

暗号資産の署名鍵を取り扱うサービス に関する調査¹

第2版

栗田 青陽²

株式会社メルカリ R4D

DP2019-2-2

2019年12月16日

<<要旨>>

2019年5月31日、「他人のために暗号資産の管理をすること」を新たに暗号資産交換業の一類型として規制対象とする「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律」が成立した。

しかしながら、「他人のために暗号資産の管理をすること」に該当する業務の範囲等の解釈については現段階では明確ではない。

そこで本稿では、暗号資産を管理する形態と実際に提供されているサービスの実態に基づき、実施可能な制度の構築や、利用者の利便性の向上の検討にあたって重要と考えられる論点の整理を行い、あわせて署名鍵の取扱形態を整理し、それぞれの形態について改正法が流出リスクと破綻リスクへの対応として業者に求める対応の必要性を分析した。

本ディスカッションペーパーの内容は執筆者の個人的見解であり、所属する組織及びCryptoassets Governance Task Forceとしての公式見解を示すものではありません。

¹ 本調査の実施に際し、ご協力を頂いた事業者や開発者の皆様に感謝申し上げます。アンダーソン・毛利・友常法律事務所の長瀬威志氏には貴重なご助言を頂いた。サイボウズ・ラボ株式会社の光成滋生氏には暗号技術について貴重なご教示とご助言を頂いた。Cryptoeconomics Labの落合涉悟氏にはPlasmaについて貴重なご助言を頂いた。松尾真一郎、楠正憲、佐古和恵、佐藤雅史、島岡政基、須賀祐治、菅原謙一、林達也、花村直親、森下真敬、澤田健都、中島博敬、寺元健太郎の各氏、ならびにCryptoassets Governance Task Force Security Working Groupの参加者の方々からは多くの有益なコメントを頂いた。ここに記して感謝申し上げます。

² <https://twitter.com/niwatoko>

1. はじめに

2019年5月31日、「情報通信技術の進展に伴う金融取引の多様化に対応するための資金決済に関する法律等の一部を改正する法律」³（以下「改正法」という。）が成立した。

改正法は、「資金決済に関する法律」（以下「資金決済法」という。）についても改正し（以下「改正資金決済法」という。）、改正資金決済法において「仮想通貨」との呼称を「暗号資産」に変更するとともに、同法に定義される「暗号資産交換業」として掲げられる行為に、「他人のために暗号資産の管理をすること（当該管理を業として行うことにつき他の法律に特別の規定のある場合を除く。）」を業として行うことを加え、この行為を「暗号資産の管理」と定義している。

改正法の成立に際して付された衆議院財務金融委員会の附帯決議⁴および参議院財政金融委員会の附帯決議⁵は、「本法により整備される各種規定の運用に際しては、民間部門が過度に萎縮することがないように法解釈の周知徹底に努めるとともに、基礎となるブロックチェーン技術の開発及び提供によるイノベーションにも十分留意すること」、「規制対象事業の実態を考慮し、整合的かつ合理的に実施可能な制度を全体として構築するよう努めること」、「他人のために暗号資産の管理のみを業として行う者に対する規制の在り方について、マネー・ロンダリング及びテロ資金供与対策という国際的要請に応えつつ、可能な限り暗号資産交換業の利用者の利便性の向上に資する観点から検討を加え、その結果に基づき、必要な措置を講ずること。」としている。

なお、暗号資産の管理のみを行う業者は「カストディ業者」とも呼ばれている⁶が、暗号資産カストディ業務への規制導入の必要性については、2018年3月8日に金融庁が設置し、2018年12月14日まで全11回にわたって開かれた「仮想通貨交換業等に関する研究会」⁷において検討された。

同研究会の報告書（以下「報告書」という。）によると、仮想通貨カストディ業務とは、「仮想通貨の売買等は行わないが、顧客の仮想通貨を管理し、顧客の指図に基づき顧客が指定する先のアドレスに仮想通貨を移転させる業務」とされ、業務を行う上で、「サイバー攻撃による顧客の仮想通貨の流出リスク、業者の破綻リスク、マネーロンダリング・テロ資金供与のリスク等、仮想通貨交換業と共通のリスクがあると考えられること」、および「仮想通貨カストディ業務を行う業者についても、マネーロンダリング・テロ資金供与規制の対象にすることを各国に求める旨の改訂 FATF 勧告が採択されたこと」を踏まえ、「決済に関連するサービスとして、一定の規制を設けた上で、業務の適正かつ確実な遂行を確保していく必要があると考えられる。」とされている。

報告書によると、「仮想通貨カストディ業務には様々な形態のものが想定されるところ、異なるリスクレベルに応じて適切な規制を課していくためにも、規制対象となる業務の範囲を明確にしていくことが重要」という意見があった。

加えて、報告書のおわりには、「引き続き、取引の実態を適切に把握していくとともに、イノベーションに配慮しつつ、利用者保護を確保していく観点から、リスクの高低等に

³ <https://www.fsa.go.jp/common/diet/198/02/houritsuanriyuu.pdf>

⁴

http://www.shugiin.go.jp/internet/itdb_rchome.nsf/html/rchome/Futai/zaimu084657CD14F91C6249258401000DC40E.htm

⁵ http://www.sangiin.go.jp/japanese/gianjoho/ketsugi/198/f067_053001.pdf

⁶ <https://www.fsa.go.jp/common/diet/198/02/setsumeimei.pdf>

⁷ <https://www.fsa.go.jp/news/30/singi/kasoukenkyuukai.html>

応じて規制の柔構造化を図ることを含め、必要に応じて更なる検討・対応を行っていくことが重要である」と記載されている。

筆者は、こうした中で暗号資産カストディ業務の実態を把握することには一定の重要性があると考え、国内のウォレット提供者に対してヒアリングを行い、その結果をまとめた「日本国内における仮想通貨ウォレットの実態調査」⁸を公表した。

同調査は、事業やサービスの性質、利用実態や運営状況の実態について着目したものであった。様々なサービスの事例を示した上で、「規模、取引内容、事業形態等によってリスクの内容や大きさはそれぞれ異なる」ことから、「事業やサービスの性質を踏まえたリスクに応じた規制とすることが肝要」であることを指摘した。

また筆者は、さらなる実態把握のため、国内で暗号資産カストディに該当すると考えられる可能性があるサービスの調査を呼びかけ、情報提供に基づいてリスト⁹を作成した。30程度のサービスが存在したが、それらのサービスの中には、規制に先立ち、すでに終了または終了を予定しているサービスもある。

本稿では、暗号資産を管理する方法の特性と、事業やサービスの形態によって利用者や業者が暗号資産の管理に対して求める事業やサービス上の要件の観点から、実態に即した実施可能な制度の構築や、利用者の利便性の向上の検討にあたって重要と考えられる論点の整理を行った。

また、関係機関にとって、規制対象となる業務の範囲や法解釈の明確化にあたっては、改正法における流出リスクと破綻リスクの軽減のため、あるいはこれらのリスクが顕在化した場合の対処のため、業者に求められる対応の必要性を把握することが重要であると考えられるため、暗号資産や暗号資産の署名鍵を取り扱う様々な形態を整理し、それぞれ改正法が求める対応の必要性を分析した。

なお、本稿に掲載するサービスや技術等はいくまで一例であり、筆者が特定のサービスや技術等について、安全性を保証したり、推奨したりするものではない。

⁸ <https://cgtf.github.io/publications/20190314/dp2019-01/>

⁹ <https://docs.google.com/spreadsheets/d/1mQPs7fCFdfDftQFLjhwqwkX82oVNr748BwXvpOHv70Y/edit#gid=0>

2. 定義

2.1 暗号資産、ブロックチェーン、ノード

「資金決済に関する法律」は改正前の同法第2条5項において、仮想通貨の定義として以下のように定めている。

一 物品を購入し、若しくは借り受け、又は役務の提供を受ける場合に、これらの代価の弁済のために不特定の者に対して使用することができ、かつ、不特定の者を相手方として購入及び売却を行うことができる財産的価値（電子機器その他の物に電子的方法により記録されているものに限り、本邦通貨及び外国通貨並びに通貨建資産を除く。次号において同じ。）であって、電子情報処理組織を用いて移転することができるもの

二 不特定の者を相手方として前号に掲げるものと相互に交換を行うことができる財産的価値であって、電子情報処理組織を用いて移転することができるもの

改正法は仮想通貨という呼称を暗号資産に改める¹⁰。本稿では呼称を暗号資産とする。代表的な暗号資産には、ブロックチェーン技術によって実現されたビットコイン¹¹がある。ビットコインのシステムは、ソフトウェアを動作させるノードと呼ばれるコンピューターがネットワークを形成し、ブロックチェーンを元帳として共有して取引を記録しあう。

¹⁰ 改正法は金融商品取引法第二条第三項に電子記録移転権利を規定しており、電子記録移転権利を表示するものは暗号資産から除くとしている。

¹¹ <https://bitcoin.org/bitcoin.pdf>

2.2 署名（デジタル署名）、署名鍵（秘密鍵）、検証鍵（公開鍵）

ビットコインを始めとする多くの暗号資産は、デジタル署名（以下、署名）を活用し、暗号資産の所有や移転を電子的に表す。

署名には、署名鍵および検証鍵と呼ばれる鍵データのペアを用いる。署名鍵を用いて作成された署名は、その署名鍵によって作成されたことを、検証鍵を用いて数学的に検証可能となる。署名や検証鍵から署名鍵を推測し、署名を偽造することは非常に困難である。

署名の利用例としては、検証鍵だけを他者に伝え、署名鍵を用いて電子データに署名を付加する。そうすることで、電子データは署名鍵の所有者が作成し、第三者によって偽造、または改ざんされたものでないことを、検証鍵を知る者らに対して証明できる。

署名が署名者によって行われるものであることを担保するためには、署名鍵は署名者のみが知るものとして、秘密を保たなければならない。また、署名の検証が行われるためには、検証鍵が検証者らに対して公開されていなければならない。

なお、署名鍵は秘密鍵、検証鍵は公開鍵と呼ばれる場合もあるが、本稿ではISO/IEC JTC1の標準文書に従い、署名に用いる鍵を署名鍵（ISO/IEC 14888-1ではSignature Key）、検証に用いる鍵を検証鍵（ISO/IEC 14888-1ではVerification Key）とする。

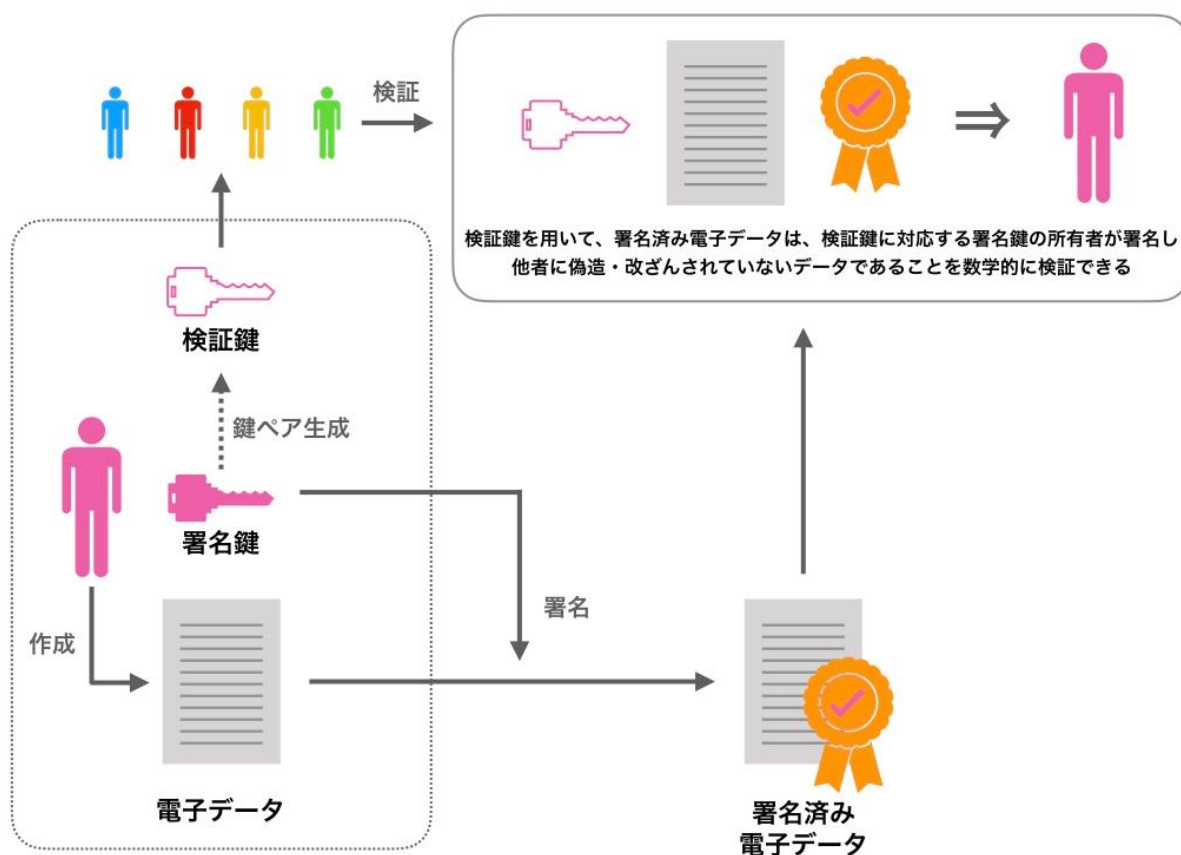


図2-1 デジタル署名

2.3 アドレス、トランザクション、トランザクション手数料

署名を活用した暗号資産では、検証鍵や、アドレスと呼ばれる検証鍵から導出されるデータに対して、暗号資産が存在するものとして記録される。

暗号資産は、トランザクションと呼ばれる取引データによって別のアドレス等へ移転される。トランザクションの作成には、暗号資産の移転元である検証鍵やアドレスに対応する署名鍵を用いた署名が必要である。

つまり、署名鍵の所有者のみが暗号資産を移転することができる。署名鍵があれば残高を移転できるため、署名鍵は、残高の管理者のみが所有している必要がある。

検証鍵やアドレスは、残高の移転を受ける際に移転元に対して伝える必要があり、他者へ移転する際にも移転先の検証鍵やアドレスを知る必要がある。

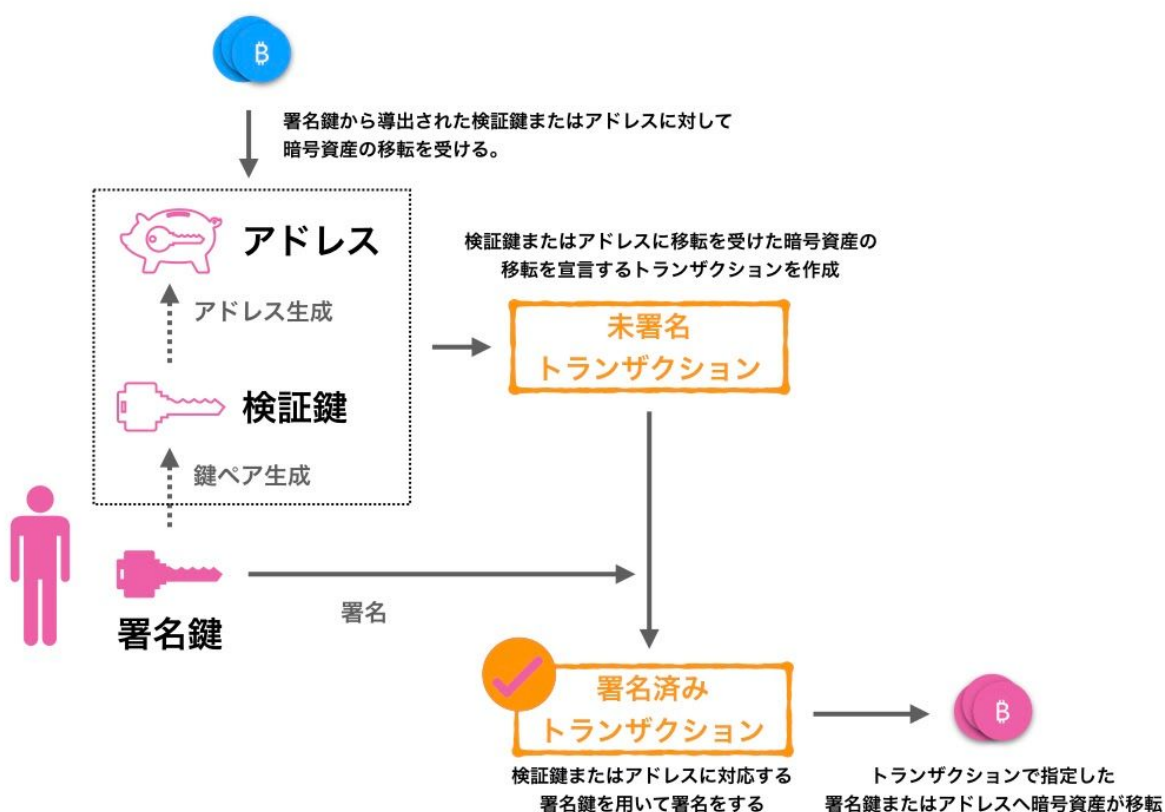


図2-2 トランザクションの作成の例

作成したトランザクションのデータは、暗号資産を実現する仕組みであるブロックチェーン等に記録される必要がある。多くの場合、トランザクションには、宛先へ移転する暗号資産に加えて、ブロックチェーン等へトランザクションが記録されるために必要な手数料となる暗号資産を含める¹²。この手数料はトランザクション手数料（トランザクションフィー）と呼ばれる。また、暗号資産によっては、トランザクション手数料が不要な仕組みによって実現されている場合もある。

¹² 手数料をゼロにすることも可能であるが、その結果として記録されるまでの処理時間が長くなる場合や、記録されない場合がある。

2.4 マルチシグアドレス

アドレスの一種としてマルチシグアドレスと呼ばれるものがある。これは、複数の検証鍵から導出されるアドレスである。

マルチシグアドレスは、残高を移転する際、検証鍵に対応する署名鍵を用いた署名が必要となる点では通常のアドレスと変わらないが、複数の署名鍵による署名を必要とすること、およびその署名数を任意に設定できる。

例えば、3つの検証鍵のうち、いずれか2つの検証鍵に対応する署名鍵を用いて署名を行えば残高を移転できる、といったマルチシグアドレスを導出できる。このとき、2 of 3などと表現される。

複数の署名鍵のうちの一部で署名可能とすることで、鍵の紛失リスク（暗号資産を移転できなくなるリスク）を軽減することが可能となる。

有効なトランザクションの生成に複数の署名鍵を必要とすることで、権限を分散し、多段階の承認プロセスや複数組織の承認プロセスを実現することや、紛失したり盗難されたりした署名鍵が用いられて意図しない暗号資産の移転が発生するリスクを軽減することができる。

マルチシグアドレスの署名済みトランザクションからは、どの検証鍵に対応する署名鍵を用いて署名が行われたのか、特定できる。暗号資産の移転時の承認プロセスや承認した組織を特定したり、暗号資産が流出した場合に不正に使用された署名鍵を特定したりすることができる。

マルチシグアドレスは検証鍵から作成できる。マルチシグアドレスの作成者は署名鍵を知る必要はない。したがって、署名鍵はそれぞれ独立して作成することが可能である。複数組織のマルチシグアドレスを作成する場合に、各組織はお互いの署名鍵を知る必要はない。

署名は署名鍵ごとに独立して行うことが可能である。例えば、2つの署名が必要な場合、1つ目の署名を行う者は2つ目の署名の署名鍵を知る必要はなく、2つ目の署名を行う者も1つ目の署名の署名鍵を知る必要がない。

なお、マルチシグアドレスを利用できない暗号資産も存在する。

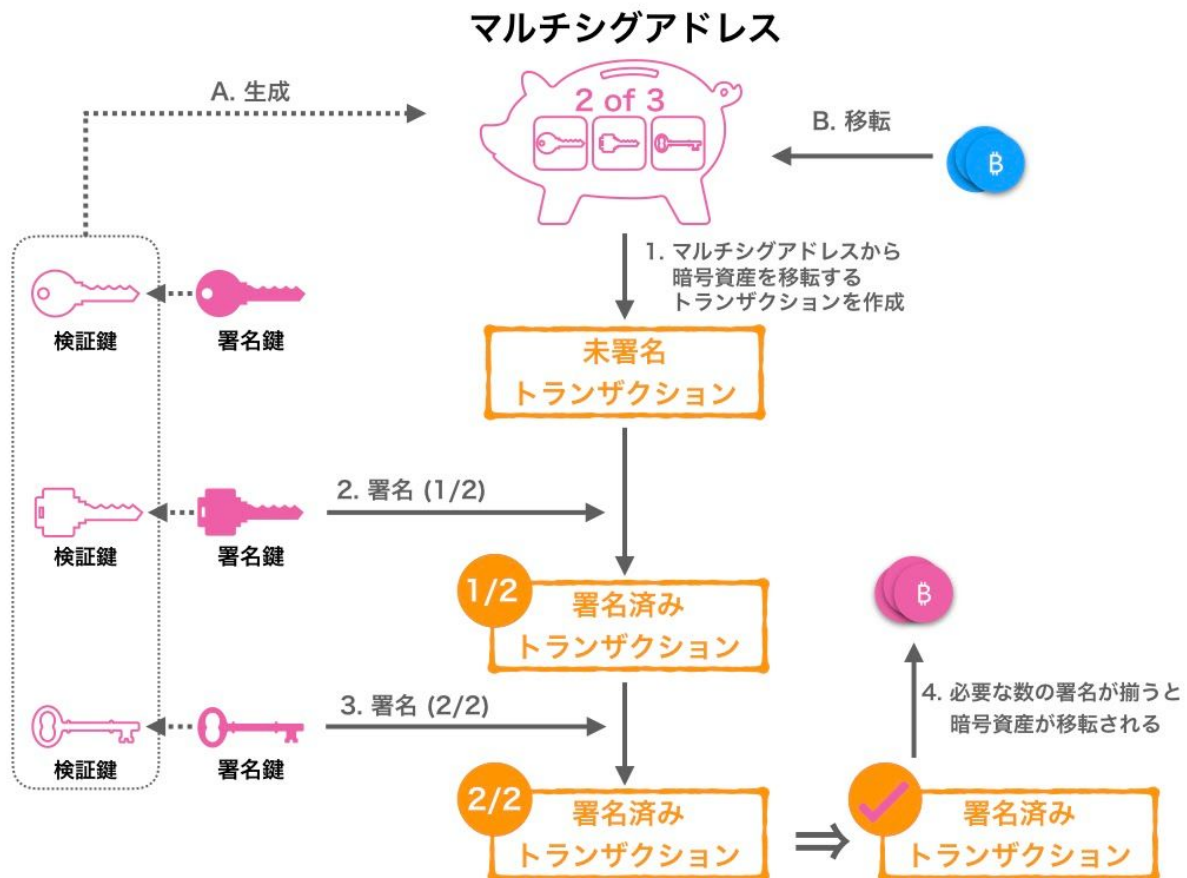


図2-3 2 of 3のマルチシグアドレスの例

2.5 スマートコントラクト、コントラクトウォレット

暗号資産の中には、スマートコントラクトと呼ばれる、プログラムの実行機能を備えたプラットフォーム上で発行されているものがある。

Etherが発行されているEthereumと呼ばれるプラットフォームでは、Solidityと呼ばれるプログラミング言語で作成したスマートコントラクトのプログラムを、トランザクションを発行することで、ブロックチェーンに書き込むことができる。

ブロックチェーンに書き込まれたスマートコントラクトには、アドレスが割り当てられる。スマートコントラクトのアドレスに対してトランザクションを発行すると、スマートコントラクトのプログラムが実行され、その結果がブロックチェーンに記録される。

スマートコントラクトのプログラムは、一度ブロックチェーンに書き込まれると、書き換えることも、実行を停止させることもできない¹³。

¹³ 一般的には、ブロックチェーンに書き込まれたスマートコントラクト自体は変更、停止できないが、事前にスマートコントラクトのプログラムに管理権限を定義し、あとから管理者が設定を切り替えるトランザクションを発行することで、変更や停止を実現する仕組みを、プログラムとして記述しておくことは可能である。また、スマートコントラクトの変更や停止が可能な仕様を備えた暗号資産プラットフォーム（EOSなど）も登場している。

スマートコントラクト自体が暗号資産の移転を受け付けることもできる。スマートコントラクトのアドレスには対応する署名鍵がなく、移転を受けた暗号資産は、そのスマートコントラクトに書き込まれたプログラムに基づいてのみ処理される¹⁴。

スマートコントラクトで入出金機能を備えるものが、特にコントラクトウォレットと呼ばれる。コントラクトウォレットは、暗号資産の移転を受け、残高として保持し、権利を持つアドレスからの指示に従って送金や残高の引き出しを行うことができるプログラムによって実現される。

コントラクトウォレットは、マルチシグアドレスの代替として利用される場合がある。例えば、Ethereumではマルチシグアドレスを利用することができないが、スマートコントラクトによって、3つの署名鍵のうち、2つの署名鍵の署名によって暗号資産の移転を行うコントラクトウォレットを作成できる。

