ビットコインボルト：ピアツーピアの盗難防止電子ゴールド

Eyal Avramovich
github.com/bitcoinvault

概要サトシ・ナカモト氏のBitcoinにおける最初のビジョンは、電子現金ーのピアツーピア版を作ることであった。成功したプロトコルのフォークの大半は、このビジョンをさらに改善し、よりスケーラブルで効率的な決済システムの提供を試みている。我々は、ビットコインの最大の可能性を、交換媒体としてではなく、価値の貯蔵庫として、現金ではなくゴールドのより良い形としてとらえている。それで当社は、価値の究極的な電子的貯蔵庫を作成することにより、この約束を達成することを目的とした、オリジナルプロトコルに対する一連の修正を提案する。ビットコインの有効な取引確認時間を、10分から24時間に増やすことで、ゴールドの一形態としてのビットコインの最大の欠点である、盗難に遭いやすいという問題に取り組むことができる。このシステムは、コーヒーの代金を支払うためのものというよりも、完全な安心感を持って生涯のための貯蓄をすることに重点を置いている。すべてのトランザクションはチェーン上で144個のブロックで警告が発せさられ、以前は使用されていなかった修復キーを使用して緊急時にキャンセルすることが可能である。このシステムのブートストラップはハードフォークではなく、迅速なマイニングのより公平なメカニズムを介しており、システムは短期間でビットコインに追いつくことができる。我々は、盗難に遭うことのない電子ゴールドというビジョンを生み出したBitcoin Royaleのホワイトペーパー [1] の作成者を賞賛したい。チームとしてさらこのアイデアを進め、以下に述べるすべての重要な機能の実装を開始し、パラグラフ6.2で追加機能として明らかにされている3番目の秘密鍵ソリューションを使用して、我々はこれをさらに高度なものにしたいと考えている。

1. はじめに

ビットコイン [2] は、実績ある金融機関を介さずとも直接取引ができるようにするために、2009年にローンチされた革新的な分散型決済システムである。このシステムは、信頼できるオペレーターを介さずに分散型台帳を維持するためのPoWに依存しており、正直なノードが攻撃者ノードのどの協力グループよりも多くのCPU能力を制御している限り、安全なものである。ビットコインは元々、その生みの親であるサトシ・ナカモトによって「電子現金システム」として説明されていた。

ビットコインのコードベースのフォークの形で、元のプロトコルの修正が何度も成功し、これまで何年にもわたってリリースがなされてきた。例えば、2011年にローンチされたLitecoin [3] は、取引確認時間を短縮し、GPUのようなコンシューマグレードのハードウェアを優先するようにPoWのアルゴリズムを変更した。2017年にローンチされたBitcoin Cash [4] は、ブロックサイズを増やすことで元のプロトコルのトランザクションスループットをスケールアップしている。Bitcoin Gold [5] も2017年に設立され、ハッシュアルゴリズムの変更によって特殊なマイニング装置を時代遅れのものにした。

当初のビジョンに忠実に、これらおよびその他のフォークの主な焦点は、ビットコインをより良いキャッシュのシステムに改善していくことである。高い取引手数料、10分の確認時間、1秒間にわずか4つの取引のみというおおよそのスループットといった、オリジナルのプロトコルの制限が、今日支配的な集中型オンライン決済システムと競争するビットコインの能力を妨げるものとなっている。

2. 電子現金か電子ゴールドか

ビットコインが電子現金として消費者に採用されてもあまり成功しなかった一方で、ビットコインは電子ゴールドの一形態としてはかなりの成功を収めてきた。ビットコインが交換媒体として優れているのか、それとも実際には価値の貯蔵手段として優れているのかについて、業界では長い間議論されてきた。ゴールドは日々の商品やサービスに対する効果的な支払い手段ではない。消費者は、インフレのリスクを見据え、将来の購買力を維持するため、主にゴールドに投資する。各国の通貨とは異なり、ビットコインはは固定的な金融政策と限られた供給量のため、この点では特に魅力的なものといえる。

