

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1版

栗田 青陽²
株式会社メルカリ R4D

DP2019-2-1
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る。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。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る。

² <https://twitter.com/niwatako>

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・ローンダー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、マネーロンダーリング・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、マネーロンダーリング・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意しつつ、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/setsumei.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。

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。

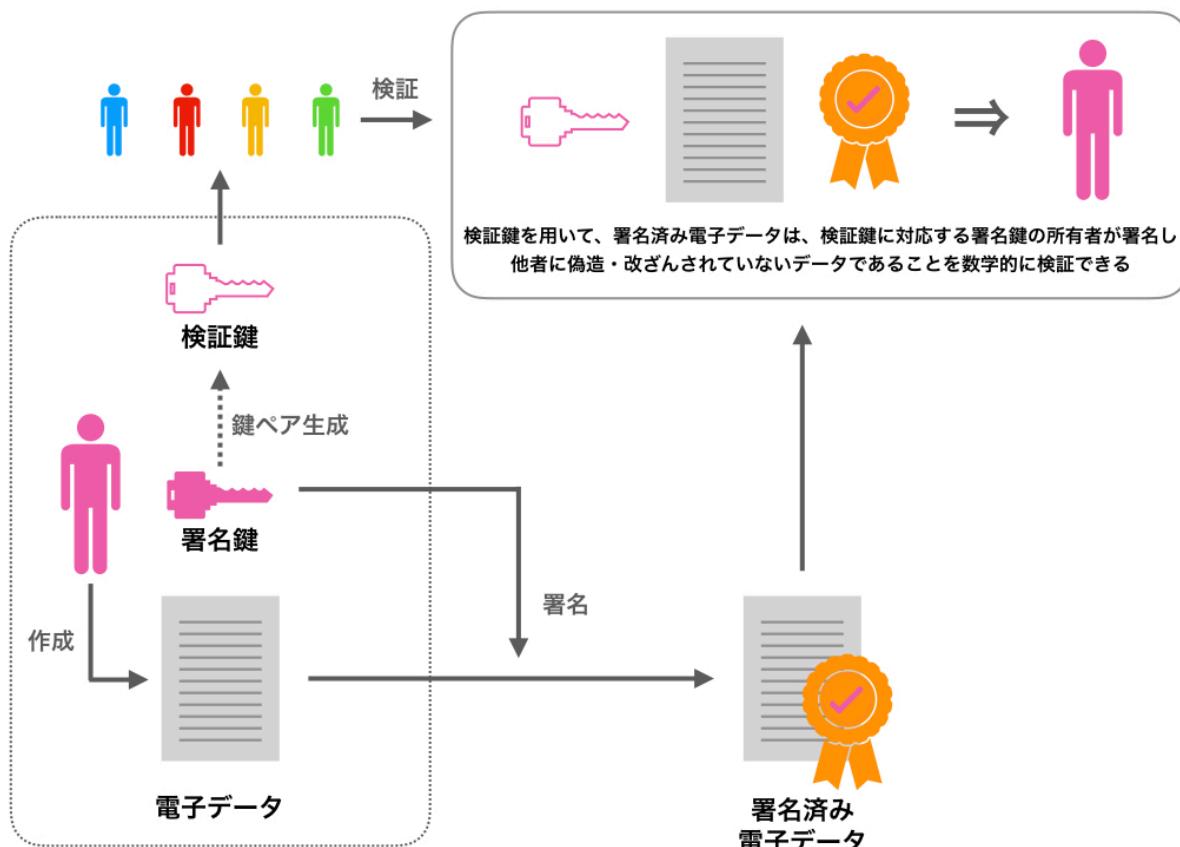


図2-1 デジタル署名

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。

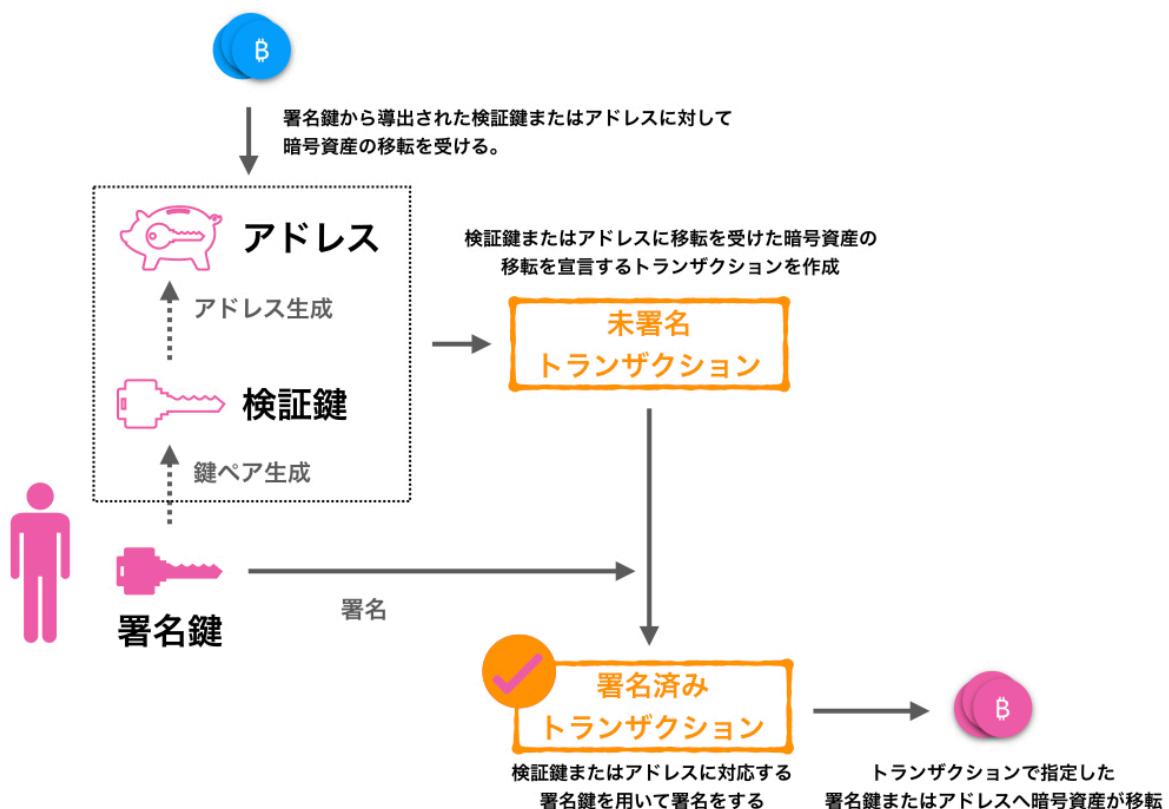


図2-2 トランザクションの作成の例

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。

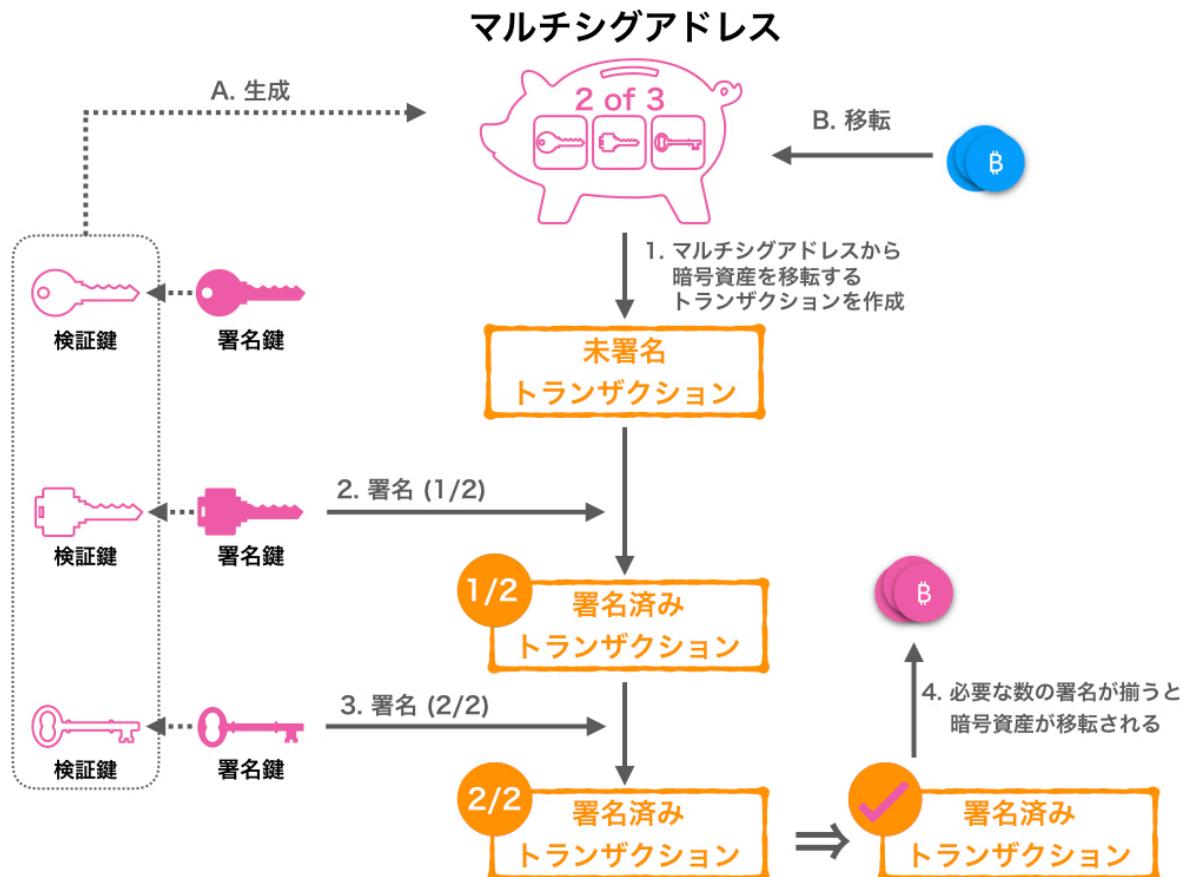


図2-3 2 of 3のマルチシグアドレスの例

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ている。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。