コントラクトウォレットを利用することにより、マルチシグアドレスを用いる場合と同様に署名鍵の紛失リスクの軽減や権限の分散が可能になる。

マルチシグアドレスの場合と同様に、署名済みトランザクションからどの検証鍵に対応する署名鍵が署名に用いられたのか、特定できる。また、署名鍵はそれぞれ独立して作成することが可能であり、コントラクトウォレットの作成者は署名鍵を知る必要はない。署名についても、署名鍵ごとに独立して行うことが可能である。

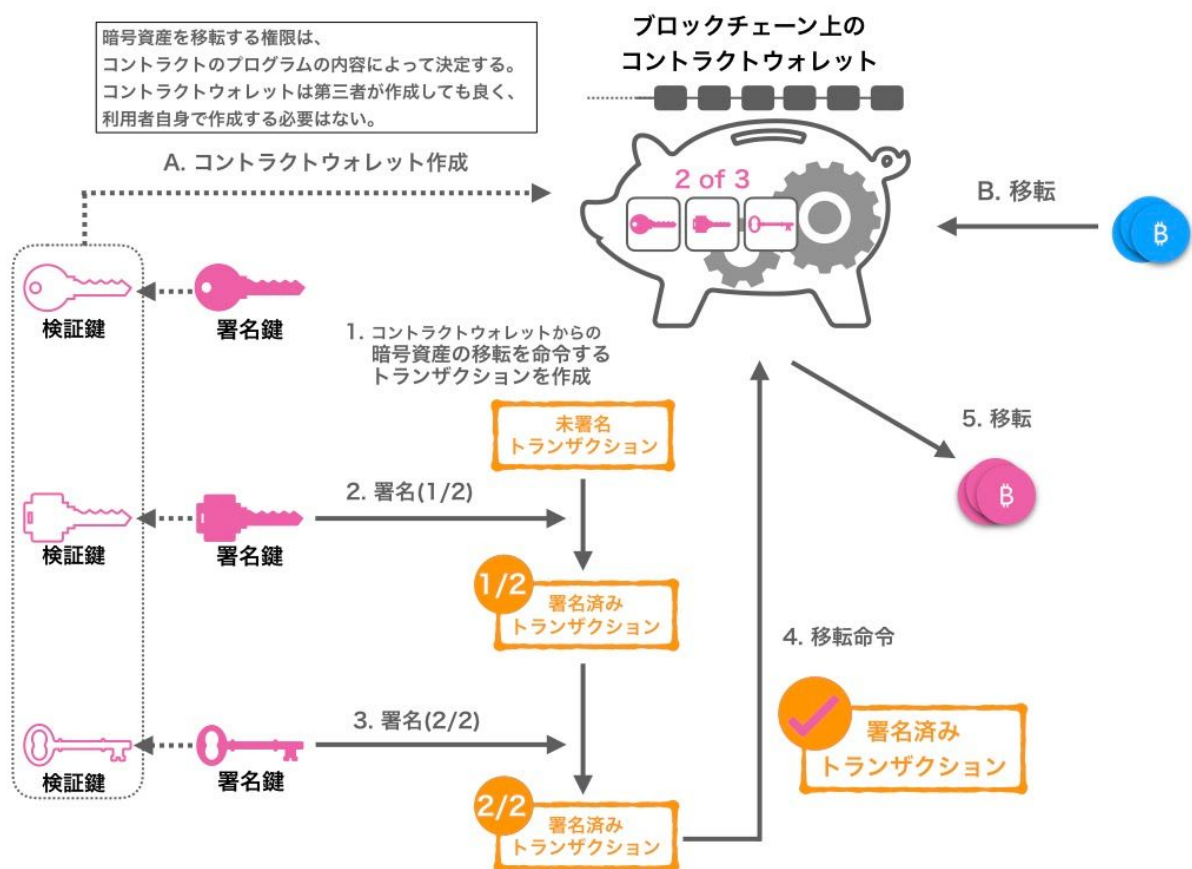


図2-4 2 of 3のコントラクトウォレットの例

¹⁴ スマートコントラクトをブロックチェーンに書き込んだ者は、スマートコントラクトのアドレスに移転された暗号資産に対して、管理者のような特別な権利は持たない。スマートコントラクトから暗号資産を移転する方法は、スマートコントラクトのプログラムの内容によって決定する。

2.6 秘密分散

秘密分散と呼ばれる手法¹⁵を用い、1つの署名鍵を、単独では利用できないデータとなる分散片（シェア）に分割する場合がある。

秘密分散においては、しきい値を設定し、そのしきい値以上の分散片を揃えることで、署名鍵を復元することがある。例えば、署名鍵を3つの分散片に分割し、3つのうち2つの分散片が揃えば署名鍵を復元できるようにすることが可能である。このとき、2 out of 3などと表現される。

この秘密分散を利用することにより、紛失リスクの軽減や権限の分散が可能になる。

ただし、署名鍵の生成や分散片への分割を行う者（ディーラー）と、分散片を集約して署名鍵を復元し署名を行う者は、分割前、または復元後の署名鍵を操作することになることから、単独でトランザクションへの署名を行える状態となり、権限の集中が生じる。

この点で、署名に必要な複数の署名鍵をそれぞれ独立して生成し、それぞれの署名鍵ごとに独立して署名を行うことができるマルチシグアドレスのような仕組みとは異なり、マルチシグアドレスの場合と同等の権限分散は行えない。

また、署名済みのトランザクションからは、どの分散片を組み合わせる署名鍵を復元し、署名に用いたのかについて、特定することはできない。

後述の秘密計算と組み合わせることで、権限の集中を避けることは可能である。

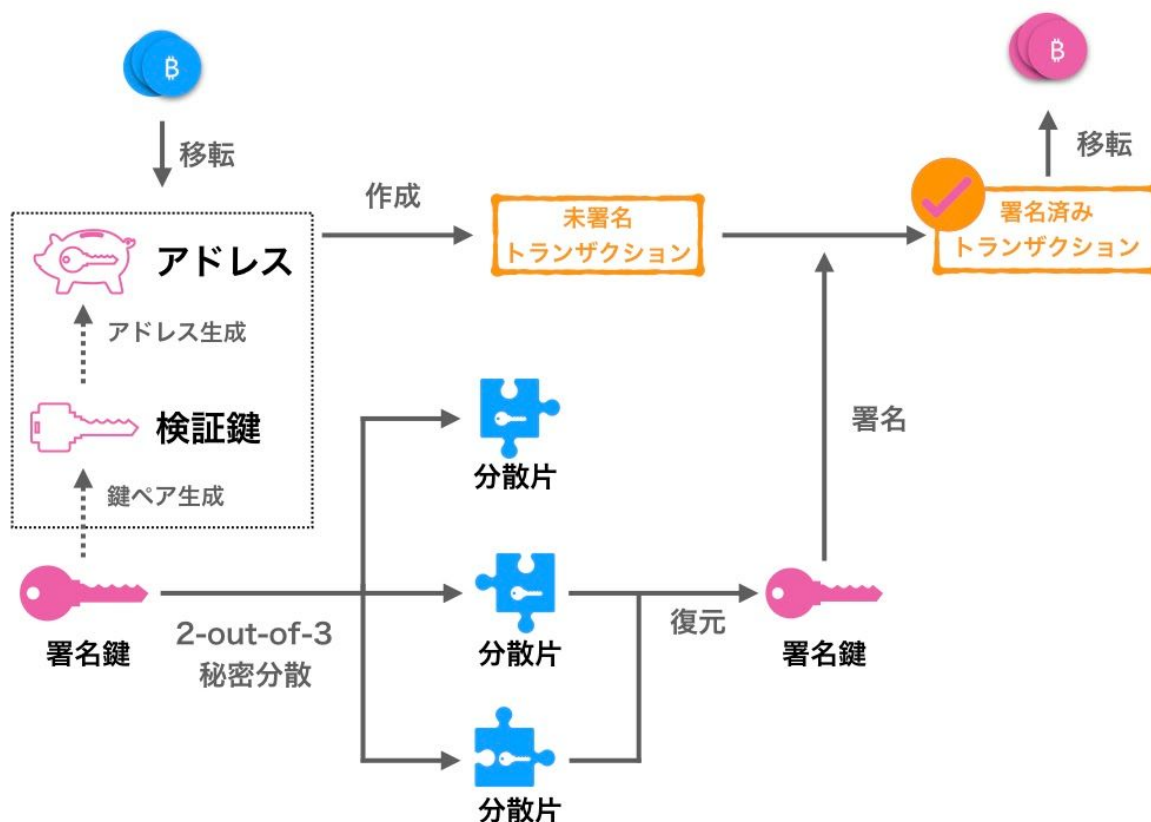


図2-5 秘密分散の例

¹⁵ 例として、Shamirによる秘密分散法と呼ばれる手法がある
(<https://dl.acm.org/citation.cfm?id=359176>)

2.7 秘密計算

データを暗号化したままの状態でする秘密計算（Secure multi-party computation）と呼ばれる手法が、秘密分散と合わせて用いられる場合がある。

2.7.1 秘密計算を署名に用いる方法

秘密計算を用いると、秘密分散した署名鍵を復元することなく、分散片の状態のまま、署名のための計算を行うことができる。

秘密分散を用いる秘密計算は、複数のコンピューターがそれぞれ分散片を用いて計算を行う。それぞれのコンピューターの計算結果は単独では意味を持たず、集約することで目的とする計算結果を導くことができる。

この方法では、署名のために署名鍵を復元する必要はなく、ある分散片を用いて秘密計算を行うコンピューターは他の分散片を知る必要もない。また、各コンピューターが行った秘密計算の結果は、単独では意味を持たない。それぞれの秘密計算の結果を集約して導出された署名から、署名鍵を推測することもできない。秘密分散だけを使用した場合、署名時に分散片を集約し署名鍵を復元する必要があるため、権限の集中が生じるが、秘密計算を署名に用いることで、署名時の権限集中を解消することができる。

ただし、署名鍵の生成や分散片への分割を行う者は、分割前の署名鍵を操作することになることから、単独でトランザクションへの署名を行える状態となり、権限の集中が生じる。

また、署名済みのトランザクションからは、どの分散片が秘密計算に利用されたか、特定することはできない。

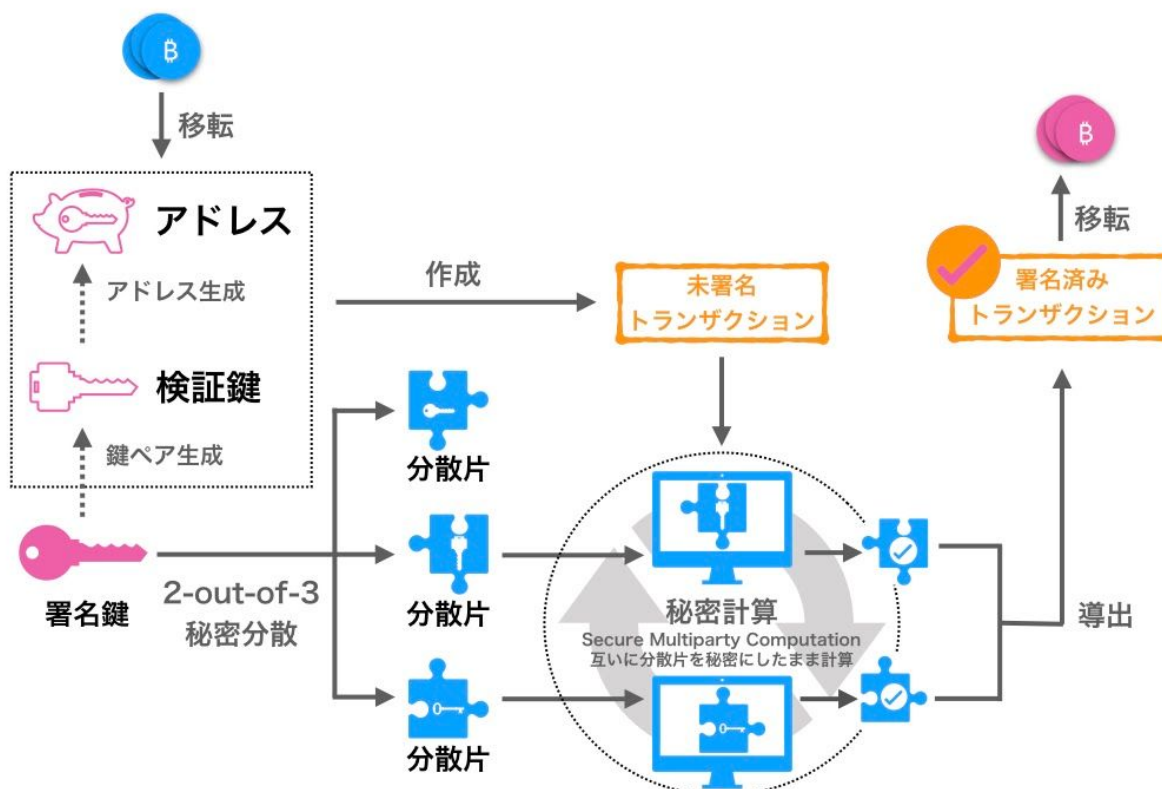


図2-6 秘密計算を署名に用いる方法の例

2.7.2 秘密計算を検証鍵の生成と署名に用いる方法

署名鍵を秘密分散によって分割する場合、署名鍵の生成や分割を行う者に権限が集中するため、複数のコンピューターで協力して計算を行い、署名鍵を生成せずに検証鍵を直接生成するとともに、それぞれのコンピューター上に分散片を直接生成し、分散片から秘密計算によって署名を導出する方法¹⁶が登場している。

この場合、署名鍵の生成や分割に伴う権限集中、および署名に伴う権限集中も解消され、マルチシグアドレスの場合と同等の権限分散が可能になる。

複数組織で検証鍵やアドレスを作成した場合、常にお互いの分散片を知る必要はなく、署名鍵を知る必要もない。

ただし、署名済みのトランザクションからは、どの分散片が秘密計算に利用されたかを特定することはできない。

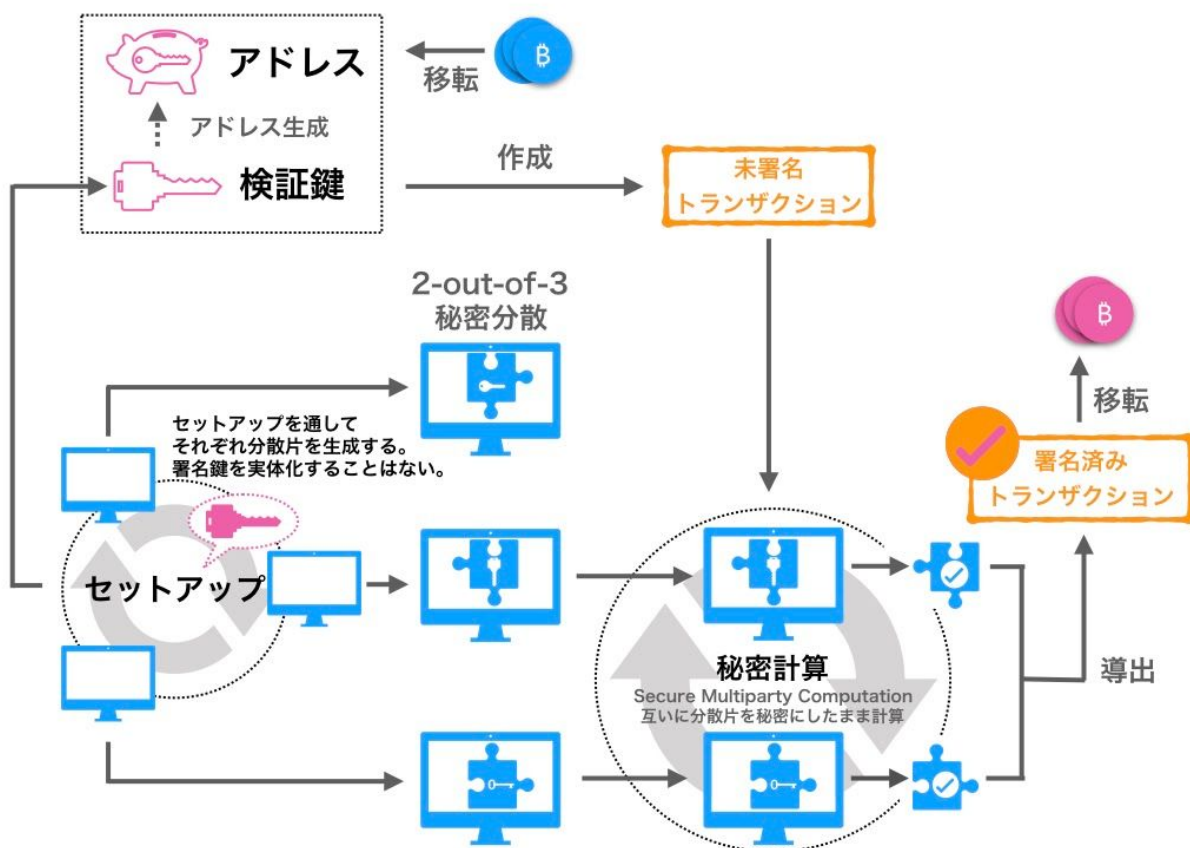


図2-7 秘密計算を検証鍵の生成と署名に用いる方法の例

¹⁶ たとえば、以下のような方法が考案されている。

Rosario Gennaro, Steven Goldfeder, and Arvind Narayanan, "Threshold-optimal DSA/ECDSA signatures and an application to Bitcoin wallet security", <https://eprint.iacr.org/2016/013>, 2016.
Yehuda Lindell, Ariel Nof, and Samuel Ranellucci, "Fast Secure Multiparty ECDSA with Practical Distributed Key Generation and Applications to Cryptocurrency Custody", <https://eprint.iacr.org/2018/987>, 2018.

Jack Doerner, Yashvanth Kondi, Eysa Lee, and abhi shelat, "Threshold ECDSA from ECDSA Assumptions: The Multiparty Case", <https://eprint.iacr.org/2019/523>, 2019

2.8 ウォレット

アドレスや検証鍵、署名鍵そのもの、または署名鍵を記録した媒体、あるいは、暗号資産の残高の操作や、署名鍵の保管、署名をするためのソフトウェアやサービスなど、暗号資産の移転を受けたり、移転を実施したりするために利用されるものがウォレットと呼ばれる。ウォレットは、一般的に概念として理解されるものであり、厳密な語義があるものではない。

2.9 オンチェーン、オフチェーン、オンチェーン取引、オフチェーン取引

ブロックチェーン上に記録が残ることはオンチェーンと呼ばれ、オンチェーンで行われる取引はオンチェーン取引と呼ばれる。ブロックチェーン上に記録が残らないことはオフチェーンと呼ばれ、オフチェーンで行なわれる取引はオフチェーン取引と呼ばれる。

オンチェーン取引には、暗号資産の移転だけではなく、後述するステーキングやデリゲート、投票のためのトランザクションをブロックチェーン上に記録するものもある。

また、ブロックチェーン上で動作するゲームやアプリケーションを操作するために、トランザクションをブロックチェーン上に記録するものも考えられる。

2.10 Proof of Stake (PoS)、ステーキング、デリゲート

ブロックチェーンへのトランザクションの記録は、ブロックチェーンのネットワークに参加するノードと呼ばれるコンピュータの中から、プロトコルに基づいて選出¹⁷されたノードによって行われる。記録を行ったノードは報酬¹⁸を得られる場合があり、これがノードとしてトランザクションの記録を行うインセンティブとなっている¹⁹。

Proof of Stake（以下、PoS）と呼ばれるプロトコルを採用するブロックチェーンでは、暗号資産を所有する量や期間等に基づいて、トランザクションを記録する権利のあるノードが選出され、選出されたノードらがランダムや輪番等でトランザクションの記録を行う。

PoSプロトコルを利用したブロックチェーンにおいて、トランザクションを記録する権利を得るために暗号資産を保有したり、担保としてスマートコントラクトに暗号資産をロックした状態にしたりすることをステーキングと呼ぶ²⁰。

PoSを採用したブロックチェーンの例として、ノードはトランザクションの記録を正しく行えば報酬を得ることができ、記録を正しく行なわなかったノードは、ステーキングしている暗号資産を失う仕組みがある。

Delegated Proof of Stake（以下、DPoS）では、自らのノードに対するトランザクションの記録を行う権利のためではなく、他のノードがトランザクションの記録を行う権利のため

¹⁷ 記録を行うノードが特定のノードに定められているブロックチェーンもある。

¹⁸ 新規に発行される暗号資産や、トランザクションに設定されている手数料が報酬となる。

¹⁹ インセンティブの一例として、ビットコインはProof of Work（以下、PoW）と呼ばれるプロトコルを採用している。PoWでは、ある一定のルールに基づく計算をノードが競い、他のノードよりも早く結果を求めたノードが、トランザクションの記録を行い、報酬を得る。

²⁰ 暗号資産を保有しているだけでステーキングができる場合や、コントラクトに移転することで暗号資産の移転が制限された状態にする必要がある場合などがある。ステーキングに利用される暗号資産は、ノードが不正なトランザクションを記録すると没収される場合などがあり、実質的に担保の役割がある。

にステーキングすることができる。他ノードの権利のためにステーキングすることを、特にデリゲートと呼ぶ。

DPoSを採用したブロックチェーンの例として、記録を正しく行ったノードと、そのノードにデリゲートしていたノードは報酬を得ることができ、記録を正しく行なわなかったノードと、そのノードにデリゲートしていたノードは、ステーキングしている暗号資産を失う仕組みが考えられる。

ステーキングやデリゲートは、ブロックチェーン上に記録する必要があるため、署名鍵による署名を伴うオンチェーン取引となる。開始後は追加の署名を必要とせずに継続される。

2.11 投票

ブロックチェーンや、スマートコントラクトによって実現されたアプリケーションの中には、ブロックチェーン上で意思決定のための投票²¹を行う仕組みを備えるものがある。

こうした仕組みでは、投票の権利や重み付けが、暗号資産を所有する量や期間等に基づいて決定される。

投票はブロックチェーン上に記録する必要があるため、署名鍵による署名を伴うオンチェーン取引となる。

²¹ 仕様の変更や、開発の方針を決定するための投票などがある。

2.12 メインチェーン、サイドチェーン

ブロックチェーンで実現されたある暗号資産を、本来のブロックチェーンとは別のブロックチェーンで扱うことがある。その際、本来のブロックチェーンはメインチェーンと呼ばれ、本来のブロックチェーンとは別のブロックチェーンはサイドチェーンと呼ばれる。

サイドチェーンを用いることで、メインチェーンとは異なる機能や性質を備えるブロックチェーンで暗号資産を扱うことができる。

メインチェーンとサイドチェーンの対応は1対1ではなく、複数の種類の暗号資産を扱うことができるサイドチェーンもある。また、複数のサイドチェーンが存在するメインチェーンもある。

メインチェーンの暗号資産をサイドチェーンで扱うには、メインチェーンで暗号資産を所有する利用者が、メインチェーン上で暗号資産をロックする²²。すると、メインチェーン上でロックされた暗号資産と同量の残高がサイドチェーン上に記録され、利用者の署名鍵で移転可能になる。サイドチェーンの暗号資産をメインチェーンに戻すには、サイドチェーンで残高を所有する利用者が、サイドチェーン上で残高を消却する。すると、サイドチェーン上で消却された残高と同量の暗号資産がメインチェーン上で開放され、利用者が移転可能になる。サイドチェーンでの取引はメインチェーンにとってオフチェーン取引である。

メインチェーン上で暗号資産をロックする仕組みや、サイドチェーンを動作させる仕組みには様々な形態が考えられる。特定の管理者が存在する場合もあれば、分散的な仕組みによって実現される場合もある。