歴史を見ればわかることだが、、システムが一度にいくつかの競合する目標を達成するように設計されることはほぼあり得ない。ビットコインをより良い交換媒体として最適化させることは、結果として価値の貯蔵手段としてビットコインが持っている可能性を減少させてしまう。同様に、有用な電子現金に必要な特性をさらに犠牲にすることで、電子ゴールドとしての有用性を大幅に向上させることができるのだ。この論文では、究極の価値の貯蔵庫を作るという一つの目標に焦点を当てて、オリジナルのビットコインプロトコルに一連の修正を提案している。

オンライン決済システムとして競争することをもはや優先しないのであれば、取引手数料や取引スループットに焦点を当てる必要はない。結局のところ、金は輸送コストが高く、通常は長期投資のために取得されるものである。当社の取り組みに特に関係のある特性とは、トランザクションが確定するまでの時間なのである。ビットコインの平均10分の確定時間を大幅に延長するなど、この点でのトレードオフは、基本的な利点をもたらす可能性がある。いずれにせよ、10分以内に各地に金の出荷が行われることはそもそも期待されていないため、この犠牲は当然のことと考えることができるだろう。

3. 盗難という問題

価値を貯蔵するという点において最重要となる要件は堅牢な永続性である。盗難は、価値のあるものを扱う際に生じる損失の主なリスクの一つである。ゴールドはこの点、かなり優れているといえる。金の物理的な窃盗は、電子資産に対する仮想的な攻撃よりも、実行するにはかなり高いリスクを冒さなければならない。さらに窃盗犯は、当局の目からその盗み出した大量の金を隠す困難なに直面しなければならない。これは、国境を越えてそれを行うときに特に顕著な問題となる。盗んた金を匿名で大量に洗浄し、清算することも簡単なことではないだろう。

残念なことに、ビットコインはこの点でかなり劣っていると言わなければならない。資金は暗号化された秘密鍵のセットでプロトコルによって保護されている。これらの鍵への電子的アクセスを得ることで、攻撃者はリモートで、即座に、そして取り返しのつかない方法で、すべての資金を奪うことができる。また、盗み出した資金の洗浄も非常に簡単である。なぜならトランザクションは偽名で行うことができ、トレーサビリティはミキサー [6] の使用により中断され、SybilのIDを大量に作成することができるからである。その結果、2018年には10億ドル以上が盗まれており、仮想通貨の盗難は増加傾向となっている[7]。コミュニティにより作成された主要なインシデントのリスト [8] は、最新のセキュリティ慣行に精通した専門機関でさえ攻撃を受けやすいことを示している。

エンドユーザーによる秘密鍵の安全な管理が、ビットコインの大きな課題の1つであることが明らかとなっている。鍵は資金とやり取りするために定期的に使用されなければならず、署名されたトランザクションはインターネット上で送信されなければならないため、最終的にはすべての鍵は脆弱なものとなってしまう。「ホット」ウォレットと「コールド」ウォレットの間で資金を分割するようなセキュリティを意識したプラクティスには非常に複雑なものとなるため、根本的な問題を解決することができない。インシデントを見れば、ホットウォレ

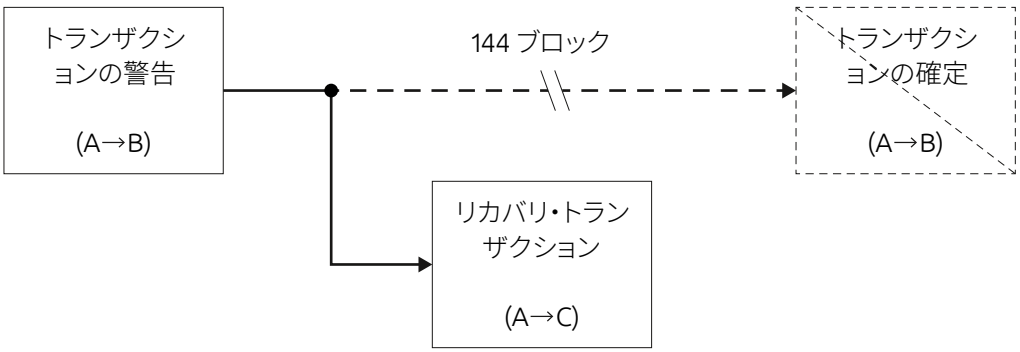
ットが不可避的にかなりの量[9, 10]を保持せざるを得ず、コールドウォレットを使用したところで鍵とのインタラクションを減少させるだけで、それが完全には排除されないことは明白である [11] 。

