1. Bitcoin Whitepaper, Satoshi Nakamoto, https://bitcoin.org/bitcoin.pdf
2. Bitcoin Royale: Peer-to-Peer No-Theft Electronic Gold, Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
3. Cryptocurrency Anti-Money Laundering and Crime Report, Spring 2020, https://ciphertrace.com/cryptocurrency-anti-money-laundering-and-crime-report-spring-2020/
4. The Chainalysis 2020 Crypto Crime Report, https://go.chainalysis.com/2020-Crypto-Crime-Report.html
5. Bitcoin, crypto-coins, and global anti-money laundering governance, Malcolm Campbell-Verduyn, https://www.researchgate.net/publication/322596368_Bitcoin_crypto-coins_and_global_anti-money_laundering_governance
6. Namecoin project, https://www.namecoin.org/
7. Bitcoin Wiki, Merged Mining Specifications, https://en.bitcoin.it/wiki/Merged_mining_specification
8. Adam Back, Hashcash – A Denial of Service Counter-Measure, http://www.hashcash.org/papers/hashcash.pdf

9. Phil Daian, Rafael Pass, Elaine Shi; Snow White: Robustly Reconfigurable Consensus and Applications, https://eprint.iacr.org/2016/919.pdf
10. Wrapped Tokens A multi-institutional framework for tokenizing any asset https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf
11. Smart Contract Extensibility with Wrapped Tokens https://yos.io/2019/07/13/smart-contract-extensibility-wrapped-tokens/#:~:text=Wrapped%20Tokens%20is%20a%20design,two%20versions%20at%20any%20time.
12. Aleksei Pupyshev, Ilya Sapranidi, Elshan Dzhafarov, Shamil Khalilov, Ilya Teterin, Graviton: interchain swaps and wrapped tokens liquidity incentivisation solution, https://arxiv.org/ftp/arxiv/papers/2009/2009.05540.pdf