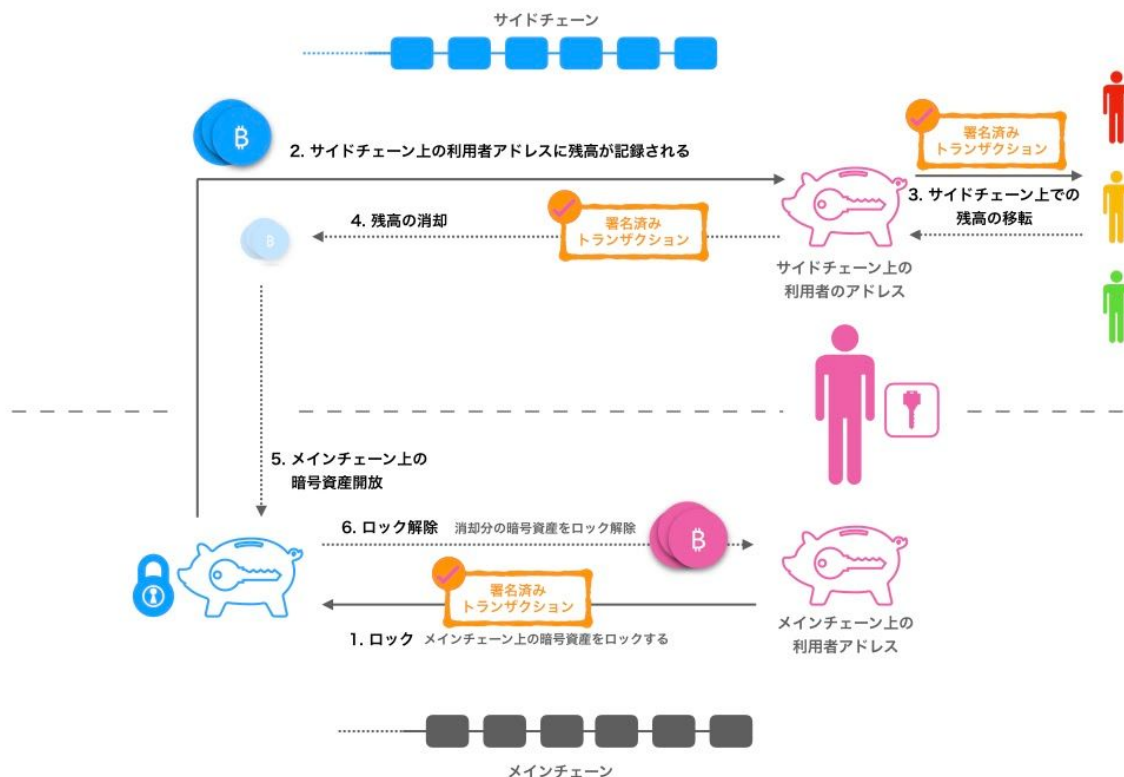


図2-8 メインチェーンとサイドチェーン

²² ロックする方法には、スマートコントラクトに暗号資産を移転する方法や、サイドチェーンを動作させているノードが管理するアドレスに暗号資産を移転する方法等がある。

3. 業者が顧客の暗号資産を管理する方法と規制の論点

暗号資産の管理にあたる業務の範囲は本稿執筆の段階では明確に法令または規制等では定められていないが、仮想通貨交換業等に関する研究会の報告書によると、規制の対象にすべきとされているカストディ業務は、「顧客の仮想通貨を管理し、顧客の指図に基づき顧客が指定する先のアドレスに仮想通貨を移転させる業務」とされている。また、「顧客の仮想通貨の管理」の方法として、「顧客の仮想通貨アドレスから、業者が秘密鍵を管理する業者の仮想通貨アドレスに、仮想通貨の移転を受けて管理する方法」²³（以下、集約管理する方法）と、「顧客の仮想通貨アドレスに対応した（仮想通貨の移転に必要な）秘密鍵を業者が管理する方法」²⁴（以下、個別管理する方法）が例として挙げられている²⁵。

すでに本稿執筆時点で規制の対象となっている暗号資産の交換等を行う事業者は、集約管理する方法を用いている。また、筆者が過去に行った調査²⁶では、国内において暗号資産の交換等以外のために暗号資産や署名鍵を取り扱う事業者についても、ほとんどが集約管理する方法を用いている。

ただし、国外においては個別管理する方法を用いるサービスも存在しており、規制にあたっては、個別管理する方法を用いるサービスについての実態の把握と、実態を踏まえた実施可能な制度の検討が重要であると考えられる。

そこで、集約管理する方法と個別管理する方法について、それぞれの特性の分析と、どのようなサービス形態で利用されているかの事例に基づき、考えられる論点を整理した。なお、それぞれの管理する方法の特性やサービスの事例、論点は、必ずしもあり得るすべてを網羅するものではない。

3.1 集約管理する方法

顧客の暗号資産アドレスから、業者が署名鍵を管理する業者の暗号資産アドレスに、暗号資産の移転を受けて管理する。

業者が移転を受ける暗号資産と顧客を対応付けるため、業者が顧客ごとに暗号資産の移転を受けるアドレスを用意する場合や、顧客に対して暗号資産を移転するトランザクションに識別情報を付加させる場合²⁷等がある。

移転を受けた暗号資産は、データベース等に顧客が所有する暗号資産の残高として記録される。顧客の残高への反映が済んだ暗号資産は、業者の管理用のアドレスに移転され、他の顧客の暗号資産とまとめられる場合がある。

²³ 暗号資産は業者のアドレスで集約管理され、その残高の明細をデータベース等により、オフチェーンで管理する方法。以降は「集約管理する方法」という。

²⁴ 暗号資産は業者が顧客ごとに用意したアドレスで個別に管理され、すべての取引をオンチェーンで管理する方法。以降は「個別管理する方法」という。

²⁵ 以降の議論をまとめやすくするため、報告書の登場順序とは異なる順番で引用している。

²⁶

<https://docs.google.com/spreadsheets/d/1mQPs7fCFdfDftQFLjhwqwkX82oVNr748BwXvpOHv70Y/edit#gid=0>

²⁷

<https://support.bitbank.cc/hc/ja/articles/115008064588-XRP%E3%81%AE%E5%AE%9B%E5%85%88%E3%82%BF%E3%82%B0%E3%81%A3%E3%81%A6%E3%81%AA%E3%82%93%E3%81%A7%E3%81%99%E3%81%8B>

サービス内での暗号資産の移転取引は、オフチェーン取引となる。ブロックチェーン上で実際に暗号資産が移転されるのではなく、データベース等に記録された顧客が所有する暗号資産の残高が付け替えられる。

顧客が業者に対して外部のアドレスへの暗号資産の移転を指示した場合には、オンチェーン取引となる。業者の暗号資産アドレスから、移転先のアドレスに暗号資産を移転するトランザクションを作成し、業者の署名鍵を用いてトランザクションに署名する。オンチェーン取引のため、トランザクションはブロックチェーンに記録される。移転元のアドレスは、業者が顧客らの暗号資産をまとめて管理しているアドレスとなり、顧客が業者に対して暗号資産を移転した際のアドレスとは異なるアドレスになる可能性がある。また移転の都度、業者が移転元として用いるアドレスは変更される可能性がある。

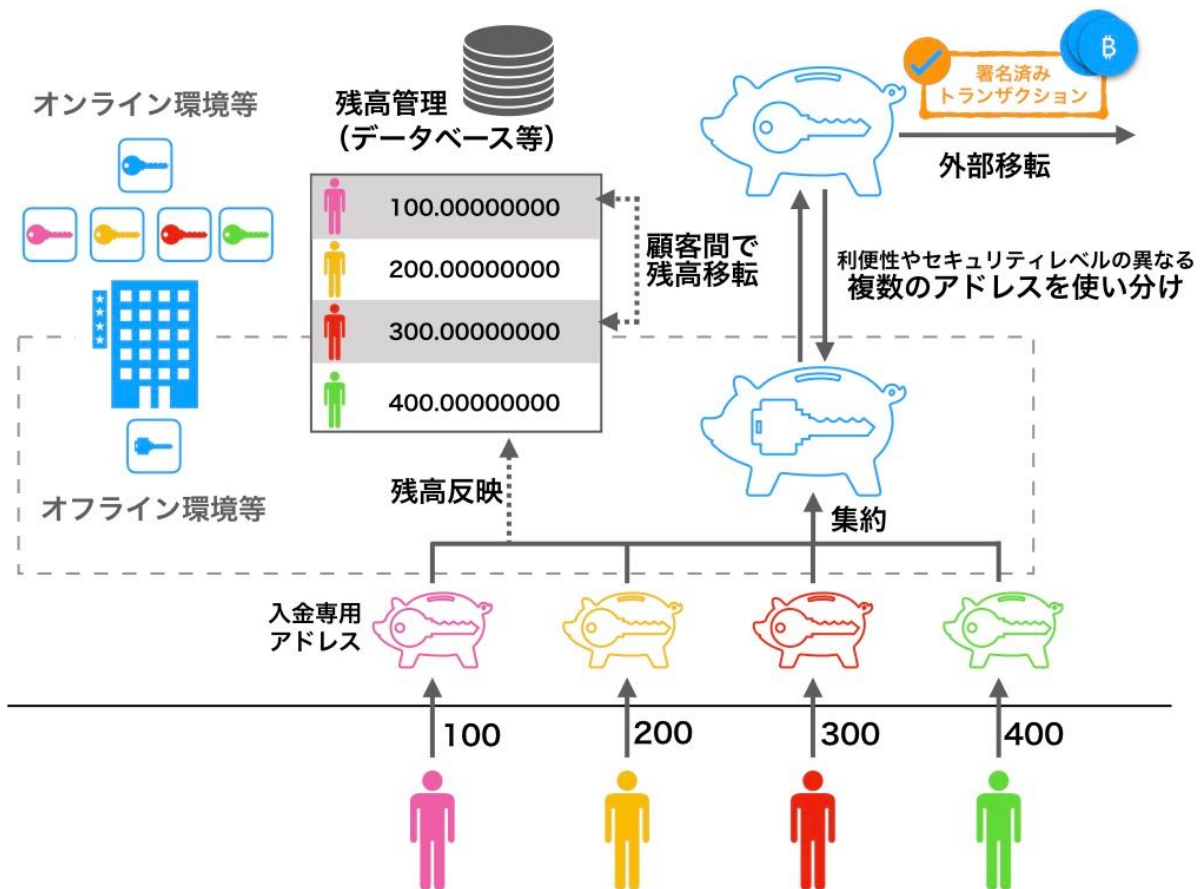


図3-1 集約管理する方法の例

3.1.1 集約管理する方法のメリット

サービス内で暗号資産の所有者が変化した際に、データベース上で顧客が所有する暗号資産の残高を付け替えることで（オフチェーン取引）、ブロックチェーン上で移転を行う場合に必要なトランザクション手数料や処理時間の負担²⁸を軽減することができる。

²⁸ ビットコインの場合、1回のトランザクションの確定には、おおむね60分ほど必要とされている。

顧客が所有する暗号資産はデータベース上に、顧客ごとに残高として管理されており、業者は顧客ごとの暗号資産を顧客ごとのアドレスで管理する必要がなく、複数の顧客の暗号資産をまとめて管理することもできる。

そのため、複数の顧客から暗号資産を移転する指示があった場合、顧客らの暗号資産をまとめて管理している業者のアドレスを移転元としてトランザクションを作成し、業者の署名鍵を使って一度に署名することができる。

また、業者は必要に応じてセキュリティレベルや利便性の異なる方法で管理されている複数のアドレスを使い分けることができる。例として、トランザクションの作成を伴う業務に必要な流動性の高い暗号資産を利便性の高い方法で保管し、それ以外の暗号資産は流出のリスクが低いことを最も重視した方法で保管する等の対応が考えられる。

複数の顧客の暗号資産をまとめて管理することで、一定量の暗号資産の残高を必要とするようなステーキングやデリゲート、投票等を業者が行えるようになる。

3.1.2 集約管理する方法のデメリット

暗号資産が顧客ごとのアドレスで管理されていないため、顧客の暗号資産の残高はブロックチェーン上では確認することができず、残高管理の信頼性は、業者の残高管理システムの信頼性に依存する。顧客が自身の残高をブロックチェーン上で確認したい場合や、第三者に残高を証明したい場合には利用できない。

また、サービス外へ暗号資産を移転する際に、移転元が、業者が複数の顧客の暗号資産をまとめて管理しているアドレスとなる可能性があるため、移転元のアドレスが顧客の所有するアドレスに対応している必要がある場合にも、この方法は利用できない。例えば、取引所等から、ブロックチェーン上で発行されるトークンを購入するための暗号資産の移転を行うと、移転元である取引所のアドレスにトークンが付与されてしまうことが考えられる。

オンチェーンでのステーキングやデリゲート、投票についても、顧客ごとに個別に対応することはできない。

ブロックチェーン上で動作するゲームやアプリケーションは、実行元となる暗号資産アドレスがユーザーアカウントの役割を果たす場合がある。そのような、利用者に対応するアドレスが実行元となる必要があるゲームやアプリケーションを、業者が顧客に代わって実行する場合、本方法では、実行元が業者のアドレスとなるため、適さないことになる。

3.1.3 集約管理する方法を利用したサービスの事例

集約管理する方法は、顧客間での暗号資産の移転等が多いサービスで用いると、顧客間の暗号資産の移転を低コストで実現できるとともに、サービス内に滞留する多くの暗号資産を、流出リスクが低いことを最も重視した方法で保管できる。そのため、交換所や送金・投げ銭サービス等で利用される例が多い。

3.1.3.1 bitFlyer（暗号資産交換所）

bitFlyerは暗号資産交換サービスを提供している。顧客ごとに暗号資産の預入アドレスが用意される。預入アドレスに移転した暗号資産は、交換所の顧客アカウントの残高に反映される。顧客らは、互いに暗号資産や日本円の残高を即座に交換できる。



図3-2 預入用アドレスとして3から始まるアドレスが表示されている

残高の暗号資産を外部のアドレスに移転すると、預入アドレスとは異なるアドレスが移転元となるトランザクションが作成される。

取引 | ビットコイン取引の詳細情報を閲覧する

bc1qwqdg6squsna38e46795at95y9atm8azzmyvckulcc7kytlcckxswvzej →

図3-3 預け入れ時とは異なるbc1から始まるアドレスより移転された

3.1.3.2 Poloniex（暗号資産交換所）

Poloniexは国外で営業されている暗号資産交換所である。

Poloniexは、ATOMというCosmos Hubブロックチェーン上の暗号資産を取り扱っている。

Cosmos HubはDPoSを採用しており、ATOMをステーキングしてブロックチェーンにトランザクションを記録するノードとなるか、またはトランザクションを記録するノードに対してATOMをデリゲートすることで、報酬（新規発行されるATOM）を得ることができる。

Poloniexは、顧客らが保有するATOMを用いてデリゲートを行っている²⁹。デリゲート先はPoloniexの提携先が運営するノードとなっており、顧客が選択することはできない。また、自身の保有するATOMをデリゲートするかどうかも選択できず、自動でデリゲートに用いられる。PoloniexがATOMをデリゲートすることによって得た報酬は、Poloniexが手数料を差し引いた上で、ATOMの残高に応じて、顧客に分配される。

DEPOSIT HISTORY

[Export Adjustments \(Learn More\)](#)[Export Complete Deposit History](#)

Status	Asset Amount
 Complete - Cosmos Staking 2019-09-14 18:01:22 Your Cosmos staking reward for Sep 14, 2019. What's this?	0.00094635 ATOM
 Complete - Cosmos Staking 2019-09-13 18:01:16 Your Cosmos staking reward for Sep 13, 2019. What's this?	0.00096438 ATOM
 Complete - Cosmos Staking 2019-09-12 18:02:45 Your Cosmos staking reward for Sep 12, 2019. What's this?	0.00093771 ATOM
 Complete - Cosmos Staking 2019-09-11 18:09:18 Your Cosmos staking reward for Sep 11, 2019. What's this?	0.00086864 ATOM
 Complete - Cosmos Staking 2019-09-10 18:00:40 Your Cosmos staking reward for Sep 10, 2019. What's this?	0.00087212 ATOM
Load 10 more rows	

図3-4 報酬のATOMが付与された記録

²⁹ <https://medium.com/circle-trader/cosmos-staking-is-live-78879f1523b4>

3.2 個別管理する方法

顧客の暗号資産アドレスに対応した（暗号資産の移転に必要な）署名鍵を業者が管理する。

業者が一人の顧客に対して複数のアドレスを用意し、それらに対応した複数の署名鍵を管理することも考えられる。

顧客の暗号資産アドレスに移転を受けた暗号資産は、顧客の指示に基づかずに業者が他のアドレスに移転することは望ましくない。

暗号資産を移転する際はオンチェーン取引となる。顧客のアドレスから、移転先のアドレスに暗号資産を移転するトランザクションを作成し、顧客のアドレスに対応する署名鍵を用いてトランザクションに署名する。オンチェーン取引のため、トランザクションはブロックチェーンに記録される。

移転を受けた際のアドレスと、移転を行う際の移転元のアドレスは、同一の顧客アドレスとなる。

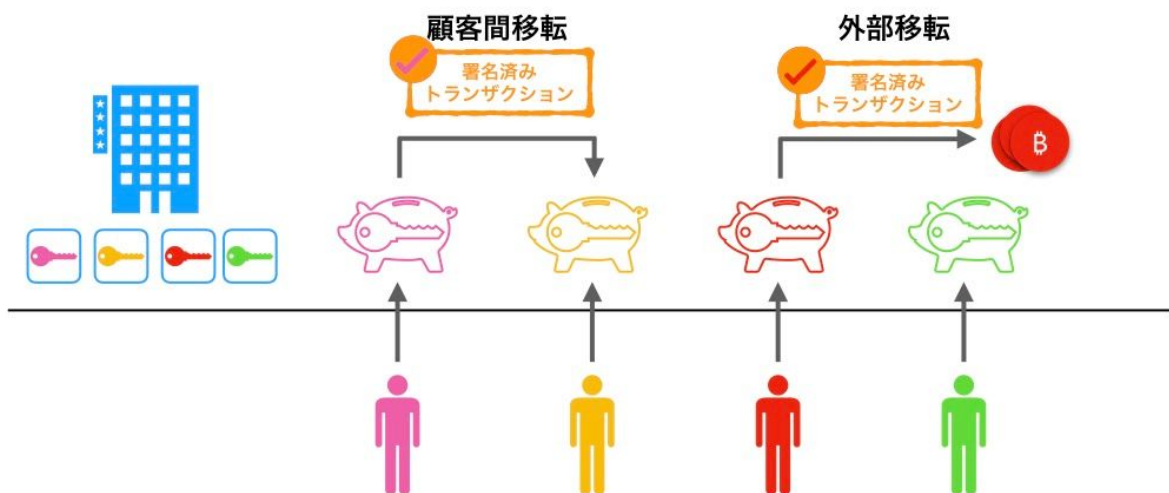


図3-5 個別に管理する方法の例

3.2.1 個別管理する方法のメリット

暗号資産が顧客ごとのアドレスで管理されているため、顧客の暗号資産の残高をブロックチェーン上で確認することができる。顧客が自身の残高をブロックチェーン上で確認したい場合や、第三者に残高を証明したい場合に利用することも可能である。

暗号資産を移転する際に、移転元のアドレスが顧客のアドレスとなる。例えば、この方法で暗号資産を管理するサービスから、ブロックチェーン上で発行されるトークンを購入するための暗号資産の移転を行うと、顧客のアドレスにトークンが付与される。

業者は、オンチェーンでのステーキングやデリゲート、投票の実施について、顧客ごとに個別に対応することができる。サービスを利用する同一の種類の暗号資産を保有する顧客らが、それぞれ別々のノードに対してデリゲートを行ったり、それぞれ別々の投票先に投票することも可能である。

利用者に対応するアドレスが実行元となる必要があるブロックチェーン上のゲームやアプリケーションを、業者が顧客に代わって実行する場合に、顧客のアドレスを実行元とすることができる。

3.2.2 個別管理する方法のデメリット

この方法では、サービス外への暗号資産の移転だけでなく、サービス内で暗号資産の所有者が変わる際にも、オンチェーン取引が必要となる。顧客のアドレス間で暗号資産を移転するトランザクションを作成し、ブロックチェーンに記録される必要があるため、トランザクション手数料や処理時間が必要となる。

顧客ごとのアドレスで暗号資産を管理することが求められるため、業者側が顧客の暗号資産をまとめて管理することができない。

そのため、複数の顧客から暗号資産の移転の指示があった場合、それぞれのアドレスを移転元とするトランザクションに、それぞれの顧客のアドレスに対応した署名鍵を用いて署名を行う必要がある。

さらに、顧客の暗号資産は顧客ごとのアドレスで保有する必要があるため、セキュリティレベルや利便性の異なる複数のアドレスを業者が用意し、業者側が必要に応じてそれらのアドレスを使い分ける、といったことができない。特に、顧客がステーキングやデリゲート、投票を行う場合、顧客のアドレスで管理されている暗号資産の額や期間が重要な場合があるが、事業者の都合で暗号資産を移転すれば、顧客のアドレスで管理されている暗号資産の額や期間は変わってしまう。

3.2.3 個別管理する方法を利用したサービスの事例

個別管理する方法は、顧客間で暗号資産の移転が行なわれることが少ない、暗号資産の保管を主な目的とするサービスや、ステーキングやデリゲート、投票等のオンチェーン取引の利用を提供するサービスで利用される例が多い。

3.2.3.1 BitGo Custody

BitGoはアメリカ合衆国サウスダコタ州より信託会社としてライセンスを受けてBitGo Custody³⁰を提供している。

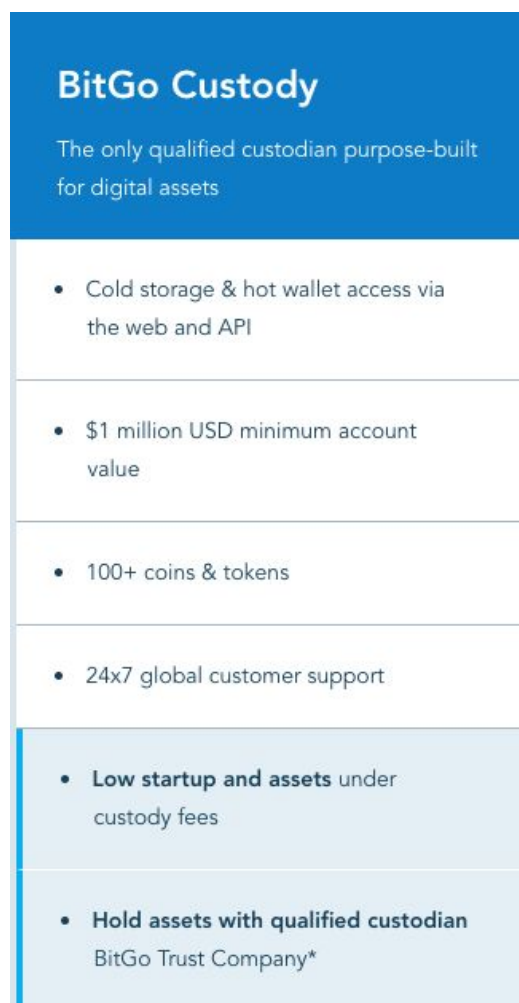


図3-6 BitGo Custodyのサービスプラン³¹

BitGo Custodyは、個別管理する方法で暗号資産を保管する。マルチシグアドレスを利用しており、暗号資産の移転には複数の署名鍵が必要となる。

暗号資産を移転する場合、顧客の指示を受けたBitGo Custodyがトランザクションを作成して署名を行い、顧客の最終確認を得た後に、さらにBitGo Custodyが追加の署名を行うこと

³⁰ <https://www.bitgo.com/services/custody>

³¹ <https://www.bitgo.com/resources/pricing>

でトランザクションが有効になり、トランザクションがブロックチェーンネットワークに送信される。

Transferring Funds



図3-7 BitGo Custodyの送金手順³²

マルチシグアドレスを利用できない暗号資産については、複数の署名を必要とするコントラクトウォレットを利用している³³。BitGoは 2 of 3 のマルチシグアドレスと同等の機能を提供するためのコントラクトウォレットのソースコードを公開している³⁴。

顧客はBitGoが署名鍵を管理する方法を選択することができる。複数のアドレスを利用し、複数の署名鍵の管理方法を組み合わせることもできる。また、署名鍵を利用する際の制限を設定することもできる。例として、インターネット接続の有無といった署名鍵の管理方法の選択や、暗号資産の移転先を制限するホワイトリストの利用、時間あたりの暗号資産の移転額の制限などの設定が可能であり、顧客の用途にあわせてウォレットの設定や組み合わせができるとしている。



図3-8 顧客の用途にあわせて構成をカスタマイズできる³⁵

³² <https://www.bitgo.com/services/custody> Customizable and Secure Wallet Configuration

³³

<https://bitgo.freshdesk.com/support/solutions/articles/27000042780-what-are-the-network-transaction-fees-related-to-ethereum->

³⁴ <https://github.com/BitGo/eth-multisig-v2>

³⁵ <https://www.bitgo.com/services/custody> Transferring Funds

3.2.3.2 Coinbase Custody

Coinbaseは、ファンド、交換所、ICOを行ったチーム等のビジネス用途に向けて³⁶、暗号資産を保管するCoinbase Custodyを提供している。Coinbase Custodyはアメリカ合衆国ニューヨーク州で信託会社としてライセンスを取得している³⁷。

Custody Pricing

<p>IMPLEMENTATION FEE</p> <p>\$0 – \$10,000 <small>DEPENDING ON USE-CASE</small></p>	<p>PRICING INCLUDES</p> <ul style="list-style-type: none"> ✓ Segregated cold storage ✓ Regulated Custody ✓ Industry-leading insurance ✓ Audited statements & financials ✓ Dedicated coverage ✓ Fast SLAs ✓ Multi-user accounts ✓ ERC20 support ✓ Staking
<p>CUSTODY FEE</p> <p>50 bps <small>ANNUALIZED</small></p>	
<p>MINIMUM BALANCE</p> <p>\$1,000,000</p>	