4. 盗難防止ソリューション

盗難を排除する手段として、我々は新しく洗練されたロックスクリプトとプロトコルの変更に基づいたソリューションを提案する。新しいロックスクリプトを使用して実行されたトランザクションは、デフォルトで24時間遅延されるものである。採掘者が新しいブロックにトランザクションを追加すると、そのトランザクションは直ちにコミットされなくなる。代わりに、144ブロック（ブロック時間を10分と仮定）の間、そのことが警告としてオンチェーンに追加されることになる。144ブロックの間放置しておけば、トランザクションは警告の状態から「確認済み」へと変わる。

オンチェーンアラートのメリットは、コインの所有者は、コインが移動されるたびに、検閲不可能な事前通知を受け取ることができるということだ。所有者は警告に基づいて行動するまで24時間の猶予があり、不正な場合には転送を上書きすることが可能である。引き出しを遅らせることは、カストディアル・ウォレットや従来の銀行システムでは、盗難防止の業界標準として実証済みだ。一例として挙げるならば、Coinbase Vault [12] の待機時間は48時間である。我々が提案するソリューションは、信頼できる第三者を介さずとも同様の保護を提供することができる。

警告状態にあるトランザクションの緊急オーバーライドは、特別なリカバリ・トランザクションを必要とし、24時間の遅延の影響を受けることなく即座に実行される。リカバリ・トランザクションには、ウォレットの作成時にロックスクリプトに組み込む必要がある特別な回復鍵が必要となる。回復鍵が指定されたウォレットに登録されると、それを変更することはできなくなる。



緊急オーバーライドに使用される秘密回復鍵は、これまで使用されたことのない新しいキーになるように設計されている。この鍵はオフラインでの生成が可能であるが、インターネットに接続したり、デバイスに入力したりしてはならない。登録プロセスでは、この鍵の公開部分のみを必要とするため、秘密鍵を確実に未使用のものとすることができる。時折使用することは避けられず、そのため盗難に遭いやすいコールドウォレットキーとは異なり、回復鍵は緊急時のオーバーライド自体で初めて使用されるため、盗難防止をより完全なものとすることができるのである。回復鍵が一度使用されることで、その鍵は侵害されたものとみなされ、すべての資金は、未使用の回復鍵で保護されている新しいウォレットにただちに転送されることとなる。

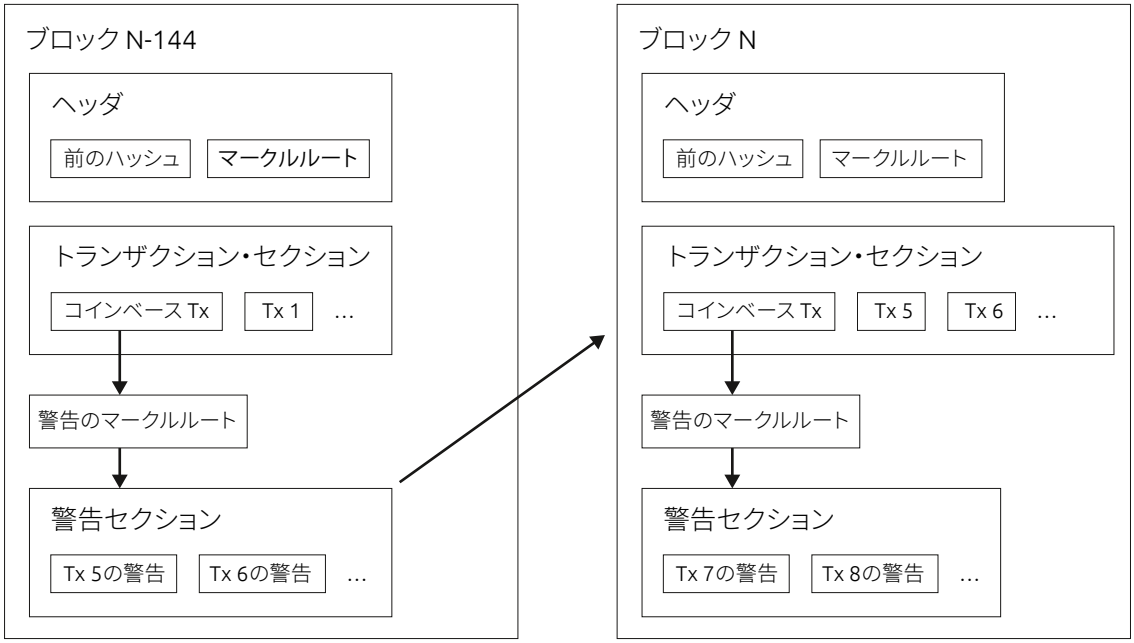
このオリジナルのデジタルゴールドというBitcoin Royaleのコンセプトでは、システム内のすべての取引を24時間遅らせることを想定しており、それが貯蔵所を安全かつ動きのゆるやかなものとしている。我々はこのコンセプトを拡張して、デジタルゴールドとデジタルキャッシュという2つの世界の最良の部分を、セキュリティの中に妥協することなく統合していきたいと考えている。

