情報処理学会論文誌 Vol.61 No.9 1364–1373 (Sep. 2020)

招待論文

暗号資産交換所のカストディリスクと鍵管理

島岡 政基[1,a)] 佐藤 雅史[1] 中島 博敬[2]

受付日 2020年4月8日, 採録日 2020年6月22日

概要：Bitcoin の出現以来，ほどなくして法定通貨の世界と暗号資産の世界をつなぐ暗号資産交換所（以下，交換所）が登場し，その後の Bitcoin を含む様々な暗号資産の急速な展開を後押ししてきた．交換所に対する最近のサイバー攻撃を中心とした多くの事件は，交換所の役割に対するユーザの認識と現実の間に大きなギャップがあることを示唆している．今日の交換所の多くは，顧客の暗号資産を預かり取引を代行する，いわゆるカストディアンであり，実態に応じた運用，保護すべき情報資産，セキュリティ管理体制などを明確にすることが社会的要請になりつつある．筆者らは，交換所の実態がカストディアンであることに着目し，その鍵管理について，交換所事業者を含めた有識者らと課題整理を行うとともにその対策に必要な技術・運用を検討してきた．本論文では，こうした交換所の課題整理と，その対策に必要な技術・運用を概観する．また，既存の鍵管理の代表例である PKI（Public Key Infrastructure）との違いを明らかにすることで，既存技術を応用するうえでの知見を示す．

キーワード：暗号資産，カストディアン，鍵管理

Custody Risk and Cryptographic Key Management in Cryptoassets Custodian

Masaki Shimaoka[1,a)] Masashi Sato[1] Hirotaka Nakajima[2]

Received: April 8, 2020, Accepted: June 22, 2020

Abstract: Since the advent of Bitcoin, cryptoassets exchanges emerged to connect the fiat currency world to the cryptoassets world and drove the rapid deployment of various cryptoassets including Bitcoin and others. Many incidents centered on recent cyber attacks in cryptoassets exchanges suggest that there is a large gap between user perceptions and reality of exchanges' roles. Most of today's exchanges are so-called custodians, who are entrusted by customers with cryptoassets and process transactions on behalf of the customers. It is a social demand to clarify their operation according to the actual situation, the information assets to be protected, and the security management system. Focusing on the fact that exchanges behave as custodians, the authors organized the issues regarding custody risk and cryptographic key management with experts including the exchange operators, and considered the technologies and operations necessary for the security controls. In this paper, the authors described the results of them. Authors described also the findings for applying the existing technologies to such issues, by clarifying the difference from the Public Key Infrastructure (PKI), which is a typical example of the technologies.

Keywords: cryptoassets, custodian, cryptographic key management

1. はじめに

1.1 背景

信頼する者（trusted party）を不要とする，いわゆる「トラストレス」なネットワークサービスを実現することは，暗号応用が目指す理想の 1 つであるが，その実現は大きな挑戦である．トラストレスなネットワークサービスを実現

[1] セコム株式会社 IS 研究所
SECOM CO., LTD., Mitaka, Tokyo 181–8528, Japan
[2] メルカリ R4D
mercari R4D, Minato, Tokyo 106–6118, Japan
[a)] m-shimaoka@secom.co.jp

するために，秘密分散法，閾値暗号，マルチパーティ計算プロトコルなど多くの暗号技術の研究が進められている一方で，運用上のミス，悪意ある行為，他者との結託など様々な障壁が存在している．

著名な暗号資産の仕組みの 1 つである Bitcoin は「意思を持った任意の二者間で，信頼できる第三者を必要とせずに相互の直接取引を可能とする，信頼に代わる暗号学的証明に基づいた電子決済システム」[1] [*1]と述べられており，同様のトラストレスな支払い方式を実現すると主張する暗号資産のなかで，最も優れた仕組みの 1 つである．

Bitcoin の支払い方式は，他の既存の支払い方式との交換ではなく，Bitcoin どうしでの支払いのみを想定している．Bitcoin を法定通貨を含む他の資産に交換するなど，Bitcoin の分散台帳の外での行為についてはいっさい言及されておらず，元論文 [1] の想定外と考えるべきである [2]．

つまり，トラストレスな暗号資産を他の資産に交換する場合は，我々は何らかの信頼を仮定する必要がある．人々の多くは，暗号資産はトラストレスな方法で運用されていると信じられているかもしれないが，実際には暗号資産交換所（以下，単に交換所）を暗黙裡に信じているといっていいだろう．

1.2 交換所かカストディアンか

このように，交換所と我々一般の間には多くの認識の隔たりがある．一般的に「交換所」という言葉から，その業態は，一般的な証券取引所のように売り注文と買い注文を照合することであると考えてられている．しかしながら，交換所の実態は，顧客が交換所に口座を開設し，当該口座に法定通貨（フィアット）の入金を行う形態が一般的である．つまり交換所は銀行と同様の機能を持っていることを示している．さらに，ほとんどの交換所では，各顧客の署名鍵（3.2 節参照）を交換所内に保持している．このように顧客の資産と同等の価値を持つ署名鍵を預けていることから，交換所がいわゆる**カストディアン**[*2]の機能を持ち合わせていることを意味している．

一部の交換所では，暗号資産の移転を行う場合に，公開ブロックチェーンに本来書き込むべきデータを格納せず，交換所が独自に管理する台帳（データベース）に書き込む運用を行っているとされている．この場合，交換所は，顧客の持つ日本円などの法定通貨と引き換えに暗号資産を「販売」しているように見えるが，客観的には顧客は暗号資産を所有していない（あくまでも顧客と暗号資産交換所の契約が成立しているのみといえる）．

交換所の顧客は，（手数料を支払って）公開ブロックチェーンへの書き込みを委託し，鍵や資産の消失に対するリスクを担保してもらうために，署名鍵を交換所に預けており，このような「交換」とも「販売」ともつかない業務が成立するのは，交換所が前述のカストディアンの機能をあわせ持つことによると考えられる．