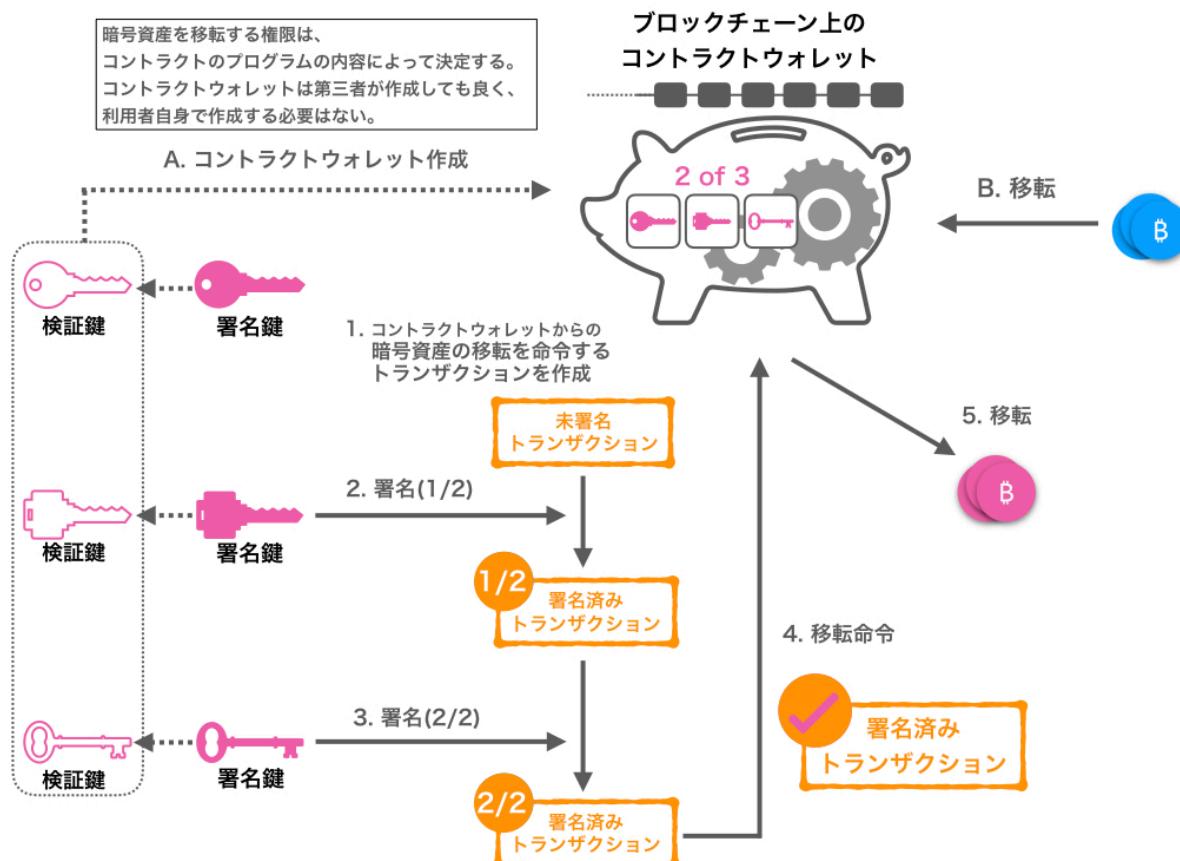


図2-4 2 of 3のコントラクトウォレットの例

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て署名鍵を復元し、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。