図3-9 Coinbase Custodyの料金案内³⁸

Coinbase Custodyは、個別管理する方法で暗号資産を保管する。

暗号資産を移転する際は、ビデオ通話等で顧客の本人確認を行い³⁹、顧客の指示に基づいてCoinbase Custodyがトランザクションを作成して署名を行い、トランザクションをブロックチェーンネットワークに送信する。

Coinbaseのセキュリティの責任者はCoinDeskの取材⁴⁰に対し、データを単独では利用できない分散片（シェア）に分割するShamirの秘密分散法を用いて署名鍵を分割し、分割した署名鍵の分散片は、地理的に分散させて保管していると説明している。

Coinbase Custody's unique features include:

- On-chain segregation of crypto assets
- Split, offline private keys that require a quorum of geographically distributed agents to use cryptographic hardware to sign transactions
- Multiple layers of security
- Robust cold storage auditing and reporting

図3-10 Coinbase Custodyの特徴⁴¹

³⁶ <https://blog.coinbase.com/coinbase-custody-is-officially-open-for-business-182c297d65d9>

³⁷

<https://blog.coinbase.com/coinbase-custody-receives-trust-charter-from-the-new-york-department-of-financial-services-532c92797215>

³⁸ <https://custody.coinbase.com/pricing> Custody Pricing

³⁹ <https://www.wired.com/story/coinbase-physical-vault-to-secure-a-virtual-currency/>

⁴⁰ <https://www.coindesk.com/coinbase-5-billion-crypto-token-expansion>

⁴¹ <https://blog.coinbase.com/coinbase-custody-is-officially-open-for-business-182c297d65d9>

Coinbase CustodyはTezosを取り扱っている。TezosはDPoSを採用する暗号資産である。Coinbase Custodyの顧客は、Tezosを保有している場合、デリゲートを行うことができる。

Coinbase Custodyは、デリゲートに用いる暗号資産についてもオフラインで保管されている⁴²。Coinbase Custodyのプロダクト担当者は、「One of the reasons we are starting with Tezos and then following on with other delegated PoS networks is specifically because we can keep our clients' funds that we will be staking in cold storage at all times.」

（筆者訳：Tezosから開始して、他のデリゲートされたPoSネットワークに展開している理由としては、顧客の資金を常にコールドストレージに保管した状態でステーキングが可能ながことが挙げられる）と述べている⁴³。

デリゲートは、オンチェーンでトランザクションを発行する必要があるため、分割して地理的に分散された署名鍵の分散片を集約して署名鍵を復元し、トランザクションに署名する必要がある。

署名鍵を復元して使用してしまうと、セキュリティレベルが下がる恐れがあるが、Tezosのデリゲートの場合、この問題を避けることができる仕組みを利用することができる。

Tezosにおけるデリゲートは、専用のコントラクトウォレットへ暗号資産を預け入れることで行われる。この専用のコントラクトウォレットには、デリゲートされた暗号資産を引き出すアドレスとして、預け入れた際のアドレスとは別のものを設定できる。

Tezosを保有するアドレスに対応した署名鍵をデリゲートを行うために用いて、新たに、分割して地理的に分散した状態で署名鍵が保管されているアドレスを用意し、引き出す際に用いるアドレスとして設定することで、セキュリティレベルを保ちながら顧客にデリゲートを提供することが可能である。

```
originate account new for mgr transferring qty from src [ --fee <amount> ] [ -D
--dry-run ] [ --verbose-signing ] [ --delegate <address> ] [ --delegatable ] [ -f --
force ] [ --minimal-fees <amount> ] [ --minimal-nanotez-per-byte <amount> ] [ --
minimal-nanotez-per-gas-unit <amount> ] [ --force-low-fee ] [ --fee-cap <amount> ]
[ --burn-cap <amount> ]
```

Open a new account.

new: name of the new contract

mgr: manager of the new contract

Can be a public key hash name, a file or a raw public key hash literal. If the parameter is not the name of an existing public key hash, the client will look for a file containing a public key hash, and if it does not exist, the argument will be read as a raw public key hash.

Use 'alias:name', 'file:path' or 'text:literal' to disable autodetect.

qty: amount taken from source in tz

Text format: `DDDDDDDD.DDDDDDD`.

Tez and mutez and separated by a period sign. Trailing and pending zeroes are allowed.

src: name of the source contract

Can be an alias, a key, or a literal (autodetected in order).

Use 'text:literal', 'alias:name', 'key:name' to force.

図3-11 Tezosのデリゲートを行うコントラクトを作成するコマンド。引き出しを行える引数[mgr]に任意のアドレスを指定できる。⁴⁴

⁴²

<https://blog.coinbase.com/coinbase-custody-launches-staking-support-for-tezos-makerdao-governance-to-follow-68f7bc51bc53>

⁴³ <https://www.coindesk.com/coinbase-leads-wall-street-to-brave-new-world-of-crypto-staking>

⁴⁴ <https://tezos.gitlab.io/master/api/cli-commands.html>

3.2.3.3 Anchorage

Anchorageはアメリカ合衆国サウスダコタ州より信託会社としてライセンスを取得しており、個別管理する方法で暗号資産を保管する。

オンチェーンで行う活動に積極的に参加できるように設計されている点が特徴である。

Safeguard your investments	Take action in real time	Get more out of your assets
A modern solution shouldn't require armed guards, secret bunkers, or Faraday tents. Our security model eliminates single points of failure, so your assets will be safer with us than anywhere else.	Your assets are accessible and auditable at any time, so you can operate with ease. We offer tiered service levels with guaranteed SLAs, letting you confidently take action on your schedule.	Unlike cold storage custody, Anchorage is designed for active participation, so you can capture yield from staking and inflation, and vote on governance questions concerning your investments.

図3-12 Anchorageの特徴⁴⁵

Anchorageは、利便性とセキュリティはトレードオフではなく独立したものであり、セキュリティについて妥協をせずに利便性を確保できるとしている⁴⁶。

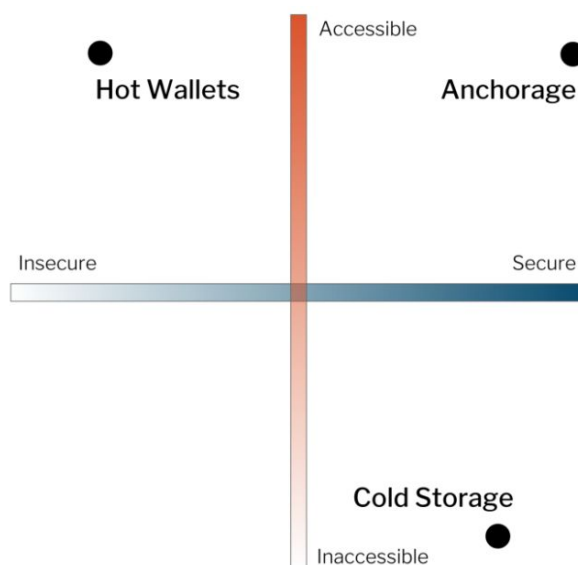


図3-13 利便性とセキュリティは独立しており、両立できるとする図⁴⁷

Anchorageは、ハードウェアセキュリティモジュール（以下、HSM）で顧客の秘密鍵を保管している。HSMはインターネットと接続されたサーバーに接続されており、サーバーが

⁴⁵ <https://anchorage.com/>

⁴⁶

<https://medium.com/anchorage/smart-storage-how-anchorage-provides-crypto-investors-greater-security-and-usability-dcaa00d1173c>

⁴⁷

<https://medium.com/anchorage/smart-storage-how-anchorage-provides-crypto-investors-greater-security-and-usability-dcaa00d1173c> Accessibility and security are independent variables

HSMに指示を出すと、HSM内で署名が行われる。顧客は、暗号資産の移転やステーキング、デリゲート、投票等をリアルタイムに行うことができる。

通常は、このような方法で署名鍵を管理する場合、HSMに署名の指示を出すサーバーに対するサイバー攻撃等により、HSMに不正な指示が送信され、暗号資産が流出するリスクが存在する。

そこでAnchorageは、利便性の高いサービスを提供しながら、セキュリティを担保するために、HSMの内部で特別な制御をしている。この制御によって、AnchorageのHSMで署名を行うには、顧客とAnchorageのそれぞれの承認が必要であることが担保されるとしている。

顧客は、user keyと呼ばれる鍵を持つ。AnchorageのHSMは、Anchorageに承認され、かつ、user keyを用いて顧客に承認されたトランザクションにのみ署名を行う。

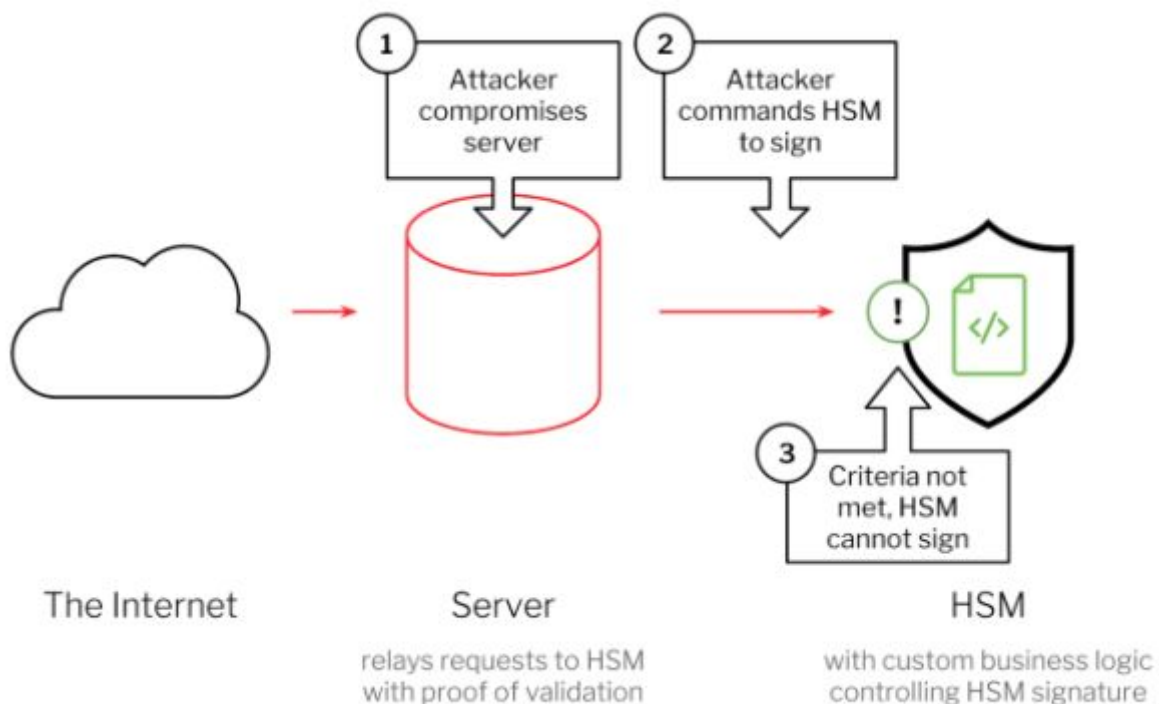


図3-14 内部で特別な制御をしているAnchorageのHSMを用いたシステム⁴⁸

このようなHSMの仕組みによって、Anchorageは、事業者と顧客がそれぞれ承認することでトランザクションが有効になることから、マルチシグアドレスを活用した複数組織の承認プロセスのようなサービスを実現している。Anchorageのサーバーがハッキングされただけでは、顧客が意図しない暗号資産を移転する署名は行われず、顧客が組織である場合、複数のuser keyを必要とすることで、顧客の組織内で権限分散を行うこともできる。

48

<https://medium.com/anchorage/smart-storage-how-anchorage-provides-crypto-investors-greater-security-and-usability-dcaa00d1173c> Figure B: HSM with custom business logic

3.3 署名鍵の管理方法と暗号資産の管理に関する規制の論点

すでに規制されている暗号資産の交換等を行う業者のほとんどは、集約管理する方法で暗号資産の管理を行っている。しかしながら、改正法で新たに規制対象となる暗号資産の管理を行う業者には、個別管理する方法を用いる業者も想定される。

集約管理する方法を用いる業者がオフチェーン取引を主に提供しているのに対し、個別管理する方法を用いる業者には、オンチェーン取引を主に提供する業者も想定される。

改正法第63条の11の1第2項において、暗号資産交換業者は、利用者の暗号資産を、「利用者の利便の確保及び暗号資産交換業の円滑な遂行を図るために必要なものとして内閣府令で定める要件」（以下、内閣府令で定める要件）に該当するものを除いて、「利用者の保護に欠けるおそれが少ないものとして内閣府令で定める方法」（以下、内閣府令で定める方法）で管理しなければならないとされている。

また、同条11の2第1項においては、内閣府令で定める要件に該当する暗号資産と同種同量の「履行保証暗号資産」を「自己の暗号資産として保有し、内閣府令で定めるところにより、履行保証暗号資産以外の自己の暗号資産と分別して管理しなければならない。この場合において、当該暗号資産交換業者は、履行保証暗号資産を利用者の保護に欠けるおそれが少ないものとして内閣府令で定める方法で管理しなければならない。」とされている。

内閣府令において、上記要件や上記方法を定めるにあたっては、実施可能な制度とするため、及び利用者の利便性の向上のため、新たに規制対象となる業態の実態を考慮しながら検討する必要があると考えられる⁴⁹。

3.3.1 内閣府令で定める要件と履行保証暗号資産について

「利用者の利便の確保及び暗号資産交換業の円滑な遂行を図るために必要なもの」には、例えば、暗号資産の交換等を行う業者においては、カバー取引や顧客の引出申請等に基づく、サービス外への暗号資産の移転のために必要な暗号資産等が含まれるものと考えられる。しかし、交換ではなく暗号資産の管理を行う業者を想定した場合には、決済に伴う暗号資産の移転や、ゲームやアプリケーションの利用、ステーキング、デリゲート、投票、場合によっては暗号資産の移転を伴わないオンチェーン取引等も含め、トランザクションを発行するために署名鍵を用いる必要がある業務を想定する必要があると考えられる。

また、BitGo Custodyのように、業者による署名鍵の管理方法を顧客が選択できる事例もある。暗号資産の管理を行う業者の顧客には、暗号資産の取り扱いについて専門的な知識を有しており、自己の用途のために必要な暗号資産の管理方法を自ら判断できる顧客も想定される。顧客が必要とする場合に、業者が内閣府令で定める方法にあたらぬ方法で暗号資産を管理することも想定する必要があると考えられる。

加えて、法文上、業者は内閣府令で定める要件に該当する暗号資産と同種同量の履行保証暗号資産を保有する必要があるとされるが、業者が履行保証暗号資産を保有するコストは最終的に顧客が負担することになると考えられる。顧客がリスクを理解した上で、顧客の意思によって内閣府令で定める方法にあたらぬ方法で暗号資産を管理する場合については、必ずしも業者が履行保証暗号資産を保有することを必要としないことも、今後検討の余地があると考えられる。

⁴⁹ 本稿執筆後、仮想通貨交換業者に関する内閣府令等の一部を改正する内閣府令（案）が公開された。（<https://www.fsa.go.jp/news/r1/sonota/20200114/20200114.html>）

3.3.2 内閣府令で定める方法について

「利用者の保護に欠けるおそれが少ないもの」には、例えば、署名鍵をオフラインで保管し、システム化された方法では署名しない方法が含まれるものと考えられる。

業者のアドレスで顧客の暗号資産を管理する方法を用いる業者においては、ほとんどの暗号資産をオフラインで保管し、サービス外への暗号資産の移転のために必要な暗号資産のみをその他の方法で保管する、といった対応が考えられる。すでに、日本仮想通貨交換業協会の自主規制規則においては、ネットワークと接続された環境で秘密鍵を管理する暗号資産は、利用者から預託を受けた全ての暗号資産の20%以下とするガイドライン⁵⁰が存在する。

しかし、個別管理する方法については、顧客のアドレスで暗号資産を管理することが求められるため、セキュリティレベルや利便性の異なる複数のアドレスを業者が用意し、業者の判断によってそれらのアドレスを使い分ける、といったことができない。

また、顧客のアドレスで暗号資産を管理することが求められるため、複数の顧客の暗号資産をまとめて管理することもできず、各顧客からのオンチェーン取引の指示に、それぞれの顧客のアドレスに対応する署名鍵を用いて署名を行わなくてはならない。

多数の顧客が存在し、いずれかの顧客からオンチェーン取引の指示が一定以上の頻度で発生する場合には、全顧客の署名鍵をオフラインで保管し、各顧客から指示があるたびに顧客ごとに手動で署名の手続きを行う運用は、現実的ではない。

一方で、システムによって自動で顧客からの指示に応じる場合、システムへのハッキングによって顧客の暗号資産が流出する可能性もある。内閣府令で定める方法として認められない方法で暗号資産を管理するには、内閣府令で定める要件を満たす必要があり、かつ、要件を満たしたとしても、履行保証暗号資産を用意する必要がある。全顧客の署名鍵を内閣府令で定める方法として認められない方法で管理した場合、履行保証暗号資産は、顧客から預かる全暗号資産と同種同量が必要となり、こちらも現実的ではない。

内閣府令で定める方法には、利用者の保護に欠けるおそれが少ないものと考えられ、かつ、各顧客のアドレスに対応する署名鍵を用いて個別にオンチェーン取引を行いやすい署名鍵の管理方法が含まれる必要があると考える。

なお、利便性を高めながら流出リスクの軽減を試みている事業者の例として、Anchorageがある。Anchorageは、顧客の承認操作がなければ署名が行なわれない仕組みを用いることで、オンラインで利便性が高いシステムでサービスを提供しながら、流出のリスクを軽減している。

⁵⁰ 日本仮想通貨交換業協会 利用者財産の管理に関する規則
<https://jvcea.or.jp/cms/wp-content/themes/jvcea/images/pdf/jvcea-guideline-6.pdf>

4. 暗号資産の管理にあたる業務の範囲について

暗号資産の管理にあたる業務の範囲は本稿執筆の段階では明確に法令または規制等では定められていないが、署名鍵を取り扱うサービスには様々な形態が考えられる。

仮想通貨交換業等に関する研究会の報告書（以下、報告書）によると、仮想通貨カストディ業務とは、「仮想通貨の売買等を行わないが、顧客の仮想通貨を管理し、顧客の指図に基づき顧客が指定する先のアドレスに仮想通貨を移転させる業務」とされ、業務を行う上で、「サイバー攻撃による顧客の仮想通貨の流出リスク、業者の破綻リスク、マネーロンダリング・テロ資金供与のリスク等、仮想通貨交換業と共通のリスクがあると考えられること」、および「仮想通貨カストディ業務を行う業者についても、マネーロンダリング・テロ資金供与規制の対象にすることを各国に求める旨の改訂 FATF 勧告が採択されたこと」を踏まえ、「決済に関連するサービスとして、一定の規制を設けた上で、業務の適正かつ確実な遂行を確保していく必要があると考えられる」とされている。

したがって、署名鍵を取り扱う様々な形態について、流出リスク、破綻リスク、マネーロンダリングやテロ資金供与のリスクの観点から、改正法において暗号資産の管理を行う業者に求められる対応の必要性を検討することに、暗号資産の管理にあたる業務の範囲を明確にするにあたって一定の重要性があると考えられる。

ただし、暗号資産の利用者が自身のために暗号資産を管理する場合にも、マネーロンダリングやテロ資金供与が行われるリスクはあると考えられる。したがって、マネーロンダリングやテロ資金供与のリスクが存在することが、他人のために暗号資産の管理を行っているかどうかを決定する要素ではないと考えられる。一方、流出リスクや破綻リスクについては、他人のために暗号資産の管理を行うことによって生じるものと考えられる。

そこで本章では、改正法における流出リスクと破綻リスクの軽減のため、あるいはこれらのリスクが顕在化した場合の対処のため、業者に求められる対応の必要性について、署名鍵を取り扱う様々な形態から検討する。

4.1 改正法が求める流出リスクと破綻リスクに対する対応

4.1.1 流出リスクへの対応

報告書によると、「受託仮想通貨の流出リスクへの対応」について、「仮想通貨交換業者には、セキュリティ対策の観点から、可能な限り、受託仮想通貨の移転に必要な秘密鍵をコールドウォレット（オフライン）で管理することが求められる」が、「日々の流通に要する一定量の受託仮想通貨については、顧客からの移転指図に迅速に対応するため、一般にコールドウォレットよりもセキュリティリスクが高いとされるホットウォレット（オンライン）で秘密鍵を管理している場合」があり、「不正アクセスを受けた複数の仮想通貨交換業者において、ホットウォレットで秘密鍵を管理していた受託仮想通貨が流出し、リスクが顕在化」した。こうしたセキュリティリスクへの対応として、「仮想通貨交換業者において、法令等で求められるセキュリティ対策を着実に講じることが重要」であり、「仮想通貨交換業者におけるセキュリティリスクに係る管理態勢を重点的にモニタリングしていくことが適当と考えられる」ことに加え、「流出事案が生じた場合の対応が予め明確であることや、顧客に対する弁済原資が確保されていることも、利用者保護の観点から重要」と考えられるため、「仮想通貨交換業者に対し、受託仮想通貨を流出させた場合の対応方針の策定・公表や、ホットウォレットで秘密鍵を管理する受託仮想通貨に相当する額以上の純資産額及び弁

済原資（同種・同量以上の仮想通貨）の保持を求めることが適当と考えられる」としている。

改正法は、第63条の11第2項において、暗号資産交換業者は、利用者の暗号資産を、内閣府令で定める要件に該当するものを除いて、内閣府令で定める方法で管理しなければならないとしている。また、第63条の11の2第1項において、内閣府令で定める要件に該当する暗号資産と同種同量の履行保証暗号資産を保有し内閣府令で定める方法で管理しなければならないとしている。

4.1.2 破綻リスクへの対応

「仮想通貨交換業者の倒産リスクへの対応」のための「受託仮想通貨の保全」については、「仮想通貨については、私法上の位置付けが明確でない中で、少なくとも過去の破綻事例において見られたような顧客財産の流用を防止する観点から、資金決済法上、仮想通貨交換業者には、受託仮想通貨について、顧客毎の財産を直ちに判別できる状態で管理することが求められている。また、それを補う観点から、仮想通貨交換業者に対し、公認会計士又は監査法人による分別管理監査及び財務諸表監査が課されている」が、「仮に、仮想通貨交換業者が適切に分別管理を行っていたとしても、受託仮想通貨について倒産隔離が有効に機能するかどうかは定かとなっていない」ため、「顧客が取引を行うに際して、仮想通貨交換業者の財務の健全性を認識できるようにする観点から、仮想通貨交換業者に対し、貸借対照表や損益計算書をはじめとする財務書類の開示を求めることが適当」と考えられ⁵¹、さらに「仮想通貨交換業者の破綻時においても、受託仮想通貨の顧客への返還が円滑に行われるようにする観点からは、顧客の仮想通貨交換業者に対する受託仮想通貨の返還請求権を優先弁済の対象とすることも考えられる」としている。

改正法は、第63条の11第2項において、暗号資産交換業者は、利用者の暗号資産を自己の暗号資産と分別して管理しなければならないとしている。また、同条の11の2第1項において、履行保証暗号資産をそれ以外の自己の暗号資産と分別して管理しなければならないとしている。また、第63条の11第3項および第63条の11の2第2項において、分別管理の状況について、「内閣府令で定めるところにより、定期に、公認会計士（公認会計士法（昭和二十三年法律第百三十三号）第十六条の二第五項に規定する外国公認会計士を含む。第六十三条の十四第三項において同じ。）又は監査法人の監査を受けなければならない。」としている。さらに、第63条の19の2第1項において、「暗号資産交換業者との間で当該暗号資産交換業者が暗号資産の管理を行うことを内容とする契約を締結した者は、当該暗号資産交換業者に対して有する暗号資産の移転を目的とする債権に関し、対象暗号資産（当該暗号資産交換業者が第六十三条の十一第二項の規定により自己の暗号資産と分別して管理するその暗号資産交換業の利用者の暗号資産及び履行保証暗号資産をいう。）について、他の債権者に先立ち弁済を受ける権利を有する」としている。

⁵¹ 報告書は、「受託仮想通貨について、倒産隔離の観点から、仮想通貨交換業者に対し、顧客を受益者とする信託義務を課すことも考えられる」が「現時点で、全種・全量の受託仮想通貨の信託を義務付けることは困難と考えられる」としており、「全ての受託仮想通貨の信託が行われ得ない現状に鑑みれば」、「仮想通貨交換業者に対し、貸借対照表や損益計算書をはじめとする財務書類の開示を求めることが適当と考えられる」としている。

流出リスクへの対応

- ・ 利用者の暗号資産を
内閣府令で定める要件に
該当するものを除き
内閣府令で定める方法で管理
(第63条の11の1第2項)
- ・ 内閣府令で定める要件に
該当する暗号資産と同種同量の
履行保証暗号資産を保有し
内閣府令で定める方法で管理
(第63条11の2第1項)

