暗号通貨カストディアンのキーマネジメントの実用的分析

Yuto Takei
Mercari, Inc., and
Tokyo Institute of Technology

Kazuyuki Shudo
Kyoto University

概要-暗号通貨のキーマネジメントについて、セキュリティとリスク管理の観点から考察する。財布の実装とセキュリティに関する先行研究は数多く見受けられたが、複雑なシステムとしての実世界の統合を包括的に分析したものはほとんどない。特に暗号通貨のカストディアンは、規制要件だけでなく、ビジネスニーズを満たすためのリスクを厳しく管理しなければならない。個々のユースケースとは異なり、様々な資産を相当量管理するために、一般的には、ホットおよびコールドウォレットの複数のレイヤーと異なるタイプの実装の組み合わせなど、より複雑なウォレット構成と操作が必要です。そこで、ソフトウェア、ハードウェア、HSM、スマートコントラクト、暗号方式など、様々なウォレット技術の適合性について議論する。また、先行研究で言及された管理者に対するいくつかの未解決の課題にも対処している。さらに、究極の例として、エアギャップ環境における参照用コールドウォレットであるExtreme-Coldを提案する。先行研究で研究されたサイドチャネル攻撃に対して耐性がある。Extreme-Coldで行ったリスク評価は、我々の体系化された知識の有効性を実証している。

索引用語-暗号通貨、ウォレット、セキュリティ、暗号、鍵管理システム、デジタル署名

I. Introduction

暗号通貨は金融資産として世界的に人気を集めており、2021年から2024年の間に時価総額が1兆円を超えることがよくあります。暗号通貨の所有者は、取引を開始するために不可欠な秘密鍵を効果的に管理する必要があります。この目的は、取引所や決済サービスプロバイダーなどの暗号通貨の管理者にとって、彼らが扱う資産の規模が大きいことを考慮すると、さらに重要になります。

暗号鍵の管理は、暗号通貨が生まれる以前から長い間研究されてきました[1]。暗号鍵の複製による損傷や喪失を防ぐための措置と、鍵の漏洩や不正使用を防ぐための暗号化や認証を強化するための措置の間にジレンマがあることが知られています[2]。したがって、暗号鍵の取り扱いを担当する組織は、バランスを取り、適切に投資する必要があります。

暗号通貨の文脈における秘密鍵の管理に関する研究は数多くあるが[3]、これらの研究の多くは、個人に適したウォレットに焦点を当てたものである。ある研究者はウォレット実装を提案し、他の研究者は既存のウォレットに対する攻撃方法について議論している。

しかし、暗号通貨のカストディアンを考慮する場合、スタンドアロンウォレットの視点だけでなく、物理的要素や人的要素など、より広い要因も考慮する必要がある。さらに、ウォレット管理に関連するビジネス環境は、特定のケースで考慮されなければならない。Jarouchehらは、トークン分類とウォレット技術を取り上げ、カストディアンの観点からレビューを実施した[4]。彼らの研究では、規制の違い、未知のセキュリティリスク、ウォレット実装の透明性、コストなど、ウォレット技術におけるいくつかの未解決の課題を浮き彫りにしました。著者が所属する暗号通貨カストディアンを含め、多くの暗号通貨カストディアンは、既存の広範な研究文献がない場合でも、現実にこれらの考慮事項に遭遇し、議論を行っています。

そこで、本論文では、暗号通貨カストディアンシップの実用性を検証し、秘密鍵管理のための効果的な実践に関する文献のギャップを埋めることを目的とする。

本論文の主な貢献は以下の通りである。

- 暗号通貨が出現する以前から暗号鍵管理に関する文献を調査し、ウォレット技術との関連性を探る。
- 企業規模でウォレット技術を検証し、相当な資産を管理し、そのセキュリティを分析する。
- 取引所に共通する、ホットとコールドのような複数のウォレットにまたがる管理戦略を検討する。
- 参照用コールドウォレット実装E XTREME -C OLDを提案し、この実装に基づく実際のリスク分析を行う。

本論文の構成は以下の通りである。セクションIIでは、まず、暗号鍵管理技術の歴史的な発展について、過去の文献から一般的なインターネット産業における最近のアプローチに至るまで、概説する。セクション III では、暗号通貨カストディアンの署名システムをモデル化し、そのセキュリティと潜在的な脅威を評価するための様々なアプローチを検討する。セクション IV では、ソルベンシーや監査といった暗号通貨取引所特有の要件について検討する。セクション V では、各技術に関連する強み、弱み、特徴、およびリスクを分析し、異なるウォレットオプションを探ります。セクション VI では、暗号通貨カストディアンにおける新規ウォレット構築の評価基準について述べる。セクションVIIでは、リスク管理の透明性を高めるために、非常に安全で自己管理された環境で動作する、E XTREME -C OLDと呼ばれるコールドウォレット構成をデモのために提案する。

第 VIII 章では、先に提案した観点に基づき、E XTREME -C OLD の評価を行う。最後に、セクション IX で、研究の将来の方向性を示すことで、結論を述べる。

II. Background

A. 暗号鍵管理の成り立ち

暗号通貨が発展する以前から、暗号鍵管理は大きな関心事であった。当初は主に軍事的な目的のために研究されていた。コンピュータの台頭により、キーマネジメントの重要性がさらに明らかになった。これは、1970年代以前の文献から明らかであり、現在でも関連性がある。

Popekらの研究では、1979年に様々な暗号技術が、その応用や関連する問題とともに、当時知られていた[5]。彼らは、暗号システムをシンプルに設計することの重要性に言及した。また、キーバックアップの必要性と、オリジナルと同様に安全性を確保するための保護についても強調しました。同年、Blakleyは、キーマネジメントへの人間関与に関連する事件を、疑惑、裏切り、合併の3種類に分類しています。彼らは、組織が保護要件に基づいて保持すべき重要なコピーの数を定式化した[2]。さらに、Shamirは秘密値を複数の当事者に安全に分配する方式を導入し、現在広く利用されている[6]。その後、Fumy らは、主要な管理サービス(KMS)を設計するための体系的なアプローチを提供した[1]。彼らは、キーのライフサイクル全体を通して、生成、配布、活性化、削除などの技術的な要件について議論しました。また、秘密鍵への平文アクセスを禁止することの重要性を強調した。

金融分野では、主要な管理手法の必要性から、1985年に米国の銀行業界の実務家によってANSI X9.17が編集された。この規格では、手動と自動の両方のプロセスについて、主要な管理手法と暗号化技術を定義している[7]。これに基づき、米国政府は、一般政府情報システムにおける暗号技術利用のガイドラインを提供するFIPS171を設立した。この規格は継続的に更新されており、現在 NIST SP 800-57 と呼ばれている。

B. インターネットインフラストラクチャのキーマネジメント

インターネットの普及により、コミュニケーション産業において重要なマネジメントが不可欠となっている。注目すべきシナリオは、アドホックメッセージングネットワークであるPretty Good Privacy (PGP)である[8]。PGPでは、各参加者が鍵ペアを生成し、公開鍵をピアと交換し、送信者認証とメッセージ暗号化を可能にする。この概念は信頼の網と呼ばれることもあり、[9]のようないくつかの研究が行われている。一方、公開鍵基盤(PKI)とDNSSEC(DNSSEC)は、特定の権威あるドメイン内で階層的に信頼を伝播するよく知られた技術である。これらのシステムでは、参加者は信頼アンカーと呼ばれる、あらかじめ定義された信頼された機関のセットを保持している。ユーザーは、これらの信頼できる機関によって認定された下位の団体を信頼することができ、信頼の連鎖を形成します。

PKIはX.509[10]で標準化され、デジタル証明書の一般的な形式を定義しています。ユーザーは、認証局(CA)が発行した自己署名証明書を信頼アンカーとし、CAは秘密鍵で下位エンティティの証明書に署名する。CAの秘密鍵が漏洩した場合、すべての下位証明書が信頼できなくなる。過去にオンラインサーバー上で動作するパブリックCAに違反し、大きな被害を受けたインシデントがありました[11]。現在、公開されている TLS 証明書を発行する CA は、運用上安全性のために CA/B フォーラムが定めるベースライン要件(BR)に準拠することが求められています[12]。BRは、ルートCAがオフラインまたはエアギャップ環境で動作することを義務付けており、証明書に署名するために明示的な人間の動作が必要である。

DNSSEC(DNSecurity Extensions)[13]は、DNSゾーンにデジタル署名し、検証するために使用されるプロトコルのセットである。ルーツ署名鍵(KSK)公開鍵のダイジェストから始まる信頼の連鎖を確立する。ルートKSKは、インターネット割り当て番号認証(IANA)により、エアギャップ環境下で管理されます。彼らは、重要な鍵管理の代表的な例として機能するインターネット操作の透明性を確保するために、Root KSKを含むすべての操作を公開しました[14]。
米国政府は、キーマネジメントの分野でいくつかの文書を発表している。NIST SP 800-57 は、前述のとおり、キーマネジメントに関する包括的なガイダンスを提供している[15]。様々なタイプの暗号鍵を分類し、そのライフサイクル管理に関するガイダンスを提供する。NIST SP 800-130 [16]は、前作と密接な関係があり、暗号鍵管理システム(CKMS)に焦点を当て、設計要件を含んでいます。また、暗号モジュールやデジタル署名アルゴリズムの規格もある。FIPS 140 [17]とFIPS 186 [18]はセクションV-Cで後述する。
IETF は RFC4107[19]で意思決定ガイドラインを提供し、主要な管理職が自動化されるべきか、それとも手動化されるべきかを判断している。暗号化データの価値が低い場合や暗号化頻度が低い場合を除き、自動化手法を強く推奨する。

C. 暗号通貨とブロックチェーンにおけるコンテキスト

暗号通貨の歴史は、ビットコインの発明から始まる[20]。多くの暗号通貨システムでは、アドレスとその暗号通貨残高の関連性を記録するために、ブロックチェーン(または分散型台帳)が使用されています。アドレスは公開鍵から導出され、ブロックチェーン上でトランザクションが記録され、あるアドレスから別のアドレスに暗号通貨を転送する。各トランザクションは、発信元アドレスに関連するプライベート署名鍵からの署名を必要とする。鍵の署名を継続する仕組みは、しばしばウォレットと呼ばれます。

署名鍵を安全かつ正確に取得することは、暗号通貨の所有者が資金をうまく送金するために極めて重要である。この技術的な風景は、PGPの時代と似ており、しばしば分散型と表現される。暗号通貨の中には、分散化を促進するために匿名性を強化するものさえある[21]。

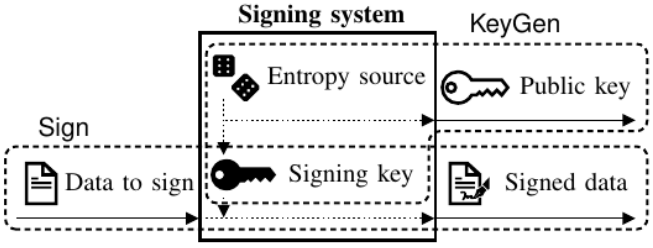

図1. 署名システムのモデル(S IG -S YS)

Eskandariらは、Bitcoinにおけるパーソナルキーマネジメントの最初の分析の一つを実施した[3]。Bonneauらは、鍵管理の課題を含むBitcoinのアーキテクチャを広範囲に検討し、一般的な研究トピックについて議論した[22]。また、暗号通貨全般のウォレットを論じた研究も存在する[23]、[24]。

暗号通貨カストディアンにおけるセキュアなキー管理は、主要なインシデントによって、時 間とともに開発・改善されてきた。秘密鍵の漏洩により暗号通貨が違法に送金された事例[25]、[26]、署名鍵が資金を流用するために不適切に利用された事例[27]、[28]、暗号化署名鍵が復号化できなくなったために暗号通貨が永久に凍結された事例[29]などがある。ただし、新たなインシデントが発生し続けていることに注意が必要です。Oosthoekらは、過去の事件を包括的にレビューしている[30]。

D. その他の最近の研究

近年、暗号通貨取引所を含む多くのシステムがクラウドインフラで運用されている。Chandramouliらは、クラウド上の仮想マシン、ストレージ、データベースに対する暗号鍵管理の課題について議論した[31]。同様に、Kuzminykh らは、様々な KMS 製品を比較・分析した[32]。これらの研究は、オンラインウォレットアーキテクチャを設計する際に有益であると思われる。

Xiao らは、複雑な認証の安全性を信頼性工学の観点から評価した[33]。彼らは、1つの鍵の平均故障時間(MTBF)に基づいて攻撃成功率を定式化した。このアプローチは、マルチシグネチャーウォレットのセキュリティを評価するために拡張することができる。

Ranaらは、様々なタイプの暗号アルゴリズムに対するKMSのアーキテクチャを広範囲に検討した[34]。

III. 符号化システムの設定

A. Model

S IG -S YS と呼ばれる署名システムの抽象的なモデルを紹介し、そのセキュリティ特性について議論する。図 1 に示すように、S IG -S YS は暗号鍵を内部で保持し、デジタル署名でデータを 保持している。

このモデルは、プロトコル自体が安全である限り、特定の署名アルゴリズムや曲線に依存しない。Bitcoinで使用されているsecp256k1のようなアルゴリズムや、非標準的な署名方法に対応することができます。暗号鍵が安全に処理されていても、署名プロトコルに潜在する欠陥が鍵の漏洩につながる可能性があることに注意することが重要である。

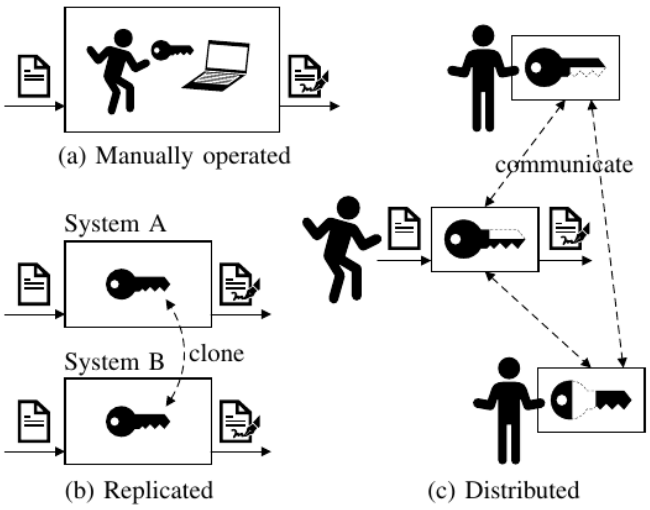

図2. S IG -S YS のバリエーション

外部から見ると、S IG -S YS はブラックボックスとして見ることができる。2つのインターフェイスを提供します。

- KeyGenはエントロピー源からプライベート署名鍵(skと呼ばれる)を生成する。どんな入力も受けません。対応する公開鍵(pk)を出力する。
- Sign uses *sk* to sign the input and produces the signature. It may also perform additional verifications on the input.