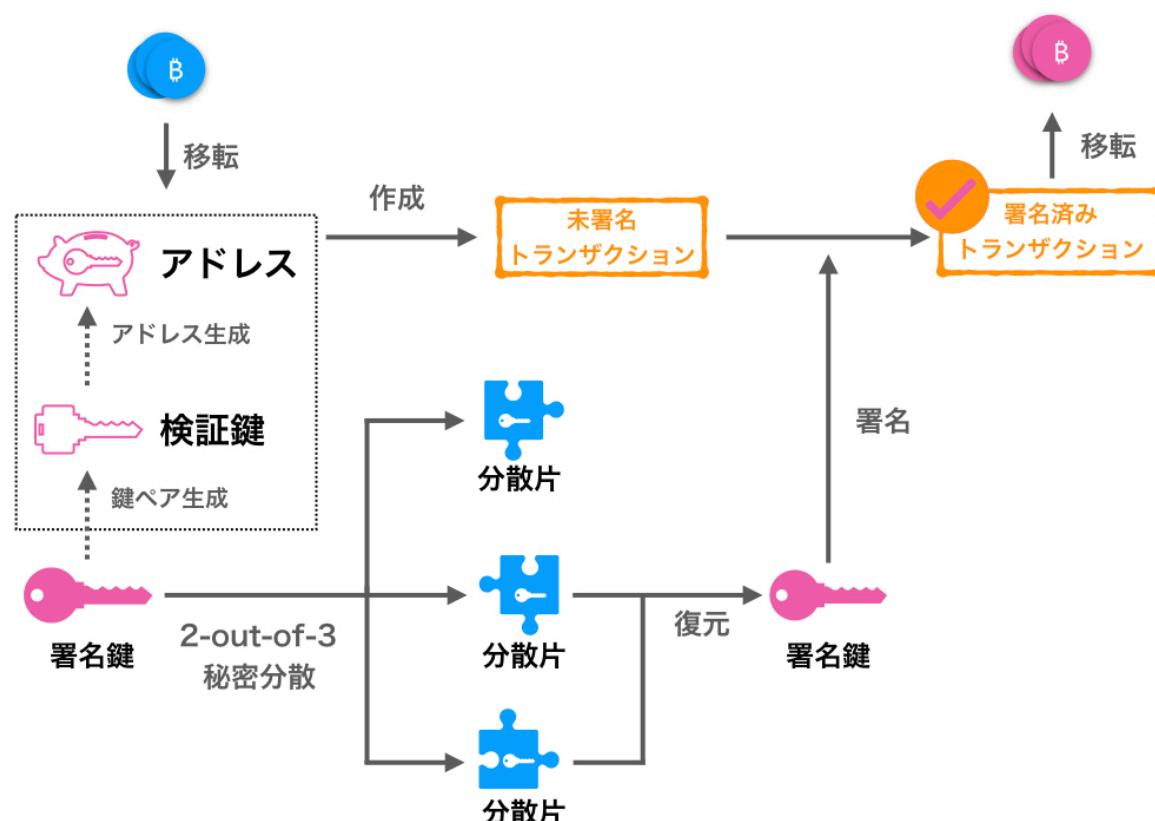


図2-5 秘密分散の例

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 密密計算

データを暗号化したままの状態で計算する秘密計算（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 密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め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。