破綻リスクへの対応

- ・ 利用者の暗号資産
(第63条の11の1第2項)と
履行保証暗号資産
(第63条の11の2第1項)を
自己の暗号資産と**分別して管理**
- ・ 分別管理の状況について
監査法人の監査を受ける
(第63条の11の1第3項、
同条の11の2第2項)
- ・ 利用者は分別管理された
利用者の暗号資産と
履行保証暗号資産について
優先弁済権を有する
(第63条の19の2第1項)

図4-1 改正法における流出リスクと破綻リスクへの対応

4.2 利用者の暗号資産の移転に必要な署名鍵や情報を取り扱うサービス

4.2.1 利用者の暗号資産の移転に必要な署名鍵や情報を取り扱うサービスの例

4.2.1.1 サービス提供者が利用者の署名鍵の生成を行う事例

4.2.1.1.1 悟（さとり）コイン

悟コインは暗号資産の署名鍵が印刷された商品である。悟コインは、株式会社来夢が仮想通貨交換業者として、印刷された署名鍵に対応するアドレスにビットコインが残高として存在する状態で販売していた。平成30年4月23日をもって販売を終了している。



図4-2 悟コイン

悟コインにはQRコードが印刷されており、署名鍵のデータが記録されている。利用者はQRコードを読み取り、署名鍵を任意のウォレットにインポートし、署名に利用できる。

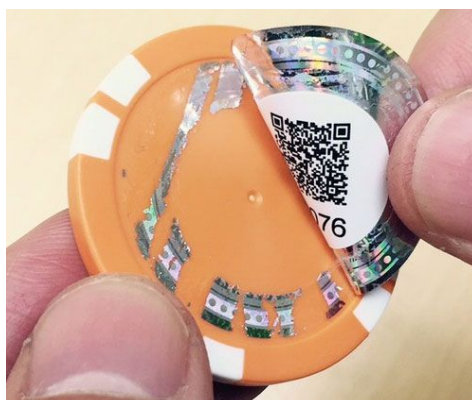


図4-3 署名鍵が記録されたQRコード

製造元である株式会社来夢は、署名鍵を作成して悟コインを製造すると、署名鍵を破棄するとしている。悟コインに印刷された署名鍵を用いて暗号資産を移転するために署名を行うのは、悟コインの利用者のみである。

秘密鍵・プライベートキー（例：パスワード）について

貴方自身がお手持ちの悟コインのホログラムシールを剥がさない限り、何人たりとも秘密鍵情報を得ることは不可能です。弊社は下記作業をすでに実行していますので、秘密鍵情報は弊社の支配下にありません。よって、お尋ねされても返答ができませんので(知り得ないため)、自己責任で管理をお願いいたします。

- ・作業工程1: 悟コイン本体に、同一シリアル番号の秘密鍵シール(QRコード)とホログラムシールを貼る。
- ・作業工程2: 価値の実装を行う。
- ・作業工程3: 価値が実装されているかを検証する。
- ・作業工程4: 弊社の支配下にあった秘密鍵データを抹消する。

図4-4 株式会社来夢は悟コインを作成後、署名鍵データを抹消する

4.2.1.2 サービス提供者が利用者の署名鍵の保管を行う事例

4.2.1.2.1 Coinbase Wallet、Google Drive、iCloud

Coinbase WalletはCoinbase社が提供するスマートフォン向けのウォレットアプリケーションである。

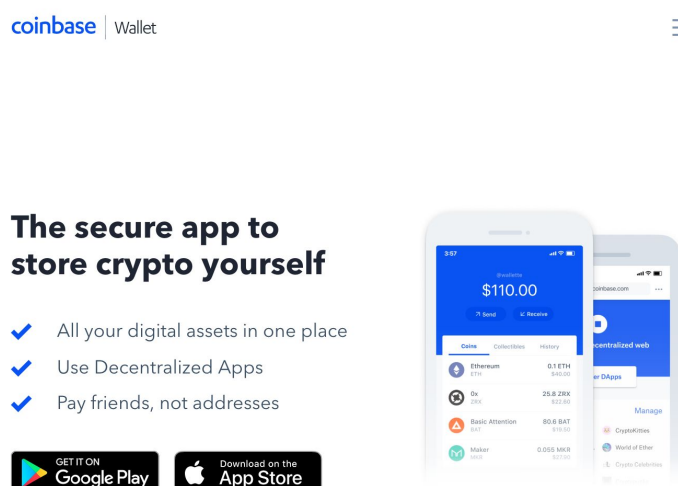


図4-5 Coinbase Wallet⁵²

Coinbase Walletは、利用者のスマートフォン上で署名鍵を生成し、利用者のスマートフォン上に署名鍵を保管する。また、利用者のスマートフォン上でトランザクションに署名する。

ただし、利用者は「クラウドバックアップ」機能を選択することが可能である。クラウドバックアップは、Androidの場合はGoogleのストレージサービスであるGoogle Driveへ、iOS(iPhoneやiPad)の場合はAppleのストレージサービスであるiCloudへ、署名鍵をバックアップすることができる⁵³。したがって、利用者がクラウドバックアップ機能を利用した場合、GoogleやAppleはCoinbase Wallet利用者の署名鍵を保管することになる。

⁵² <https://wallet.coinbase.com/>

⁵³

<https://blog.coinbase.com/backup-your-private-keys-on-google-drive-and-icloud-with-coinbase-wallet-3c3f3fdc86dc>

なお、Coinbase Walletは、Google DriveやiCloudに署名鍵をバックアップする際、利用者が設定するパスワードによって署名鍵の暗号化を行う。Google Driveを提供するGoogleやiCloudを提供するAppleはバックアップされた署名鍵を平文で読み取ることはできず、そのままでは署名鍵を署名に利用することもできない。

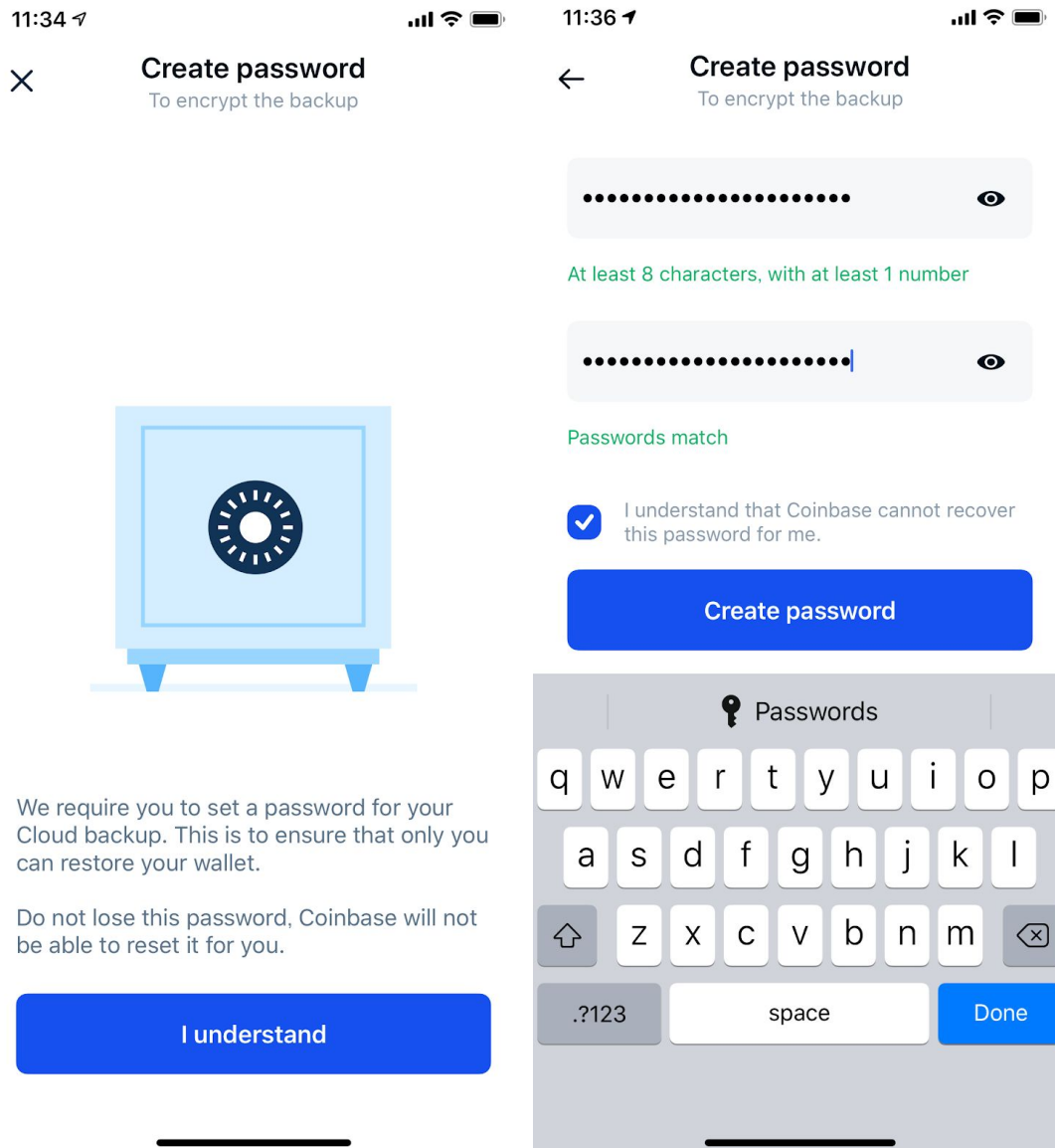




図4-6 利用者が設定するパスワードによって署名鍵を暗号化してバックアップする

利用者は、スマートフォンを買い替えた場合などに、新しい端末にCoinbase Walletをインストールすると、Google DriveやiCloudより暗号化した状態でバックアップされている署名鍵をダウンロードできる。利用者がスマートフォン上でパスワードを入力することで、署名鍵が復号され、利用可能となる。



Password

Created for this wallet

..... 

At least 8 characters, with at least 1 number

Coinbase does not store any of your data, so we cannot recover your password for you.

Restore Wallet

Restore your wallet with the 12 word recovery phrase that you have written down.

Restore with iCloud

[Restore with recovery phrase](#)

Continue

q	w	e	r	t	y	u	i	o	p
a	s	d	f	g	h	j	k	l	
⬅	z	x	c	v	b	n	m	➡	
.?123	space							done	

図4-7 利用者が設定したパスワードを入力してバックアップを復号する

4.2.1.3 サービス提供者と利用者の双方が、署名のために署名鍵を共有している場合

4.2.1.3.1 Cool X Wallet

Cool X Wallet は株式会社 SBI BITSが提供するハードウェアウォレットであり、SBI VC トレード株式会社が提供する暗号資産交換所の利用者が申し込むことで利用できる。



図4-8 Cool X Walletの特徴⁵⁴

利用者は通常、Cool X Walletと、Cool X WalletにBluetoothで接続する専用のスマートフォンアプリケーションを用いて暗号資産の移転を行う。

Cool X Wallet サービス約款⁵⁵によると、Cool X Walletは株式会社 SBI BITSから利用者に対して貸与される。株式会社 SBI BITSは署名鍵のシード⁵⁶を管理しており、利用者が紛失等によりCool X Walletを利用できない状態になった場合、株式会社 SBI BITSはシードを用いて署名鍵を再生成し、利用者が直接管理しているアドレスに暗号資産を移転する。

⁵⁴ <https://www.sbicxw.com>

⁵⁵ <https://www.sbivc.co.jp/wallet/pdf/wallet-agreement.pdf>

⁵⁶ 署名鍵を生成する基となるデータ。

4.2.1.3.2 Blockchain Wallet

Blockchain WalletはBlockchain Luxembourg S.A.が一般向けに提供しているWebウォレットである。



図4-9 Blockchain Walletのダッシュボード

利用者は通常、Blockchain WalletのWebサイトにアクセスしてログインし、Blockchain Walletが保管している署名鍵を用いて暗号資産の移転を行う。

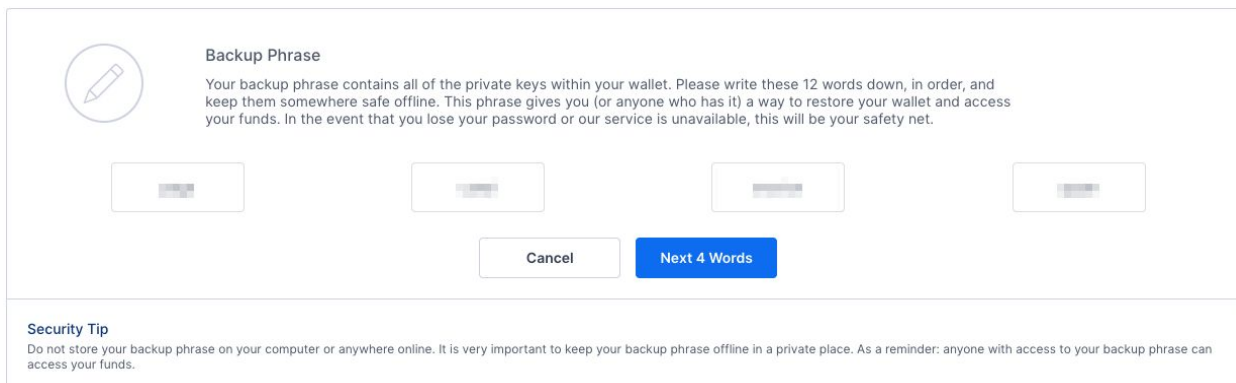
The screenshot shows a 'Send Bitcoin' transaction form. At the top, it says 'Sent From' and 'Send Bitcoin'. The form fields are:

- From:** My Bitcoin Wallet
- To:** [Redacted address]
- Amount:** \$40.90 (0.00498663 BTC)
- Fee:** \$0.10 (0.00001337 BTC)
- Total:** \$41.01 (0.005 BTC)

At the bottom, there is a large blue button labeled 'Send Bitcoin' and a smaller link labeled 'Go Back'.

図4-10 暗号資産の移転操作

Blockchain Walletでは、利用者が自身の手元に署名鍵をバックアップできる⁵⁷。バックアップ時には12単語から構成されるリカバリーフレーズが表示され、それを書き留める。利用者がバックアップを行うと、Blockchain Walletと利用者がそれぞれ署名鍵を有する状態となる。



Backup Phrase

Your backup phrase contains all of the private keys within your wallet. Please write these 12 words down, in order, and keep them somewhere safe offline. This phrase gives you (or anyone who has it) a way to restore your wallet and access your funds. In the event that you lose your password or our service is unavailable, this will be your safety net.

Cancel Next 4 Words

Security Tip
Do not store your backup phrase on your computer or anywhere online. It is very important to keep your backup phrase offline in a private place. As a reminder: anyone with access to your backup phrase can access your funds.

図4-11 4単語ずつ3回に分け、計12単語のリカバリーフレーズが表示されるバックアップ操作

リカバリーフレーズはBIP39に従っており⁵⁸、Blockchain Walletが利用できなくなっても、他のウォレットにリカバリーフレーズを入力することで署名鍵を復元し、利用することができる。反対に、他のウォレットからバックアップしたBIP39のリカバリーフレーズをBlockchain Walletに入力し、署名鍵を復元して利用することもできる。

また、Blockchain WalletのWebサイトにログインするためのパスワードを忘れた場合は、バックアップしたリカバリーフレーズを入力すれば、ウォレットを復元して署名鍵を利用することができる。

⁵⁷ <https://support.blockchain.com/hc/en-us/articles/209564506-Make-a-Wallet-Backup>

⁵⁸ <https://support.blockchain.com/hc/en-us/articles/115001298143-Your-Recovery-Phrase-The-Failsafe>

図4-12 BIP39に従ったリカバリーフレーズを入力して利用できるリカバリー機能⁵⁹

Blockchain Walletで管理されている暗号資産は、利用者の指示にしたがってBlockchain Luxembourg S.A.が移転を行う場合と、利用者がバックアップからリカバリーした他のウォレットによって移転が行われる可能性がある。

Blockchain Luxembourg S.A.は利用規約において「5.1.1 The Wallet is provided to you exclusively by Blockchain Luxembourg S.A. At no point will Blockchain ever take custody of Virtual Currency stored in a Wallet.」としている。

⁵⁹ <https://login.blockchain.com/#/recover>

4.2.1.4 サービス提供者が、署名に必要な署名鍵や情報のうち、一部のみを利用できる場合

4.2.1.4.1 Casa Keymaster

Casa Keymasterは、2 of 3や3 of 5のマルチシグアドレスの署名に必要な署名鍵のうちの1つを保管し、緊急時に利用者の要請に応じて署名を行うサービスを提供している。⁶⁰

利用者はマルチシグアドレスの署名に必要な数の署名鍵を自身で管理しており、通常、暗号資産を移転する際に、Casaが保管する署名鍵を使用する必要はない。

しかし、利用者が管理している署名鍵が何らかの原因により使用できなくなり、マルチシグアドレスの署名を行う署名鍵が不足した場合は、利用者はCasaに署名を依頼できる。

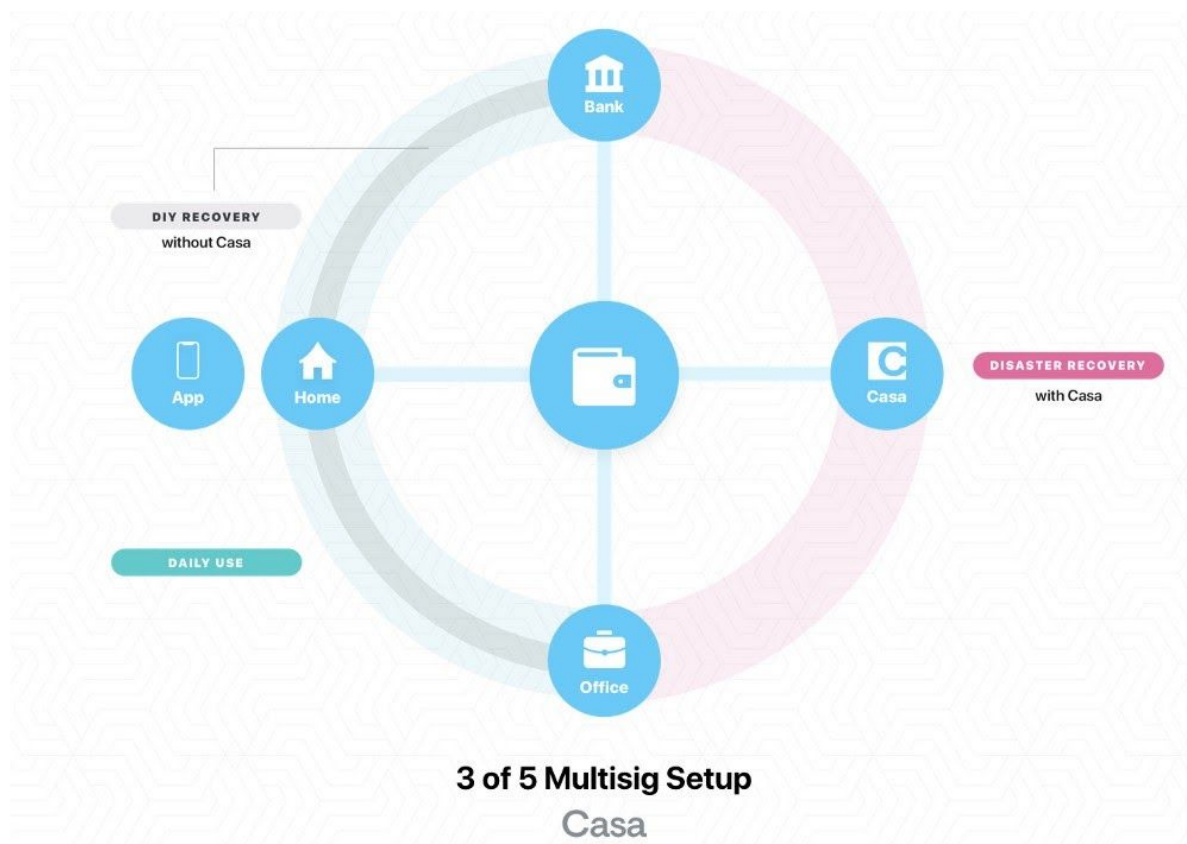


図4-13 3 of 5のマルチシグアドレスに用いる署名鍵のうち、4つを利用者が保管し、1つをCasaが管理する⁶¹

Casaが保管している署名鍵の数はマルチシグアドレスの署名に必要な数に満たないため、Casaの裁量だけで暗号資産を移転することはできない。

また、利用者がマルチシグアドレスの署名に必要な数以上の署名鍵を持っているため、Casaが保管している秘密鍵が失われても、利用者は暗号資産を移転することができる。

⁶⁰ <https://keys.casa/keymaster-features/>

⁶¹ <https://blog.keys.casa/manage-your-keys-with-casa/>

- You have full control by holding 4-of-5 total keys.
- The risk of theft is reduced by spreading keys across locations (and never having more than two keys in one location) because more time and travel means a higher chance of thieves being caught.
- Casa can help you in emergencies because we hold 1-of-5 keys.
- Casa can never access your funds because we hold only one key. And any thieves attacking Casa can also never access your funds.

図4-14 Casa Keymasterはマルチシグアドレスの署名に必要な秘密鍵の1つだけを保管する⁶²

4.2.1.4.2 Curv

Curvは法人向けに提供されている秘密分散と秘密計算を利用したウォレットである。

Curvと利用者はそれぞれ署名鍵の分散片を作成し、保管する。署名は、Curvと利用者がそれぞれの分散片を秘密に保ちながら、協力して署名を導出するための秘密計算を行う。またその際、Curvはトランザクションが顧客によって定義されたポリシーに従っていることを検証する。

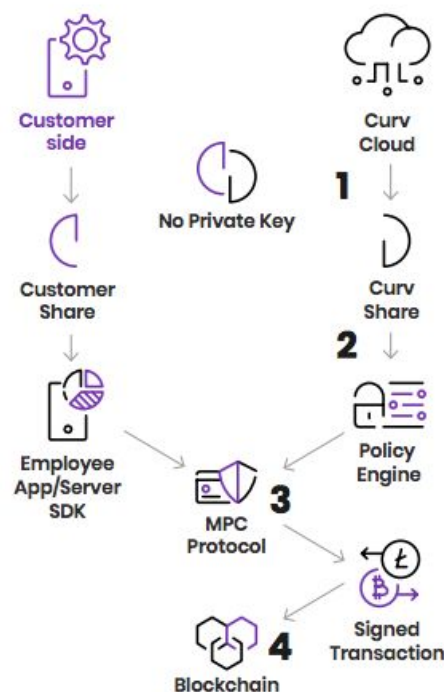


図4-15 Curvの署名フロー⁶³

Curvが扱う分散片の数は署名のための秘密計算に必要な数に満たないため、Curvの裁量だけで暗号資産を移転することはできない。

⁶² <https://blog.keys.casa/manage-your-keys-with-casa/>

⁶³ CurvのWhitepaperより (<https://www.curv.co/> から取得)

4.2.1.4.3 BitGo Pay As You Go

BitGoは個人向けのウォレットサービスも提供している。BitGo Pay As You Goは、2 of 3 のマルチシングアドレスを作成し、顧客とBitGoがそれぞれ2つずつの署名鍵を保管する。

顧客は通常、BitGoのWebサイトにアクセスし、BitGoに保管された署名鍵を用いて暗号資産の移転を行う。顧客が保管する2つの署名鍵はバックアップ目的で保管される。BitGoのサービスが何らかの原因で利用できなくなった場合、顧客はバックアップとして保管されている2つの署名鍵を使って暗号資産を移転することができる⁶⁴。

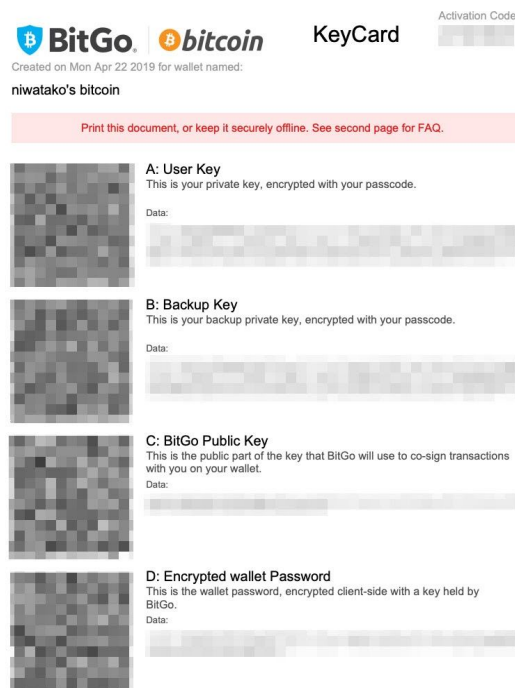


図4-16 バックアップ用に生成される署名鍵の情報が記録されたPDFファイル

BitGoが保管する2つの署名鍵のうち1つは、顧客が生成したものであり、顧客のみが知るパスワードによって暗号化されている。

顧客が暗号資産の移転を行う場合、顧客はBitGoのWebサイトにアクセスし、ログインする。

顧客は送金トランザクションをWebブラウザ上で作成する。Webサイトでトランザクションへの署名を行う際、JavaScriptによってパスワードによって暗号化された署名鍵がダウンロードされる。

顧客がブラウザにダウンロードされた署名鍵を復号するパスワードを入力すると、署名鍵がブラウザ上で復号され、トランザクションに1つ目の署名が行われる。

署名鍵を復号するためのパスワードや、復号された署名鍵がBitGoに送信されることはない。1つ目の署名が行われたトランザクションは、BitGoに送信される。BitGoは必要に応じて検証を行い、問題がなければ、BitGoが保管しているもう一つの署名鍵で、2つ目の署名を

⁶⁴ バックアップした鍵からリカバリーするための支援ソフトウェアはオープンソースで公開されている (<https://github.com/BitGo/wallet-recovery-wizard>)。

行う。2つの署名が揃ったトランザクションは、ブロックチェーンネットワークに送信され、暗号資産が移転される。⁶⁵

Authenticate

.....