これらのインタフェースの安全性を確保するために、ユーザーや外部システムを認可するための適切なメカニズムを実装する必要があります。S IG -S YS 内に統合することも、外部に追加のセキュリティ層として実装することも可能です。

また、S IG -S YS は、暗号通貨には適さない sk を破壊する破壊を定義することができる。筆者の知る限り、アドレスの通信を省略できるブロックチェーンは存在しない。skの破壊は推奨しませんので、これ以上詳しくは説明しません。

図 2 は S IG -S YS の異なるバリエーションである。(a)に示すように、S IG -S YSは必ずしも完全自動化とは限らない。エアギャップシステムのような場合、マニュアルや機械的なメカニズムが必要な場合があります。

さらに、S IG -S YS はモノリシックではなく、複数のコンポーネントで構成されている可能性がある。例えば、あるコンポーネントが sk を保持し、その暗号化されたバージョンを別のコンポーネントに送信して、より高い可用性を得ることができる、と(b)に示すように。また、(c)に示すように、セクションV-Gで議論した秘密分割技術を使用して、複数の端末にskを分散させることが可能である。

B. 形式的アプローチによる安全性分析

以下の2つの要件を満たす必要があります。

1) S IG -S YS の境界内に sk の任意のビットが保持される。2) データは、署名で要求され、他の署名が生成されない場合にのみ、sk によって署名されるべきである。

これらの要件は、特に同期ソフトウェア実装の場合、正式な方法を用いて検証することができます。

複数のプロセスを持つ分散実装の場合、マルチプロセスソフトウェアの正しさを証明するためのLa

mportの方法[35]を採用することができる。これは、システムが望ましくない状態に達しないことを保証する、以下の安全特性を実証することを含む。

- skは変化せず、失われることはありません。
- S IG -S YSからのいかなる出力も、skの暗号化されていないビットを含んでいない。

- Signからの出力はその入力に対応する。と、以下のような活性度特性を持ち、最終的にシステムが望ましい状態に到達することを保証します。

- skは最終的にKeyGenが呼び出された後に生成されます。入力mでS
- ignが呼ばれた後、メッセージmに対してskによるデジタル署名が最終的に生成される。

しかし、暗号プロセスを徹底的に形式化することは、しばしば困難でコストがかかる。

C. CIA Triadを用いた安全性解析

形式的な方法の代替として、情報システムのセキュリティは、一般的にCIAの三項対立として知られている機密性、完全性、可用性の原則を使用して評価することができます[36]、[37]。それぞれが特定の要件を表している:(C)秘密情報がシステムの境界から離れないようにすること、(I)情報およびシステムのプロセスの不正な変更を防ぐこと、(A)必要なときにシステムが動作することを保証すること。例えば、Warkentinら[38]は、CIAのトライアドを使用して、公共部門向けのブロックチェーンアプリケーションのセキュリティを検証しています。
S IG -S YS は、sk の漏洩を防ぐために複数の認証と暗号化を採用することができ、(C)を強化したり、(I)と(A)を強化して、損傷や損失を避けるために sk をバックアップのために複製したりすることができます。これらの措置は互いに矛盾しており、合理的なバランスを維持する必要がある。
以下の点を考慮する必要がある。1) skの信頼性:エントロピーの不足や乱数アルゴリズムの不適切な実装は、脆弱性の一般的な原因である。予測可能な乱数は、シード値を推測することができる攻撃で利用することができます。このような乱数発生器(RNG)に対する攻撃は、様々なオペレーティングシステムで広く研究されている[39], [40]。RNGでは、署名時に電磁波から鍵を復元するサイドチャネル攻撃も存在する[41]。暗号通貨ウォレットのキーが弱いと資金が失われる可能性があり、攻撃が成功した事例が報告されている[42]。

2) S IG -S YS の完全性 : S IG -S YS が悪意を持って改ざんされている場合、Sk のビットは Sign の出力にステガノグラフィとして埋め込まれる可能性がある。このリスクは、エアギャップ環境から暗号通貨ウォレットを盗む方法として、Guriによって提案されている[43]。

3) KeyGenの出力pkの完全性。S IG -S YSの境界内でKeyGenの出力を変更することで攻撃者が資金を盗むのを防ぐため、ユーザはpkの真正性を確保する必要がある。最も単純な対策として、pkのアドレスから少額引き出されるかどうかをテストすることができます。

4) サインの入力mの完全性:上記と同様に、攻撃者は暗号通貨の転送をリダイレクトするために、事前に署名されたデータを改ざんする可能性があります。ユーザーはS IG -S YSの完全性に頼らず、むしろSignの出力を検証する必要があります。

D. Threats

S IG -S YS の安全性を損なう様々な脅威があります。脅威の起源を分析することができる。

1) システムに対する外部脅威。敵対的な環境では、攻撃者はS IG -S YSの認証を回避したり、論理的または物理的な手段で秘密鍵を盗むことによって、不正な署名要求を生成しようとすることがある。自然災害は、S IG -S YS の利用可能性を損なうこともある。

2) システムに対する内部脅威。S IG -S YSの内部構成要素もまた、敵対的である可能性がある。S IG -S YS がソフトウェアやハードウェアで実装されている場合、開発者が意図的または非意図的な不具合を導入している可能性があります。人間が S IG -S YS のプロセスに関与している場合、Blakley [2]が示唆するように、情報漏洩、タスク拒否、破壊的行為などの不正行為のリスクを軽減することが重要である。

E. 暗号技術の利用におけるセキュリティへの配慮

1) 隠れた数の問題:ECDSA[44]では、攻撃者は複数の署名から同じnonceで秘密鍵を計算することができる。このタイプの攻撃は、隠れ数問題[45]として知られ、他の暗号アルゴリズムでも研究されている。ECDSAにおけるnonce再利用問題は、メッセージから署名へnonceを選択するための決定論的方法を提案するRFC 6979で対処されている[46]。

2) 非正規エンコーディング。ビットコインに見られるように、トランザクションの可鍛性により、攻撃者はデジタル署名を維持したまま、異なるトランザクションを生成することができます。この種の攻撃に使用される1つの技術は、(r, s)と(r, -s)の両方が等しく有効なECDSA署名であるという事実を利用することである。攻撃者グループは、Mt.Goxにビットコインを預ける取引を成功させた[47]。暗号通貨取引所は、厳密な検証を行い、このような異なる取引や署名のインスタンスの正統性を確保する必要があります。

IV. 著作権侵害の発生メカニズム

A. アーキテクチャと運用

ほとんどの暗号通貨取引所は、法通貨と暗号通貨の交換を促進し、また、プロセス利用者の入出金も促進します。顧客の資金を通常保管するためにウォレットを管理する。また、セクションV-Aで後述するように、取引を監視するためにブロックチェーンノードを運用することもできる。現代の暗号通貨取引所のアーキテクチャについては、IEEE規格があります[48]。

取引所の運営者の中には、アーキテクチャを簡素化するために外部のブロックチェーンAPIに依存する者もいる。複数のAPIやデータソースに接続するなどして、受信情報の正確さやシステムの可用性を確保する必要があります。
1) 預け入れ。1)預け入れ:取引所は要求に応じて各顧客に固有の預け入れ先を割り当て、預け入れ先への移転を監視する。顧客の口座残高は、預金が確認された後、それに応じて更新されます。

ある種のブロックチェーンでは、Symbolのmessage、Rippleのtag、Stellarのmemoなど、追加のデータをトランザクションに添付することができます。取引所では、同じ入金先住所を提供しながら、顧客ごとに固有のデータを指定することができます。このアプローチは、ウォレット構造を簡素化し、取引コストを削減するのに役立ちます。

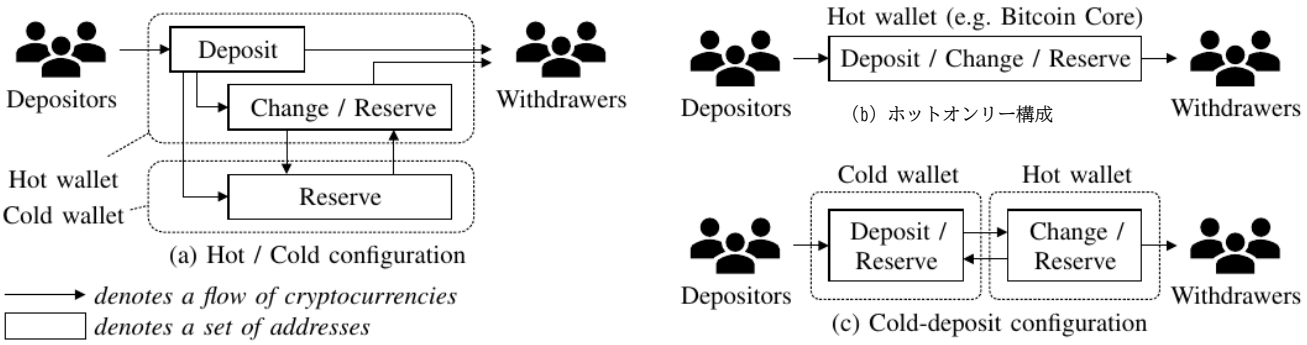

図3. 様々なウォレット管理構成

しかし、このような情報は第三者による追跡にも利用することができ[49]、プライバシーに関する懸念に対処するために複数の入金アドレスを提供する取引所もある[50]。
2) 撤退。顧客が引き出しを要求すると、取引所はウォレットから発信される取引を開始する。取引所がこれらの取下げを自動化することはよくあることですが、金融犯罪を防ぐために疑わしい要求をスクリーニングすることも必要で、その場合、数時間かかることがあります。

3) ウォレット管理。現代の取引所におけるウォレットの構成は、図3(a)に描かれている。ホットウォレットは、取引所にある他のシステムに接続されているオンライン署名システムです。それらは即時撤退のために設計されています。一方、コールドウォレットはオフラインまたはエアギャップシステムで、より安全なストレージを提供することを目的としています。この構成はいくつかの利点を提供します。

- ウォレットの温度に応じて、異なるセキュリティポリシーを適用することができます。
- ビットコインのような暗号通貨では、取引所は未使用の取引アウトプット(UTXO)の選択を最適化することで、取引手数料を節約することができます。

図3(b)は、著者の経験をもとにしたビットコイン取引所の初期設定を示したものである。取引所はソフトウェアを使ってウォレットをホストし、ウォレットはブロックチェーン同期中にオンライン接続されました。
典型的な構成に代わるものとして、図3(c)に示すように、取引所は顧客の入金先住所にコールドウォレットを使用することができる。これらのアドレスからすぐに取り出す必要がないため、コールドウォレットは適切なオプションを提供します。しかし、取引所は、コンプライアンス上の理由から、これらのアドレスに対する支配力を証明する必要がある場合がある[51]。
その後の変更が困難な場合があるため、ウォレット管理の設定を慎重に設計することが重要です。

B. Regulations

暗号通貨取引所は、多くの国の当局によって規制されています。規制は管轄区域によって異なるが、交換業務の様々な側面をカバーしている。

その一つが、Proof of Reserveとも呼ばれるソルベンシー要件です。これは、Mt.Gox事件を受けて導入されたもので、顧客に支払うべき十分なビットコインが持っていない。

Dagherらは、取引所の残高を証明するために、Merkle Treesを用いた方法を提案した[52]。いくつかの取引所は、ゼロ知識証明技術でこの方法を拡張し、そのソルベンシーを示している[53], [54]。米国では、会計士の組織が監査基準を制定している[55]。一部の監査人は、秘密鍵の所持を確認するために、実際の引き出しを証明するよう取引所に要求さえしています。
もう一つの規制は、コールドウォレットに対する要件である。PKIのエアギャップ慣行と同様に、暗号通貨取引所の資産の大半をコールドウォレットに保存することを義務付けている国もあります。例えば、日本では、95%以上の資産[56]がコールドウォレットで運用されなければならない。コールドウォレットは、インターネットに接続されたことのない電子機器と定義されている[57]。つまり、日本の取引所では、オンラインアクティベーションや認証を必要とするデバイスをコールドウォレットとして使用することはできない。この厳しい規制は、2022年のFTXの破綻時に日本の顧客の資産を保護する上で重要な役割を果たした[58]。

さらに、暗号通貨の転送を開始するための複数の個人の関与や、鍵の署名のためのバックアップの作成など、追加要件が適用される場合がある。

V. A V. 既存研究の成果に関する分析

A. Software Wallets

1) 概要 ソフトウェアウォレットは、ウォレット実装の中で最も単純なタイプである。コンピュータの秘密鍵の生成と管理、およびトランザクションの署名を行うことができます。ソフトウェアウォレットのアイデアは、Satoshi NakamotoがC++で書いたオリジナルのBitcoinクライアントまで遡ることができます。現在、様々なタイプの暗号通貨やトークンをサポートするソフトウェアウォレットを提供する様々な開発者が存在します。ソフトウェアウォレットは、デスクトップアプリケーション、ブラウザ拡張機能、スマートフォン用モバイルアプリなど、さまざまな形態があります。
ソフトウェアウォレットはブロックチェーンノードと密接に関連している。多くのブロックチェーンシステムにおいて、ブロック情報を参照することは、引き出し取引を作成する際に不可欠である。その結果、多くのブロックチェーンクライアントは、ノードとウォレットの両方の機能を結合していますが、必要に応じて独立して動作させることができます。例えば、Bitcoin Coreはセキュリティ上、複数のウォレットを作成・管理し、ウォレット機能を無効にすることができます[59]。ノードには様々な種類があり、それぞれがウォレット機能に関する関係やリスクが異なります。

フルノードは最も一般的なタイプのノードである。UTXOや世界の状態など、すべてのブロックとトランザクションの完全な履歴と、最新の実行状態を保持します。新しい取引の一貫性を検証することができ、取引所における預金の確認に不可欠である。完全に同期されていれば、ウォレットは有効なトランザクションを生成することができます。しかし、フルノードを実行すると、かなりの量のストレージスペースが必要になる場合があります。例として、2023年12月時点で、ビットコインのブロックチェーンは512GBを超えています[60]。

スマートフォンのような限られた容量のシステムにウォレットを実装するには、軽量なノードが適しています。最近のブロックとトランザクションのみを保持し、特定のストレージ容量に収まるように古い情報を破棄する。しかし、これはノードが新しいトランザクションの有効性を独自に検証することを妨げ、ウォレットは信頼できる完全なノードに依存しない限り、自分自身に宛てた無効なトランザクションを受け入れることができる。ビットコインベースの暗号通貨では、SPV(Simple Payment Verification)プロトコルにより、ブルームフィルタを使用して、他のフルノードから特定の監視対象アドレスに関連するトランザクションを抽出することができます。過去の全ブロックのヘッダのみを保持し、必要に応じて関心のあるトランザクションを含むブロックをフェッチする[20]。リップルのような分散型台帳は、過去の台帳を同期させる必要がないものがあります。

アーカイブノードはEthereumのような複雑な状態を持つブロックチェーンアーキテクチャにおいて、過去のすべての状態を保持し、通常のノードは最新の状態のみを保持する。アーカイブノードは、過去の状態を復元し、過去の特定の時点で特定のNFTの所有者をチェックするなど、関数呼び出しを実行することができます。アーカイブノードは主にデータ解析に使用され、高い性能を必要とする。例えば、イーサリアムのアーカイブノードは、2023年12月時点で約16TBのストレージ容量を必要とします[61]。その目的を考えると、ウォレット機能をアーカイブノードで動作させることは非常に稀である。