1.3 交換所へのサイバー攻撃

交換所では，その歴史を通じて多くの事件が発生している．2013 年，Mt. Gox はサーバへの攻撃とトランザクション展性（transaction malleability）により，多くの Bitcoin を失った [3]．2018 年，Coincheck は標的型攻撃を受け約 26 万人の顧客が預けていた XEM のうち約 580 億円相当の XEM を失った [4] [*3]．同年，Zaif も約 70 億円相当を失った [5]．さらに 2019 年には，Binance と Bitpoint が同様に多額の資産を失ったとされている [6], [7]．暗号資産に関する事件は他にも世界中から数多くの事例が報告されている．このため，これらの事業者は暗号技術や鍵管理に対するサイバー攻撃を含むあらゆる種類の攻撃に対して，十分な安全性を考慮する必要がある．しかしながら，こうしたセキュリティ上の懸念に対して，交換所の実装と運用に関して専門知識と人材が不足しているのが実状である．

このように交換所は，顧客の資産（に相当する署名鍵）を預かるカストディアンである以上，カストディリスクを想定すべきであり，そのリスクを低減させるためにはカストディとして管理する鍵の安全性を高めることが求められる．本論文では，交換所のカストディリスクについて，特に鍵管理の視点から分析を行い，有効な管理策を検討するにあたり必要な技術や運用を示す．これらは，筆者らの過去の取組み [8], [9] をもとに再構成している．また鍵管理の先例である PKI との比較考察を加え，交換所固有の鍵管理の問題に知見を与える．

2. 暗号資産交換所の現状分析

2.1 交換所固有の問題

交換所がカストディアンと位置付けられるからには，その企業経営や顧客保護・資産保護については金融システムに共通するところが多いと考えられよう．カストディアンとして金融システム一般の考え方を基本的に踏襲しつつ，本節では従来の金融システムにはない，交換所固有の考慮すべき点について説明していく．

暗号資産における鍵管理は，既存の PKI とは異なる要件が必要となる．特に，交換所で用いる鍵のライフサイクルに関しては，注意する必要がある．たとえば，情報資産，攻撃界面，脅威，リスクは，ビジネス環境ごとに異なる．そこで本論文では，こうした留意点をふまえて，3 章にお

[*1] An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.

[*2] 投資家に代わり有価証券の管理・保管などの業務を行う機関．

[*3] 文献 [4] では NEM と表現されているが，NEM は暗号資産のプラットフォームの一種であり，その通貨単位は XEM とされていることから，本文中では XEM で表記を統一した．

いて交換所のカストディリスクについて分析を行う．

なお，匿名性の高い暗号資産を扱う交換所においては，資金洗浄など犯罪・テロ組織対策についても，匿名性の高い暗号資産を扱う場合には当然ながら，通常の金融サービスよりも多くの問題を引き起こすものとして注意が必要であるが，鍵管理とは異なる論点となるため本論文では言及しない．

2.2 コールドウォレット

交換所が扱う署名鍵や検証鍵（いずれも 3.2 節参照），また検証鍵から生成されるアドレスを管理する機構は，一般にウォレットと呼ばれている [10]．ウォレットの運用形態として，オンラインでネットワークに接続されているものをホットウォレット，通常時はネットワークから切断され，非活性状態（4.2.2 項参照）にあるものをコールドウォレットと呼ぶ．コールドウォレットは，署名時には何らかの明示的な操作によって活性化する必要がある．活性状態では署名鍵の消失，漏洩・盗難，不正利用のリスクが高まるため，可能な限り非活性状態におくことが望ましいとされている．このことについては 4.2.1 項で後述するが，その要件（たとえば程度や閾値）については様々な議論がある．

典型的には，活性化の頻度や，活性状態と非活性状態の期間（あるいはその割合）に依存する．また，ウォレットにひもづく暗号資産の価値が少なければ，必ずしもコールドウォレットでなくとも構わない，すなわちリスク受容できる，というケースも考えられよう．ウォレットにひもづく暗号資産の価値やウォレットの活性状態の管理方法なども含めて考慮する必要が生じる．

2.3 鍵管理のインセンティブ設計における問題

Coincheck 事件では，預けられた顧客資産の多くが 1 つのホットウォレットに集約して管理されており，短時間で多額の暗号資産が盗まれた原因となった [11]．同社が 1 つのアドレスで多額の資産を管理した理由は明らかではないが，一般論として，交換所がホットウォレットで多くの暗号資産を管理する理由について分析する．

一般に交換所は，その暗号資産をホットウォレットとコールドウォレットに分けて管理している．交換所が暗号資産の移転などトランザクションを実行するには，必要な額の暗号資産がホットウォレットに存在している必要がある．トランザクションの頻度や規模によっては，ホットウォレットに存在する暗号資産の額はそれなりに大きくなることが容易に想像がつくだろう．

Coincheck 事件で被害にあった XEM も含め，いくつかの暗号資産では，Proof-of-Stake（PoS）と呼ばれるコンセンサスメカニズムを採用している．一般論として PoS タイプの暗号資産は，1 つの鍵で多くの資産を管理することでより多くのマイニング（または同様の）報酬を得ることができる．こうしたコンセンサスメカニズムなどもまた，ホットウォレットに存在する暗号資産の額が肥大化する理由の 1 つであろう．

このように，交換所の取引規模や頻度，また暗号資産の報酬の仕組みによっては，交換所が 1 つのアドレスに大量の暗号資産をまとめて扱うことに極端なインセンティブを与えうる．交換所へのサイバー攻撃がしばしば巨額の被害をもたらす背景には，こうした事情もあることを理解しておくべきであろう．

3. 交換所のカストディリスク

3.1 交換所のシステムモデル

筆者らの知る限り，交換所のためのソフトウェア・ハードウェアの標準化されたアーキテクチャや実装は，現時点で存在していない．文献 [10] において，交換所の安全な実装と運用を論じるための一例としての交換所のシステムモデルが示されている．本論文もこれを参照することとして**図 1** に示す．モデルの詳細は文献 [10] の 5.2 節を参照されたい．