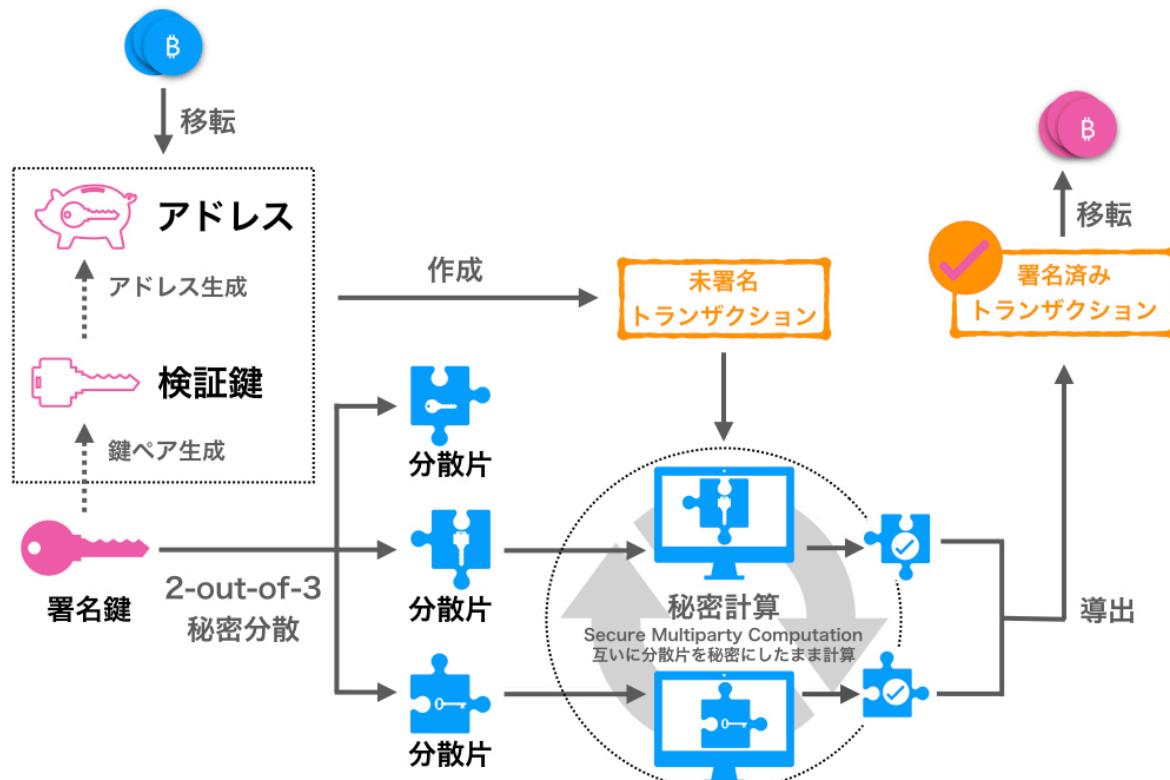


図2-6 密密計算を署名に用いる方法の例

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。

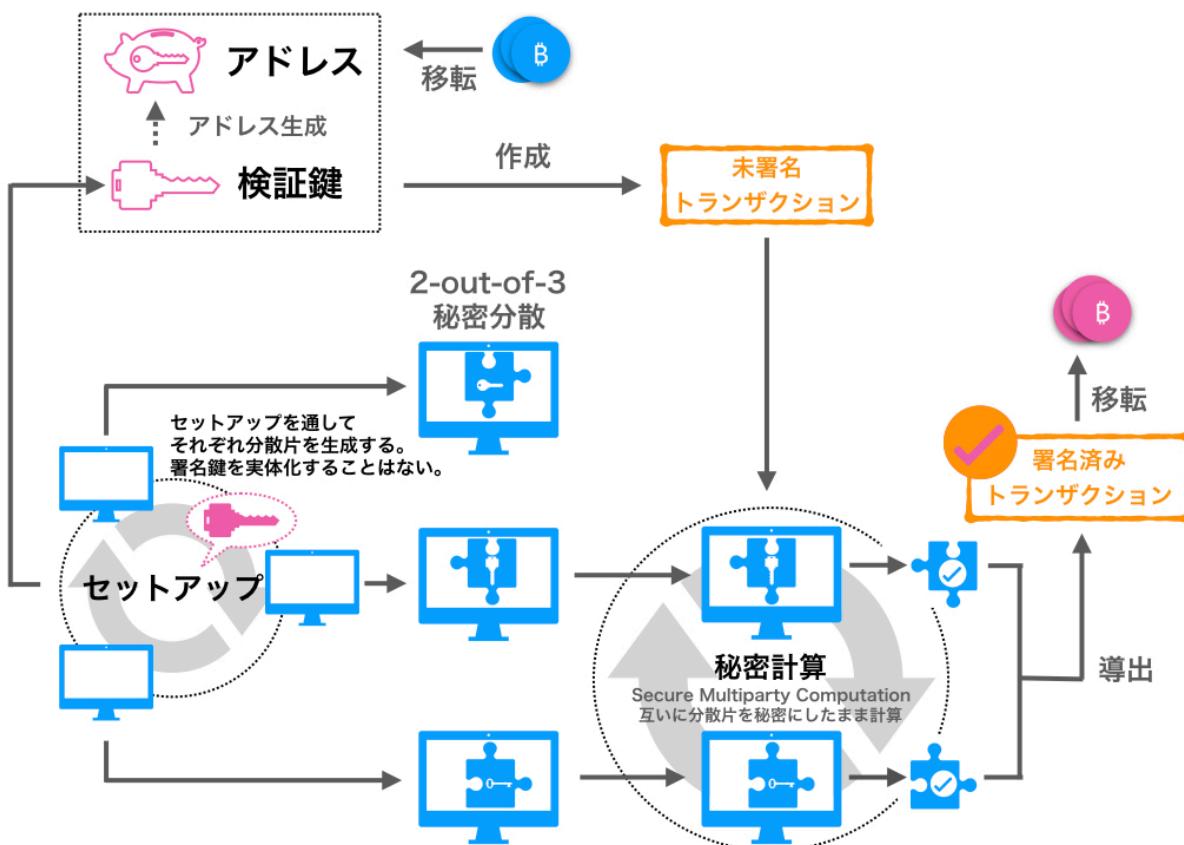


図2-7 秘密計算を検証鍵の生成と署名に用いる方法の例

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。

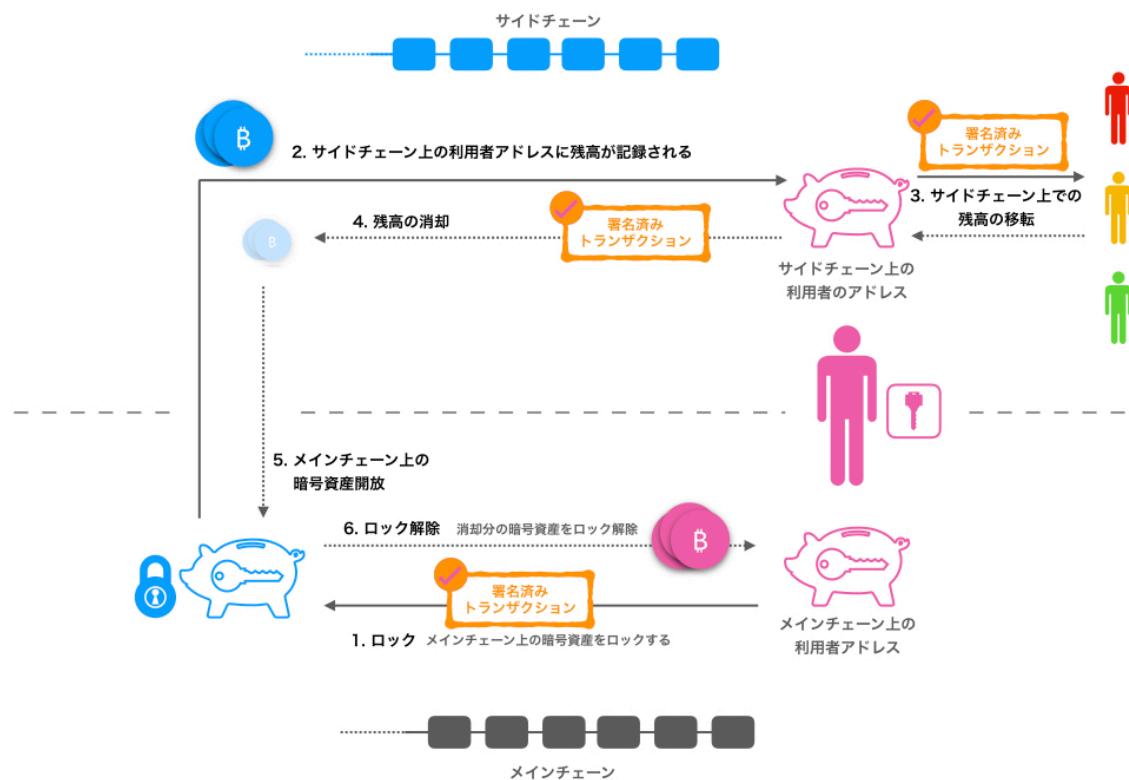