ネットワーク構成やブロックチェーン設計が異なるノードは、他にも存在する。例えば、採掘ノードはプルーフオブワークブロックチェーンでブロックを作成することに特化し、中継ノードはブロック伝播に特化し、イーサリアムのコンセンサスノードは新しく提案されたブロックの検証結果の証明と署名に特化する。これらはウォレットの機能とは直接関係ありません。

逆に、ブラウザの拡張機能やスマートフォンアプリなど、ウォレット実装の中には、ノードを伴わないものがあります。軽量ノードと同様に、これらのノードレスウォレットは、暗号通貨残高や取引のブロードキャストをAPI経由で信頼できる外部ノードに依存しています。例えば、Khan らは、データ交換のために単純に QR コードを使用するノードレス Androidウォレットを開発しました[62]。

2）利点と欠点。(a) ユーザーは通常のコンピュータしか必要とせず、特別なデバイスを必要としない、(b) ソフトウェアウォレットは通常、高速な更新サイクルを持ち、これにより、管理者は新しい暗号通貨やトークン、最新のDeFiサービス、ブロックチェーンの技術更新を楽に更新し続けることができ、(c)生じた問題や誤動作に迅速に対応し解決することができる、などの利点がある。

また、(d) ソフトウェアウォレットは主に個人向けに設計されており、複雑な承認ワークフローなどの企業機能が不足している可能性がある、(e) オンライン用に設計されていることが多く、通信が暗号化されているためセキュリティ制御が困難である、(f) 実行環境のセキュリティに最も影響を受けやすい、などの欠点もある。

3）リスク ソフトウェアウォレットに関連するリスクには、少なくとも2つのカテゴリーがあります:(x) ソフトウェア自体に起因するもの、(y) ユーザーの行動または行動に起因するもの。

x-1）開発者の悪意ある意図。開発者またはコミット者は、同意なしにユーザーの暗号通貨を転送するためにウォレットをプログラムするか、外部当事者に秘密鍵を送ることができる。これは、コードベースにバックドアを隠すか、ウォレットが使用する他のオープンソースソフトウェアによって実現できます。

x-2）偶発的な誤動作:skは未知の欠陥により、外部当事者に破損または開示されることがある。古典的なバグや暗号の脆弱性などが原因で起こることがあります。

y-1）不適切な設定または不正な使用。ソフトウェアウォレット構成におけるエラーは、攻撃者による悪用につながる可能性があるため、潜在的な結果を過小評価してはならない。例えば、Buiらは、適切な認証設定なしに、ノードのAPIへの不正アクセスを実証した[63]。また、ユーザーインターフェースの問題で、ウォレットの操作が正しく行われない可能性もあります。Voskobojnikovらによって、ソフトウェアウォレットに関連するユーザビリティの懸念について広範な研究が行われてきた[64]。

y-2）汚染された実行環境。攻撃者はマルウェアを使用して、秘密が保存されているファイルやメモリに直接アクセスしたり、キーロギング技術を取り入れたりすることができます。Horstらは、ソフトウェアウォレット処理の記憶を分析することで、秘密鍵を盗む実験を行った[65]。Voletyらは、ブルートフォース法を用いた同様の攻撃に着目している[66]。He らは Android wallet を標的とした様々な攻撃ベクトルを分析した[67]。他のマルウェアは、アドレスポイズニングと呼ばれる攻撃 [68]を使用しており、表示されるアドレスを完全に検証する際に人間の過失を悪用しています。Ivanovらは、クリップボード上のユーザーコピーされた宛先アドレスを、元のアドレスに部分的に類似した攻撃者のアドレスに置き換えるマルウェアを紹介する[69]。ウォレット開発者の対策として、SSHキーアート[70]のコンセプトに似た、視覚的に区別できる表現の実装が考えられる。

y-3）偽造ソフトウェアの使用。類似した名前や外見のため、ユーザーがフィッシングソフトウェアと正規のソフトウェアを区別することはしばしば困難である。これは特にブラウザ拡張ウォレット[71]で顕著である。

(x)と(y)のリスクを軽減するために、オープンソースのソフトウェアウォレットの検証済みリリースを、開発者の成熟したコミュニティで使用することを検討することができます。未知の脆弱性の影響を最小化するために、コードベース上でコード監査を行い、複数の保護レイヤーを実装することで、深い防御のアプローチを採用することも推奨されます。

B. Auxiliary Wallets

1）概要 ウォレット情報をコンピュータの外部に保持するために、いくつかのオフライン手法が知られている。これらの方法には、紙に書かれた情報をペーパーウォレットと呼ばれるように書くこと、

金属ウォレットと呼ばれる金属プレートに刻むこと、またはブレインウォレットと呼ばれるように記憶することが含まれます。これらの方法をまとめて補助ウォレットと呼ぶことにする。なぜなら、これらすべてを包含する単一の項は存在しないからである。

補助ウォレットは2種類の情報を保持することができます。

- Cryptocurrency address or public key
- 秘密鍵またはそれを導き出すために必要な情報

前者は他人から支払いを受けるときの自分の住所を表示するためにのみ使用されるので、これ以上の議論はしない。後者は、以下のいずれかになります。

PK:16進数、Base58、QRコードの秘密鍵 MNEMO:12から24語の連続(ニーモニック) PWD:パスワードまたは consequently ENC:上記の暗号化された情報またはシャード情報

2) 共通の利点と欠点。(a)これらのウォレットはソフトウェアやハードウェアウォレットのバックアップとして機能し、欠陥や攻撃によるウォレットの損失のリスクから保護できる、(b)インターネット経由の直接の盗難のリスクは低い、という情報の種類に関係なく、補助ウォレットに共通する利点がある。

ただし、(c)補助ウォレットは単独で使用できず、他のウォレットにロードして使用する必要があります。その結果、補助ウォレットは彼らと同じリスクプロファイルを共有する。

3) 記憶の種類による特徴 紙や金属財布のような物理的手法は耐久性が高く、PKやMNEMOに最もよく使用される。QRコードは誤り訂正機能を持ち、部分的な損傷にも強い。同様に、MNEMOは数文字の損失があっても復元可能です。しかし、物理的な財布は盗難や損失からの保護を必要とし、偶発的なビデオ録画からの復旧が容易なため、守秘義務が低くなります(例:[72])。

脳内ウォレットは、記憶している人が安全であれば、安全を確保する。MNEMOやPWDによく使われる。十分に安全なパスワードを使用することで、ウォレットのセキュリティは向上しますが、他の人と共有することは不便です。さらに、複数の個人間で情報を分離することは現実的に困難である場合がある。例えば、悪意のある人は、単に半分に分割すれば、残りの半分を回復することができるかもしれません。これらのウォレットは物理的なウォレットと比較して機密保持に優れているが、可用性が損なわれる可能性がある。これを補完するために、Sansらは、所有者の電子メールアドレスをルックアップキーとして、特別なブロックチェーン上にMNEMOを保存することを提案した[73]。このアプローチは、他のタイプの情報にも理論的に適用できますが、メールシステムのセキュリティと特定のブロックチェーンに依存しているため、普遍的に適用できるものではありません。

4) 情報の種類別の特徴。現代のソフトウェアウォレットはMNEMOを使用してシードをエンコードし、当初はビットコインの初期にはPKが主要なオプションでした。暗号通貨アドレスの再利用は一般に推奨されないため、この移行はプライバシーへの懸念によるものである[74]。BIP-32は階層型決定論的(HD)ウォレットのアルゴリズムを定義し、HMACアルゴリズム[75]を用いて種から一連の署名鍵を導出し、決定論的にアドレス指定を行うことができる。

MNEMOの各単語は、BIP-39[76]で定義された2048個の単語から選択され、11ビットの情報を表します。

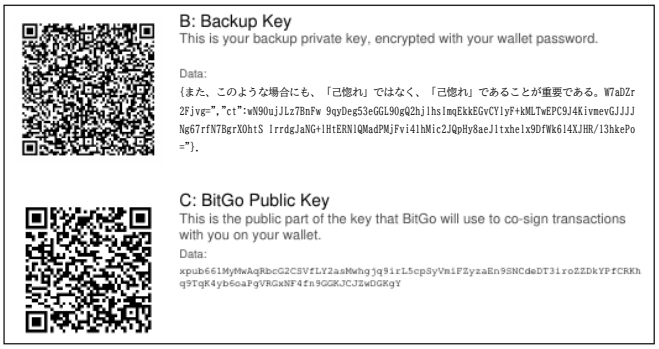

図4. 暗号化された論文のウォレットの例

チェックサムを除いた、12単語の特定の順列は256ビットのデータをエンコードしています。認識可能な単語の使用は、PGP Word [77]のような概念に類似している。ニーモニクスは簡単に記憶できるが、例外的な即時記憶を持つ個人が観察すると、盗難の危険性がある。

PWDは、関数の種類と塩の種類とともに、PBKDF2やscryptのような主要な導出関数によってウォレットを一意に導出することができる。しかし、実際には弱いパスワードが一般的に使用されており、その結果、即時攻撃が発生する[78]。

図 4 の ENC の例は、暗号化または秘密分散アルゴリズムによって生成されたものである。この方法は、盗難や損失に対する保護を強化しますが、暗号文とパスワードの両方を別々に安全に管理する必要があり、その結果、懸念事項が増加します。

C. ハードウェアセキュリティモジュールの使用

1) 概要 安全な暗号プロセッサを搭載したデバイスをハードウェアセキュリティモジュール(HSM)と呼びます。HSM は、界面が明確に定義された自己完結型ユニットとして実装され、図 1 のようなモデルに当てはまります。

PKI業界では、暗号鍵管理のためにHSMが広く使用されています。CAは、通常、閉じたエアギャップネットワークを介して、安全な環境でHSMを動作させます。HSM は、通信や金融の分野でも高性能なオンライン処理に利用されている。クラウドベンダーは、このような需要に対応するため、仮想 HSM 装置を提供しています。

Shbairらは、クラウドHSMを使用してEthereumのキー管理を実装した[79]。Alrubeiらは、企業目的に合わせたプライベートブロックチェーンにHSMを採用した[80]。また、暗号通貨の管理者がHSMを採用する公開事例もある[81]。Dornseiferらは、AWS KMS[82]を使用してEthereumトランザクションに署名するためのチュートリアルを提供しています。

2) Advantages:

a) 耐タンパー性。電気分析を含む改ざんの試みをHSMが検出すると、内部記憶装置の復号化キーが速やかに消去される。管理者は、HSMの完全性を確認した後にのみ、外部バックアップ媒体から復号化キーを復元することができます[83]。これにより、機密保持と可用性のバランスがとれます。

b) 信頼性 b) 信頼性:セキュリティ監査や審査を受けたHSMは信頼性が高いと考えられる。HSMの品質は、ISO/IEC 19790[84]、FIPS 140-3[17]、共通基準などの確立された基準によって確保される。

これらの規格は、インターフェース、認証、動作環境など、さまざまな側面から要件を指定します。米国では、Cryptographic Module Validation Program (CMVP) [85] が暗号モジュールの実装を検証し、認証している。CMVP の主な目的は政府機関によるモジュールの使用を承認することであるが、認証された HSM も広く信頼され、非政府目的で利用されている。

c) 攻撃に対する耐性。Bardouらが一般にアクセス可能なインターフェースから鍵を推測するために提案した方法[86]など、HSMに対する攻撃は知られているが、攻撃方法の範囲は比較的限定的である。明確なインターフェースと物理的回復力の要件は、潜在的な攻撃者にとって大きな抑止力となります。

3) Disadvantages:

d) 暗号アルゴリズムのサポート不足。暗号通貨はしばしば、secp256k1カーブではECDSA、Curve25519カーブではEdDSAを使用する。これらのアルゴリズムをサポートする認証済みHSMはほとんど存在しないが、これは主に、これらの曲線が業界からのフィードバックを受けて2023年に米国政府によって承認された[18]ためである[87]。さらに、Polkadotで使用されているsr25519や、イーサリアムのビーコンチェーンで採用されているBLSシグネチャ[88]をサポートするHSMを市場に見つけることができませんでした。また、他の研究者は、かなり新しい暗号アルゴリズムを持つHSMの利用可能性が限られていることを指摘している[89]。

e) 暗号通貨のメカニズムの欠如。最近のウォレットは、複数の暗号通貨アドレスを導出するためにHDウォレットを使用することが多いが、それを支持するHSMはほとんどない。BIP-39 のようなニモニックもほとんどサポートされていません。これは、これらの暗号通貨固有の特徴が、現在HSMの標準の範囲外であるためです。一部のHSMはカスタムメカニズムを定義する機能を提供しますが、そのようなカスタマイズがセキュリティを損なわないことを保証するのはユーザーの責任です[90]。

f) ストレージ容量。HSMは内部ストレージ容量に制約されることが多く、高品位HSMでは単位あたり数万個の鍵がかかることが多い。この制限は、複数の暗号通貨やシードを持つ管理者にとって、多数のユーザーを管理するための実用的な課題となり得る。Han らは、HSM を Intel SGX と組み合わせてストレージ容量を拡張する方法を提案した[91]。また、クラウドでHSMを利用することで、これらの制約を緩和することができます。

g) コスト。g) コスト:企業グレードの製品は、1台あたり1万米ドルを超えることが多い。

D. ハードウェアウォレット

1) 概要 ハードウェアウォレットは、暗号通貨を安全に保存するために設計された特殊なデバイスである。これらのデバイスには様々な種類があります。基本的なハードウェアウォレットモデルの中には、マイクロコントローラを備えたシンプルな回路で構成されるものもあれば、より高度なモデルはHSMと同様の構造を持つものがある。多くの製品は、ベンダー提供のソフトウェアを搭載したコンピュータからの USB インターフェースで使用できるように設計されています。Arapinisらはハードウェアウォレットの形式化された モデルを提供した[92]。ハードウェアウォレットの初期の例のいくつかは、Gamertsらによって提案された[93]。

POS(Point-of-Sale)デバイスなどの決済端末とBluetooth上で通信を行います。デバイスは支払い端末から符号なしトランザクションを受け取り、そのトランザクションに署名し、端末に返します。Rezaeighalehら[94]によって提案された別の実装は、Androidスマートフォンと一緒に使用できるスマートカードウォレットである。また、古典的な鍵交換の手法で、複数のカード間の鍵をバックアップする方法を提案した。さらに、多数の市販のハードウェアウォレット製品が販売されています。

2) 利点と欠点。ほとんどのハードウェアウォレットは、ユーザーフレンドリーになるように設計されています。これらを利用する利点は以下の通りです。(a) 秘密鍵を物理デバイスに格納する直感的な性質、(b) 多くのベンダーが提供するすぐに使えるソフトウェア、(c) 暗号通貨使用のための特殊なファームウェア、(d) 新しい暗号通貨の出現に対応するための高速なファームウェア更新サイクル、などである。これらの利点は、HSMと比較してベンダーの設計上の制約が少ないことに起因しています。
欠点は、(e) 製品の完全性に対するベンダーの信頼の要件、(f) ソフトウェアウォレットと同様の企業機能の欠如、および (g) 企業設定における署名力の分離における複雑さのリスク、である。