動きのゆるやかなアラートに加えて、我々は動きの速い「インスタント」取引を、一定の条件のもとに維持してゆく。最高のセキュリティを提供するために、このようなトランザクションを送信するには、ウォレットの作成時に提供される3番目の鍵を使用して、ブロックチェーン・ベースの2 FAを実行することが必要となるであろう。

5. ブロック

オリジナルのBitcoinプロトコルと同様に、すべてのブロックには確認済みのトランザクションのリストが含まれており、ヘッダにはこれらのトランザクションのマークルルート・ハッシュが保持されている。一部のトランザクションはオンチェーンで24時間待たなければならないため、ブロックのトランザクション・セクションにすぐに追加することはできない。その代わりに、オリジナルのビットコインのプロトコルには存在しなかった新しい特別なセクション、つまり警告セクションに追加される。警告セクションのマークルルート・ハッシュは、オリジナルのビットコインとのブロックヘッダ互換性を維持しながら、コインベース・トランザクションの入力に格納される。

新しいブロックが採掘されると、採掘者は144ブロックをさかのぼり、ブロックN-144の警告セクションを調べる。まだ有効なトランザクションの警告はすべて確認済みとなり、新しいブロックのトランザクション・セクションに入力される。



ブロック Nの採掘ステップは以下の通り：

1) ブロック Nの警告セクションに新しい通常のトランザクションを追加する（未確定）
2) ブロック Nのトランザクション・セクションに新しいインスタント・トランザクションを追加する（確定済み）
3) ブロック Nのトランザクション・セクションに新しい通常のトランザクションを追加する（確定済み）
4) ブロックN-144の警告セクションに移動し、ブロックNのトランザクション・セクション（確認済み）に有効なトランザクションを追加する。

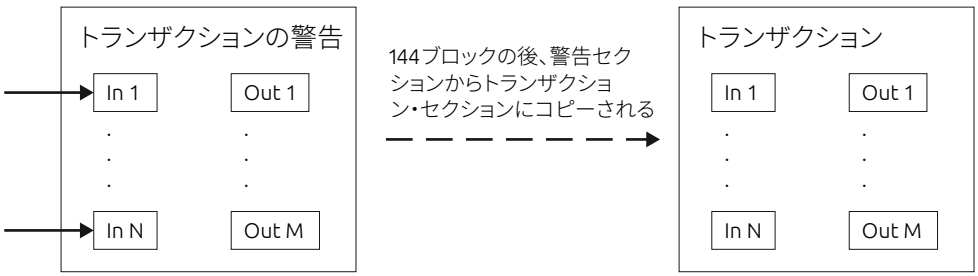
6. スクリプト

Bitcoin Vaultのコア機能は、高度なロックスクリプトを通じて利用可能であり、アンロックスクリプトで提示された署名の数に応じて動作が異なるというものである。以下の2つのバリエーションが用意されている：

1. 警告ロックスクリプト ― 1つまたは2つの署名を必要とする。1つの署名が提示されると、警告トランザクションが生成される。2つの署名が提示されると、リカバリ・トランザクションが生成される。
2. 警告＋インスタント・ロックスクリプト ― 1つ、2つ、または3つの署名いずれかを必要とする。1つの署名が提示されると、警告トランザクションが生成される。2つの署名が提示されると、警告トランザクションが生成される。3つすべての署名が提示されると、リカバリ・トランザクションが生成される。