このモデルは各機能要素を定義し，機能を論理的に区別したものであり，実際のシステム上の配置を示したものではないことに留意されたい．たとえば，検証鍵管理は実際には統合データベースで管理されるかもしれない．また，複数の機能はパッケージによって統合されているかもしれない．たとえば，トランザクション署名部の各機能要素は，顧客資産管理系と統合されている場合もあり，あるいは他のシステムとして動作しても構わない．

3.2 暗号資産交換所で用いられる鍵

交換所で用いられる鍵は 4 種類に分類できる．

(1) 署名鍵：トランザクションの署名に用いる私有鍵
(2) 検証鍵：トランザクションの検証に用いる公開鍵
(3) Key Encryption Key（KEK）：署名鍵の機密性を保つための共有鍵
(4) マスターシード：決定性ウォレットで署名鍵を生成する際に用いられるシード（乱数など）

署名鍵と検証鍵は，非対称鍵暗号の鍵ペアである．本論文では署名鍵と KEK をもって秘密鍵と呼ぶ．また，検証鍵以外はいずれも秘密情報として扱われる必要がある．署名鍵と検証鍵のペア（以下「鍵ペア」）が生成された後，トランザクションを受信するためのアドレスが検証鍵から生成される．

署名鍵の非活性状態とは，署名鍵が図 1 の**署名鍵管理**[*4]に安全に保管されている状態であり，たとえば KEK によって署名鍵が暗号化された状態である．逆に，活性化は，非活性状態の署名鍵を復号し，署名に使用できるようにする

[*4] 交換所が管理する複数の署名鍵のデータを保管するとともに，個々の署名鍵の状態管理，権限分離に基づくアクセス制御，適切なバックアップなどの機能を提供する．

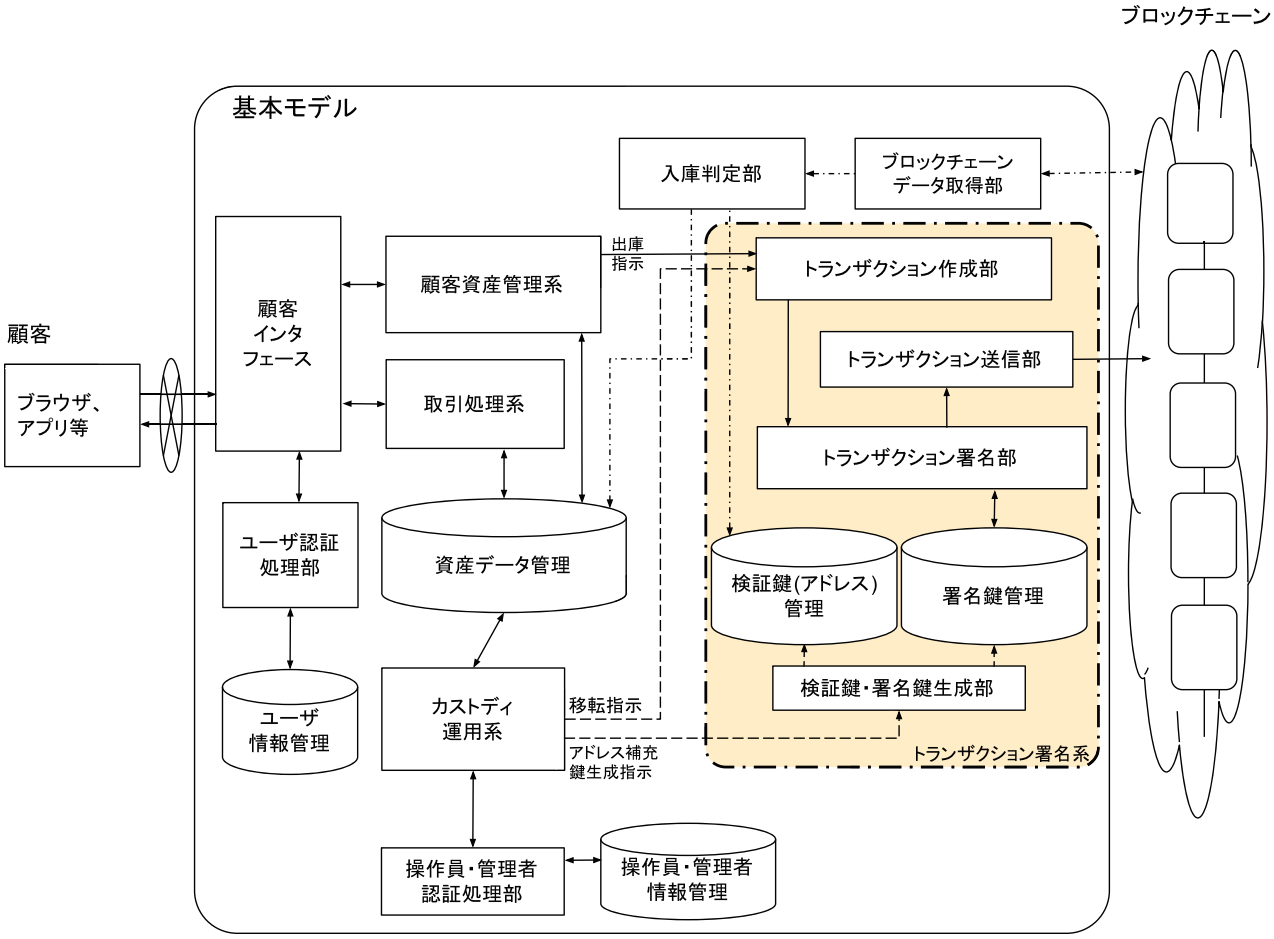

図 1 暗号資産交換所のシステムモデル
Fig. 1 System model of cryptoassets custodian.