3) リスク ハードウェアウォレットは、ソフトウェアウォレットと同様のリスクを共有する。以下は、特に注目すべき点です。

x-1) ファームウェアとサーキットのリスク。ハードウェアウォレットには、ユーザーの期待とは異なる動作をするファームウェアが付属している可能性がある。ハードウェアウォレットのメーカーが鍵バックアップサービスを発表し、オプションのファームウェアの更新を提案した。この発表は、当初不可能と宣伝されていた、デバイスから署名鍵を抽出する機能の存在を示唆するものであり、ユーザの間で懸念を抱かせるものであった[95]。ファームウェアのソースコードは、これらの懸念に対応するために一般に公開され、監査される必要があり、できれば、ユーザービルドのファームウェアをプログラムできるようにする必要があります。ハードウェア回路の検証は、最大限の予防策を講じるために必要かもしれません。

y-2) 攻撃されやすさ。広く受け入れられている技術標準に準拠する FIPS 認証 HSM とは異なり、ハードウェアウォレットのセキュリティは標準化されておらず、その品質は様々である。例えば、KeepKeyとTrezorについて、異なる研究者による電気的解析と信号操作によっていくつかの試みがなされている[96]-[98]。内部で TEE を使用する Ledger Nano S(次節で説明)を Volokitin で調べ、保護境界を横切るメモリアクセスを実証した[99]。

y-3)調達のリスク ボロキチンは、出荷時に悪意のあるコードをプリロードすることで、本物のハードウェアウォレットを侵害する可能性があることを示唆している[99]。暗号通貨が、評判の良い商品に似た偽造ハードウェアウォレットから盗まれた例もある[100]。

E. TEE-based Wallets

専用の暗号プロセッサに依存することなく、コンピュータ上でウォレットを作成するアプローチの1つは、Trusted Execution Environment (TEE)の活用です。通常のCPUにTEEを確立することで、この保護機構の下で署名システムを構築することができる。

TEE内では、デジタル署名付きの検証済みソフトウェアが、他のアプリケーションから論理的に分離して動作します[101]。実装によって、ハードウェアメモリは分割され暗号化されます。一部の研究者は、ウォレットを実装するためにArm TrustZoneまたはIntel SGXを調査した[102]、[103]。
TEEベースのウォレットの利点は、(a)ソフトウェアウォレットと比較してセキュリティが高く、偽造や脆弱性のリスクをある程度軽減できること、(b)様々なプラットフォームに展開できるため汎用性があることである。
しかし、(c)プログラミングの制約によりTEEベースのソフトウェアを開発するコストが大きく、(d)ハードウェアウォレットと同様に、ユーザーはプロセッサベンダーを信頼する必要がある、(e)攻撃事例が報告されているため、一定のセキュリティ対策が必要である[104]、という欠点がある。Schaikらは、機密ブロックチェーンプラットフォームであるSecret Network上でトランザクションを復号化する能力を表明している[105]。

F. スマートコントラクトウォレット

1) 概要 Ethereum [106]のようないくつかのブロックチェーンでは、暗号通貨を直接操作するためにスマートコントラクトと呼ばれるプログラムを書くことができる。ユーザーに代わって、自動的に資産を管理するために使用することができます。
一例として、オンチェーン国債運用のためのオープンソース契約であるSafe Contracts [107]がある。リクエスト者の認証設定、最大引き出し制限の定義、引き出し先アドレスの制限など、ユーザーが暗号通貨の引き出しに関する様々な条件を指定することができる。同様に、分散型取引所(DEX)であるUniswapは、入出金プロセスを管理するスマートコントラクトを通じて完全に運営されています。このデザインは、人間の介入を最小限に抑える。
Vitalikらは、個人使用を念頭に置いて設計されたソーシャルリカバリーウォレット[108]のアイデアを提案している。この仕組みにより、特定の署名鍵を定期的な引き出しに使用することができます。一方、保護者と呼ばれる事前登録された他の鍵のセットは、緊急時にウォレット所有者に代わって別の鍵にリセットすることができます。このコンセプトは、カストディアンが使用するウォレット契約にも拡張することができます。
2) リスク リスク:DeFiプロジェクトの中で最も古いDAOの再参入バグは、2016年に攻撃者が資金を流出させることを可能にした[109]。翌年、個人で広く使われているスマートコントラクトウォレット「パリティ」の脆弱性により、資金が凍結した。これらのケースは、スマートコントラクトの実装エラーによって引き起こされる重大なリスクを浮き彫りにしています。Praitheeshanらは、スマートコントラクトの脆弱性に関する系統的な分析を行った[110]。
契約の欠陥に関連する固有のリスクを考慮すると、スマートコントラクトウォレットの安全性を確保することは極めて重要である[111]。Bhargavanらは、スマートコントラクトの形式的証明のために、F*の使用を提案した[112]。Jiang らは、自動化された脆弱性発見のための ContractFuzzer というツールを紹介しました[113]。He らは、Oyente や Mythril などのツールを採用することで、コード監査の重要性を強調した[114]。Praitheeshanらは、これらのツールを用いて、管理者が使用するスマートコントラクトを評価した[115]。Cassezらは、Dafny[116]を用いてイーサリアム仮想マシンを正式に評価した。
それでも、スマートコントラクトウォレットからの撤退を開始するためには、キーマネージメントが不可欠である。キーマネジメントの必要性を排除するものではありません。

G. 分割符号化パワー

署名鍵を複数の構成要素に分割し、暗号や体系的な仕組みによって複数の個人に署名力を分散させることができる様々な技術が開発されている。一般化されたアプローチでは、N 株のうち M 株の参加者が必要である。
正しく実装された場合、これらの技術は署名者の冗長性を提供し、少数の個人が署名力を完全に制御することを妨げる。しかし、セクション III-C で述べたように、N= M を設定することで、可用性に対するリスクが高まり、N を M よりも大幅に大きくすると機密性に対するリスクも高くなる。
以下は、この力を分割する注目すべき技術である: 1) マルチシグナル ビットコインベースの暗号通貨では、M-of-Nのマルチシグナルアドレスを作成することができます。もう一つの暗号通貨であるフローでは、ユーザーが任意の数の公開鍵を重みでアカウントに登録することができます。Flowアカウントからの引き出しは、ある重みの閾値を超えるデジタル署名を伴う場合にのみ行うことができる[117]。これらは、M個の署名を単純に検証するために系統的にブロックチェーン上にネイティブに実装されているが、取引サイズがMに対して線形に増加するユーザーには欠点がある。Ethereumをはじめとする一部の企業は、本来サポートしていないため、マルチシグネチャはキーマネジメントで普遍的に利用できるわけではありません。

2) 秘密分散。2) 秘密分散:秘密を複数共有に分割する方法を提案した[6]。この方法は、最初の分割時に完全な秘密を分割し、M個の共有を結合して秘密を回復するため、信頼される側を必要とする。S IG - S YS で使用された場合、信頼される側は保護されなければならない。

また、信頼できるパーティに依存しないバリエーションもあります。Pedersenは、検証可能な秘密分散スキームの構築において、分散鍵生成(DKG)を導入し、参加者は、結合された秘密の完全性を証明する一方で、秘密分散を維持することができる[118]。

3) 閾値署名方式。ビットコインはSchnorr署名[119]を導入し、署名サイズを大きくすることなく、複数の独立したデジタル署名の非対話的な組み合わせを可能にした[120]。これを基にした多信号方式も提案されているが[121]、[122]、参加者全員が署名しなければならない構成に限定される。

信頼できる第三者に依存せず、DKGを拡張した対話型閾値署名方式に関する研究は他にもいくつかある[123]-[125]。これらのマルチパーティ計算スキームは、キーシェアが異なる役員によって個別に生成・管理されるシナリオに適しています。しかし、これらの既知の方法は、1つのシグネチャを作成するために、シグナラー間の通信を複数回行う必要がある。さらに、攻撃方法については、[126]のような研究が頻繁に行われている。検証が不十分なため、脆弱な実装が報告されている[127]。暗号通貨カストディアンにおいて、これらの手法を採用するためには、さらなる検討が必要であると考える。

H. Custodial Wallet

カストリアールウォレットは、第三者への署名鍵または鍵の共有の代表団を締結する。個人の場合、これは通常、暗号通貨を個人口座に預けることを含み、暗号通貨の交換を行う。同様に、取引所や機関投資家は、自ら鍵を処理するのではなく、鍵管理を顧客サービスプロバイダに委ねることがあります。

カストリアウォレットでは、署名鍵のセキュリティはサービスプロバイダのの好意に依存する。Antonopoulosは、暗号通貨を保管するために保管サービスに依存することは、個々のユーザーのコントロールを超えたリスクをもたらすと主張している[128]。彼は、秘密鍵の所有の重要性を強調するハードウェアウォレットの使用を提唱している。

履歴書ウォレットの企業ユーザーは、通常、サービスプロバイダーの財務諸表およびSOC2レポートに基づいてリスクを評価します。しかし、詳細なセキュリティ対策について、包括的な理解が不足している可能性があります。この不透明なリスクを軽減するために、企業ユーザーは、保管されている資金に対する保険適用などの法的救済を求めることができる。

VI. 符号化システムの評価基準

暗号通貨カストディアンは、先に述べた様々なウォレット技術を組み合わせて、独自の署名システムを構築する柔軟性を持っています。カストディアンが行う一般的なタスクを包含する評価基準の例を示す。

A. Withdrawal

撤退シナリオの評価は、最も頻繁に行われるタスクであるため、非常に重要である。ウォレットの設定やビジネス上の必要性に応じて、要件が異なる場合があります。以下は、引出しの典型的なシナリオである。

- コールドウォレットからホットウォレット、またはその逆から定期的に行われる引出し。このプロセスは、ホットウォレットに一定のリザーブを維持し、ユーザーへの自動引き出しを確実に行うことができます。
- ホットウォレットの残高が所定の閾値を下回るときに行われる予定外の引き出し、通常は暗号通貨価格が不安定な時に行われます。

The following enumerate some perspectives for evaluation:
1) Security: The potential attack vectors should be examined, including through defined interfaces or physical threats.
2）ターンアラウンドタイム 1回の署名試行に要する総時間を評価する。コールドウォレットは一般的にターンアラウンド時間が長くなります。

3）スケーラビリティ。3）スケーラビリティ:システムが保持できる鍵の数を示す能力と、単位時間当たりに処理可能な署名試行回数を示す性能を測定する必要がある。

4）コスト コスト:カストディアンは、設備やメンテナンスに関する継続的な費用を削減することを目指すが、通常、一定の初期投資額で正当化される。

B. 異常の予測と対応

十分な対策とリスク管理が整っていても、システムの故障やセキュリティの侵害が発生する可能性があります。このような兆候を予測し、その影響を評価するとともに、復旧に必要な時間とコストを見積もることが重要である。

1）インシデント検出の容易さ。1）インシデント検出の容易さ:署名システムのアーキテクチャは、異常を検出する能力について評価する必要がある。例えば、ホットウォレットは出力を監視し、必要に応じて自動的に切断する別のシステムを持つことができ、一方、コールドウォレットは監視カメラのようなより基本的な技術を持つことができます。

2）緊急対応の複雑さ。攻撃者が鍵の制御を受けると、かなりの部分の資産が排出される場合でも、署名システムにはパニックボタンが入ることがある。破損していない鍵を使って、残りの資産を迅速かつ確実に避難させることで、損害を最小限に抑えることができるかもしれません。

C. システムの更新

ブロックチェーンシステムは、互換性を確保するために、ソフトフォークの形で頻繁にプロトコルの更新を受ける。ビットコインの分離された証人[129]やイーサリアムの取引手数料仕様の更新[130]など、いくつかの注目すべき例がある。これらの更新は、トランザクション形式の変更を伴います。もう一つの重要なアップデートはThe Merge in Ethereumで、これはブロックチェーンアーキテクチャに大きな影響を与えた[131]。Nem to Symbol の移動もこのカテゴリーに入る。一方、BitcoinのTaproot更新は、引き出しプロセスに直ちに影響を与えず[132]、他の様々な更新が定期的に発生する。
ソフトウェアとハードウェアのハードウェアハードウェアのアップデートは、脆弱性に対処し、最新の仕様を採用するために重要です。ただし、システムの安全性を損なわないように注意する必要があります。検体線検査は、セキュリティが直ちに脅かされない限り、更新の延期を検討すべきである。これにより、更新時に発生する脆弱性を最小限に抑えることができます。
1）頻度。ウォレットを設計する際には、システムの更新が義務付けられる頻度を予想する必要がある。これには、ホットウォレットのOSやファームウェアの更新、コールドウォレットの施設の保守などが含まれる。
2）更新の容易さ 2）更新プロセスの複雑さと安全性を評価する。これには、ソフトウェアの完全性の検証や明確な手順の確立が含まれる。

3）ベンダーの依存性。顧客は、特定のウォレット製品によって提供されるユニークな機能によって、特定のベンダーにロックすることが許容されるかどうかを評価する必要があります。この評価では、信頼、コスト、サポートなどを考慮する必要があります。

VII. 実装例 : 極限 - 極限

A. Overview

このセクションでは、E XTREME -C OLD と呼ばれるコールドウォレットの参照実装を紹介します。この実装は、これまで説明した背景とセキュリティの考察に基づいています。この実証実験の主な目的は、リスク管理における最大限の透明性を確保することである。

本論文の前半で述べた概念を完全に探るために、図2(a)に示すような複雑な環境と人間の関与を伴うシナリオを想定している。シモナイト[133]が言及した米国の交流で採用されたファラデーケージ法には類似点があるが、彼の論文では具体的な詳細が記載されていない。

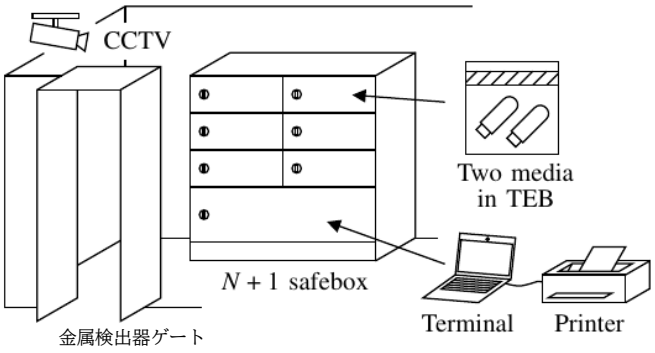

図5. KMFセットアップの例

ここで説明する方法は、著者自身の考察に基づくものである。先行研究では、エアギャップ環境からの秘密鍵の抽出が検討されており[43]、[134]、そのような攻撃に対する対策も議論する予定である。

B. 施設および設備

1）鍵管理施設 鍵の管理を効果的に行うためには、物理的に安全な部屋、すなわち鍵管理施設(KMF)が不可欠である。図 5 は、その構成例である。災害の影響や、KMF内のスタッフによる破壊的な行動の可能性から、2つ以上のKMFを地理的に独立した複数の施設に設置することが必要である。

KMFの物理的なセキュリティ対策と論理的なセキュリティ対策を適切に行うことが重要です。例えば、米国連邦政府は、高セキュリティ施設の構造的要件を確立している[135]。KMFのチェックリストを表Iにまとめた。

KMFはロッカーにN+1個以上のコンパートメントを装備する必要があります。このうち、N個のコンパートメントは、N個の秘密株式を安全に保存するために使用され、それらは別々の保管媒体に記録される。もう一つの区画、できれば大きな区画は、操作端末とプリンターを保存するために使用されます。各区画のキーと秘密分散は、対応する会計監査人が独占的に保有する必要があり、機器を搭載した区画のキーは、すべての会計監査人に複製することができます。

サイドチャネル攻撃や不正なデータ抽出のリスクを軽減するため、個人の電子機器の存在を禁止するポリシーを実施することを推奨します。この方針は、金属検出器を使用することで実施することができます。

2）端末とプリンター 各KMFでは、秘密鍵を処理するために、信頼できるコンピュータ、操作端末、プリンターを装備する必要があります。これらの機器は、一般的に入手可能なあらゆる製品ですが、安全なサプライチェーンを通じて調達する必要があります。準備の際、バッテリー、ストレージ、通信モジュール、オーディオデバイスなど、動作端末の特定のコンポーネントを削除する必要があります。これにより、サイドチャネル攻撃のリスクを排除し、複数の署名セッションにまたがるデータを持続させる能力を排除することができます。

TABLE I
KMFのセキュリティ・インサイダーメント

Physical perspectives	Fire	KMFはガス状消火方式か?
	Water damage	洪水を防ぐために、KMFはより高い階に位置していますか?漏水に対する防水処理は行われているか?
	Structure	KMFは地震やハリケーンの被害に対して建築基準法を満たしているか?
	Power supply	アクセス制御、監視、照明のための緊急電源はありますか?電気系統の防雷装置は整備されていますか?
	Interior elements	KMFは破壊的な行為に耐えられる非可燃性で堅牢な材料で仕上げられていますか?
	Windows	KMFは窓がないのですか?開口部には金網やその他の物理的遮断を設けていませんか?
	Access routes	KMFへの正常なアクセスルートは1つだけですか?ドアや緊急の出口は、緊急時に内部からしか開けないように設計されているか?
	Signs	建物の内側や外側にKMFの目に見える表示はありませんか?
	Alarms	その建物には緊急時の警報システムがあるか?
Logical perspectives	Authentication	KMFに参加するすべての人は、IDカード、パスコード、バイオメトリクスなど複数の要素によって認証されているか?ある一定期間、記録は保持されるか?
	Access control	KMFの単独での居住を禁止するための技術的な統制は設けられていますか?
	Surveillance	Can the KMF be monitored by cameras, incuding during power outages? Is the video footage retained?
	Metal detection	Is there a metal detector to prevent unauthorized bringing in or taking out of electronic equipment?