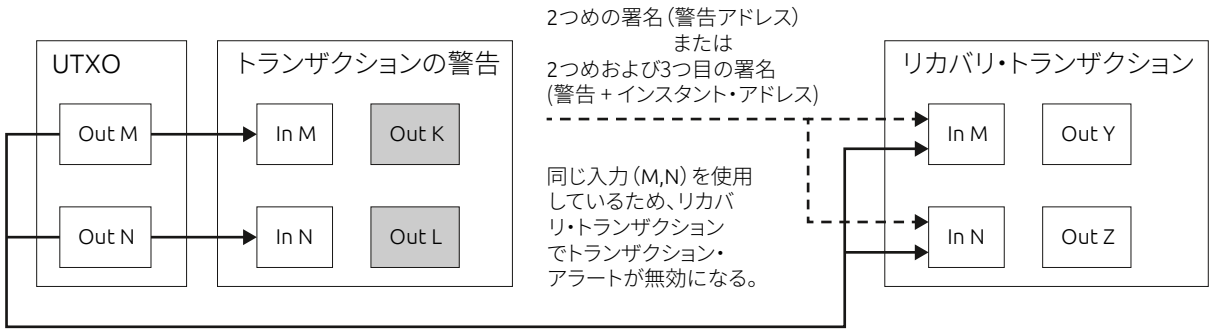
7. トランザクション

コインの転送は、ビットコインのプロトコルと同じ通常のトランザクションを使って行われる。警告セクションからトランザクション・セクションに移動しても、フォーマットは変わらない。



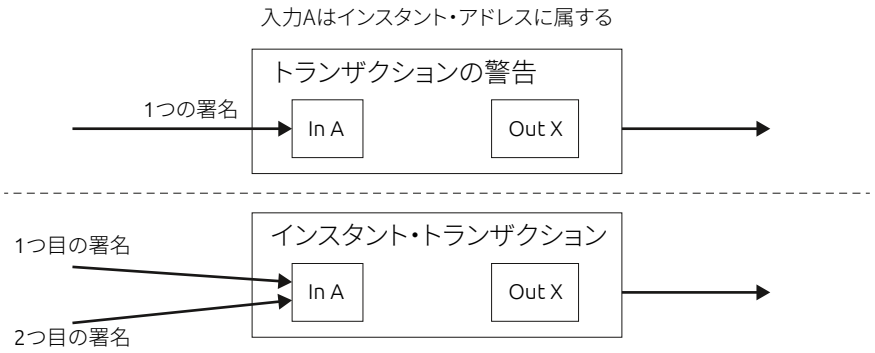
7.1. リカバリ・トランザクション

リカバリ・トランザクションは、リカバリされたアラートと同じUTXOを消費する。その違いは、同じUTXOに対してより多くの署名を提示することである：警告ロックスクリプトの場合は2つ、アラート+インスタント・ロックスクリプトの場合は3つである。リカバリ・トランザクションが処理されると、回復したUTXOが消費されるため、このUTXOに依存している既存の警告が無効となり、24時間の遅延を超えて確認されるのを防ぐことができる。



7.2. インスタント・トランザクション

インスタント・トランザクションでは、取引確定のためのデフォルトの24時間の遅延を回避し、取引確定を約10分に短縮することができる。そのメカニズムはmultisig（マルチシグ）ウォレットのそれに類似している。これは、別の場所に安全に保存されなければならない別の秘密鍵からの追加署名を必要とする。そのため、インスタント・トランザクションは特別なP2SHアドレス、つまりア警告 + インスタント・ロックスクリプトから生成されたインスタント・アドレスからのみ送信することができる。



8. 互換性

我々の設計は、オリジナルのビットコインのプロトコルと可能な限りの互換性を持ったものにすることを試みている。基本的な目標としては、既存のビットコインのフルノード、ウォレット、プール、採掘者への必要なコード変更を最小限にすることである。ただし、既存のブロックチェーン上で変更を行う場合は、ハードフォークが必要となる。

ブロックヘッダのフォーマットが変更され、コインがビットコインASICマイナーと互換性がなくなるのを避けるために、警告セクションのマークルルート・ハッシュは、標準のコインベース・トランザクションの入力に格納される。