383091

Authenticate

Cancel

[Forgot Password?](#) | [Need Help?](#)

図4-17 パスワード入力画面。入力したパスワード（上段）はBitGoに送信されず、暗号化された署名鍵の復号にのみ利用され、下段の2段階認証コードのみがBitGoに送信される。⁶⁶

BitGoが保管する2つの署名鍵のうち、BitGoが使用できる状態となっている署名鍵の数は1つであり、常にマルチシグアドレスの署名に必要な数（2つ）に満たないため、BitGoの裁量だけで暗号資産を移転することはできない。

⁶⁵ https://www.bitgo.com/info/p2sh_safe_address

⁶⁶ 2要素認証のコードは送信され、正規のユーザーによるトランザクション作成操作であるかの検証に用いられる。

4.2.1.5 署名に必要な署名鍵や情報が、複数の業者に管理されている事例

4.2.1.5.1 BITBOX、BitGo Business Wallet

BITBOXはLINE Tech Plus株式会社が国外において運営する暗号資産交換所である。

LINE DEVELOPER DAY 2018にて⁶⁷、LINE株式会社シニアセキュリティエンジニアの発表要旨として「BITBOXは、すべてのウォレットをマルチシグアドレスにしている。また、暗号資産の移転に用いる署名鍵は、BITBOXと第三者が保有している。」と説明している。

顧客の暗号資産が管理される 2 of 3 のマルチシグアドレスに対応する署名鍵のうち、2つをBITBOXが管理しており、残りの1つは第三者が管理している。BITBOXが管理している2つの署名鍵のうち1つは障害復旧のためにBITBOXによって暗号化されて保管されており、通常の署名にはもう1つの署名鍵だけが用いられる。暗号資産の移転に必要なもう1つの署名は、第三者が管理する署名鍵によって行われる。

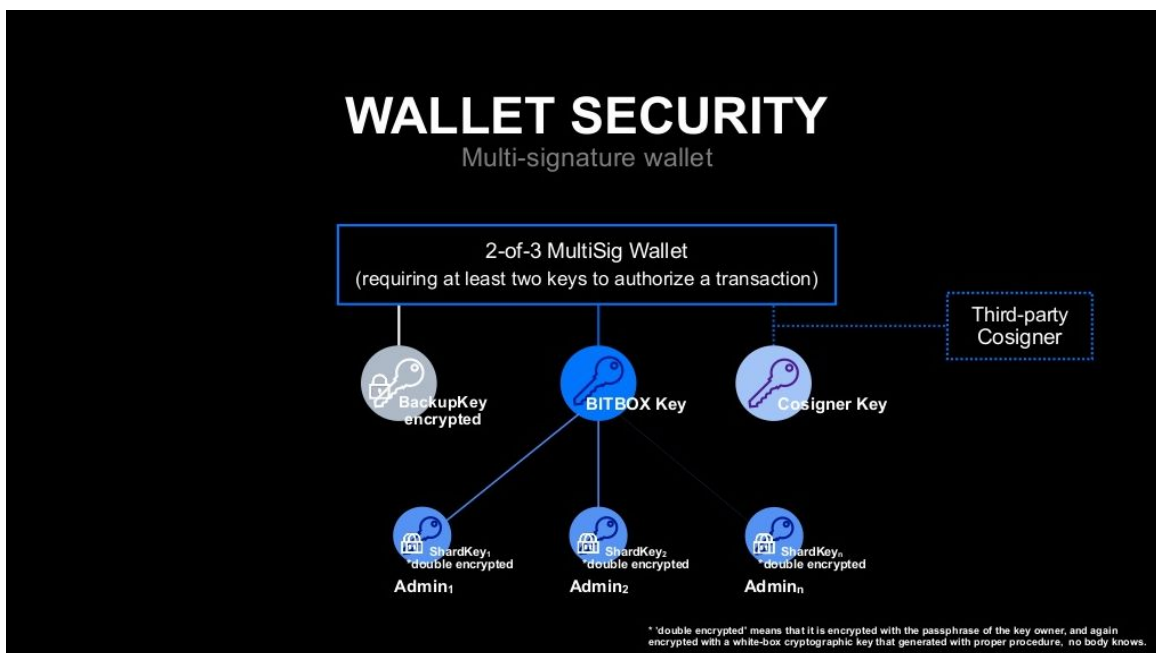


図4-18 BITBOXは第三者の署名を必要とするマルチシグアドレスを用いている⁶⁸

BITBOXはBitGoと連携していることを発表している⁶⁹。また、BitGoはこのような形態で暗号資産を管理する場合に、BitGoが第三者として鍵を管理するサービスであるBitGo Business Wallet⁷⁰を提供している。BITBOXがこのような形態で暗号資産を管理するために利用しているサービスがBitGo Business Walletと同一であるかは明らかではないが、本稿ではBitGo Business Walletをこの形態で暗号資産を管理する場合の事例として取り上げる。

BitGo Business Walletは、マルチシグアドレスの署名に必要な署名鍵のうちの1つをBitGoが保管するサービスである。

⁶⁷ <https://logmi.jp/tech/articles/320400>

⁶⁸ <https://logmi.jp/tech/articles/320400#s9>

⁶⁹ <https://linefinancialcorp.com/ja/pr/news/2018/1>

⁷⁰ <https://www.bitgo.com/services/cryptocurrency-wallet>

BitGo Business Wallet	
The only institutional-grade, multi-signature, multi-coin transactional wallet	
• Hot wallet access via the web and API	
• \$1 million USD minimum monthly transaction volume	
• 100+ coins & tokens	
• 24x7 global customer support	
• Variable fees based on transaction volume	

図4-19 BitGo Business Walletのサービスプラン⁷¹

BitGo Business Walletは、2 of 3 のマルチシグアドレスの署名に必要な署名鍵のうち、2つを利用者が保持し、残りの1つをBitGoが保管する。利用者は保持する2つの署名鍵のうち、1つを暗号資産の移転のための署名に用い、もう1つを緊急時のバックアップとして保管する。



図4-20 BitGo Business Walletは顧客とBitGoが共同で署名する。

暗号資産の移転を行う際は、トランザクションに対して、利用者が1つ目の署名を行う。2つ目の署名は、BitGoが、利用者によって事前に設定されたポリシーに基づいてトランザクションの検証を行った上で行う。ポリシーには、送金額の制限を設定することや、複数の管理者による承認を必要とすること、ホワイトリストによる送金先を限定すること等が可能である。

⁷¹ <https://www.bitgo.com/resources/pricing>

Wallet Policies

To further enhance security an administrator can create policies can be created by an Administrator to limit the ability to transfer digital currencies into or out of a wallet. Policies include:



Transaction Limit

Restricts the number of digital assets that can go out in a transactions



Velocity Limit

Defines a maximum number of digital tokens that can go out within a specified period of time



Multiple Approvers

Requires X of Y administrators to approve the transaction prior to being signed by BitGo



Final Approver

Gives final approval to a transactions approved by the administrator



Whitelist

Limits the transfer of digital assets only to a list of approved addresses

図4-21 BitGoが署名するポリシーを設定できる

BitGoが保管している署名鍵は、2 of 3 のマルチシグアドレスの署名に必要な署名鍵のうちの1つであるため、BitGoが単独で利用者の暗号資産を移転することはできない。また、利用者がマルチシグアドレスの署名に必要な数以上の署名鍵を持っているため、仮にBitGoが保管している署名鍵が失われても、利用者は暗号資産を移転することができる。

利用者が緊急時のバックアップとして保管する署名鍵を厳重に管理することで、通常の署名には必ず利用者とBitGoの双方の署名が必要となる。このため、それぞれが署名するトランザクションを確認することで不正や事故を防止し、単独で暗号資産を管理する場合よりもサイバー攻撃による流出リスクを軽減することができる。

なおBitGoはマルチシグアドレスを利用できない暗号資産については、複数の署名を必要とするコントラクトウォレットを利用している⁷²。

72

<https://bitgo.freshdesk.com/support/solutions/articles/27000042780-what-are-the-network-transaction-fees-related-to-ethereum->

4.2.2 利用者の暗号資産の移転に必要な署名鍵や情報を取り扱うサービスの形態の分類

事例より、利用者の暗号資産の移転に必要な署名鍵や情報について、サービス提供者が生成のみ行う場合、保管のみ行う場合、署名を行う場合が考えられる。

サービス提供者が取り扱う利用者の暗号資産の移転に必要な署名鍵や情報は、単体で暗号資産の移転に用いることができる署名鍵である場合や、利用者が暗号化した署名鍵、秘密分散によって分散片に分割された署名鍵、マルチシグアドレスやマルチシグアドレスと同等の権限分散が可能なコントラクトウォレット（以下、「マルチシグアドレス等」）に対応する署名鍵のうちの一部等、暗号資産の移転を行うための署名には不十分な情報である場合が考えられる。

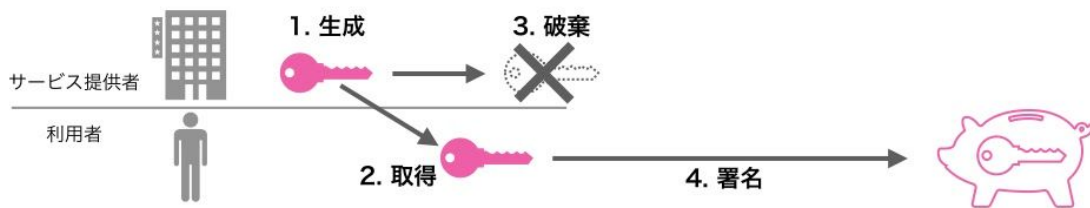
そこで、利用者の暗号資産の移転に必要な署名鍵や情報を取り扱うサービスの形態について、以下のように分類する。

- サービス提供者が暗号資産の移転のための署名を行わない場合
 - サービス提供者が署名鍵の生成を行う場合
 - サービス提供者が署名鍵の保管を行う場合
 - サービス提供者が署名に不十分な情報の保管を行う場合
- サービス提供者が暗号資産の移転のための署名を行う場合
 - サービス提供者だけが暗号資産の移転を行う場合
 - サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合
 - サービス提供者と利用者の双方が、暗号資産の移転を行う場合
 - サービス提供者が利用者と協力することで暗号資産の移転を行う場合

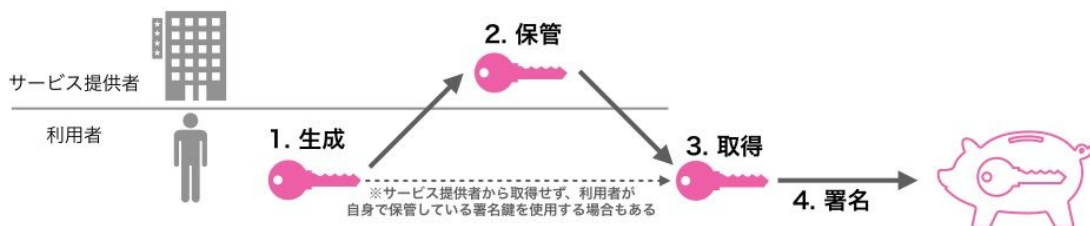
「サービス提供者が暗号資産の移転のための署名を行わない場合」は、サービス提供者は暗号資産の移転を行うための署名を行わず、署名鍵の生成や保管のみを行う。この場合には、さらに「署名鍵の生成を行う場合」、「署名鍵の保管を行う場合」、「署名に不十分な情報の保管を行う場合」が考えられる。

「署名鍵の生成を行う場合」は、サービス提供者が生成した署名鍵を利用者に提供し、利用者が暗号資産の移転のために使用する。「署名鍵の保管を行う場合」は、利用者が暗号資産の移転のために使用する署名鍵を、サービス提供者が保管する。「署名に不十分な情報の保管を行う場合」は、利用者のみが知るパスワード等で暗号化された署名鍵や、マルチシグアドレス等の暗号資産を移転するために必要な署名鍵の数に満たない数の署名鍵など、そのままでは暗号資産の移転を行う署名のためには不十分な情報を保管する。

サービス提供者が署名鍵の生成を行う場合の例



サービス提供者が署名鍵の保管を行う場合の例



サービス提供者が署名に不十分な情報の保管を行う場合の例

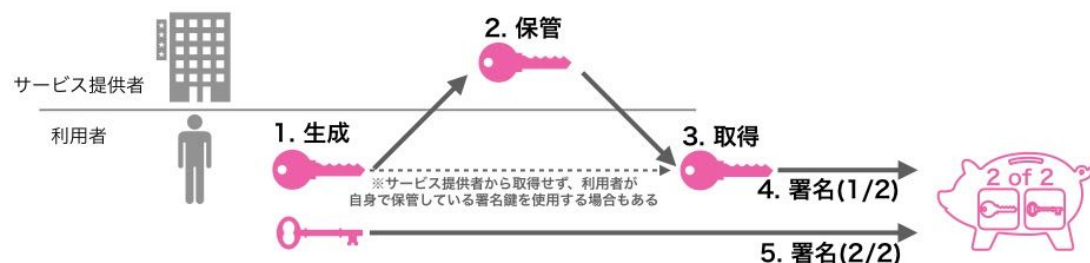


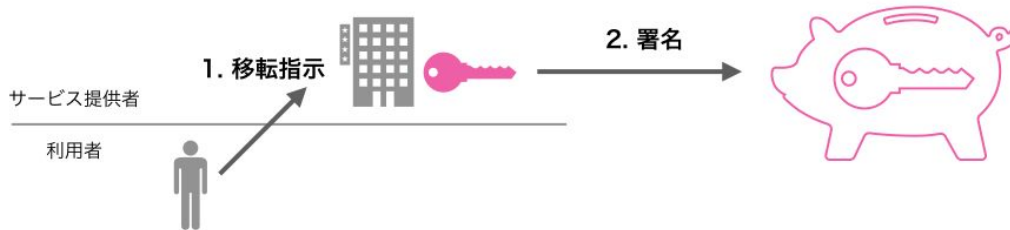
図4-22 サービス提供者が暗号資産の移転のための署名を行わない場合の例

「サービス提供者が暗号資産の移転のための署名を行う場合」は、サービス提供者が暗号資産の移転のための署名に関与する。この場合には、さらに「サービス提供者だけが暗号資産の移転を行う場合」、「サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合」、「サービス提供者と利用者の双方が、暗号資産の移転を行う場合」、「サービス提供者が利用者と協力することで暗号資産の移転を行う場合」が考えられる。

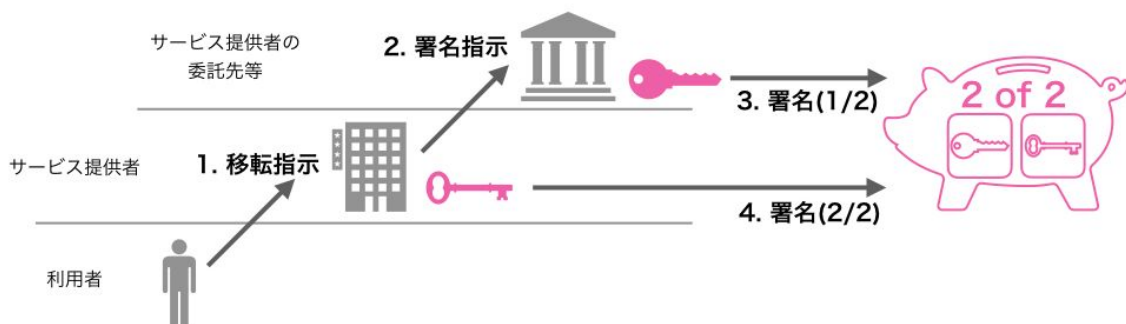
「サービス提供者だけが暗号資産の移転を行う場合」は、暗号資産の署名鍵をサービス提供者が生成して保管し、利用者の指図に基づきサービス提供者が暗号資産を移転する。利用者が署名鍵を取得することはない。「サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合」は、利用者がサービス提供者に暗号資産の移転を指図すると、サービス提供者が委託先等と共同で暗号資産を移転するための署名を行う。マルチシグアドレス等から暗号資産を移転するために、サービス提供者が有する署名鍵と委託先が有する署名鍵のそれぞれによって署名が必要な場合等が考えられる。利用者が署名鍵を取得することはない。「サービス提供者と利用者の双方が、暗号資産の移転を行う場合」は、サービス提供者と利用者の双方が、暗号資産を移転するための署名を行うことができる。サービス提供者と利用者がそれぞれ同一の署名鍵を共有する場合や、マルチシグアドレス等の暗号資産を移転するために必要な数の署名鍵をサービス提供者と利用者のそれぞれが保有している場合等が考えられる。「サービス提供者が利用者と協力することで暗号資産の移転を行う場合」は、サービス提供者と利用者の双方が、暗号資産の移転に用いられるがそれだけでは暗号資産の移転を行うための署名には不十分な情報を有する。サービス提供者と利用者が協力し、それぞれが有する情報を用いることで、暗号資産の移転のための署名を行う。マルチシグアドレ

ス等から暗号資産を移転するために、サービス提供者が有する署名鍵と利用者が有する署名鍵のそれぞれによって署名が必要な場合等が考えられる。

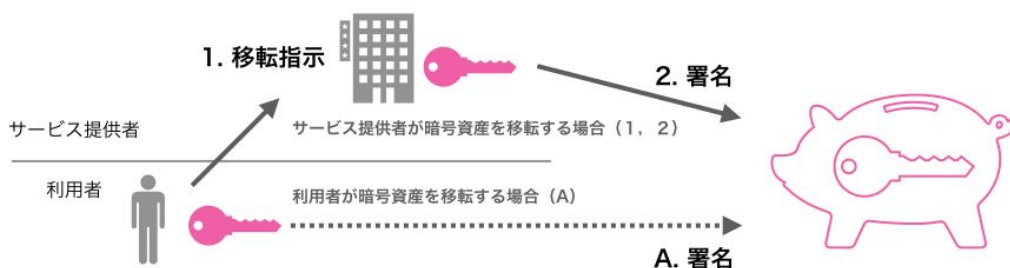
サービス提供者だけが暗号資産の移転を行う場合の例



サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合の例



サービス提供者と利用者の双方が、暗号資産の移転を行う場合の例



サービス提供者が利用者と協力することで暗号資産の移転を行う場合の例

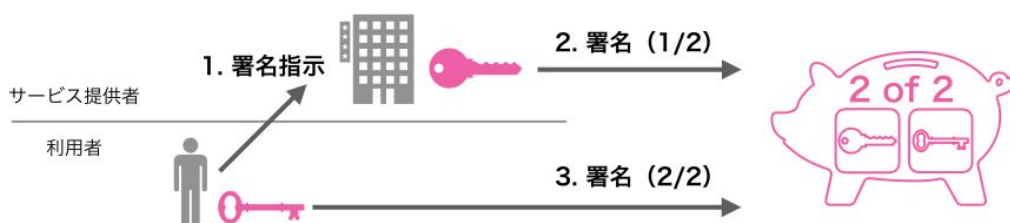


図4-23 サービス提供者が暗号資産の移転のための署名を行う場合の例

なお、これらの形態は、必ずしもあり得るすべてを網羅するものではなく、ここに挙げた形態を複数組み合わせた形態や、今後の技術進化によって新たな形態が出現することも考えられる。

4.2.3 形態ごとの流出リスクと破綻リスクへの対応の必要性の分析

4.2.3.1 サービス提供者が暗号資産の移転等のための署名を行わない場合

4.2.3.1.1 サービス提供者が署名鍵の生成を行う場合

サービス提供者は署名鍵の生成を行い、署名鍵を利用者に提供する。その後、サービス提供者は署名鍵を破棄する。利用者は提供された署名鍵を用いて暗号資産の移転のために署名を行うことができる。

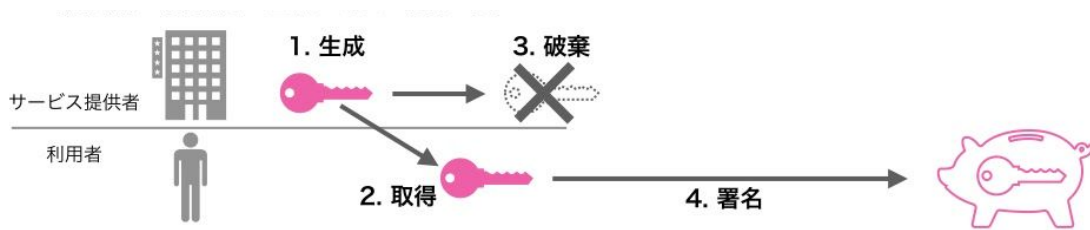


図4-24 サービス提供者が署名鍵の生成を行う場合の例

この場合に該当する例として、サービス提供者が署名鍵を印刷した物理的な媒体を販売する場合や、サービス提供者が署名鍵を利用者に代わって生成する場合等が考えられる。

サービス提供者は署名鍵の提供のみを行ない、署名鍵を保管せず、利用者の暗号資産の移転のために署名を行うことはなないため、サービス提供者は、内閣府令で定める方法で管理する対象となる暗号資産や、同種同量の履行保証暗号資産の保有が必要となる暗号資産、分別管理の対象となる暗号資産を有しない。

サービス提供者が破綻した場合、利用者が署名鍵を有しており、自身の暗号資産を移転することができる。サービス提供者は署名鍵を有しておらず、暗号資産の移転は行わないため、利用者はサービス提供者に対して暗号資産の移転を目的とする債権を有しておらず、優先弁済権を必要とすることもないと考えられる。

なお、サービス提供者が署名鍵を生成してから破棄するまでの間と、サービス提供者から利用者への署名鍵の伝達経路において、署名鍵が漏洩する可能性はある⁷³。漏洩した署名鍵に対応するアドレスに暗号資産が移転されると、漏洩した署名鍵が利用されて暗号資産が不正に移転される可能性がある点には注意が必要である⁷⁴。

⁷³ サービス提供者は署名鍵を利用者に提供すると署名鍵を破棄することから、漏洩する署名鍵は、その時点で生成されており、まだ破棄されていない署名鍵に限定される。

⁷⁴ 利用者が自身で管理している署名鍵がサービス提供者の不備によって漏洩し暗号資産が不正に移転されるリスクは、サービス提供者が利用者に対して暗号資産を管理するハードウェアやソフトウェアを提供し、利用者がそれらを使用して自身で署名鍵を管理している場合にも生じる。ソフトウェアの開発段階で混入した不正なプログラムによって暗号資産が流出した事例にHB Walletがある。HB Walletは、利用者のスマートフォン上で署名鍵を生成、保管し、暗号資産を移転する署名を行うソフトウェアである。2018年5月に、退職済みの元社員が、不正に所持していたHB Walletソフトウェアのリリース用のAPIキーを用いて、スマートフォン上に保管された署名鍵を外部に送信する不正なプログラムを混入させたソフトウェアアップデートをリリースした。13のアドレスに被害が発生し、外部に送信された署名鍵が利用されてEthereumが924.0288582ETH、Tronixが14829TRX、不正に移転された（<https://www.itmedia.co.jp/news/articles/1805/28/news052.html>）。

4.2.3.2 サービス提供者が署名鍵の保管を行う場合

サービス提供者は利用者の署名鍵を保管し、利用者は必要に応じて保管された署名鍵を取得し、暗号資産の移転のための署名に用いる。

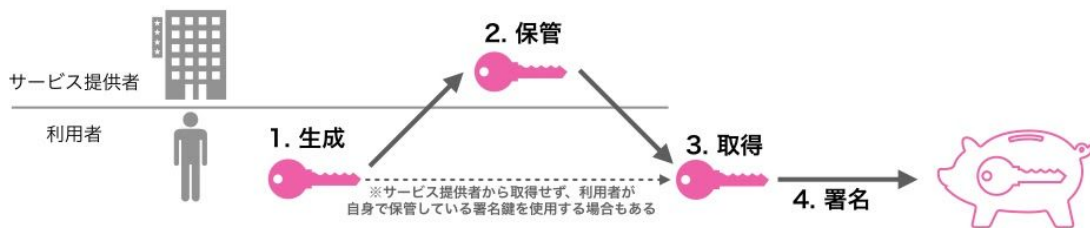


図4-25 サービス提供者が署名鍵の保管を行う場合の例

この場合に該当する例として、利用者が任意のデータを保管できるクラウドストレージやスマートフォンのオンラインバックアップサービスに署名鍵が保管される場合や、暗号資産の署名鍵データの保管を専門とするサービスに署名鍵が保管される場合、利用者がメッセージやデータを送受信できる電子メールサービスやソーシャルネットワーキングサービスで署名鍵の送受が行われる場合、サービス提供者が署名鍵の記録された媒体を保管する場合等が考えられる。