OSOSとKMFの外側との間の情報交換は、QRコードで表示され、紙に印刷されます。そのため、動作端末には内蔵されたカメラが必要です。

操作端末は、KeyGenとSignのプログラムを実行します。これらのプログラムは、任意の方法で実装することができます。参考文献[136]では、キーマネージメントプログラムを備えたカスタム Linux 画像を紹介しています。IANA もオフライン端末から HSM を動作させるために、同じように COEN [137] を開発している。

これらのデバイスの完全性は非常に重要です。したがって、デバイスは使用しないまま改ざんを防ぐために安全に保管され、実行中のソフトウェアのハッシュ値は動作時に検証されなければならない。

3）ストレージメディア。3）ストレージメディア:秘密鍵は、本アプローチではN株に分割される。これらの各株式は、それぞれ異なる会計監査人に対応する。各共有は、USBメモリスティックなどのストレージ媒体に記録され、冗長性のために少なくとも2つのコピーに複製されます。これらのコピーは、次に改ざん防止袋(TEB)にしっかりと入れられ、使用されない場合は対応する会計人のコンパートメントに保管される。さらに、バックアップとして、各KMFのTEBの正確な重複セットが準備される。

C. ヒトの関与

我々のアプローチでは、N人の会計担当者のうちM人が署名手続きを行う必要がある。各宝庫は、各KMFの個々のコンパートメントに保管される鍵の特定の部分を確保する責任を負います。このような、一般に二人完全性(以上)と呼ばれるプロセスに複数人を必要とする管理方針は、米国政府機関だけでなく、他の高セキュリティ施設でも採用されている。

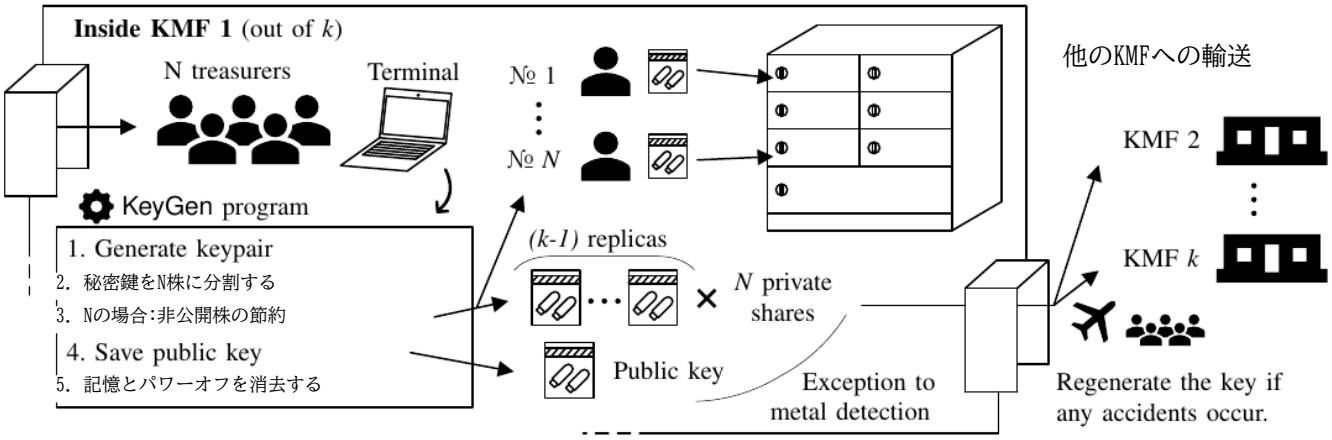

Fig. 6. Outline of KeyGen process

TABLE II
Iフラッド・トリアンの例です。

Motivation	• 大量の暗号通貨に移行する。
Opportunity	会社に対する不満や憤り。署名キーがロードされた動作端末への物理的な存在感。
Justification	– "私の給料は高くない。手続き上の誤りを非難されるべきではない。" • "私は経営者から公平に扱われていない。彼らは得るものに値する"

1）不正行為の防止と談合。クレッシーは、不正行為の条件を特定し、その中には、不正をコミットする動機、詐欺をコミットする機会、合理化または正当化の存在などが含まれる[138]。これらは現在、詐欺の三角形として広く知られている[139]。表 II は、KMF で発生しうる不正の要素の例である。

個人が不正をしようとする尤度pが全メンバーで一様であるとき、N人のメンバーのうちM人が特定の時点で談合する確率は、(1)に示す単純な二項確率として計算することができる。これは潜在的な不正リスクを定量化するのに有効である。

$$F = \binom{N}{M} p^M (1-p)^{N-M} \tag{1}$$

現実には、職業や人間関係、給与格差、階層的な違いなどの環境上の理由から、pがすべての会計人と等しいと仮定することは不可能かもしれません。また、例えば、法的な通貨支出に必要な承認者数に基づいて、十分なMを決定することもできる。

2）運用ミスの防止 意図的な誤行動とは別の視点として、人間はタスクを実行する際に意図しないミスによってミスをする可能性がある。さらに、重要な機器を扱わなければならないという心理的なプレッシャーがあるため、手順を忘れてしまう可能性もあります。そこで、作業進行度チェックリストを作成しました。

D. KeyGen – 鍵生成

図6に示すように、N人の会計専門職は1つのKMFに集まり、秘密鍵を生成し、それを営業端末上でN株に分割する。すべての株式が物理的に他のKMFに輸送されると、KeyGenは完全であるとみなされます。

1）乱数生成。セクション III-A で述べたように、プライベート署名鍵の生成に用いるエントロピー源は、理想的には完全ランダムであるべきである。OpenSSL の CTR_DRBG 実装を採用しました。これは、NIST SP 800-90A に準拠した決定論的ランダムビット生成アルゴリズムの一つであり、FIPS 140-2 となります。その他のオプションとしては、真の乱数発生器やストリーム暗号を使用する方法があります。

CTR_DRBG については、Campagna は鍵長が 112 ビット以外の場合、期待されるランダム性が達成されない脆弱性を示しているが [140]、ほとんどの暗号通貨は数百 ビット以下の署名鍵を使用するため、新しい種でアルゴリズムを初期化し、望ましい長さに達するとかなり容易に解決することができる。Woodageらは、RNGの内部状態が観測できる場合の脆弱性について議論し、OpenSSLの実装を検討した[141]。しかし、本手法のKeyGenはKMFのエアギャップされた動作端末で行われることを考慮すると、これは大きな問題にはならない。また、StrenzkeはOpenSSLのランダムアルゴリズムの実装についても検討した[142]。

2）Secretを破棄する。署名鍵をShamirの方法で分割し、使用するブロックチェーンや署名アルゴリズムの種類に依存しない方法で鍵を分割することができる。このアプローチの利点は、アルゴリズムが単純であるため、実装エラーのリスクが低いことである。VSSやMPCは、動作端末の整合性を信頼しているため、必要ありません。

3）秘密鍵の分配。すべての会計係は署名鍵を各KMFに転送する。すべてのKMFが、生成された鍵を問題なくそれぞれの区画にうまく装備したら、対応する暗号通貨アドレスをすぐに使用できるようにすることができます。交通事故のリスクについては、第 VIII-A3 章で説明する。

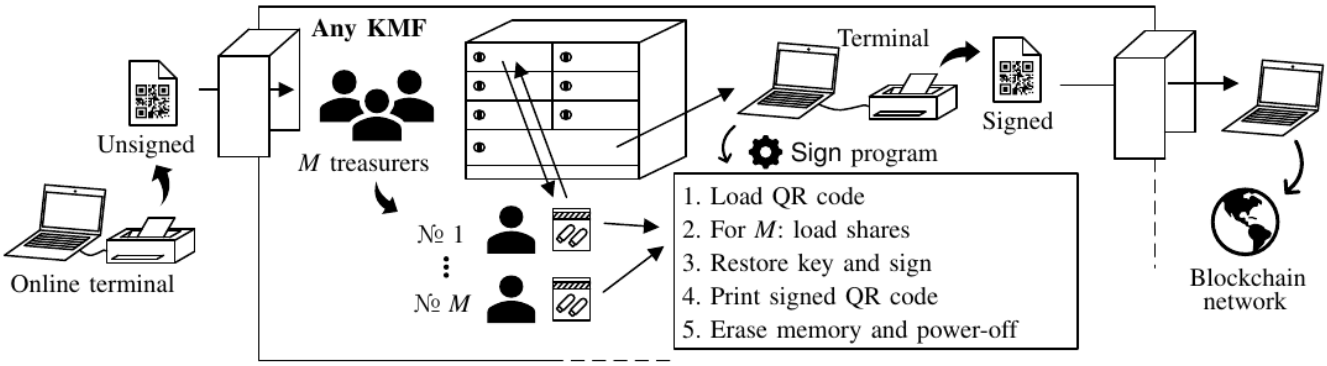

図7. サインプロセスの概要

E. 署名 – 署名の取引

図7に示すように、会計監査人は、KMFに符号なし取引を持ち込み、引き出しを行う。これはSignの入力となる。署名プロセスは、複数の会計監査人の監督のもと、営業端末上で行われます。署名された取引は、会計監査人との間で外部に出し、ブロックチェーンネットワークにブロードキャストされます。

1) KMF外での署名なし取引の準備:いずれかの会計担当者は、完全同期のオンラインブロックチェーンノードを使用して、KMF外で署名される引き出し取引を準備する。この取引はQRコードに変換され、紙に印刷され、他の宝庫が検証するための人間が読める詳細とともに表示されることが望ましい。

2) KMFの締結:M個の宝庫の組み合わせであれば、KMFに登録し、一緒に取引を行う。QRコードの改ざんや署名鍵のロードを伴う実行中の動作端末の搬出など、不正な行為を防ぐため、全プロセスを通じてKMFへの入退出が禁止されています。

3) 署名プロセス。会計係は、営業端末を使用して取引に署名する。

1) QRコードをスキャンし、トランザクションをデコード
2) する。転送の量と転送先を確認する。M個の鍵シャード
3) から署名鍵を復元する。トランザクションに署名する。
4)
5) Encode the signed transaction into a QR code.
6) Print the QR code on a sheet of paper.
7) Power off the operating terminal.

上記のステップ2において、宝庫は、追加のメタデータや情報なしに、QRコードのエンコードされたデータが予想される引き出しの詳細、すなわち目的地と金額と正確に一致することを保証しなければなりません。ステップ3では、M個の宝庫がそれぞれの鍵シャードを取り出し、それを動作ターミナルにロードし、シャードをその区画に戻し、安全にロックします。

4) KMFの退出と取引のブロードキャスト。KMFから印刷されたQRコードが実行された後、いずれかの宝物者がスキャンしてオンラインブロックチェーンノードにロードし、ブロックチェーンネットワークにブロードキャストする。QRコードの付いたシートは廃棄することができます。

F. 異常事態への対応

1) 単一媒体の故障:もし会計監査人の媒体に欠陥がある場合、会計監査人は同じ区画の他の媒体を複製して回収することができます。欠陥のある媒体は完全に破壊されなければならない。両方のメディアに欠陥がある場合、シャードはKeyGenの手順と同様に、他の宝庫のメディアを使用して再作成する必要があります。N – Mセット以上の失敗は、キーが回復不可能で、新しいキーを生成する必要がある次のケースと同等として扱われるべきです。

2) 災害 KMF に影響する KMF:N – M 組以上の宝くじが被害を受けた場合、被害を受けた KMF の鍵は本質的に失われていると仮定することができる。
最も安全なアプローチは、一時的にまたは永久に新しいKMFを確立し、KeyGenプロセスによって新しいキーを生成することです。影響を受けた住所の資金は、残存リスクを最小化するために新しい住所に移転される べきである。さらに、流動性供給者など、古い住所を知っているステークホルダーには、新しい住所を通知する必要があります。

また、影響を受けたKMFの完全性を回復し、他の信頼性の高いKMFからキーを複製することも可能です。ライブオペレーションキーのトランスポートについては、次のセクションで説明します。

3) メディアの損失または派手性。メディアの損失:メディアが突然失われた場合、影響を受けるシャードの数に関係なく、その鍵は侵害されたものと考えるべきである。そのような場合、新しい署名鍵を生成することが重要である。回復の手順は、前回のケースと変わりません。

G. 代替的な実装と比較

1) より単純な KMF を使う:堅牢な KMF を構築することは困難な作業であり、場合によっては実行不可能な場合がある。サイドチャネル攻撃に対する脆弱性が理論的に増加し、物理的なブルートフォース侵入のリスクも増加するにもかかわらず、適切な代替制御が実装されれば、軽量設備を利用できる可能性がある。

盗難を防ぐための対策を検討することは特に重要である。オリジナルの方法では、HSMやハードウェアウォレットが提供するセキュリティとは異なり、鍵は媒体に保存され、いかなる暗号プロセッサにも拘束されませんでした。それらのデバイスでは、デバイスが盗まれたとしても鍵は保護され、すぐに侵害されることはないでしょう。