もしハードフォークが必要な場合、既存のコインユーザーにとって可能な限り簡単に移行できるようにすることが我々の目標である。既存のスクリプトタイプはすべて動作を変更しないため、ハードフォークの前に存在していたコインはすべて通常の方法で使用することが可能である。しかしながら、我々としてはより安全な新しいスクリプトに切り替えることを強く推奨する。

9. インセンティブ

このシステムは、過去10年間で成功の実績を持つビットコインのインセンティブモデルを利用している。警告の組込みには、このモデルに若干の変更を加えることが求められる。採掘者は、アウトプットとインプットの価値の差から計算された手数料が得られるとの約束に基づき、ブロックにトランザクションの警告を含めることでインセンティブを与えられる。料金は将来のブロック・トランザクションから計算され、トランザクションの警告を含むオリジナルの採掘者に分配される。

採掘者は以後も、新しいブロックを採掘したことに対するブロック報酬、新しいインスタント、登録およびリカバリ・トランザクションからのすべての手数料、およびトランザクションの警告に基づく将来の手数料の約束を引き続き受け取ることができるのである。採掘者は、N-144ブロックから回収されたものを除くすべての警告を、トランザクション・セクションに含めることがコンセンサスルールによって義務づけられている。

警告が解除された場合、警告の元の採掘者の手数料は回収不能であり、合計コストは元の警告の手数料に回収取引の手数料を加えたものとなる。

10. 関連する作業

我々は、MalteMöserらのBitcoin Covenants [13] に関する研究はとりわけ感銘を受けている。彼らのビットコイン・スクリプト言語の拡張は、将来のコインの使用に関する制限を可能にし、様々なセキュリティ対策を実装するために使用することを可能にするものである。その主要なものとして、遅延引き出しメカニズムであり、我々の提案するボルト取引はそれに類似するものである。

我々は、ウォレットによって実装されるカスタムスクリプトの再帰的配列を必要としない、よりシンプルな実装を選択した。我々が提言しているのは、オプションの拡張ではなく、トランザクションに広く強制的な影響を与えるプロトコルへの根本的な変更なのである。これにより、実装の負担を採掘者に移し、エンドユーザーのトランザクション体験をデフォルトと同じにすることで、真の電子ゴールドを創造するという我々の使命をよりよく遂行することが可能になるであろう。

参考文献

1. Ian Duoteli Fleming, https://bitcoinroyale.org/bitcoinroyale.pdf
2. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://www.bitcoin.org/bitcoin.pdf, 2008.
3. Litecoin Project, “Litecoin, open source P2P digital currency”, https://litecoin.org, 2014.
4. “Bitcoin Cash”, https://www.bitcoincash.org, 2018.
5. bitcoingold.org, “Bitcoin Gold”, https://bitcoingold.org, 2018.
6. J. H. Ziegeldorf, F. Grossmann, M. Henze, N. Inden, and K. Wehrle, “Coinparty: Secure multi-party mixing of bitcoins”, In: *CODASPY ’15*, 2015.
7. CipherTrace, “Cryptocurrency Anti-Money Laundering Report, 2018 Q4”, https://ciphertrace.com/crypto-aml-report-2018q4, 2019.
8. “BLOCKCHAIN GRAVEYARD”, https://magoo.github.io/Blockchain-Graveyard, 2019.
9. C. Zhao, “Binance Security Breach Update (May 7 2019)”, https://binance.zendesk.com/hc/en-us/articles/360028031711, 2019.
10. J. Buck, “Coincheck: Stolen $534M In NEM Were Stored On Low Security Hot Wallet“, https://cointelegraph.com/news/coincheck-stolen-534-mln-nem-were-stored-on-low-security-hot-wallet, 2018.
11. J. Preissler, “Important Notice: Only trade TIO on trade.io”, https://medium.com/@trade.io/important-notice-only-trade-tio-on-trade-io-823d59fd7104, 2018.
12. KM. Cutler, “Coinbase Launches A More Secure Bitcoin Storage Option Called ‘Vault’”, https://techcrunch.com/2014/07/02/coinbase-vault, 2014.
13. M. Möser, I. Eyal, E. Gün Sirer, “Bitcoin Covenants”, In: *Financial Cryptography and Data Security, FC 2016, Lecture Notes in Computer Science*, Vol. 9604. Springer, Berlin, Heidelberg.