この場合の、流出リスクに対する対応の必要性について述べる。

サービス提供者が署名鍵を保管し、署名鍵に対応するアドレスには暗号資産の残高が存在する状態となるため、署名鍵が漏洩した場合には、暗号資産が流出する可能性がある。したがって、サービス提供者が保管する署名鍵について、内閣府令で定める方法で管理することは、保管された署名鍵に対応するアドレスに存在する暗号資産の残高の流出を防ぐ上で一定の効果はあると考えられる。

一方で、利用者が何を保管し、どのように利用しているかについて、サービス提供者が知るべきではない場合⁷⁵も考えられる。また、暗号資産の署名鍵は、一般的な電子署名に用いられる場合も考えられ、保管されている署名鍵が暗号資産の管理に用いられているかどうかは、必ずしもサービス提供者が知ることはできない。仮に暗号資産の管理に用いられているとしても、同一の署名方式を採用する暗号資産が複数存在する場合もあり、サービス提供者は署名鍵に対応する暗号資産の存在有無を必ずしも知ることはできない。さらに、署名鍵がマルチシグアドレスの署名に必要な署名鍵のうちのひとつとして利用される場合、マルチシグアドレスを生成する署名鍵の組み合わせや組み合わせる順番によってアドレスが変化する場合があることから、サービス提供者が署名鍵に対応するマルチシグアドレスを判別することができない場合がある。サービス提供者が保管する署名鍵について内閣府令で定める方法で管理しない場合に、サービス提供者が履行保証暗号資産を保有することが必要とされた場合、サービス提供者は履行保証暗号資産として保有すべき暗号資産の種類や量を判断することができない可能性がある。

また、利用者が署名鍵を保管する可能性のあるクラウドストレージや電子メールサービス等が、保管するデータに署名鍵が含まれる可能性があることから規制の対象となった場合に、内閣府令で定める方法でデータを管理しなければならないとされれば、利用者にとって利便性が大きく低下する可能性や、サービスが成立しなくなる可能性もある。

⁷⁵ 電気通信事業法は、第三条において「電気通信事業者の取扱中に係る通信は、検閲してはならない。」としている。また第四条において、「電気通信事業者の取扱中に係る通信の秘密は、侵してはならない。」としている。

したがって、改正法において求められる流出リスクに対する対応については、その管理形態や業態に応じて柔軟に対応する必要があるものであり、一律に規制の対象とすべきではないと考えられる。

次に、破綻リスクに対する対応の必要性について述べる。

サービス提供者は利用者の署名鍵の保管のみを行い、暗号資産の移転のための署名は常に利用者が行うため、署名鍵や署名鍵に対応するアドレスは利用者毎に異なり、利用者の暗号資産がサービス提供者のアドレスに混合して保管されることはない。利用者の署名鍵に対応するアドレスに存在する残高は利用者自身がブロックチェーン上で確認できる。利用者は、署名鍵を用いた電子署名によって、アドレスやアドレスに存在する暗号資産が自身のものであることを第三者に対して証明することも可能である。また、実際に暗号資産を移転させることも可能である。したがって、分別管理やその状況について監査を受けることを義務付ける必要性は低いと考えられる。また、利用者はサービス提供者に対して暗号資産の移転を目的とする債権を有しておらず、同債権についての優先弁済権は必要ないと考えられる。

したがって、改正法において破綻リスクの観点から求められる対応について、必要性は低いと考えられる。

なお、署名鍵が電子データとしてサービスに保管される場合、電子データは所有権の対象とならないことから、契約において、署名鍵が利用者のものとして保管されることとされ、利用者の意図しない暗号資産の移転が行われないよう保管される署名鍵の利用目的について制限されていることが重要と考えられる。

また、サービス提供者が署名鍵の生成と保管を兼ねる場合は、利用者が一度も署名鍵を取得しないまま、サービス提供者において事故等によって署名鍵が消失すると、利用者は暗号資産を移転することができなくなる。そのため、署名鍵の生成後に、利用者がバックアップを取得することを必須とすることが望ましい。

4.2.3.3 サービス提供者が暗号資産の移転に不十分な情報の保管を行う場合

サービス提供者は、暗号資産の移転に用いられるがそれだけでは暗号資産の移転を行うための署名には不十分な情報を保管する。利用者は必要に応じて保管された情報を取得し、利用者が保有する他の情報と組み合わせて暗号資産の移転のための署名に用いる。

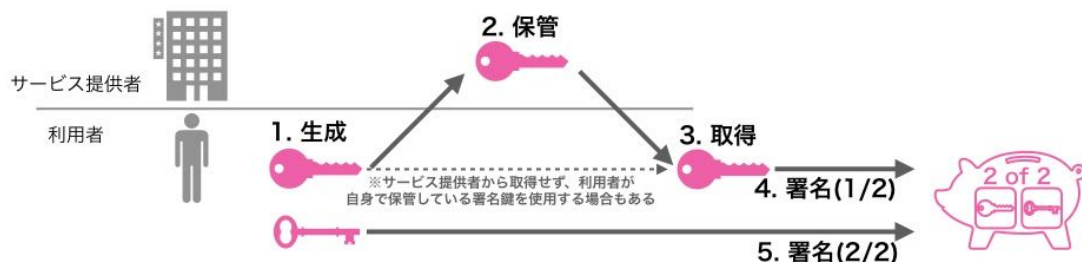


図4-26 サービス提供者が暗号資産の移転に不十分な情報の保管を行う場合の例

サービス提供者が、マルチシングアドレス等の暗号資産の移転に必要な数に満たない数の署名鍵を保管する場合⁷⁶や、暗号資産を移転するために必要な署名鍵を復元するのに必要な数に満たない数の分散片を保管する場合⁷⁷、利用者が暗号化した署名鍵を保管する場合⁷⁸等が考えられる。

この場合、サービス提供者が保管している情報によって暗号資産を移転させることは技術的に不可能であり、サービス提供者が保管する情報について、内閣府令で定める方法で管理する必要はないと考えられる。また、サービス提供者が保管する情報によって暗号資産が流出する恐れもないため、履行保証暗号資産を保有する必要はないと考えられる。したがって、改正法において求められる流出リスクに対する対応の必要性はないと考えられる。

サービス提供者は暗号資産の移転を行うための署名には不十分な情報の保管のみを行い、暗号資産の移転のための署名は常に利用者が行うため、署名鍵や署名鍵に対応するアドレスは利用者毎に異なり、利用者の暗号資産がサービス提供者のアドレスに混合して保管されることはない。加えて、サービス提供者が利用者の暗号資産を移転することは技術的に不可能である。そのため、分別管理やその状況について監査を受けることを義務付ける必要性はないと考えられる。また、利用者はサービス提供者に対して暗号資産の移転を目的とする債権を有しておらず、同債権についての優先弁済権は必要ないと考えられる。したがって、改正法において求められる破綻リスクに対する対応の必要性はないと考えられる。

なお、サービス提供者が破綻した場合、暗号資産の移転のための署名に必要な情報を利用者が単独で有していれば、利用者は暗号資産を移転することができる。暗号資産の移転のために、利用者が有している情報に加えてサービス提供者が保管している情報が必要となる場合は、サービス提供者が保管する必要な情報が記録された媒体の所有権が利用者にあることが重要であると考えられる。必要な情報が電子データである場合、電子データは所有権の対象とならないことから、契約において、保管されるデータが利用者のものとして保管されることとされていることが重要と考えられる。

⁷⁶ 例として、2 of 3 のマルチシングアドレスに対応するの3つの署名鍵のうちの1つをサービス提供者が保管する等。

⁷⁷ 例として、2 out of 3 の秘密分散で署名鍵が3つに分割された分散片のうちの1つをサービス提供者が保管する等。

⁷⁸ 例として、利用者のみが知るパスワード等で暗号化された署名鍵をサービス提供者が保管する等。

また、サービス提供者が顧客のみが知るパスワードによって暗号化された署名鍵を保管する場合においては、サービス提供者から暗号化された署名鍵が漏洩した際に、顧客が設定したパスワードの強度が低いと、署名鍵が復号されて署名に利用され、暗号資産が不正に移転される可能性がある。サービス提供者は、利用者に対して十分な強度のパスワードを設定するよう利用者に対して案内することが望ましい。サービス提供者が利用者に対して署名鍵を暗号化するソフトウェア等を提供する場合は、ソフトウェア等の仕組みとして、十分な強度のパスワードを設定することを強制することが望ましい。

4.2.3.2 サービス提供者が暗号資産の移転のための署名を行う場合

この場合には、サービス提供者は署名鍵等の情報を扱い、暗号資産の移転等を行うための署名のために署名鍵等の情報を利用する。

4.2.3.2.1 サービス提供者だけが暗号資産の移転を行う場合

暗号資産の署名鍵をサービス提供者が生成して保管し、利用者の指図に基づきサービス提供者が暗号資産を移転する。利用者が署名鍵を取得することはない。

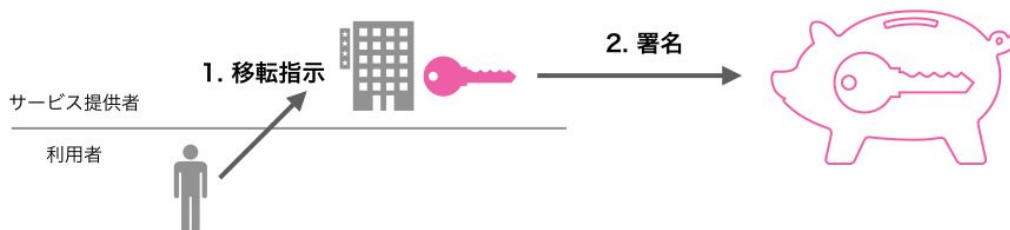


図4-27 サービス提供者だけが暗号資産の移転を行う場合の例

サービス提供者が署名鍵を保管し、暗号資産の移転のための署名を行うため、サービス提供者から暗号資産が流出する可能性がある。そのため、内閣府令で定める方法で管理することや、内閣府令で定める方法で管理しない暗号資産と同種同量の履行保証暗号資産を保有する必要があると考えられる。

利用者の暗号資産は、サービス提供者のアドレスに集約され混合して管理される場合がある。そのため、分別管理やその状況について監査を受ける必要があると考えられる。また、利用者は自身で暗号資産を移転することができず、サービス提供者に対して暗号資産の移転を目的とする債権を有しており、同債権についての優先弁済権が必要であると考えられる。

したがって、改正法が求める流出リスクと破綻リスクに対する対応が必要であると考えられる。

4.2.3.2.2 サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合

利用者がサービス提供者に暗号資産の移転を指図すると、サービス提供者が委託先等と共に暗号資産を移転するための署名を行う。利用者が署名鍵を取得することはない。

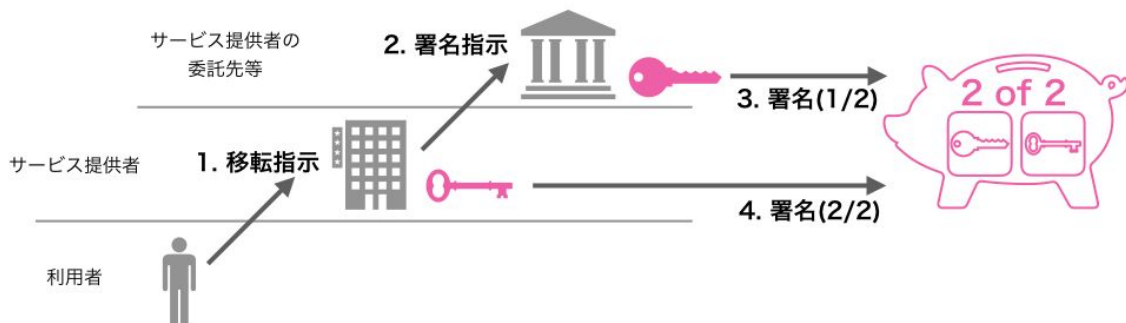


図4-28 サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合の例

マルチシグアドレス等からの暗号資産の移転のために、サービス提供者が有する署名鍵と委託先が有する署名鍵のそれぞれによって署名が必要な場合や、署名鍵が秘密分散によって分散片に分割されており、サービス提供者が有する分散片と委託先が有する分散片を集約して署名鍵を復元する、または署名のための秘密計算に用いる必要がある場合等が考えられる。

サービス提供者や委託先が単独では暗号資産を移転できない場合、どちらか一方から署名鍵等が漏洩しても、暗号資産を不正に移転されることがない点で、流出リスクは軽減される。しかしながら、サービス提供者の指図に従って委託先が署名を行うことが自動化されている場合等では、サービス提供者に対するサイバー攻撃等による不正な暗号資産の移転指図によって、暗号資産が流出することもあると考えられる。そのため、サービス提供者が委託先の管理を行った上で、サービス提供者が委託先と共同で管理する暗号資産について、内閣府令で定める方法で管理することや、内閣府令で定める方法で管理しない暗号資産と同種同量の履行保証暗号資産を保有する必要があると考えられる。

利用者の暗号資産は、サービス提供者とその委託先のアドレスに集約され混合して管理される場合がある。そのため、分別管理やその状況について監査を受ける必要があると考えられる。また、利用者は自身で暗号資産を移転することができず、サービス提供者に対して暗号資産の移転を目的とする債権を有しており、同債権についての優先弁済権が必要であると考えられる。

したがって、改正法が求める流出リスクと破綻リスクに対する対応が必要であると考えられる。

4.2.3.2.3 サービス提供者と利用者の双方が、暗号資産の移転を行う場合

サービス提供者と利用者の双方が、暗号資産を移転するための署名を行うことができる。

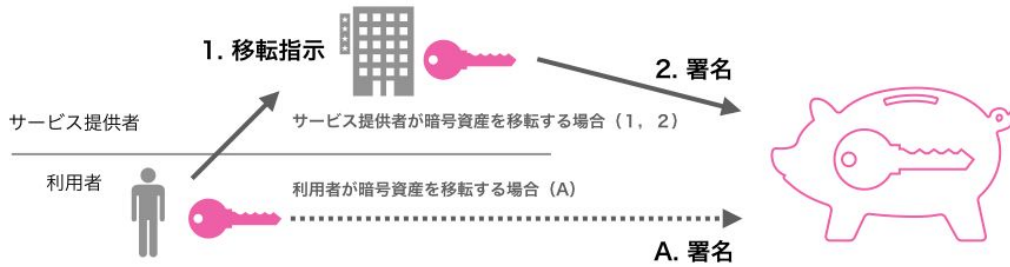


図4-29 サービス提供者と利用者の双方が、暗号資産の移転を行う場合の例

サービス提供者が利用者の暗号資産を管理するために用いる署名鍵を利用者が取得できる場合や、利用者がサービスに対して他のウォレットから署名鍵をインポートできる場合など、サービス提供者と利用者がそれぞれ同一の署名鍵を共有する場合や、マルチシグアドレス等の暗号資産を移転するために必要な数の署名鍵をサービス提供者と利用者のそれぞれが保有している場合⁷⁹等が考えられる。

まず、流出リスクへの対応の必要性について述べる。

サービス提供者が単独で暗号資産を移転できるため、サービス提供者から暗号資産が流出する可能性がある。そのため、サービス提供者が有する署名鍵について、内閣府令で定める方法で管理することや、内閣府令で定める方法で管理しない場合に署名鍵に対応するアドレスに存在する暗号資産と同種同量の履行保証暗号資産を保有する必要性はあると考えられる。

加えて、サービス提供者と利用者がそれぞれ同一の署名鍵を共有する場合、署名鍵によって作成された署名から、サービス提供者と利用者のどちらが管理する署名鍵によって署名が行われたのか、判別することはできない。そのため、暗号資産の流出が生じた場合に、サービス提供者と利用者のどちらが原因となって流出が生じたか、技術的に判別できない可能性がある点に注意が必要である。マルチシグアドレス等を用いて、サービス提供者が使用する署名鍵と、利用者が使用する署名鍵を異なる組み合わせにすることで、サービス提供者と利用者のどちらが管理する署名鍵によって署名が行われたかを判別可能にすることが望ましい。

次に、破綻リスクへの対応の必要性について述べる。

利用者の暗号資産を保管するアドレスには、利用者と共有している署名鍵に対応するアドレスや、利用者が有する署名鍵を含むマルチシグアドレスを利用するため、アドレスは利用者ごとに異なる。そのため、利用者らの暗号資産が混合して管理されることはない。

また、アドレスに存在する暗号資産は利用者が有する署名鍵によって自由に移転できるため、利用者のアドレスにサービス提供者の暗号資産を保管することも考えられず、利用者サービス提供者の暗号資産が混合して管理されることもない。

利用者のアドレスに保管される暗号資産は利用者の暗号資産のみであり、残高は利用者自身がブロックチェーン上で確認できる。利用者は、署名鍵を用いた電子署名によって、アドレスやアドレスに存在する暗号資産が自身のものであることを第三者に対して証明することも可能である。また、実際に暗号資産を移転させることも可能である。

⁷⁹ 例として、2 of 3 のマルチシグアドレスに対応する3つの署名鍵のうち2つを、サービス提供者と利用者がそれぞれ有し、暗号資産の移転に用いる等。

そのため、利用者の暗号資産については、サービス提供者に分別管理やその状況について監査を受けることを義務付ける必要性は低いと考えられる。

しかし、流出リスクへの対応として履行保証暗号資産の保有を義務付ける場合、履行保証暗号資産はサービス提供者の暗号資産と混合して管理される可能性があるため、サービス提供者に対して分別管理やその状況について監査を受けることを義務付ける必要があると考えられる。

利用者は暗号資産の移転を目的とする債権を有している。サービス提供者の破綻時には、利用者は自身で暗号資産を移転することができるが、サービス提供者も暗号資産を移転することができる。利用者が自身で暗号資産を移転する前に、サービス提供者の財産として暗号資産が移転され、破産債権となる恐れがあるため、優先弁済権が必要と考えられる。また、流出リスクへの対応として履行保証暗号資産の保有を義務付ける場合、履行保証暗号資産について利用者が他の債権者に先立ち弁済を受けるためにも、優先弁済権は必要と考えられる。

4.2.3.2.4 サービス提供者が利用者と協力することで暗号資産の移転を行う場合

サービス提供者と利用者の双方が、暗号資産の移転に用いられるがそれだけでは暗号資産の移転を行うための署名には不十分な情報を有する。サービス提供者と利用者が協力し、それぞれが有する情報を用いることで、暗号資産の移転のための署名を行う。

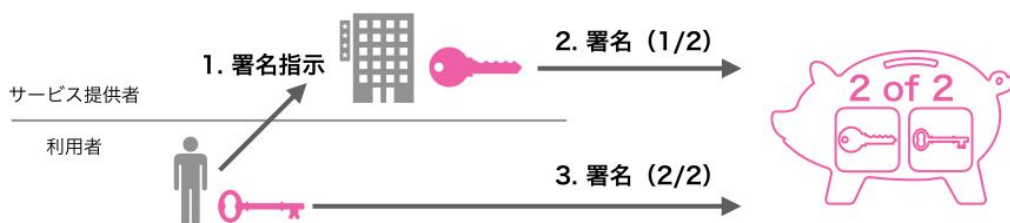


図4-30 サービス提供者が利用者と協力することで暗号資産の移転を行う場合の例

マルチシグアドレス等から暗号資産を移転するために、サービス提供者が有する署名鍵と利用者が有する署名鍵のそれぞれによって署名が必要な場合⁸⁰等が考えられる。

この場合、サービス提供者が有する情報のみによって暗号資産を移転させることは技術的に不可能であり、サービス提供者が有する情報について、内閣府令で定める方法で管理する必要性はないと考えられる。また、サービス提供者が有する情報のみによって暗号資産が流出する恐れもないため、履行保証暗号資産を保有する必要性はないと考えられる。したがって、改正法において求められる流出リスクに対する対応の必要性はないと考えられる。

サービス提供者が有する情報と利用者が有する情報の組み合わせによって移転できる暗号資産は利用者の暗号資産のみであり、サービス提供者や他の利用者の暗号資産と混合されることはなく、サービス提供者が単独で利用者の暗号資産を移転することも技術的に不可能であるため、分別管理やその状況について監査を受けることを義務付ける必要性はないと考えられる。

サービス提供者は利用者の協力がなければ暗号資産を移転することができない。利用者は、意図しないアドレスへの暗号資産の移転について、署名に協力しないことで、移転を阻止することができる。利用者は自身が意図する暗号資産の移転に対してのみ署名に協力する

⁸⁰ 例として、サービス提供者と利用者がそれぞれ異なる署名鍵を有し、それら2つの署名鍵に対応した2 of 2 のマルチシグアドレスから暗号資産を移転するトランザクションに、サービス提供者と利用者がそれぞれ署名し、暗号資産の移転を行う等。

ことができる。このような利用者の暗号資産について、サービス提供者の破綻の際にサービス提供者の財産として扱われ、処分されることは考えにくく、優先弁済権は必要ないと考えられる。したがって、改正法において求められる破綻リスクに対する対応の必要性はないと考えられる。

なお、サービス提供者と利用者が協力することで暗号資産の移転を行う場合として、秘密分散を用いる方法も考えられる。秘密分散によって署名鍵を分割し、サービス提供者と利用者がそれぞれ署名鍵の復元に必要な数に満たない分散片を有した場合、暗号資産を移転する署名のために、サービス提供者と利用者が協力することが必要となる。

ただし、署名鍵を生成して分割する者は分割前の署名鍵を取り扱う。また、分散片を集約して署名鍵を復元する者は復元後の署名鍵を取り扱う。分割前の署名鍵や復元後の署名鍵を取り扱う者は、単独で暗号資産の移転を行うための署名に十分な情報を有してしまう。

秘密分散によって、サービス提供者が暗号資産の移転を行うための署名には不十分な情報のみを有している状態を保つには、署名鍵の分割や復元を利用者が行うことが考えられる（この場合、サービス提供者は暗号資産の移転のための署名を行わないため、「暗号資産の移転に不十分な情報の保管を行う場合」に等しいと考えられる）。

または、署名鍵の復元をサービス提供者が行った場合、署名鍵に対応するアドレスから必ずすべての暗号資産を移転し、署名鍵を再利用することで移転できる暗号資産を残さない方法も考えられる。

さらに、秘密計算を用いて、署名鍵を生成せずにサービス提供者と利用者のそれぞれのコンピュータ上に分散片を直接生成する方法や、サービス提供者と利用者が互いの分散片を知らないまま署名を導出する方法を用いることも考えられる。

4.3 特定のエンティティが利用者の暗号資産を自己の裁量のみで自由に移転することができる状態とならないように工夫した技術

ブロックチェーン上でトランザクションを発行すると、発行の都度手数料がかかる。また、日本最大のカード決済総合サービスであるCAFISが1秒あたり平均310件以上の決済を処理している⁸¹のに対して、ビットコインは1秒あたり7トランザクションの処理が仕様上の上限とされており、同時に多数のユーザーがトランザクションを発行するとすぐに処理が滞る。この処理時間を短縮しようとするとうとトランザクション発行手数料が高騰する。

ブロックチェーン上で暗号資産の移転を行う場合に必要なトランザクション手数料や処理時間の負担を軽減するためには、サービス提供者が利用者の暗号資産を集約管理する方法（「3.1 集約管理する方法」参照）を用いて、サービス内で暗号資産の所有者が変化した際に、データベース上で利用者の残高を付け替える（オフチェーン取引）ことが考えられるが、サービス提供者が利用者の暗号資産を管理する場合、サービス提供者から暗号資産が流出するリスクや、サービス提供者が破綻するリスクがある。

ブロックチェーン上で暗号資産の移転を行う場合に必要なトランザクション手数料や処理時間の負担を軽減しつつ、流出リスクや破綻リスクも軽減する方法として、利用者の暗号資産を取り扱うが、特定のエンティティが利用者の暗号資産を自己の裁量のみで自由に移転することができる状態とならないように工夫した技術がある。

このような技術の形態として、「独立した複数のエンティティが協調して利用者の暗号資産を移転する場合」と「特定のエンティティが利用者の暗号資産を移転できるが、利用者が不正を阻止できる場合」のそれぞれの事例を取り上げ、暗号資産の管理にあたる業務の範囲についての論点を示す。なお、これらの形態は例であり、他にも様々な技術があり得る。また、今後の技術進化によって新たな形態が出現することも考えられる。

- 特定のエンティティが利用者の暗号資産を自己の裁量のみで自由に移転することができる状態とならないように工夫した技術の例
 - 独立した複数のエンティティが協調して利用者の暗号資産を移転する場合
 - 特定のエンティティが利用者の暗号資産を移転できるが、利用者が不正を阻止できる場合