プロセスである．署名鍵の活性状態・非活性状態については後述の**図 2** も参照されたい．

活性化は，図 1 のトランザクション署名部において実行されることを想定している．ウォレット[*5]に活性化・非活性化機能が実装されている場合もある．署名鍵は，トランザクションへの署名が実行されるまでは不要のため，それまでは署名鍵はオフラインで管理し，オンラインでは検証鍵とアドレスのみを保存しておくことも可能である．

3.2.1 複数の鍵の利用について

一般的な暗号資産の利用場面において，1 ユーザが 1 つのアドレスを使うケースもあれば，1 ユーザが多数のアドレスを使うケースもある．交換所においても暗号資産の種類や管理の方法によって，管理対象となるアドレスおよび鍵ペアの数は異なる．また，暗号資産の種類だけでなく，ホットウォレットやコールドウォレットによる管理，暗号資産の額に応じた分散管理など，リスク評価のうえで複数のアドレスおよび鍵ペアを使い分けることも考えられる．

なお，一般的な暗号資産の利用において，1 度使った鍵ペアは再利用しないことを推奨されていることもある．しかし，これは個人利用において，取引を特定されにくくする目的が主であり，交換所において実効性や実用性がある手法とは考えにくい．交換所ではリスク評価と管理目的を考慮したうえで適切な管理策を実施することが必要である．

3.2.2 鍵の利用停止における注意点について

鍵の利用停止はあくまでも交換所内での運用であり，暗号資産の仕組み上は 1 度送信したトランザクションの取消しを行うことはできない．また，利用停止以降においても署名鍵を破棄することが難しい場合がある．たとえば，破棄された署名鍵に対応するアドレスに対して，顧客が誤って暗号資産を移転してしまうこともあり，誤って入庫されたアドレスから元の顧客に暗号資産を返却するためには，その署名鍵が必要となる．このような事態などを想定し，署名鍵の破棄は慎重に検討する必要がある．

3.2.3 署名鍵のリスク分析

暗号資産の移転において，署名鍵の持つ役割とリスクは極めて大きい．その理由としては単に暗号資産の移転（transfer）を可能とするにとどまらず，暗号資産が有する

[*5] 図 1 における署名鍵管理を核としながら，検証鍵・署名鍵生成部や検証鍵管理，トランザクション署名部なども実装したソフトウェアまたはハードウェア．

匿名性により暗号資産を消失するリスクがあることや，漏えい・盗難に対し，署名鍵の失効（revocation）やトランザクションのロールバックによる対処が困難という性質による．署名鍵の消失，漏洩・盗難，および価値の棄損につながる可能性のある不正使用のリスクについて分析する必要があるが，想定される脅威，システム構成，脅威のモデリングなどによって，リスク分析の結果は異なる．ここでは，署名鍵に関する脅威と，その脅威を起こしうる因子を以下のように想定した．消失，漏洩・盗難，不正利用における具体的なリスクなどは文献 [10] の 6.2.1 節を参照されたい．

脅威：消失，漏洩・盗難，不正使用

脅威の因子：

誤操作　システムの正当な利用者（操作員・管理者なども含む）による意図せず行われる操作．たとえば，本来 10 万円分を移転する操作を，誤って 100 万円分を移転してしまう操作など．

正当者の悪意ある行為　システムの正当な利用者（操作員・管理者なども含む）が，悪意を持って行う行為．たとえば，内部不正による署名鍵の盗難や不正利用など．なお，ここでは因子となりうる行為の識別が目的であり，行為の目的やインセンティブなどは問わない．

正当者へのなりすまし　システムの正当な利用者以外が，正当な利用者認証情報を盗用して何かしらの操作を行う行為．たとえば，外部の攻撃者が顧客になりすまして暗号資産の売買・移転指示を行う，あるいは操作員や管理者権限を持たない内部犯が操作員・管理者権限でシステムにアクセスして資産移転指示やトランザクション生成・署名などを不正に行うなど．

部外者の悪意ある操作　部外者のなりすまし以外の方法による悪意を持ったシステムに対する操作．たとえば，システムのぜい弱性を利用して外部から不正侵入する，操作員・管理者への標的型メールなどを介して交換所のシステムにマルウェアを混入させ外部から署名鍵（ないしトランザクション作成など）を不正に遠隔操作するなど．

システムの意図しない挙動　操作の意図とは無関係に，システムが設計者ないし操作員・管理者の想定しない挙動をすること．たとえば，カストディ運用系のバグにより署名鍵が漏えいする，操作内容にかかわらず間違った額のトランザクションが作成される，ユーザインタフェースが分かりにくく意図とは異なる挙動をしてしまう，など．

4. カストディリスクのための鍵管理

前章までの分析から，署名鍵を中心とした交換所特有のカストディリスクに有効な管理策を検討するにあたり，必要な技術と運用についてそれぞれ検討する．

4.1 必要な技術

4.1.1 マルチシグネチャ

マルチシグネチャは，トランザクションの生成に複数のステークホルダーによる承認プロセスを必要とする仕組みとして導入される技術であり，各ステークホルダーの管理する署名鍵による署名をもって実現される．トランザクションの不正な生成に対する，汎用的な対策としての効果が期待できるが，個別の署名鍵の漏洩・消失の脅威に対しては別途対策する必要がある．

4.1.2 基礎的な暗号技術と実装

暗号鍵の管理において，耐タンパ性を備えるハードウェア内に鍵を保持した鍵管理装置を用いて，適切なアクセスコントロールを行うことは，外部からの不正侵入のリスクや漏えい・盗難の脅威に対して有効な方法である．PKI における認証局では，第三者機関の評価と認証を受け，耐タンパ性が保証された Hardware Security Module（HSM）を用いて，より厳格に管理を行うことが一般的である．

ウォレットを実装する場合も，本来であれば HSM のように技術的安全性が保証されている製品を用いることが望ましい．しかし，現状では暗号資産が利用する一部の暗号アルゴリズムや楕円曲線のパラメータなどに未対応である場合が多く，必ずしも利用できるとは限らない．導入においては，より多くの暗号アルゴリズムやパラメータをサポートする HSM が必要であり，場合によっては今後各暗号アルゴリズムの標準化も必要であろう．

4.1.3 鍵管理とウォレット

多くの交換所では，オンライントランザクションのためにネットワークに接続されたホットウォレットとは別に，ネットワークから切断されたコールドウォレットを併用しながら資産を管理している．ホットウォレットは，実装上の安全性を高めるため，Cryptographic Module Validation Program（CMVP）のような認証プログラムの認証を受けた製品を利用することが求められる．