2）HSMの利用:暗号通貨をサポートする汎用HSMが市場に出回っている。このようなHSMを使用する場合、鍵導出のための種が生成され、HSM内に内部に格納され、署名鍵は必要に応じてエフェメラルに導出される。E XTREME -C OLDでHSMを使用する利点は、物理的な操作を簡素化でき、N + 1個のロッカーが不要になる代わりに、HSMを保管するための安全なものだけが必要になることです。さらに、KeyGenとSignソフトウェアは、PKCS #11のCryptokiを使用してHSMにコマンドを送るだけでよい[143]。
しかし、HSM を使用することで、必ずしも人間の関与が単純化されるわけではありません。FIPS-140はセキュリティレベルを定義しており、通常、レベル3またはレベル4は高セキュリティ環境で使用され、HSMの保護ストレージにアクセスするために厳格な認証が必要です。M-of-N認証の設定では、HSMの保護されたストレージは、スマートカードまたは専用トークンに分散して格納される鍵で暗号化されます。このプロセスは我々のアプローチと何ら変わりはなく、人員交代が発生した場合にも同様の課題を提起する。

実世界の例では、Root KSK管理ではレベル4と認証されたHSMが使用されています。HSM上のRoot KSKの復号キーは、3-of-7構成でCrypto Officer(CO)が保持する複数のスマートカードに分割されています。HSM が運用されるか、CO が交換されるたびに、3 つ以上の CO が施設に移送される。

3）ハードウェアウォレットの使用。ストレージメディアやHSMを使用する代わりに、前節で説明したリスクを受け入れ、ハードウェアウォレットを利用するという代替オプションがあります。
ほとんどのハードウェアウォレット製品は、ニーモニックフレーズを使用してHDウォレットを生成し、バックアップ目的でニーモニックを表示する関数を提供することが多いです。この製品設計に合わせるため、保管者は、会計係がそれを覚えるリスクを最小限に抑えるために、24語のニーモニックフレーズを選択する必要があります。そして、ニーモニックフレーズは、できれば物理的な材料で、補助的な財布としてバックアップされる必要があります。トレジャーは、ウォレットがCCTVカメラの視界から外れないようにする必要があります。また、特にハードウェアウォレットは通常1つのパスワードで保護されているため、M-of-N認証の実装は技術的に困難である可能性があることも注目すべき点です。N + 1 ロッカーも不適当かもしれません。

スケーラビリティの面では、多くのハードウェアウォレット製品に、容量の制約から1台のユニットでサポートできる暗号通貨の数に制限があります。したがって、カストディアンが複数のブロックチェーンにまたがって多くの鍵をホストするつもりである場合、それに応じて鍵を配布するために複数のユニットを調達することを検討する必要があります。
4）ストレージメディアのオプション。4）ストレージメディアのオプション:鍵を格納するための適切なストレージメディアは、組織の選択に基づいて調達する必要がある場合があります。機密性を高めるために、[144]で示されたように、ハードウェア暗号化で取り外し可能なメディアを使用することができます。より高い耐久性を得るためには、より安定したメモリセルを持つ産業グレードのデバイスを使用することができます。企業の完全性を維持するために、[145]で説明されているようなライト・オン・メモリを使用することができる。残念ながら、今回の調査では、これらの機能をすべて備えた製品は見つかりませんでした。現実には、ある種の妥協が必要かもしれません。

5）TEE上のKeyGenとSignのプログラム。本アプローチでは、動作端末上で通常のプログラムとして動作するソフトウェアを実装した。しかし、シャミールの秘密分散方式を利用したため、動作中に完全な形式の鍵がメモリに存在することに注意することが重要です。これは、宝庫がKMFの権力がまだ継続している状態で、そのようなターミナルを取る場合、セキュリティリスクを発生させます。ソフトウェアをTEEで動作させることで、開発コストは上がるかもしれませんが、実行中の端末からキーを抽出するリスクを低減できる可能性があります。

VIII. Evaluation of Extreme-Cold

A. Security

E XTREME -C OLD は、視覚、電磁、音声の脆弱性を悪用するサイドチャネルを含む様々な既知の攻撃を効果的に緩和し、これまでの研究で潜在的な攻撃ベクトルとして同定されていると確信しています。以下の段落では、我々のアプローチの背後にある追加的な考察と推論について述べる。

1）金属検出。金属検出ゲートの実装は、不注意または意図的にKMFにアイテムを導入または除去することに対する予防措置として機能する。例えば、サイドチャネル攻撃に使用できるスマートフォンや、コンパートメント内の本物のメディアと交換できるリムーバブルメディアは禁止されるべきです。

例外もあります。鍵盤の物理的な鍵は、ダイヤルロックでない限り、また、通過するソフトウェアや鍵のメディアも許可されるべきです。後者の場合、メディアはプラスチック製ケースにしっかりと収められ、TEB内に配置されなければならない。これは、TEBにダメージを与えることなく、メタルプローブでメディアを読むことができないようにするためです。
2）トレジャーの誤動作。KeyGenはN人の会計監査人、SignはM人の会計監査人によって一緒に行われます。その過程で、そのうちの一人が不正行為を行う可能性があることに変わりはありません。

署名鍵の機密性を維持するために、不正行為が疑われる場合は、最初からKeyGenプロセスを開始することをお勧めします。同様に、署名の場合、責任ある宝庫は操作端末を強制的にシャットダウンし、ロードされた鍵をメモリから消去する必要があります。

3）KeyGen 中の鍵の物理的輸送。KMF の外部での損失や不正アクセスなど、輸送中の事故のリスクを軽減するため、会計担当者は鍵を運用する前に、各 KMF において TEB 内のすべての鍵共有の完全性を確保する必要があります。トレジャーは、互いにクロスチェックを行い、TEBに欠陥がないことを確認することが要求される。欠陥が検出された場合、鍵はゼロから再生成されなければならない。このクリティカルキーの輸送方法は、まだナイーブですが、DNSSECのRoot KSKの管理にも採用されています[14]。
4）異常後の運用キーの物理的輸送。原理的には、KMFの外部で運用キーを輸送することは安全ではないが、確立された鍵分配法を用いて、運用KMF_{src}から損傷KMF_{dst}への鍵の複製が可能である.

KMF_{dst}の安全性が確認された後、M個の宝庫を合わせると以下のような方法で行うことができます。

1) Generate an encryption keypair (ek, dk) in $\mathrm{KMF_{dst}}$.
2) ekの代替を防ぐため、複数の宝庫にKMF_{dst}からKMF_{src}に輸送させる。
3) KMF_{src} で ek の完全性が確認されたら、sk を ek で端末上の暗号 c に暗号化する。
4) cをKMF_{dst}に安全に戻し、dkで復号化します。得られた sk を M-of-N コンフィギュレーションにリシャードし、コンパートメントに格納します。

この鍵の輸送方法は、HSM間の鍵の複製に似ており、宛先HSMはHSM間の安全な輸送チャネルを作成するためのラッピング鍵を生成する。Diffie-Hellman鍵交換と同様に、中間者攻撃にも脆弱であるため、ekの完全性を独自に確保する必要がある。

5) 悪意のあるソフトウェアによる鍵情報の流出。Naor らは、視覚的な方法を用いて秘密分散を行う方法を提案している[146]。この応用として、単一または複数の QR コードを用いたステガノグラフィが、機密情報を埋め込むために研究されている［147], [148]。QRコードに隠された情報と通常の情報を区別することは困難です。なぜなら、結果として得られるQRコードに多くのエラーセルが存在することが唯一の指標だからです。署名されたトランザクションの生成と印刷の際に秘密鍵の埋め込みを防ぐために、QRコード処理アルゴリズムの完全性を確保することが重要である。
6) CCTV Recorded Footing: KMFの物理的セキュリティ対策は厳格であるが、監視カメラのような搾取可能な情報チャネルが残っている。監視カメラの映像は、潜在的な不正行為を調査するための証拠として極めて重要であり、要求事項から除外することはできない。KMFのキーボード入力の秘密性を確保するため、操作端末に画面フィルタを実装し、キーボード入力を隠すためのカバーを貼った。

B. ターンアラウンドタイム

モックアップ施設を建設し、実験を行った。我々のセットアップは、4つのうち3つの宝くじの閾値を設定したビットコインテストネットをターゲットとした(N＝ 4 , M＝ 3)。

実験から、KeyGenはかなり時間がかかることを学びました。平均して3回程度の試行で、1回目のKMFで署名鍵の生成に約50分、2回目のKMF(予算の関係上同じ部屋を再利用)で保存するのに約35分かかった。この長い期間には、(1)メディアと鍵の完全性を厳密に検証する必要性、(2)参加者が重要だが知らない作業を行う際の精神的プレッシャーなど、いくつかの要因が観察された。

符号に関しては、15回の試行のうち、1回の取引にサインする最初の2回の試行は、KMFへの参入から退出まで1時間以上かかった。しかし、参加者はプロセスに慣れてくると、最後の6回の試行の間、30分でそれを終了させることができた。通常の暗号通貨取引所におけるコールドウォレット操作性として許容範囲と考える。

C. Scalability

E XTREME -C OLD では、HDウォレットは実験していないが、1つの秘密鍵から複数のコールドアドレスを生成するために使用することができる。複数の鍵を単一の媒体に格納することは技術的に可能であり、異なるシードやブロックチェーンからの様々なアドレスの管理が可能である。

署名性能の面では、この方法は、複数のトランザクションを同時にバッチで署名することを可能にする。プロセスを効率化する一つの方法は、トランザクションデータをエンコードするQRコードを順次スキャンすることです。しかし、冷蔵倉庫からの頻繁な引き出しが必要な場合は、ホットウォレットの多用を検討する価値があるかもしれません。

D. Cost

コンピュータ、プリンター、ストレージメディア、CCTV などの機器の初期セットアップコストは、本実験では約 3,000 ドルであった。これらのデバイスは一般的に寿命が長いため、コストが正当化される。

KMFの施設賃料は、この設計の全体的なコストに大きな影響を与える、大きな経常的費用である。KMFがデータセンターのコロケーションとして導入されている場合、月額コストは数千ドルから変動する可能性があります。コスト削減の一つの方法は、一般的なラックをロッカーとして使用することです。もう一つの選択肢は、私たちが選んだオフィスルームを利用することです。

E. 不正の予測のしやすさ

KMF施設には、ドアセンサーやCCTVのような従来の侵入防止対策が搭載されており、侵入者をリアルタイムで迅速に特定することができる。また、不正行為があった場合の監査証跡として機能します。

さらに、このアプローチでは、TEBにおけるシールメディア、コンパートメントへの保存、金属検出器の使用など、様々な操作手順にクロスチェック動作を組み込んでいる。これにより、担当の会計監査人が不正な行為や不正行為を容易に発見することができます。

F. Updates

1) トレジャーの交換(Changing N)。スタッフの交換は、組織でよく見られることである。新しい宝庫を追加する場合、既存のM個の宝庫はKMFのキーを復元し、新しい宝庫のために新しいシャードを作成することが要求されます。一方、宝庫が退職し、宝庫の数が減少しても、M以下でなければ、単に退職者 の区画の内容を破壊するだけで十分である。これらのアクションは、各KMFで実行する必要があります。スタッフ交換の場合、ロッカーの内容の確認は奨励されるが、ロッカーのキーやダイヤルの組み合わせを新しいものに渡す出発者のような単純なプロセスがあり得る。

2) しきい値の変更(Mの変更)。必要な宝庫の数をM_{old}からM_{new}に変更することは、Shamirの秘密分散の特性により、より複雑になります。この変更を実装するためには、N人全員が存在し、M_{old}人を使ってキーを復元し、閾値がM_{new}になるようにシャードを再作成する必要があります.さらに、各区画のN個の古いメディアをすべて破壊しなければならない。すべて の KMF について、それぞれ同じことを行ってください。

3）署名鍵の追加。KeyGenは新しい署名鍵を追加するとき、例えば新しいウォレット、新しい暗号通貨、新しいブロックチェーンのために毎回実行されなければならない。このプロセスは、既存のキーに影響を与えません。
4）ソフトウェアの更新。プロトコルの更新が暗号通貨やブロックチェーンに与える潜在的な影響は簡単である。組織は、(1)KeyGenまたはSignのための更新されたソフトウェアを作成し、(2)アルゴリズムの正しさをチェックし、(3)ハッシュまたはコードシグニ ングでその完全性を確保する必要がある。(4) 旧メディアを置き換えるために、TEB 内の USB メモリースティックなどのストレージメディアを使用して、更新されたソフトウェアを KMF に持ち込む必要があります。古いメディアは破壊されるべきです。

G. ベンダー依存性

この方法は、機器や機器の特定のベンダーから独立したものです。KMFの物理的な構造は、移動の必要性がある場合、大きな課題となるかもしれないが、どのような場所でも確立することができる。KMFで使用される動作端末、プリンター、メディア、TEB、その他の機器には特定の要件がなく、様々な製品に対応することが可能です。

IX. Conclusion

暗号通貨は広く利用されており、暗号通貨の管理者はこのエコシステムにおいて重要な役割を担っている。一部の愛好家は中央集権化の流れに反対しているが、現在、大多数のユーザーは暗号通貨を現実の取引所に委託している。したがって、暗号通貨の管理者は、顧客の資産を安全に管理する必要があります。

本論文では、ウォレット実装をS IG S YSとしてモデル化し、セキュリティとリスク管理について考察した。また、重要な資産を扱うための合理的なアプローチとして、コールドウォレットの慣行に重点を置いてきた。しかし、いくつかの未解決の問題はまだ解決する必要があります。
1）軽量なコールドウォレットを実装する。参照例E XTREME -C OLDに含まれる操作は、リソースを大量に消費することを認識する。セキュリティを確保し、リスクを効果的にコントロールしながら、コールドウォレットを簡単に導入できるような、より軽い経営手法を模索するために、さらなる研究が必要である。

2）効率的なウォレット操作。ウォレット間の資産管理の側面、特にホット層とコールド層の間のバランシングやタイミング転送の観点からは、これまで議論していない。この点については、消費者との集中型取引所、大口取引所を扱う流動性供給者、分散型取引所など、さまざまなタイプのビジネスが異なる慣行を持っていると考えています。さらに、暗号通貨の貸し出しやステークの選択肢も、これらの慣行に影響を与える可能性があります。残念ながら、この特定のトピックに関する関連文献を見つけることができませんでした。
3）非ファンジブルタイプの資産 本手法は、一般的なブロックチェーンのネイティブトークンや、ERC-20や通常のウォレットで管理可能な互換トークンなど、主要な暗号通貨に着目している。しかし、2021年以降、非可逆トークン(NFT)が注目されており、他の派生トークンも活発に開発されている[149]。例として、金、債券、不動産などのオフチェーン資産に裏打ちされた実世界の資産(RWA)がある[150]。これらのタイプの資産は本質的にユニークであり、異なるプラクティスを必要とする場合があります。