図2-8 メインチェーンとサイドチェーン

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、業者が顧客か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。

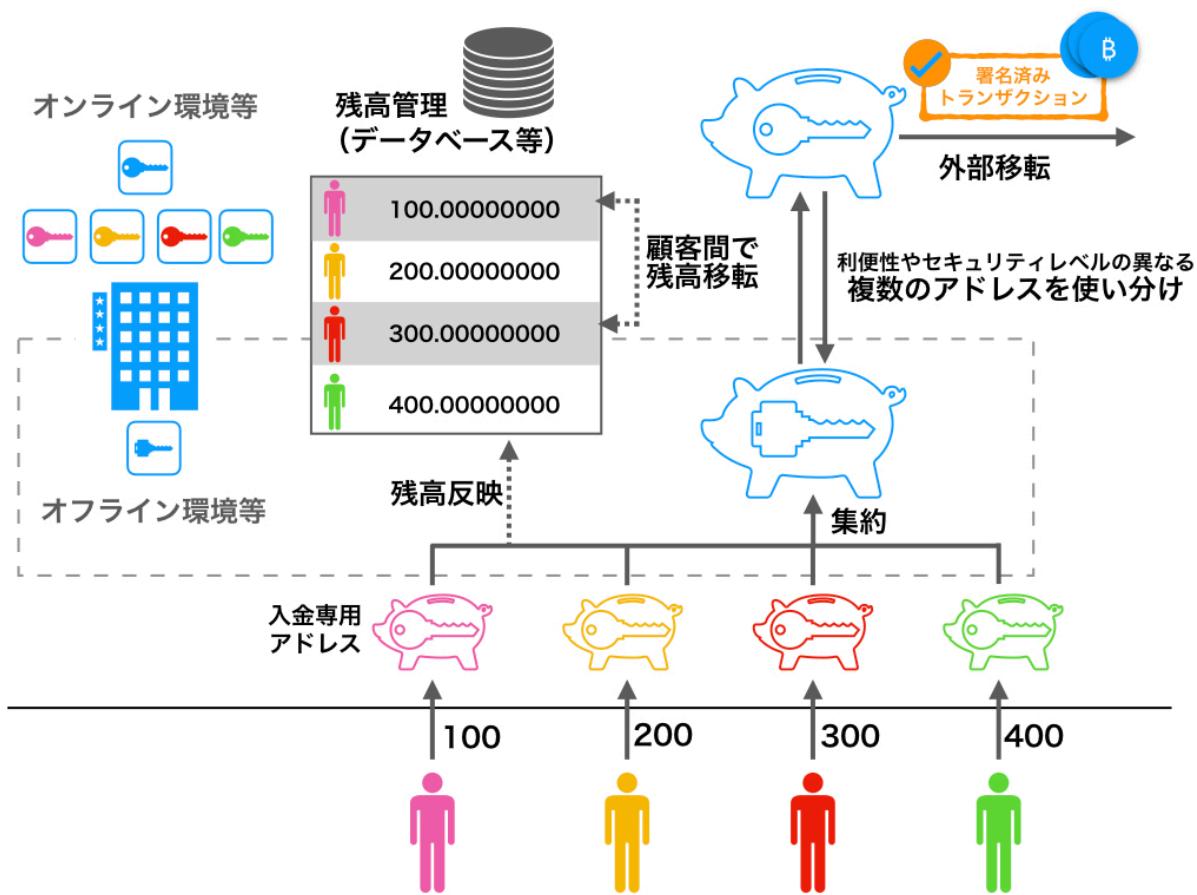


図3-1 集約管理する方法の例

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成本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