4.2 必要な運用

4.2.1 鍵管理の基本

一般的に，署名鍵や KEK などの秘密鍵は他の情報資産から隔離（isolate）されるべきであり，秘密鍵へのアクセスは可能な限り最小限に制限し，意図しない消失・漏洩に備える必要がある．これらを実現するための，基本的な管理策として (1) 状態管理，(2) 権限分離と相互けん制，(3) バックアップがあげられる．これらの管理策について 4.2.2 項以降で述べる．

4.2.2 署名鍵の状態管理

図 2 に示したように，署名鍵は一般に複数の状態を持ち，運用中においては主に活性・非活性状態のいずれかにある．署名演算を行うには，署名鍵の状態は活性化されている必要がある．非活性状態の署名鍵を活性化するには，

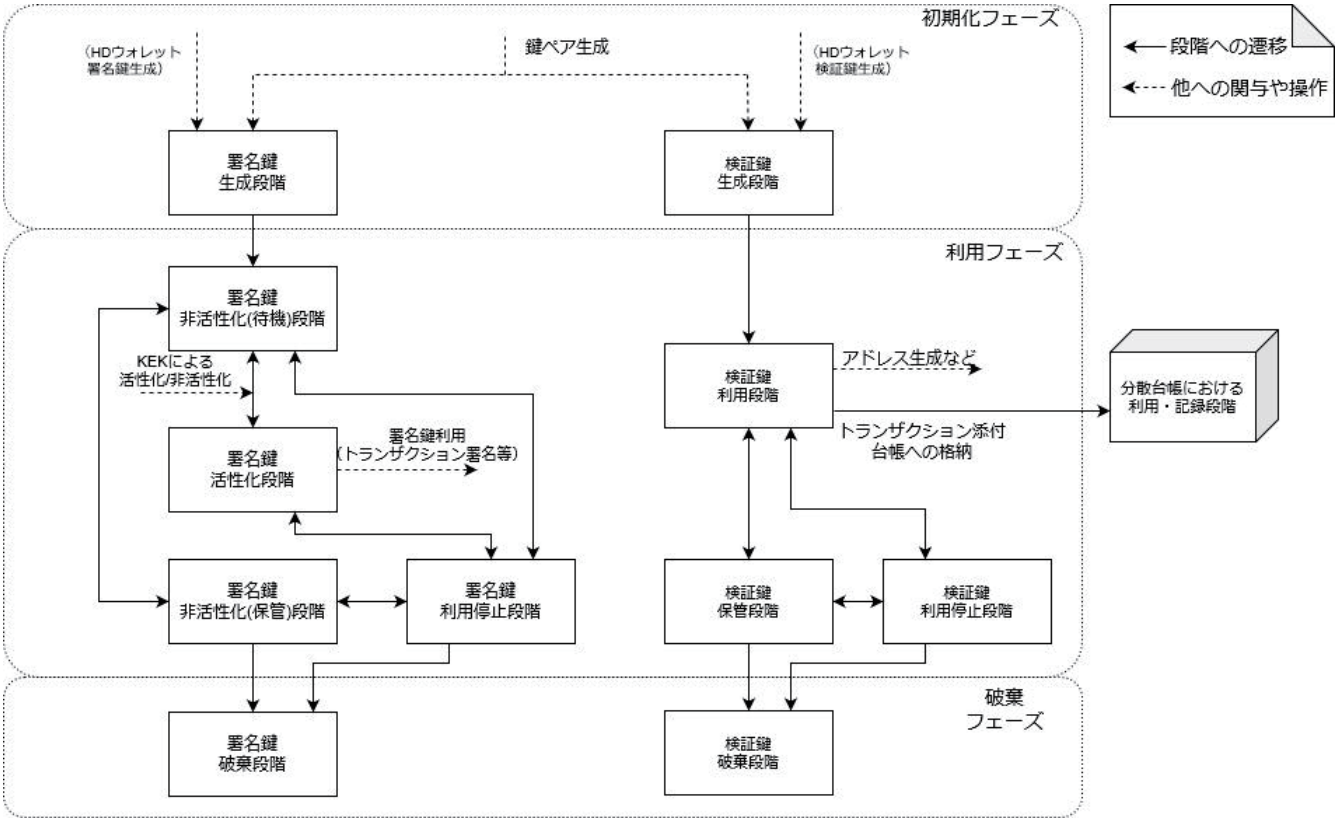

図 2 暗号資産交換所における鍵のライフサイクル
Fig. 2 Key lifecycle at cryptoassets custodian.

何らかの秘密情報の入力を必要とすることが望ましい．これにより，非活性状態にある限りは，この秘密情報を合わせて入手しない限り署名鍵の不正利用は困難であり，漏えい・盗難に対しても同様である．

また，署名鍵の不正利用リスクを最小化するためには，活性状態の期間を業務合理的な範囲で必要最小限に留めることが望ましい．最も業務合理的なのはつねに活性状態にあることだが，明らかに操作不要な時間帯に活性状態としておくことは，漏えい・盗難も含めリスクを高めることになる．逆に，署名操作を必要とするつどに活性化・非活性化の操作を行うことは，操作頻度が高い場合には非合理的といえる．

どこまできめ細かく制御するかは業務合理性と安全性のバランスによって決める必要があり，またそのようなリスク受容に基づいて鍵管理が行われていることを，鍵管理規程の開示などにより利用者が確認できることが望ましい．

4.2.2.1 オフライン管理

外部からの不正侵入による鍵の漏えい・盗難を防ぐために，システムを構成するネットワーク上に鍵を配置しない，いわゆるオフライン管理（交換所の文脈ではコールドウォレット）という手法がある．この場合，システムが鍵を利用するには何らかのオフライン操作が必要となる．たとえば，利用時のみ鍵をネットワークにつなげるために鍵を金庫から取り出してシステムに接続する，オンラインシステムとオフラインの鍵管理端末との間の入出力を，USB メモリなど可搬記憶媒体を介して行う，などがあげられる．ただし，鍵の不正利用などを防止するには，明示的な承認プロセスが別途欠かせない．