References

[1] W. Fumy and P. Landrock, “Principles of key management,” *IEEE Journal on Selected Areas in Communications*, vol. 11, no. 5, pp. 785–793, 1993.
[2] G. R. Blakley, “Safeguarding cryptographic keys,” in *1979 International Workshop on Managing Requirements Knowledge (MARK)*, 1979, pp. 313–318.
[3] S. Eskandari, D. Barrera, E. Stobert, and J. Clark, “A first look at the usability of bitcoin key management,” 2015. [Online]. Available: https://www.ndss-symposium.org/ndss2015/ndss-2015-usec-programme/first-look-usability-bitcoin-key-management/
[4] Z. Jaroucheh and B. Ghaleb, “Crypto assets custody: Taxonomy, components, and open challenges,” in *2023 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2023, pp. 1–6.
[5] G. J. Popek and C. S. Kline, “Encryption and secure computer networks,” *ACM Comput. Surv.*, vol. 11, no. 4, pp. 331–356, dec 1979.
[6] A. Shamir, “How to share a secret,” *Commun. ACM*, vol. 22, no. 11, pp. 612–613, nov 1979.
[7] ASC X9, *ANSI X9.17, Financial Institution Key Management (Wholesale)*. American Bankers Association, Apr. 1985. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/FIPS/fipspub171.pdf
[8] P. Zimmermann, *PGP Source Code and Internals*. Mit Press, 1995.
[9] S. Capkun, L. Buttyán, and J. P. Hubaux, “Self-organized public-key management for mobile ad hoc networks,” *IEEE Transactions on Mobile Computing*, vol. 2, no. 1, pp. 52–64, 2003.
[10] ITU-T, “X.509 (10/19) : Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks,” Oct. 2019.
[11] R. Charette, “DigiNotar certificate authority breach crashes e-government in the Netherlands,” *IEEE Spectrum*, 2011.
[12] CAB Forum, “Baseline requirements for the issuance and management of publicly-trusted certificates - version 2.0.1,” p. 42, Aug. 2023.
[13] S. Rose, M. Larson, D. Massey, R. Austein, and R. Arends, “RFC 4033, DNS Security Introduction and Requirements,” Mar. 2005.
[14] IANA, “Key signing ceremonies.” [Online]. Available: https://www.iana.org/dnssec/ceremonies
[15] E. Barker, *SP 800-57, Recommendation for Key Management: Part 1 – General*. National Institute of Standards and Technology, May 2020.
[16] E. Barker, M. Smid, D. Branstad, and S. Chokhani, *SP 800-130, A Framework for Designing Cryptographic Key Management Systems*. National Institute of Standards and Technology, Aug. 2013.
[17] J. Wilbur L. Ross and W. Copan, *FIPS 140-3, Security Requirements for Cryptographic Modules*. National Institute of Standards and Technology, Mar. 2019.
[18] G. M. Raimondo and L. E. Locascio, *FIPS 186-5, Digital Signature Standard (DSS)*. National Institute of Standards and Technology, Feb. 2023.
[19] S. Bellovin and R. Housley, “RFC 4107, Guidelines for Cryptographic Key Management,” Jun. 2005.
[20] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.
[21] E. Ben Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza, “Zerocash: Decentralized anonymous payments from Bitcoin,” in *2014 IEEE Symposium on Security and Privacy*, 2014, pp. 459–474.
[22] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in *2015 IEEE Symposium on Security and Privacy*, 2015, pp. 104–121.
[23] S. Suratkar, M. Shirole, and S. Bhirud, “Cryptocurrency wallet: A review,” in *2020 4th International Conference on Computer, Communication and Signal Processing (ICCCSP)*, 2020, pp. 1–7.
[24] Y. Erinle, Y. Kethepalli, Y. Feng, and J. Xu, “Sok: Design, vulnerabilities, and security measures of cryptocurrency wallets,” Jul. 2023. [Online]. Available: https://arxiv.org/abs/2307.12874
[25] P. Alpeyev and Y. Nakamura, “How to launder $500 million in digital currency,” Jan. 2018. [Online]. Available: https://www.bloomberg.com/news/articles/2018-01-29/how-to-launder-500-million-in-digital-currency-quicktake-q-a

[26] W. Zhao, “Crypto exchange zaif hacked in $60 million bitcoin theft,” Sep. 2018. [Online]. Available: https://www.coindesk.com/markets/2018/09/20/crypto-exchange-zaif-hacked-in-60-million-bitcoin-theft/

[27] OSC, “QuadrigaCX: A review by staff of the Ontario Securities Commission,” Apr. 2020. [Online]. Available: https://www.osc.ca/quadrigacxreport/

[28] FTX, “Exhibit A – Document #1242, Attachment #1,” Apr. 2023, case 22-11068-JTD. United States Bankruptcy Court, District of Delaware.

[29] M. D. Detmer, “Petition for appointment of receiver, temporary injunction, and other permanent relief,” Jun. 2023, case A-23-872963-B. Eighth Judicial District Court, Clark County, Nevada.

[30] K. Oosthoek and C. Doerr, “From hodl to heist: Analysis of cyber security threats to Bitcoin exchanges,” in *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2020, pp. 1–9.

[31] R. Chandramouli, M. Iorga, and S. Chokhani, *Cryptographic Key Management Issues and Challenges in Cloud Services*. Springer New York, 2014, pp. 1–30.

[32] I. Kuzminykh, B. Ghita, and S. Shiaeles, “Comparative analysis of cryptographic key management systems,” in *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*, O. Galinina, S. Andreev, S. Balandin, and Y. Koucheryavy, Eds. Cham: Springer International Publishing, 2020, pp. 80–94.

[33] S. Xiao, W. Gong, D. Towsley, Q. Zhang, and T. Zhu, “Reliability analysis for cryptographic key management,” in *2014 IEEE International Conference on Communications (ICC)*, 2014, pp. 999–1004.

[34] S. Rana, F. K. Parast, B. Kelly, Y. Wang, and K. B. Kent, “A comprehensive survey of cryptography key management systems,” *Journal of Information Security and Applications*, vol. 78, p. 103607, 2023.

[35] L. Lamport, “Proving the correctness of multiprocess programs,” *IEEE Transactions on Software Engineering*, vol. SE-3, no. 2, pp. 125–143, 1977.

[36] D. L. Evans, P. J. Bond, and A. L. Bement, Jr., *FIPS 199, Standards for Security Categorization of Federal Information and Information Systems*. National Institute of Standards and Technology, Feb. 2004.

[37] A. Avižienis, J. C. Laprie, B. Randell, and C. Landwehr, “Basic concepts and taxonomy of dependable and secure computing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 1, no. 1, pp. 11–33, 2004.

[38] M. Warkentin and C. Orgeron, “Using the security triad to assess blockchain technology in public sector applications,” *International Journal of Information Management*, vol. 52, p. 102090, 2020.

[39] Z. Gutterman, B. Pinkas, and T. Reinman, “Analysis of the Linux random number generator,” in *2006 IEEE Symposium on Security and Privacy (S&P’06)*, 2006.

[40] L. Dorrendorf, Z. Gutterman, and B. Pinkas, “Cryptanalysis of the random number generator of the Windows operating system,” in *ACM Trans. Inf. Syst. Secur.*, vol. 13, no. 1, nov 2009.

[41] Y. Yu, F.-X. Standaert, O. Pereira, and M. Yung, “Practical leakage-resilient pseudorandom generators,” in *Proceedings of the 17th ACM Conference on Computer and Communications Security*, ser. CCS ’10. Association for Computing Machinery, 2010, pp. 141–151.

[42] ISE, “Ethercombing: Finding secrets in popular places,” Apr. 2019. [Online]. Available: https://www.ise.io/casestudies/ethercombing/

[43] M. Guri, “BeatCoin: Leaking private keys from air-gapped cryptocurrency wallets,” in *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, 2018, pp. 1308–1316.

[44] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ECDSA),” *International Journal of Information Security*, vol. 1, 2001.

[45] D. Boneh and R. Venkatesan, “Hardness of computing the most significant bits of secret keys in Diffie-Hellman and related schemes,” in *Advances in Cryptology — CRYPTO ’96*, N. Koblitz, Ed. Springer Berlin Heidelberg, 1996, pp. 129–142.

[46] T. Pornin, “RFC6979, Deterministic Usage of the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA),” Aug. 2013.

[47] C. Decker and R. Wattenhofer, “Bitcoin transaction malleability and MtGox,” in *Computer Security - ESORICS 2014*, M. Kutyłowski and J. Vaidya, Eds. Cham: Springer International Publishing, pp. 313–326.

[48] “IEEE standard for general requirements for cryptocurrency exchanges,” *IEEE Std 2140.1-2020*, 2020.

[49] Y. Tsuchiya and N. Hiramoto, “How cryptocurrency is laundered: Case study of Coincheck hacking incident,” *Forensic Science International: Reports*, vol. 4, p. 100241, 2021.

[50] “Exchanges which let you create multiple deposit addresses,” Nov. 2020. [Online]. Available: https://bitcointalk.org/index.php?topic=5292667

[51] T. Hardjono, A. Lipton, and A. Pentland, “Wallet attestations for virtual asset service providers and crypto-assets insurance,” May 2020. [Online]. Available: https://arxiv.org/abs/2005.14689

[52] G. G. Dagher, B. Bünz, J. Bonneau, J. Clark, and D. Boneh, “Provisions: Privacy-preserving proofs of solvency for bitcoin exchanges,” in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS ’15. Association for Computing Machinery, 2015, pp. 720–731.

[53] OKX, “Proof of reserves.” [Online]. Available: https://www.okx.com/proof-of-reserves

[54] Binance, “Proof of reserves.” [Online]. Available: https://www.binance.com/en/proof-of-reserves

[55] AICPA, “Accounting for and auditing of digital assets, practice aid,” p. 60, Jul. 2023, aU Chapter 2, IV-A.

[56] “Cabinet office order on cryptoasset exchange service providers,” Mar. 2017, article 27, paragraph (2) and (3). [Online]. Available: https://www.japaneselawtranslation.go.jp/en/laws/view/4315#je_ch2at15

[57] Financial Services Agency of Japan, “Guideline for supervision of crypto-asset exchange service providers,” p. 46, Jun. 2021, iI-2-2-3-2 (3) (v). [Online]. Available: https://www.fsa.go.jp/common/law/guide/kaisya/e016.pdf

[58] J. Koning, “Japan was the safest place to be an ftx customer,” Dec. 2022. [Online]. Available: https://www.coindesk.com/consensus-magazine/2022/12/13/japan-was-the-safest-place-to-be-an-ftx-customer

[59] A. M. Antonopoulos, *Mastering Bitcoin*. O’Reilly Media, Inc., 2014.

[60] Blockchain.com, “Blockchain size.” [Online]. Available: https://www.blockchain.com/explorer/charts/blocks-size

[61] Etherscan, “Ethereum full node sync (archive) chart.” [Online]. Available: https://etherscan.io/chartsync/chainarchive

[62] A. G. Khan, A. H. Zahid, M. Hussain, and U. Riaz, “Security of cryptocurrency using hardware wallet and QR code,” in *2019 International Conference on Innovative Computing (ICIC)*, 2019, pp. 1–10.

[63] T. Bui, S. P. Rao, M. Antikainen, and T. Aura, “Pitfalls of open architecture: How friends can exploit your cryptocurrency wallet,” in *Proceedings of the 12th European Workshop on Systems Security*, ser. EuroSec ’19. Association for Computing Machinery, 2019.

[64] A. Voskobojnikov, O. Wiese, M. Mehrabi Koushki, V. Roth, and K. K. Beznosov, “The U in crypto stands for usable: An empirical study of user experience with mobile cryptocurrency wallets,” in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, ser. CHI ’21. Association for Computing Machinery, 2021.

[65] L. Van Der Horst, K.-K. R. Choo, and N.-A. Le-Khac, “Process memory investigation of the Bitcoin clients Electrum and Bitcoin Core,” *IEEE Access*, vol. 5, pp. 22 385–22 398, 2017.

[66] T. Volety, S. Saini, T. McGhin, C. Z. Liu, and K.-K. R. Choo, “Cracking bitcoin wallets: I want what you have in the wallets,” *Future Generation Computer Systems*, vol. 91, pp. 136–143, 2019.

[67] D. He, S. Li, C. Li, S. Zhu, S. Chan, W. Min, and N. Guizani, “Security analysis of cryptocurrency wallets in Android-based applications,” *IEEE Network*, vol. 34, no. 6, pp. 114–119, 2020.

[68] MetaMask, “Address poisoning scams.” [Online]. Available: https://support.metamask.io/hc/en-us/articles/11967455819035

[69] N. Ivanov and Q. Yan, “EthClipper: A clipboard meddling attack on hardware wallets with address verification evasion,” in *2021 IEEE Conference on Communications and Network Security (CNS)*, 2021, pp. 191–199.

[70] A. Perrig and D. Song, “Hash visualization : a new technique to improve real-world security,” *International Workshop on Cryptographic Techniques and E-Commerce*, vol. 25, 1999.

[71] A. Sarkar, “MetaMask scammers take over government websites to target crypto investors,” Sep. 2023. [Online]. Available: https://cointelegraph.com/news/metamask-scam-government-websites-crypto-investors

[72] S. Ro, “Bloomberg’s Miller Bitcoin gift stolen,” Dec. 2013. [Online]. Available: https://www.businessinsider.com/bloomberg-matt-miller-bitcoin-gift-stolen-2013-12

[73] T. Sans, Z. Liu, and K. Oh, “A decentralized mnemonic backup system for non-custodial cryptocurrency wallets,” in *Foundations and*

セキュリティの実践, G.-V. Jourdan, L. Munitier, C. Adams, F. Sèdes, and J. Garcia-Alfaro, Eds.Cham: シュプリンガー・ネイチャー・スイス、2023年、pp.355-370.

[74] E. Androulaki, G. O. Karame, M. Roeschlin, T. Scherer, and S. Capkun, "Evaluating user privacy in bitcoin," in *Financial Cryptography and Data Security*, A.-R. Sadeghi, Ed. Springer Berlin Heidelberg, 2013, pp. 34–51.

[75] P. Wuille, "Hierarchical deterministic wallets." [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki

[76] M. Palatinus, P. Rusnak, A. Voisine, and S. Bowe, "Mnemonic code for generating deterministic keys." [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0039.mediawiki

[77] P. Juola and P. Zimmermann, "Whole-word phonetic distances and the PGPfone alphabet," in *Proc. 4th International Conference on Spoken Language Processing (ICSLP 1996)*, 1996, pp. 98–101.

[78] M. Vasek, J. Bonneau, R. Castellucci, C. Keith, and T. Moore, "The bitcoin brain drain: Examining the use and abuse of bitcoin brain wallets," in *Financial Cryptography and Data Security*, J. Grossklags and B. Preneel, Eds. Springer Berlin Heidelberg, 2017, pp. 609–618.

[79] W. M. Shbair, E. Gavrilov, and R. State, "HSM-based key management solution for Ethereum blockchain," in *2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, 2021, pp. 1–3.

[80] S. Alrubei, E. Ball, and J. Rigelsford, "Adding hardware security into IoT-blockchain platforms," in *2022 IEEE Latin-American Conference on Communications (LATINCOM)*, 2022, pp. 1–6.

[81] Thales, "Securing digital currency with bitgo multi-signature and thales hsms - solution brief," Feb. 2020. [Online]. Available: https://cpl.thalesgroup.com/resources/encryption/bitgo-hsm-solution-brief

[82] D.-P. Dornseifer and T. von Bomhard, "How to sign ethereum eip-1559 transactions using aws kms," Feb. 2022. [Online]. Available: https://aws.amazon.com/jp/blogs/database/how-to-sign-ethereum-eip-1559-transactions-using-aws-kms/

[83] Thales, "Tamper, secure transport, and purple ped keys." [Online]. Available: https://thalesdocs.com/gphsm/luna/6.3/docs/usb/Content/overview/security_features/purple_keys_tamper_and_secure-transport.htm

[84] *ISO/IEC 19790:2012 – Information technology – Security techniques – Security requirements for cryptographic modules*. International Organization for Standardization, Aug. 2012.