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は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。

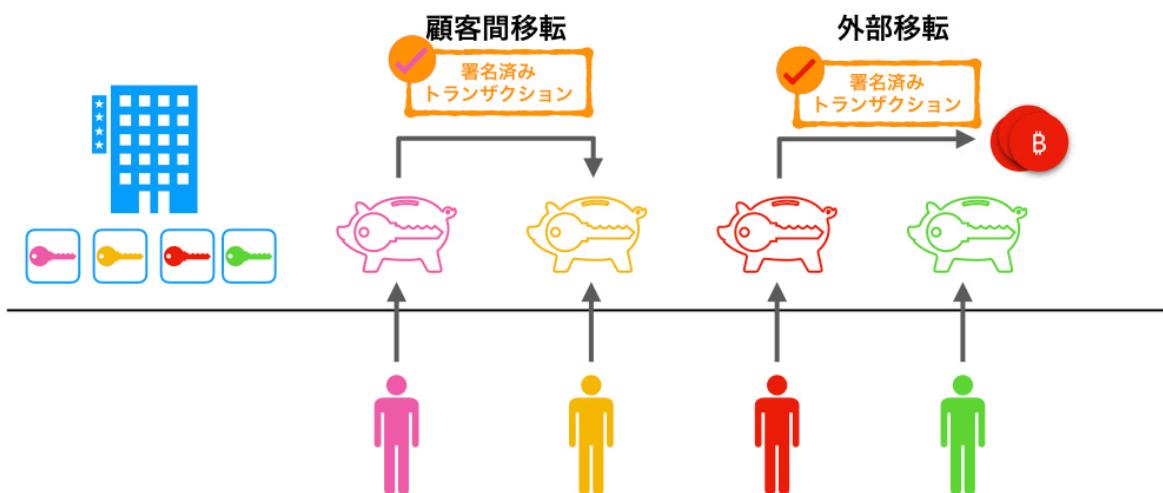


図3-5 個別に管理する方法の例

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ので、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。

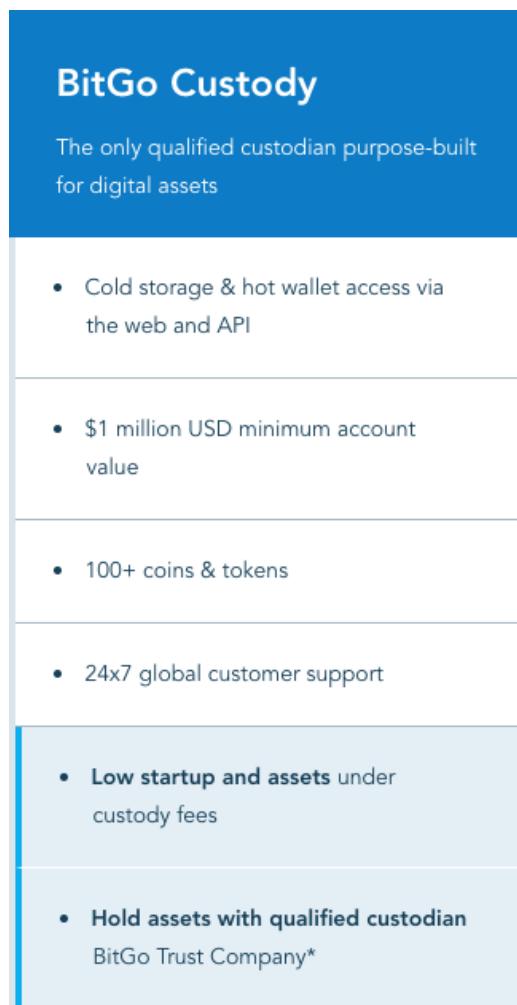


図3-6 BitGo Custodyのサービスプラン³¹

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らず、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