4.2.3 署名鍵管理の権限分離と相互けん制

内部不正や誤操作を防ぐには，署名鍵を用いるクリチカルな操作に関して複数人による操作を必須とすることが基本となる．たとえば署名操作を行う権限と，署名操作が可能な区画への入室を承認する権限を排他的に設定することで，単独犯が誰かに知られずに不正に署名を行うことは困難となる．さらに，たとえば署名操作で複数名による立会いなど，リスクに応じて相互けん制措置を必須とすることは，内部不正や誤操作に対する有効な管理策となる．

署名鍵の権限を複数のエンティティに分散することもまた有効なセキュリティ管理策の 1 つである．よく知られている技術としては，秘密分散法やマルチシグネチャといったものがある．詳細は文献 [10] の 7.3.6.3 で説明されている．

4.2.4 署名鍵のバックアップ

署名鍵が消失・破壊されれば，当該署名鍵による署名演算が不可能になるため，署名鍵のバックアップは重要な管理策である．一方で，バックアップした署名鍵の漏えい・盗難リスクもまた十分に考慮する必要があり，4.2.2 項で述べた非活性状態での保管が欠かせない．バックアップ媒

体の漏えい・盗難などのリスクは媒体の種類によって異なるため，それぞれに適切なアクセス管理などを行う必要がある．典型的な方法は，耐タンパ性を有する鍵管理装置へのクローニング，電磁記録媒体へのバックアップ，紙媒体へのバックアップである．

また，不適切なバックアップの実施や，通常利用しないアドレスの不正利用を検知するため，当該アドレスからの移転が実施されていないかブロックチェーンをモニタリングすることも有効であろう．詳細は文献 [10] の 7.3.6.4 で説明されている．

5. 考察：PKI との違い

既存の鍵管理の典型として，PKI における一連の鍵ライフサイクルをフェーズごとに改めて見直すと，交換所に対しても PKI の知見が適用可能な箇所もある一方で，暗号資産やその安全性の基盤となるブロックチェーンや分散台帳技術においては，PKI とは大きく異なる特有の性質により，改めて検討が必要な部分もあった．本章では，その違いについて述べる．

5.1 鍵のライフサイクル

従来の署名作成時には，署名者が署名鍵を保持し，署名対象のデータ（例：契約書の電子データ）に対し，署名演算を行うことが一般的である．1 度，このように署名付きデータを作成すれば，署名者が当該署名鍵を削除しても，受領者は当該署名鍵と対となる検証鍵によって署名の有効性を検証することができ，署名対象データの内容に従った処理（例：契約の履行）を行うことができる．基本的に署名鍵は署名を行う際に存在すればよいため，署名鍵の保管期間を短くすることや，瞬間的なワンタイムの署名鍵生成などの運用も可能である．

後述する鍵の失効性の不備と合わせて，暗号資産の署名鍵は非常に長い（場合によっては期限のない）保管期間になりうる．署名鍵の管理負担を軽減するために，階層的決定性（HD：Hierarchy Deterministic）ウォレットなどの仕組みもある．HD ウォレットでは，先に検証鍵（アドレス）だけを作成し，署名鍵が必要となったときに対となる署名鍵を作成することが可能である．ただし，こうした仕組みは署名アルゴリズムに依存するため，すべての暗号資産に適用できるわけではない点に注意されたい．

5.2 鍵の失効性

PKI では署名鍵に対する失効処理を行うことができる．失効処理とは，署名鍵の消失や漏洩が発覚した場合など[*6]に，公開鍵証明書を発行した認証局が，署名者などの要求に基づき，公開鍵証明書の利用停止処理を行うものである．認証局は，当該公開鍵証明書の失効状態を記載した失効リスト（CRL：Certificate Revocation List）の発行などを行う．署名の検証者は失効リストを参照することで，失効済みの公開鍵証明書を確認することができ，当該署名鍵による署名データの（内容の）受入れを拒否することができる．

一方，Bitcoin など暗号資産の仕組みの多くは，トランザクションの仮名性[*7]や第三者機関の排除などの設計方針も背景にあり，認証局のような役割を担うオーソリティが存在せず，PKI のような失効処理を実現できない．署名鍵の漏洩や不正使用によって，暗号資産を不正に移転するトランザクションが作成され，ブロックチェーン上で承認されてしまうと，失効機能を有していないがゆえに，ユーザの意思によってそのトランザクションを取り消すことはできない．また，アドレスに対しても使用停止することができないため，1 度公開されたアドレスに対して，暗号資産の移転を拒むことができない．故意か否かによらず，あるアドレスに暗号資産が移転される可能性があるため，その暗号資産を他に移転できるように，当該アドレスと対となる署名鍵を安全に保管し続けることが必要に応じて求められる．

5.3 鍵管理装置のサプライチェーンリスク

暗号資産においては，ハードウェアウォレットと呼ばれる（署名）鍵管理装置が多種登場している．ハードウェアウォレットは内部で署名鍵を保持し，トランザクションへの署名が必要となる局面で，USB や Bluetooth などで PC やスマートフォンと接続して使用する．ハードウェアウォレットは 2 次流通も多いが，その過程で安全でない製品が出回り，ハードウェアウォレットに保管されていた暗号資産が消失した事例も確認されている[*8]．

このような供給過程において安全でない，または不正な製品が混入するという，いわゆるサプライチェーンリスクへの対処として，第三者機関の評価と認証を受けた鍵管理装置がある[*9]．各認証制度は評価内容が異なり，それぞれに異なるレベルが設けられている．鍵管理装置の選定にあたっては，評価基準やレベルの違いとともに，評価や認証の対象についても注意が必要である．また，鍵管理装置内部の一部のチップに対する認証の場合もあれば，鍵管理装置全体に対して認証を受けている場合もある．

PKI における認証局で，第三者機関の評価と認証を受け

[*6] 他にもアルゴリズムの危殆化など様々な理由がある．

[*7] ゼロ知識証明などを応用した一部の暗号資産を除けば，必ずしも厳密な匿名性を有さない．

[*8] たとえば以下の記事．Man's Life Savings Stolen from Hardware Wallet Supplied by a Reseller, https://news.bitcoin.com/mans-life-savings-stolen-from-hardware-wallet-supplied-by-a-reseller/