[85] NIST, "Cryptographic module validation programs." [Online]. Available: https://csrc.nist.gov/projects/cryptographic-module-validation-program

[86] R. Bardou, R. Focardi, Y. Kawamoto, L. Simionato, G. Steel, and J.-K. Tsay, "Efficient padding oracle attacks on cryptographic hardware," in *Advances in Cryptology – CRYPTO 2012*, R. Safavi-Naini and R. Canetti, Eds. Springer Berlin Heidelberg, 2012, pp. 608–625.

[87] "Public comments received on draft nist sp 800-186: Recommendations for discrete logarithm-based cryptography: Elliptic curve domain parameters," Jan. 2020. [Online]. Available: https://csrc.nist.gov/files/pubs/sp/800/186/final/docs/sp800-186-draft-comments-received.pdf

[88] D. Boneh, B. Lynn, and H. Shacham, "Short signatures from the Weil pairing," in *Advances in Cryptology — ASIACRYPT 2001*, C. Boyd, Ed. Springer Berlin Heidelberg, 2001, pp. 514–532.

[89] K. Chalkias, F. Garillot, Y. Kondi, and V. Nikolaenko, "Non-interactive half-aggregation of eddsa and variants of schnorr signatures," in *Topics in Cryptology – CT-RSA 2021*, K. G. Paterson, Ed. Cham: Springer International Publishing, 2021, pp. 577–608.

[90] Thales, "Functionality modules." [Online]. Available: https://thalesdocs.com/gphsm/luna/7/docs/network/Content/Product_Overview/fms.htm

[91] J. Han, S. Kim, T. Kim, and D. Han, "Toward scaling hardware security module for emerging cloud services," in *Proceedings of the 4th Workshop on System Software for Trusted Execution*, ser. SysTEX '19. Association for Computing Machinery, 2019.

[92] M. Arapinis, A. Gkaniatsou, D. Karakostas, and A. Kiayias, "A formal treatment of hardware wallets," in *Financial Cryptography and Data Security*, I. Goldberg and T. Moore, Eds. Cham: Springer International Publishing, 2019, pp. 426–445.

[93] T. Bamert, C. Decker, R. Wattenhofer, and S. Welten, "Bluewallet: The secure bitcoin wallet," in *Security and Trust Management*, S. Mauw and C. D. Jensen, Eds. Cham: Springer International Publishing, 2014, pp. 65–80.

[94] H. Rezaeighaleh and C. C. Zou, "New secure approach to backup cryptocurrency wallets," in *2019 IEEE Global Communications Conference (GLOBECOM)*, 2019, pp. 1–6.

[95] A. Sarkar, "Ledger co-founder clarifies 'there is no backdoor' in 'Recover' firmware update," May 2023. [Online]. Available: https://cointelegraph.com/news/ledger-co-founder-clarifies-there-is-no-backdoor-in-recover-firmware-update

[96] J. Datko, C. Quartier, and K. Belyayev, "Breaking Bitcoin hardware wallets," Jul. 2017. [Online]. Available: https://media.defcon.org/DEF%20CON%2025/DEF%20CON%2025%20presentations/DEF%20CON%2025%20-%20Datko-and-Quartier-Breaking-Bitcoin-Hardware-Wallets.pdf

[97] A. Gkaniatsou, M. Arapinis, and A. Kiayias, "Low-level attacks in bitcoin wallets," in *Information Security*, P. Q. Nguyen and J. Zhou, Eds. Cham: Springer International Publishing, 2017, pp. 233–253.

[98] D. Park, M. Choi, G. Kim, D. Bae, H. Kim, and S. Hong, "Stealing keys from hardware wallets: A single trace side-channel attack on elliptic curve scalar multiplication without profiling," *IEEE Access*, vol. 11, pp. 44 578–44 589, 2023.

[99] S. Volokitin, "Software attacks on hardware wallets," Aug. 2018. [Online]. Available: https://i.blackhat.com/us-18/Wed-August-8/us-18-Volokitin-Software-Attacks-On-Hardware-Wallets-wp.pdf

[100] S. Golovanov, "Case study: fake hardware cryptowallet," May 2023. [Online]. Available: https://www.kaspersky.com/blog/fake-trezor-hardware-crypto-wallet/48155/

[101] M. Sabt, M. Achemlal, and A. Bouabdallah, "Trusted execution environment: What it is, and what it is not," in *2015 IEEE Trustcom/BigDataSE/ISPA*, vol. 1, 2015, pp. 57–64.

[102] M. Gentilal, P. Martins, and L. Sousa, "TrustZone-backed Bitcoin wallet," in *Proceedings of the Fourth Workshop on Cryptography and Security in Computing Systems*, ser. CS2 '17. Association for Computing Machinery, 2017, pp. 25–28.

[103] N. Lehto, K. Halunen, O.-M. Latvala, A. Karinsalo, and J. Salonen, "CryptoVault - a secure hardware wallet for decentralized key management," in *2021 IEEE International Conference on Omni-Layer Intelligent Systems (COINS)*, 2021, pp. 1–4.

[104] S. Fei, Z. Yan, W. Ding, and H. Xie, "Security vulnerabilities of sgx and countermeasures: A survey," *ACM Comput. Surv.*, vol. 54, no. 6, jul 2021.

[105] S. van Schaik, A. Seto, T. Yurek, A. Batori, B. AlBassam, C. Garman, D. Genkin, A. Miller, E. Ronen, and Y. Yarom, "Sok: Sgx. fail: How stuff get exposed," 2022. [Online]. Available: https://sgx.fail/

[106] G. Wood *et al.*, "Ethereum: A secure decentralised generalised transaction ledger," 2014.

[107] "Safe contracts." [Online]. Available: https://github.com/safe-global/safe-contracts

[108] V. Buterin, "Why we need wide adoption of social recovery wallets," Jan. 2021. [Online]. Available: https://vitalik.ca/general/2021/01/11/recovery.html

[109] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *Principles of Security and Trust*, M. Maffei and M. Ryan, Eds. Springer Berlin Heidelberg, 2017, pp. 164–186.

[110] P. Praitheeshan, L. Pan, J. Yu, J. K. Liu, and R. Doss, "Security analysis methods on ethereum smart contract vulnerabilities: A survey," Aug. 2019. [Online]. Available: http://arxiv.org/abs/1908.08605

[111] G. Destefanis, M. Marchesi, M. Ortu, R. Tonelli, A. Bracciali, and R. Hierons, "Smart contracts vulnerabilities: a call for blockchain software engineering?" in *2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE)*, 2018, pp. 19–25.

[112] K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, and S. Zanella-Béguelin, "Formal verification of smart contracts: Short paper," in *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, ser. PLAS '16. Association for Computing Machinery, 2016, pp. 91–96.

[113] B. Jiang, Y. Liu, and W. K. Chan, "Contractfuzzer: Fuzzing smart contracts for vulnerability detection," in *Proceedings of the 33rd ACM/IEEE International Conference on Automated Software Engineering*, ser. ASE '18. Association for Computing Machinery, 2018, pp. 259–269.

[114] D. He, Z. Deng, Y. Zhang, S. Chan, Y. Cheng, and N. Guizani, "Smart contract vulnerability analysis and security audit," *IEEE Network*, vol. 34, no. 5, pp. 276–282, 2020.

[115] P. Praitheeshan, L. Pan, and R. Doss, "Security evaluation of smart contract-based on-chain ethereum wallets," in *Network and System Security*, M. Kutyłowski, J. Zhang, and C. Chen, Eds. Cham: Springer International Publishing, 2020, pp. 22–41.

[116] F. Cassez, J. Fuller, M. K. Ghale, D. J. Pearce, and H. M. Quiles, "Formal and executable semantics of the Ethereum virtual machine in Dafny," in *Formal Methods*, M. Chechik, J.-P. Katoen, and M. Leucker, Eds., vol. 14000 LNCS. Cham: Springer International Publishing, 2023, pp. 571–583.
[117] Flow, "Accounts." [Online]. Available: https://developers.flow.com/build/basics/accounts
[118] T. P. Pedersen, "Non-interactive and information-theoretic secure verifiable secret sharing," in *Advances in Cryptology — CRYPTO '91*, J. Feigenbaum, Ed. Springer Berlin Heidelberg, 1992, pp. 129–140.
[119] C. P. Schnorr, "Efficient identification and signatures for smart cards," in *Advances in Cryptology — EUROCRYPT '89*, J.-J. Quisquater and J. Vandewalle, Eds. Springer Berlin Heidelberg, 1990, pp. 688–689.
[120] P. Wuille, J. Nick, and T. Ruffing, "Schnorr signatures for secp256k1." [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki
[121] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple schnorr multi-signatures with applications to Bitcoin," *Designs, Codes, and Cryptography*, vol. 87, 2019.
[122] J. Nick, T. Ruffing, and Y. Seurin, "MuSig2: Simple two-round Schnorr multi-signatures," in *Advances in Cryptology – CRYPTO 2021*, T. Malkin and C. Peikert, Eds. Cham: Springer International Publishing, 2021, pp. 189–221.
[123] R. Gennaro and S. Goldfeder, "Fast multiparty threshold ECDSA with fast trustless setup," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. Association for Computing Machinery, 2018, pp. 1179–1194.
[124] Y. Lindell and A. Nof, "Fast secure multiparty ecdsa with practical distributed key generation and applications to cryptocurrency custody," in *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '18. Association for Computing Machinery, 2018, pp. 1837–1854.
[125] J. Doerner, Y. Kondi, E. Lee, and abhi shelat, "Threshold ECDSA in three rounds," Cryptology ePrint Archive, Paper 2023/765, May 2023. [Online]. Available: https://eprint.iacr.org/2023/765
[126] J.-P. Aumasson and O. Shlomovits, "Attacking threshold wallets," Cryptology ePrint Archive, Paper 2020/1052, Sep. 2020. [Online]. Available: https://eprint.iacr.org/2020/1052
[127] N. Makriyannis and O. Yomtov, "Gg18 / gg20 tss beta parameter vulnerability," Aug. 2023. [Online]. Available: https://www.cve.org/CVERecord?id=CVE-2023-33241
[128] A. M. Antonopoulos, Apr. 2016. [Online]. Available: https://twitter.com/aantonop/status/720784384572465152
[129] E. Lombrozo, J. Lau, and P. Wuille, "Segregated witness (consensus layer)." [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0141.mediawiki
[130] V. Buterin, xEric Conner, R. Dudley, M. Slipper, I. Norden, and A. Bakhta, "Eip-1559: Fee market change for eth 1.0 chain." [Online]. Available: https://eips.ethereum.org/EIPS/eip-1559
[131] "The merge." [Online]. Available: https://ethereum.org/roadmap/merge/
[132] P. Wuille, J. Nick, and A. Towns, "Taproot: Segwit version 1 spending rules." [Online]. Available: https://github.com/bitcoin/bips/blob/master/bip-0341.mediawiki
[133] T. Simonite, "Why you need a physical vault to secure a virtual currency," Aug. 2018. [Online]. Available: https://www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency/
[134] A. Davenport and S. Shetty, "Air gapped wallet schemes and private key leakage in permissioned blockchain platforms," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 541–545.
[135] NCSC, "Technical specifications for construction and management of sensitive compartmented information facilities, version 1.5," Mar. 2020. [Online]. Available: https://www.dni.gov/files/Governance/IC-Tech-Specs-for-Const-and-Mgmt-of-SCIFs-v15.pdf
[136] Y. Takei, "Operating environment for EXTREME-COLD." [Online]. Available: https://github.com/takeiyuto/extreme-cold
[137] IANA, "Root ksk ceremony operating environment." [Online]. Available: https://github.com/iana-org/coen
[138] D. R. Cressey, *Other People's Money: A Study in the Social Psychology of Embezzlement*. Free Press, 1953.
[139] A. Schuchter and M. Levi, "The fraud triangle revisited," *Security Journal*, vol. 29, 2016.
[140] M. J. Campagna, "Security bounds for the nist codebook-based deterministic random bit generator," *IACR Cryptology ePrint Archive*, 2006. [Online]. Available: https://eprint.iacr.org/2006/379
[141] J. Woodage and D. Shumow, "An analysis of NIST SP 800-90A," in *Advances in Cryptology – EUROCRYPT 2019*, Y. Ishai and V. Rijmen, Eds. Cham: Springer International Publishing, 2019, pp. 151–180.
[142] F. Strenzke, "An analysis of OpenSSL's random number generator," in *Advances in Cryptology – EUROCRYPT 2016*, M. Fischlin and J.-S. Coron, Eds., vol. 9665. Springer Berlin Heidelberg, pp. 644–669.
[143] C. Zimman and D. Bong, "PKCS #11 Cryptographic Token Interface Base Specification Version 3.0," Jun. 2020. [Online]. Available: https://docs.oasis-open.org/pkcs11/pkcs11-base/v3.0/os/pkcs11-base-v3.0-os.html
[144] L. M. Bolotin and S. B. Johnson, "Us 9,813,416 b2: Data security system with encryption," Nov. 2017. [Online]. Available: https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/9813416
[145] S. Y. Yu, C. S. Moore, J. S. Whetstone, R. Barzilai, and H. Ino, "Us 8,533,414 b2: Authentication and securing of write-once, read-many (worm) memory devices," Sep. 2013. [Online]. Available: https://image-ppubs.uspto.gov/dirsearch-public/print/downloadPdf/8533414
[146] M. Naor and A. Shamir, "Visual cryptography," in *Advances in Cryptology — EUROCRYPT'94*, A. De Santis, Ed. Springer Berlin Heidelberg, 1995, pp. 1–12.
[147] T. V. Bui, N. K. Vu, T. T. Nguyen, I. Echizen, and T. D. Nguyen, "Robust message hiding for QR code," in *10th International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2014, pp. 520–523.
[148] Y.-W. Chow, W. Susilo, G. Yang, J. G. Phillips, I. Pranata, and A. M. Barmawi, "Exploiting the error correction mechanism in QR codes for secret sharing," in *Information Security and Privacy*, J. K. Liu and R. Steinfeld, Eds. Cham: Springer International Publishing, 2016, pp. 409–425.
[149] Y. Takei, *Complete Guide to the Theory and Practice of NFTs (translated)*. Ohmsha, 5 2023.
[150] S. Jagati, "Token adoption grows as real-world assets move on-chain," Oct. 2023. [Online]. Available: https://cointelegraph.com/news/token-adoption-real-world-assets-blockchain

APPENDIX

A. 署名済みQRコードの例

本手法の QR コードのサイズを示すために、Bitcoin Testnet における実際の署名付き引き出しトランザクションを図 8 に示す。データサイズは416バイトであり、これは69セルのQRコード(バージョン13)にエンコードされている。

Transaction hash:
`47489ba139ca848537ba54829e62f0787d8ea2a3abb51b79085c95257dcedf6c`

Fig. 8. Example QR Code of a Signed Transaction