「独立した複数のエンティティが協調して利用者の暗号資産を移転する場合」は、複数のエンティティが、それだけでは利用者の暗号資産の移転を行うための署名には不十分な情報を有し、各エンティティがそれぞれ独立に利用者の指図に従い、協調して利用者の暗号資産や残高の移転を行う。

「特定のエンティティが利用者の暗号資産を移転できるが、利用者が不正を阻止できる場合」は、利用者の暗号資産の移転や残高の記録を行う特定のエンティティが存在するが、不正な暗号資産の残高記録が行われた場合や、移転が行われようとした場合、利用者がそれを技術的に阻止できる。

⁸¹ CAFISによると（https://solution.cafis.jp/about/img/monthly_data.pdf）、2018年度末の月間処理件数は8億401万件であり、1秒あたりの処理件数は平均約310件である。

4.3.1 独立した複数のエンティティが協調して利用者の暗号資産を移転する場合

複数のエンティティが、それだけでは利用者の暗号資産の移転を行うための署名には不十分な情報をそれぞれ有し、各エンティティがそれぞれ独立に利用者の指図に従い、協調して利用者の暗号資産や残高の移転を行う。利用者の残高は、すべてのエンティティ、または一定数以上のエンティティが合意することで記録される。利用者の暗号資産は、すべてのエンティティ、または一定数以上のエンティティが署名等を行うことで移転される。

4.3.1.1 Liquid Networkの例

このような例に、Liquid Network⁸²がある。Liquid Networkは、サイドチェーンのひとつである。Liquid Networkでは、ビットコイン等の暗号資産を扱うことができる。

Liquid Networkでは、Functionaryとよばれる15のノードによってブロックチェーンへの記録が行われている。15のFunctionaryノードは交換業者等で構成されており、Liquid Networkは交換所間の決済等を目的としたネットワークである⁸³。ただし、15のFunctionaryノードとして参加する交換所以外の交換所や、一般の個人も利用することができる。

Liquid Networkへビットコインの残高を移す場合、ビットコインブロックチェーン上（以下、メインチェーン）において、15のFunctionaryノードの検証鍵から生成されたマルチシグアドレスにビットコインを移転する。これにより、ビットコインはロックされた状態となり、Functionaryノードによって、Liquid Network上の利用者のアドレスに、同量のビットコイン残高が記録される。Liquid Networkへビットコインの残高を移すことはPeg-Inと呼ばれる。

Liquid Network上の利用者のアドレスに記録された残高について、利用者は自身の署名鍵を用いて自由に移転することができる。利用者が署名を行った残高の移転のためのトランザクションは、15のFunctionaryノードによって検証され、それぞれのノードによって矛盾や不正がないことが確認されるとLiquid Networkのブロックチェーンに記録される。

Liquid Network上の利用者のアドレスに記録された残高をメインチェーン上でビットコインとして利用するには、利用者が、Liquid Network上の残高を消却してメインチェーンに引き出すための署名を行う。すると、Liquid Network上から利用者の残高が消却され、ビットコインがロックされているメインチェーン上の15のFunctionaryノードの検証鍵から生成されたマルチシグアドレスから、利用者のアドレスへ、消却された額と同量の暗号資産が移転される。Liquid Network上の残高をビットコインの残高に戻すことはPeg-Outと呼ばれる。

⁸² <https://blockstream.com/liquid/>

⁸³ https://docs.blockstream.com/liquid/technical_overview.html

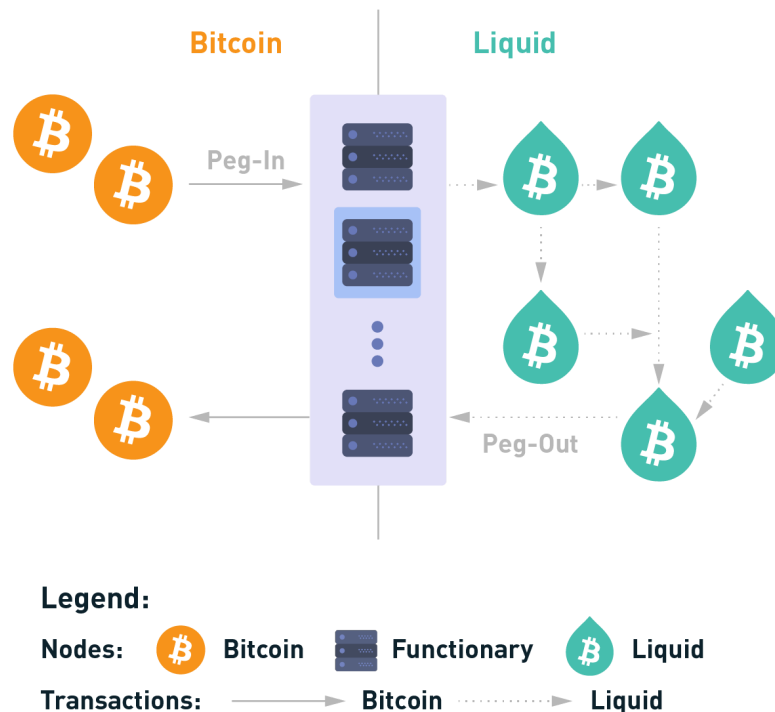


図4-31 Functionaryノードを介したBitcoinのPeg-InとPeg-Out⁸⁴

Functionaryノードの検証鍵から生成されたマルチシグアドレスは、11 of 15 となっており、11のノードが署名を行えば、ロックされた暗号資産は移転される。Functionaryノードは、利用者がLiquid Network上で署名したビットコインの引き出しのための署名を独立して検証し、正しい場合にのみ、メインチェーン上のマルチシグアドレスからのビットコインの移転のためのトランザクションに署名する。他のノードに対して署名を指図できる特定のノードは存在しない。したがって、特定のノードがメインチェーン上のマルチシグアドレスからビットコインを不正に移転しようとしても、他のノードは署名しないため、マルチシグアドレスからのビットコインの移転に必要な数の署名は集まらない。

⁸⁴ https://docs.blockstream.com/liquid/technical_overview.html

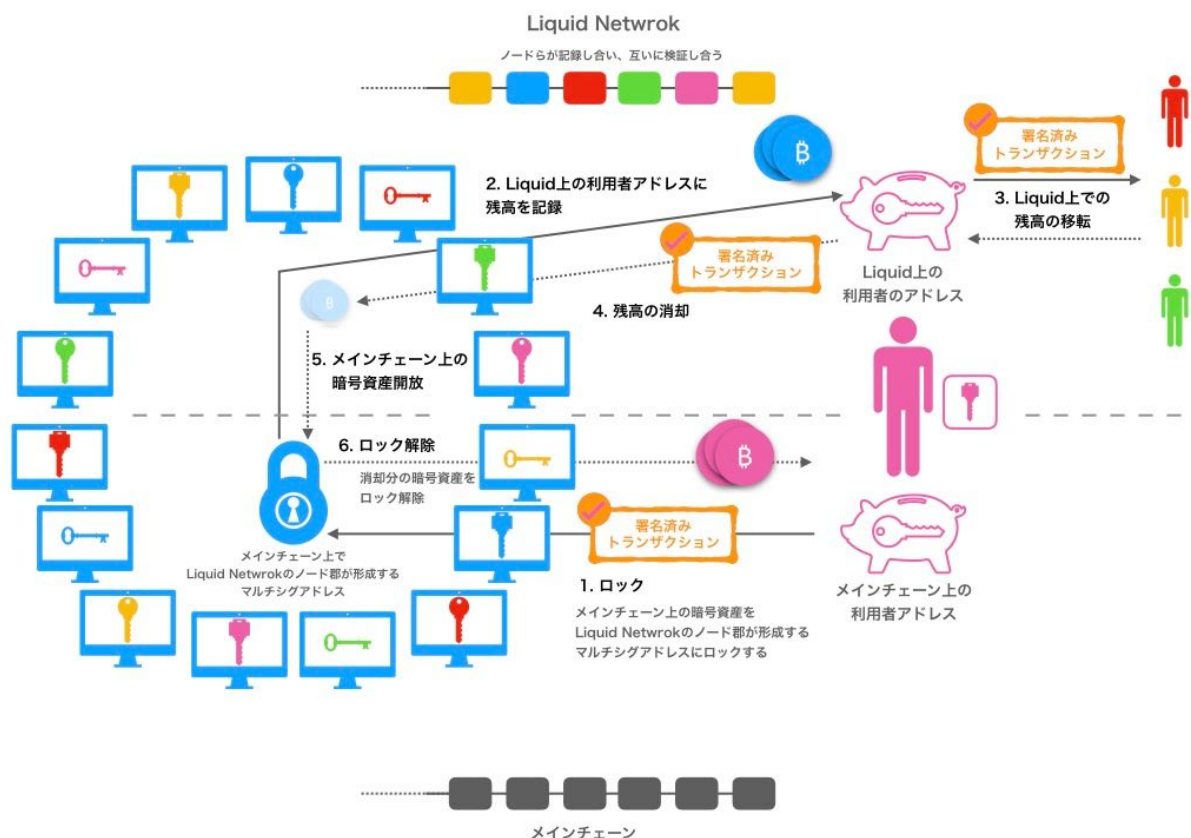


図4-32 Liquid Networkの仕組み

4.3.1.2 独立した複数のエンティティが協調して利用者の暗号資産を移転する場合の流出リスクと破綻リスクへの対応の必要性の分析

Liquid Networkは、メインチェーン上で複数のノードのマルチシグアドレスに利用者の暗号資産をロックし、サイドチェーン上で利用者が自身の署名鍵を用いて署名したトランザクションに従って、ノードが互いに検証し合いながら、サイドチェーン上の利用者の残高の移転を記録したり、メインチェーン上の利用者の暗号資産のロックを解除したりする。

このように、独立した複数のエンティティが協調して利用者の暗号資産を移転する場合、単独のエンティティが有する情報によって利用者の暗号資産を移転させることは技術的に不可能であり、利用者の暗号資産を移転できる特定のエンティティは存在しない。また、単独のエンティティが有する情報によって利用者の暗号資産が流出するおそれもない。

Liquid Networkの場合、サイドチェーン上で利用者の残高を記録するが、サイドチェーン上の利用者の残高についても、利用者が自身の署名鍵を用いて署名するトランザクションに基づき、複数のエンティティが検証し合いながら記録するため、自己の裁量によって移転させることができる特定のエンティティは存在しない。

したがって、個別のエンティティごとの観点からは、流出リスクや破綻リスクへの対応の必要性はないと考えられる。

しかしながら、それぞれのエンティティが有する情報は単独では利用者の暗号資産の移転を行うための署名には不十分な情報であっても、サイバー攻撃等により各エンティティから情報が流出し、攻撃者が流出した情報を集約することで利用者の暗号資産を移転するおそれが無いとは言えない。

また、Liquid Networkは利害関係の異なる15の交換業者等の参加者で実現されているが、同様の仕組みは様々なエンティティから構成される可能性がある。参加するエンティティが常に固定されている場合だけでなく、増減する場合や入れ替わる場合もある⁸⁵。資本関係や協力関係のあるエンティティ同士や、実質的な支配者が同一であるエンティティ同士が、このような仕組みによって利用者の暗号資産を取り扱う場合、特定のエンティティや支配者が自己の裁量によって利用者の暗号資産を移転できる立場となりうる。そのような場合には、「4.2.3.2.1 サービス提供者だけが暗号資産の移転を行う場合」や「4.2.3.2.2 サービス提供者が委託先等と共同して利用者の暗号資産の移転を行う場合」に準じて改正法において求められる対応が必要と考えられる。

独立した複数のエンティティが協調して利用者の暗号資産を移転する分散型技術について、実態に即したリスク評価を行うとともに、個別のエンティティには流出リスクや破綻リスクはなく、複数のエンティティの集合としては流出リスクや破綻リスクが考えられる場合について、法解釈の明確化や、求めるべき対応の有無やその内容についてさらなる検討が必要であると考ええる。

4.3.2 特定のエンティティが利用者の暗号資産を移転できるが、利用者が不正を阻止できる場合の例（Plasma）

利用者の暗号資産の移転や残高の記録を行う特定のエンティティ（以下、オペレーター）が存在するが、不正な暗号資産の残高記録が行われた場合や、移転が行われようとした場合、利用者がそれを技術的に阻止できる。利用者が必要に応じて不正を阻止する必要があるが、オペレーターは自己の裁量のみによって利用者の暗号資産の残高記録や移転を行うことはできない。

4.3.2.1 Plasma

このような例に、Plasma⁸⁶がある。Plasmaはイーサリアムのサイドチェーンとして用いることを想定して考案された仕組みの総称である。具体的な仕様には様々なものがあるが、ここでは一例を示す。

イーサリアムブロックチェーン（以下、メインチェーン）上の暗号資産をPlasmaチェーン上で利用するには、利用者が暗号資産をメインチェーン上のスマートコントラクトにロックする。すると、Plasmaチェーン上の利用者のアドレスに残高が記録され、利用者は自身の署名鍵を用いてPlasmaチェーン上で自由に残高を移転できる。利用者は、サイドチェーン上の残高を消却することで、メインチェーン上で同量の暗号資産をスマートコントラクトからロック解除して移転することができる。

Plasmaチェーン上での残高の移転は、単独または複数からなる特定のオペレーターによってブロックチェーンへ記録される。多数のノード同士が検証しあいながら記録を行うブロックチェーンと比べて、特定のオペレーターによって記録が行われるPlasmaチェーンは、高速に記録を行うことができる。

ただし、そのままでは、検証が行われないことで、不正な残高の移転が記録される恐れがある。オペレーターが不正な残高をサイドチェーンに記録した場合、不正な残高に基づいて

⁸⁵ 例として、一定量の暗号資産をステーキングしたエンティティが、メインチェーンで利用者の暗号資産をロックしたり、サイドチェーンで利用者の残高を記録したりする役割となる場合等が考えられる。

⁸⁶ <https://www.plasma.io/plasma.pdf>

スマートコントラクトから暗号資産がロック解除され、メインチェーン上で不正に暗号資産が移転されるおそれがある。

そこで、Plasmaチェーン上での不正な残高の記録に基づいて、メインチェーン上のスマートコントラクトにロックされている暗号資産が不正に引き出せないような仕組みが用意されている。

Plasmaチェーンで残高を消却してからメインチェーンの暗号資産が引き出されるまで、7日間等、一定の期間が必要となる。この期間、メインチェーン上のスマートコントラクトは、利用者から不正の証明を受け付ける。Plasmaの仕組みとして、利用者は、Plasmaチェーン上での自己の残高や他者の不正な残高、オペレーターによる不正な記録を、メインチェーン上のスマートコントラクトに対して数学的に証明することができる。不正が証明された場合、引き出しは失敗する。不正の証明は数学的に行われ、スマートコントラクトのプログラムによって機械的に判定されるため、オペレーターや利用者が不正を働くことはできない。

不正が証明された場合、利用者の残高は、不正な記録が行われる前の残高までロールバックされる。期間を超過した場合や、利用者が不正を証明しなかった場合、不正に記録された残高に基づいて暗号資産が移転され、オペレーターの裁量によって暗号資産の移転が行われる。

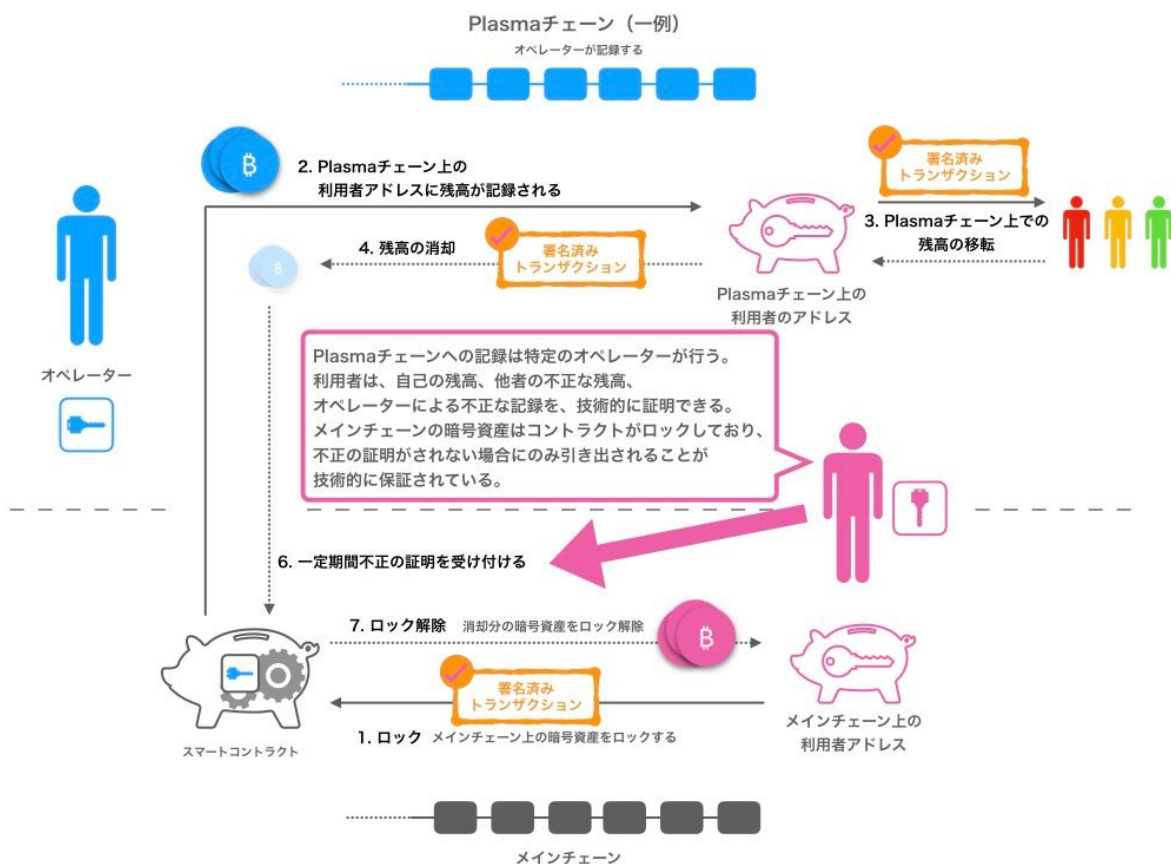


図4-33 Plasmaの仕組み

4.3.2.2 特定のエンティティが暗号資産を移転できるが、利用者が不正を阻止できる場合の流出リスクと破綻リスクへの対応の必要性の分析

Plasmaの仕組みでは、利用者がメインチェーン上でスマートコントラクトに暗号資産をロックし、オペレーターがその残高と利用者間の残高の移転をPlasmaチェーンに記録する。スマートコントラクトにロックされた暗号資産はPlasmaチェーンの残高記録に基づいて利用者が移転することができる。オペレーターは、スマートコントラクトにロックされた利用者の暗号資産を直接移転することは出来ないが、Plasmaチェーン上の利用者の残高を操作することで、利用者の暗号資産を移転することが可能である。ただし、オペレーターが不正な残高の記録を行ったことを利用者が発見した場合、利用者はスマートコントラクトに対してオペレーターの不正を証明し、不正な暗号資産残高の記録や、それに基づくメインチェーン上での暗号資産の移転を阻止することができる。利用者がオペレーターの不正を検知し、阻止する限りにおいて、オペレーターは自己の裁量のみで利用者の暗号資産を移転することはできない。

このように、特定のエンティティが利用者の暗号資産を移転できるが、利用者の意図しない不正な暗号資産の移転が行われようとした際に、利用者が阻止できる場合、利用者が不正を阻止する限りにおいては、同エンティティが有する情報のみによって利用者の暗号資産を移転することは出来ず、暗号資産が流出するおそれはない。また、同エンティティが破綻した場合に、利用者の暗号資産を同エンティティが自己の財産として処分することもできない。

しかしながら、利用者が不正に気づかなかった場合や、不正を阻止しなかった場合、特定のエンティティが有する情報によって利用者の暗号資産が流出するリスクや、同エンティティの破綻時に利用者の暗号資産が同エンティティの財産として処分されるおそれがある。

また、Plasmaの具体的な実装には様々なものが考えられることから、実態に即したリスク評価を行う必要があると考える。

特定のエンティティが利用者の暗号資産を移転できるが、利用者が不正を阻止できる場合について、実態に即したリスク評価を行うとともに、一定の条件において流出リスクや破綻リスクがない場合について、法解釈の明確化や、求めるべき対応の有無やその内容についてさらなる検討が必要であると考ええる。

4.4 暗号資産の管理にあたる業務の範囲に関する論点

暗号資産は署名鍵があれば移転することができるが、クラウドストレージやメール等、必ずしも利用者の暗号資産を取り扱うことを目的としていないサービスが利用者の署名鍵を取り扱う場合も考えられる。利用者の暗号資産を取り扱うことを目的としている場合についても、サービス提供者が取り扱う利用者の暗号資産の移転に必要な署名鍵や情報は、単体で暗号資産の移転に用いることができる署名鍵である場合や、利用者が暗号化した署名鍵、秘密分散によって分散片に分割された署名鍵、マルチシグアドレスやマルチシグアドレスと同等の権限分散が可能なコントラクトウォレットに対応する署名鍵のうちの一部等、暗号資産の移転を行うための署名には不十分な情報である場合も考えられる。

利用者の暗号資産の移転に必要な署名鍵や情報を取り扱うサービスには様々な形態がありうるため、一律に規制するのではなく、実態に応じた柔軟性の高い規制が必要と考える。

また、暗号資産の流出リスクや破綻リスクがない場合であっても、取り扱う署名鍵や情報が顧客にとって重要なデータである場合、相続や税務調査の対象となる場合、サービス提供者がサイバー攻撃の対象となる場合、犯罪やマネーロンダリングに利用される場合も考えられる。サービス提供者においては、規制の対象とならない場合であっても、取り扱う情報を保護するための適切な安全管理措置を実施し、事故や犯罪の追跡に必要なアクセスログや操作ログ等の取得や取引記録等の作成および適切な期間の保管⁸⁷を行い、万が一情報が漏洩した場合には直ちに利用者に周知することが望ましい。

ブロックチェーン技術を活用した決済やアプリケーション等のイノベーションの実現にあたっては、暗号資産の移転を行う場合に必要なトランザクション手数料や処理時間の負担を軽減することや、流出リスクや破綻リスクを軽減することが可能な、特定のエンティティが利用者の暗号資産を自己の裁量のみで自由に移転することができる状態とならないように工夫した技術を応用することも重要である。このような技術の利用にあたっては、イノベーションを阻害しない観点から、法解釈の明確化や、求めるべき対応の有無やその内容についてさらなる検討が必要であると考えられる。

⁸⁷ 「仮想通貨交換業者に関する内閣府令」第26条において、仮想通貨交換業者は仮想通貨交換業に係る取引記録や総勘定元帳、顧客勘定元帳について少なくとも十年間、各営業日における管理する利用者の金銭の額及び仮想通貨の数量の記録や各営業日における信託財産の額の記録、分別管理監査の結果に関する記録について少なくとも五年間、当該帳簿書類を保存しなければならないとされている。

「サイバー犯罪に関する条約」第16条第2項において、「締約国は、ある者が保有し又は管理している特定の蔵置されたコンピュータ・データを保全するよう当該者に命令することによって1の規定を実施する場合には、自国の権限のある当局が当該コンピュータ・データの開示を求めることを可能にするために必要な期間（九十日を限度とする。）、当該コンピュータ・データの完全性を保全し及び維持することを当該者に義務付けるため、必要な立法その他の措置をとる」とされている

（https://www.mofa.go.jp/mofaj/gaiko/treaty/pdfs/treaty159_4a.pdf）。

「不正アクセス行為の禁止等に関する法律」の規定に違反した場合の公訴時効は三年である。

「刑法」第二百四十六条第二項 電子計算機使用詐欺 の公訴時効は七年である。

「国税通則法」第70条において、国税の更正、決定等の期間は最大の場合で十年とされている。

5. おわりに

規制に先立ち、すでに終了または終了を予定しているサービスもある中で、衆議院財務金融委員会、参議院財政金融委員会の附帯決議にも記載されている通り、サービス提供者や開発者が過度に萎縮することがないよう、法解釈の周知徹底がなされることが望ましい。

暗号資産の管理を新たに規制の対象とすることで、従来とは管理形態やサービス形態の異なる様々な事業者が新たに規制の対象となりうる。具体的な規制の内容を定めるにあたっては、新たに規制対象となる業態の実態を考慮しながら検討する必要があるとともに、技術やサービスの進展に伴い、今後必要に応じて制度の見直しが行われることが望ましい。

暗号資産の管理にあたる業務の範囲を定めるにあたっては、暗号資産の管理を目的としないサービスが提供できなくなることを避け、その定義については十分に留意し、様々なサービスの形態を考慮して解釈が明確化されることが望ましい。また、特定のエンティティが利用者の暗号資産を自己の裁量のみで自由に移転することができる状態とならないように工夫した技術の活用等について、適切にリスクを評価するとともに、イノベーションを阻害しないよう配慮しながら、さらなる検討が必要と考えられる。

2019年12月16日 初版発行

2020年1月24日 第2版発行 4章以降を追記