[*9] たとえば，国際的な評価・認証制度として，米国政府の調達基準である FIPS 140-2 に基づく認証（Cryptographic Module Validation Program, CMVP）や，ISO/IEC 15408（Common Criteria, CC）に基づく認証がある．

たHSMが使われていることは4.1.2項で述べた．認証局が用いる署名・暗号アルゴリズムはおよそ標準化されており，また必要とされる認証基準も明確に業界標準とされていることから，それに準拠した製品を調達する限りはおよそ心配はない．一方の交換所においては，暗号アルゴリズムやパラメータなどの面でも，対応したHSMが少ないといった制約があり，また暗号資産の方式や運用の形態がまだ収斂していないため，一概に標準的な認証基準を指定することは難しい状況にある．このため，交換所は個別に適切な認証基準やレベルを選定する必要があり，また認証範囲（装置全体か一部のチップかなど）についても適切に選定する必要がある．鍵管理装置内部の一部のチップに対する認証の場合には，チップ周辺やその他の構成要素に対する攻撃リスク[12][*10]も考慮する必要があるなど，認証基準の適切な選定も求められる．

5.4 暗号アルゴリズムのAgility

ブロックチェーンはトランザクションへの署名や，アドレスやブロックの生成におけるハッシュ関数の利用など様々な場面で暗号技術を利用しており，ブロックチェーンの安全性もこれらの暗号技術に依存している．Bitcoinブロックチェーンは，運用開始から現在に至るまでの過去のすべてのトランザクションを保持し続けることで，暗号資産の発行と移転の一貫性を維持する仕組みとなっている．ブロックチェーンを将来長期的に運用し続けた場合，計算機の性能向上や解読手法の進展により，使用されている署名アルゴリズムやハッシュ関数が脆弱なものとなり，また過去利用していた鍵長も十分な強度を維持できなくなることが考えられる．将来的にアルゴリズムや鍵長が脆弱化した場合，ブロックチェーンの過去のトランザクションの記録が不正に書き換えられたり，署名鍵の不正な複製などにより悪意ある第三者が正当な暗号資産の保有者になりすまして暗号資産の移転を行うことも可能となる恐れがある．これらの暗号技術に対する攻撃が現実なものとなる前に，ブロックチェーンのプラットフォームとなるソフトウェアが適切なアルゴリズムや鍵長に移行する必要がある．しかし，現状の代表的なブロックチェーンは暗号移行するための適切なメカニズムを備えていない．ブロックチェーンの暗号移行では，トランザクション生成に用いる署名鍵の移行と，ブロックの真正性を維持するためのハッシュ関数の移行について考える必要がある[2]．

5.4.1 署名鍵の移行

署名鍵の移行では，鍵長あるいは署名アルゴリズムの移行が考えられ，そのいずれの場合でもブロックチェーンノードの機能を提供するソフトウェアとユーザの署名鍵管理を行うウォレットソフトウェア・ハードウェアでの対応が必要となる．さらに，移行前の署名鍵に対応する旧アドレスから，移行後の署名鍵に対応する新アドレスへ暗号資産を移転する必要がある．交換所においても同様で，古い署名鍵に対する攻撃が現実的となる前に，必要に応じたブロックチェーンノードのソフトウェア変更やウォレット機能の変更にともなう交換所システムの改修と，管理している署名鍵の移行処理を完了する必要がある．

5.4.2 ハッシュ関数の移行

ブロック生成に必要なハッシュ関数のアルゴリズム移行では，ブロックの生成や検証に関わる機能を提供する各ブロックチェーンノードでの対応が必要となる．新規に生成するブロックだけでなく，過去に生成されたブロックについても考慮する必要がある．過去に生成されたブロックが当時のままである場合，ハッシュ関数に関する攻撃によって，過去のトランザクションの記録が書き換えられてしまう恐れがあるためである．過去のトランザクションの記録の改ざんが可能であれば，暗号資産の発行と移転に関する一貫性は維持できない．過去に作成された記録の真正性を保ちつつ，新たなハッシュ関数に移行する手法として，長期署名[*11]がある．これらの技術は，PKIを前提とした署名やタイムスタンプ技術[*12]を用いて作成された記録について，より強度の高いハッシュ関数などのアルゴリズムを採用したタイムスタンプ技術を過去の記録に対して適用し，アルゴリズムを強化するとともに過去の記録の時刻証明（存在証明）の有効性を維持していくものである．認証局やタイムスタンプ局の存在の有無など，PKIとブロックチェーンは前提が異なるものの，過去の記録の真正性を維持しながら，新しいアルゴリズムに移行するという考え方は応用できる．

その1つとして，PKIのタイムスタンプ局がもたらす時刻証明の代わりに，ブロックチェーンの時系列順序の証明に着目した移行方法の提案がある[13]．ブロック生成に関わるアルゴリズム移行は，ブロック生成を行うノードの負担を強いることになるため，ブロック生成や検証に関わるノードの支持が不可欠となる．特にProof-of-Workのようなメカニズムの場合は，ブロック生成ノード（マイナー）の経済合理性との関係によって，移行についてすべてのノードの賛同が得られるとは限らない．緩やかにアルゴリズムを移行する場合には，過去のアルゴリズムとの相互運用を行いつつ移行を進めるソフトフォークが望ましいが，アルゴリズムの移行が急務である場合や，開発コミュニティでの意見の相違などにより，ハードフォーク（その結果，暗号資産の分岐）となる場合もありうる．交換所においては，

[*10] これもサプライチェーンリスクの一種といえよう．

[*11] EN 319 122-1: Electronic Signatures and Infrastructures (ESI); CAdES digital signatures; Part 1: Building blocks and CAdES baseline signatures や ERS (RFC 4998: Evidence Record Syntax) など

[*12] RFC 3161: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

アルゴリズム移行にともなうソフトウェア移行はその他の仕様変更と同様に，開発コミュニティを含む主要なステークホルダーの移行方針に注意を払い，移行を進める必要がある．