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

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

と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

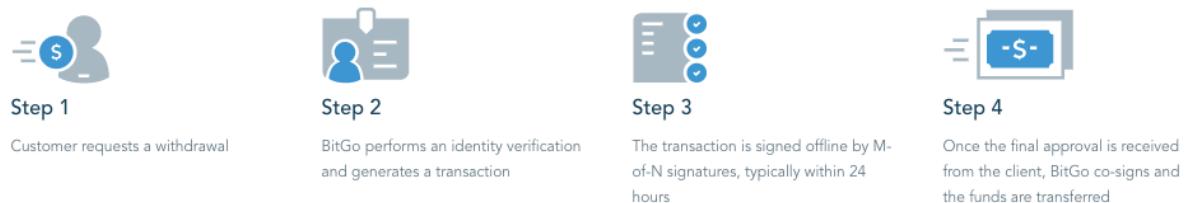


図3-7 BitGo Custodyの送金手順³²

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

IMPLEMENTATION FEE	\$0 – \$10,000 DEPENDING ON USE-CASE	PRICING INCLUDES
CUSTODY FEE	50 bps ANNUALIZED	<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
MINIMUM BALANCE	\$1,000,000	

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るとしている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 tezos

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。

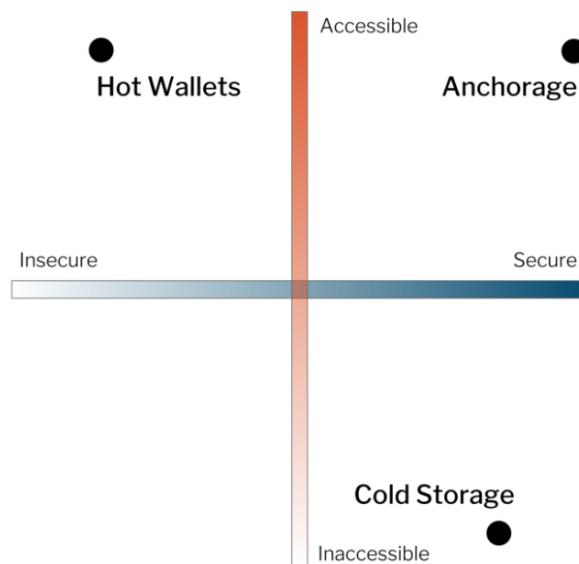


図3-13 利便性とセキュリティは独立して
おり、両立できるとする図⁴⁷

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。

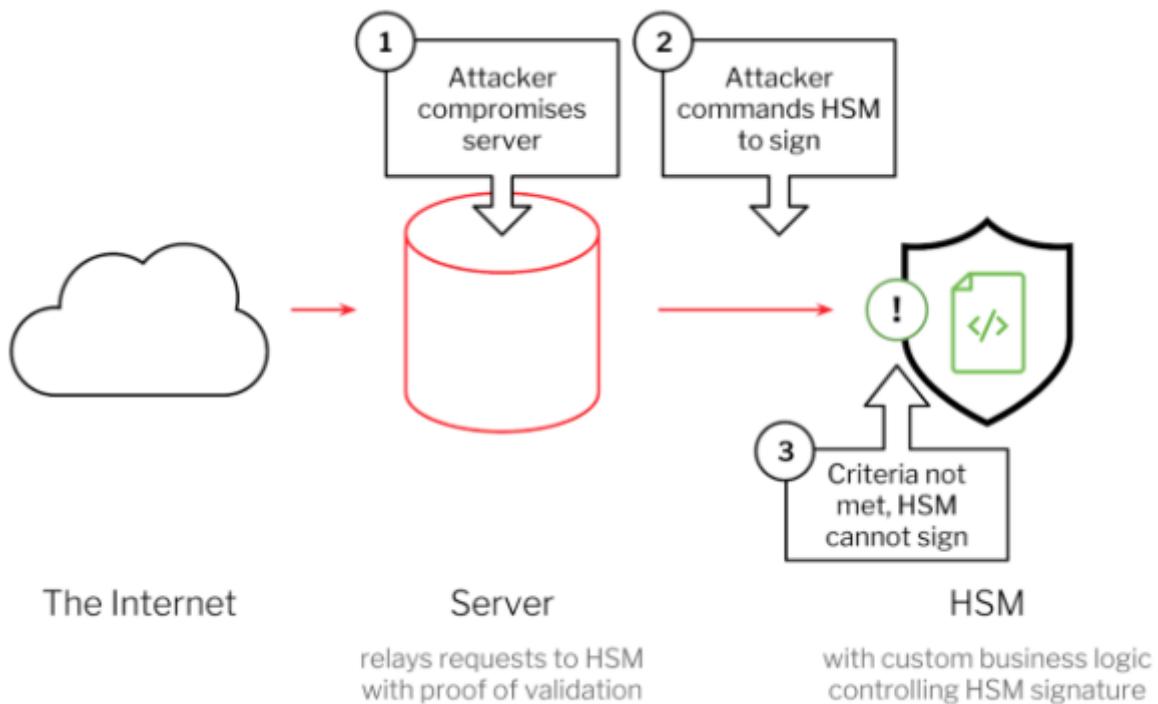


図3-14 内部で特別な制御をしているAnchorageのHSMを用いたシステム⁴⁸

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ない。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ある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。

3.4 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ない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ない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る。

3.5 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あるもの」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⁴⁹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な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あるものと考えられ、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。

⁴⁹ 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>