6. おわりに

本論文では，交換所の実態がカストディアンであることに着目し，その鍵管理について，課題整理とともにその対策に必要な技術・運用を示した．また，既存の鍵管理の代表例である PKI との違いを明らかにすることで，既存技術を応用するうえでの知見を示した．

トラストレスといわれた Bitcoin をはじめとする暗号資産も，社会基盤化するなかで，本来なかったカストディリスクがその社会基盤に埋め込まれ，これを最小化するためには交換所を信頼せざるを得なくなった．暗号・セキュリティ・プライバシの各技術が実社会を支えていくためには，そうした社会基盤化していくなかで生じるリスクを最小化すること，またそのための知見をステークホルダーと共有していくことが重要であろう．

謝辞 本論文は Cryptoassets Governance Task Force (CGTF)[*13]の活動を通じて得られた知見をもとにしている．同 TF のメンバに謝意を表する．

参考文献

[1] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system, Bitcoin Project (online), available from ⟨https://bitcoin.org/bitcoin.pdf⟩ (accessed 2020-06-13).
[2] 松尾真一郎，楠 正憲，崎村夏彦ほか：ブロックチェーン技術の未解決問題，日経 BP (2018).
[3] Decker, C. and Wattenhofer, R.: Bitcoin Transaction Malleability and MtGox, *European Symposium on Research in Computer Security* (*ESORICS2014*), pp.313–326, Springer (2014).
[4] 産経ニュース：コインチェック，NEM 約 580 億円分が不正に外部送金 仮想通貨の取引を一時停止（オンライン），入手先 ⟨https://www.sankei.com/affairs/news/180126/afr1801260067-n1.html⟩（参照 2020-06-13）.
[5] テックビューロ株式会社：仮想通貨流出事件に関する状況報告，及び顧客対応状況について（オンライン），入手先 ⟨https://prtimes.jp/main/html/rd/p/000000094.000012906.html⟩（参照 2020-06-13）.
[6] Binance: Binance Security Breach Update (online), available from ⟨https://binance.zendesk.com/hc/en-us/articles/360028031711⟩ (accessed 2020-06-13).
[7] Zhao, W.: Bitpoint Exchange Hacked for $32 Million in Cryptocurrency, coindesk (online), available from ⟨https://www.coindesk.com/japanese-exchange-bitpoint-hacked-by-32-million-worth-in-cryptocurrencies⟩ (accessed 2020-06-13).
[8] Suga, Y., Shimaoka, M., Sato, M. and Nakajima, H.: Securing Cryptocurrency Exchange: Building up Standard from Huge Failures, Bernhard, M. et al. (Eds.), *Financial Cryptography and Data Security, FC 2020*, Lecture Notes in Computer Science, Vol.12063, Springer, DOI: 10.1007/978-3-030-54455-3_19 (2020).
[9] Sato, M., Shimaoka, M. and Nakajima, H.: General Security Considerations for Cryptoassets Custodians, Internet Engineering Task Force (online), available from ⟨https://datatracker.ietf.org/doc/html/draft-vcgtf-crypto-assets-security-considerations-06⟩(accessed 2020-06-18).
[10] 栗田青陽，菅原謙一：暗号資産カストディアンのセキュリティ対策についての考え方（案）第 2 版，Cryptoassets Governance Task Force（オンライン），入手先 ⟨https://cgtf.github.io/news/20200603/⟩（参照 2020-06-13）.
[11] 和田晃一良，大塚雄介：【全文 3/5】コインチェック，騒動の背景には「人手が集まらない」あらためて問われる内部管理体制，ログミー Biz（オンライン），入手先 ⟨https://logmi.jp/business/articles/272863⟩（参照 2020-06-13）.
[12] 須賀祐治：RSA アルゴリズム鍵生成モジュールの実装問題（ROCA），Internet Infrastructure Review（IIR），Vol.39, 株式会社インターネットイニシアティブ (2018).
[13] Sato, M. and Matsuo, S: Long-term public blockchain: Resilience against compromise of underlying cryptography, *2017 26th International Conference on Computer Communication and Networks* (*ICCCN*), pp.1–8, IEEE (2017).

[*13] https://cgtf.github.io/

島岡 政基 （正会員）

1998 年慶應義塾大学大学院理工学研究科修士課程修了．同年セコム（株）入社．2004 年同 IS 研究所．2005～2010 年国立情報学研究所特任准教授（後に客員准教授），2019 年筑波大学システム情報系客員准教授，2020 年より同システム情報工学研究群准教授（協働大学院）を兼務．2014 年総合研究大学院大学複合科学研究科情報学専攻博士課程修了．博士（情報学）．認証基盤とトラストの研究開発に従事．情報処理学会コンピュータセキュリティ研究会幹事（2016～2019 年），同会セキュリティ心理学とトラスト研究会運営委員（2014～2017 年），同会論文誌ジャーナル編集委員会副編集長/ネットワークグループ主査（2018 年）．

佐藤 雅史

1999 年東京工業大学大学院総合理工学研究科修士課程修了．同年セコム（株）入社．情報セキュリティ分野，特に電子認証，電子署名の関連分野の研究開発に従事．標準活動にも従事し，電子署名プロファイルの JIS 規格や ISO 規格の原案作成委員や ISO14533 シリーズのプロジェクトリーダを務める．日本ネットワークセキュリティ協会電子署名 WG サブリーダ，日本トラストテクノロジー協会リモート署名 TF サブリーダ，トラストサービス推進フォーラム調査研究 WG 主査．ISO/TC 154 エキスパート，ISO/TC307 国内審議委員会 WG2 作業部会主査．

中島 博敬

2012 年慶應義塾大学大学院政策・メディア研究科修士課程修了．2010〜2014 年慶應義塾大学大学院政策・メディア研究科研究員（後に特任助教），2014〜2017 年慶應義塾インフォメーションテクノロジーセンター本部助教．2017 年より（株）メルカリ R4D リサーチャー，2020 年同 JP Site Reliability Engineering．W3C や IETF において HTML5 や HTTP/2 等 Web 技術に関する標準化活動に従事．ISOC Japan Chapter Officer（2015〜2018 年），ISO TC307 国内審議委員会委員（2018 年）．