ADD VNTR.

MPCで安全性と利便性を両立した企業向けウォレット

MACNICA | 兎号屋

Table of Contents

1 はじめに P.3

2 WaaS(Wallet as a Service)について P.4

3 MPCとは P.7

4 Fireblocksの紹介 P.9

5 まとめ P.12

1. はじめに

グローバルプラットフォーマーによる個人情報の一元管理の弊害を認識し、自らの情報を主体的に管理したいという人々の声は日に日に高まっています。分散型という特徴を持つブロックチェーン技術が支える Web3 の時代に突入し、従来のプラットフォームに依存しない非中央集権的なデジタル経済圏を構築し、取引コストの削減、国境やプラットフォームを超えた価値交換、そして新たなビジネスモデルや社会課題解決への道を切り開き、新しいデジタル経済圏を目の当たりにしていくことでしょう。

しかし、安全性と利便性を両立させることなくして、社会実装は不可能です。トークンセキュリティへの脅威は、真の Web3 社会の実現を阻む最大の壁となるでしょう。

私たちは、これら新たなデジタル資産のセキュリティ担保のための戦略的な取り組みが急務であると考えています。このホワイトペーパーでは、 Web3 という新たなフロンティアでの安全性と利便性のバランスをどのように達成し、個人の価値を守りながら社会全体の利益を最大化するかについて探求していきます。

2. WaaS(Wallet as a Service)について

暗号資産、トークン、Web3。これらの言葉は、もはや未来創造や小説の中の話ではなく、現実のものとなっています。技術の急速な発展に伴い、顧客からの暗号資産の預かりや、企業自身による暗号資産の保有が増加し、トークン型社会への移行はもはや待ったなしの状況にあるとも言えます。

トークン型社会におけるトークンの例

- **セキュリティトークン**
  企業の株式や債券などをトークン化したもの
- **合同会社型 DAO（通称トークン式会社）**
  自社発行トークンを用いて運営される新しい形態の会社
- **ステーブルコイン・CBDC（中央銀行が発行するデジタル通貨）**
  法定通貨に連動した価値を持つデジタル通貨
- **RWA（リアルワールドアセット）**
  不動産、カーボンクレジット、IoT デバイスなど、現実世界の資産をトークン化し、FT / ST / NFT などを権利証として用いる
- **NFT（Non-Fungible Token）**
  デジタルアートや音楽作品など、唯一無二の価値を持つトークン
- **株の代わりにトークン投資**
  トークンを用いて企業に投資する新しい投資形態

このようなトークン型社会の広がりと共に、企業はトークンを保持するニーズが顕著に高まっており、多くの企業にとって新たなビジネスチャンスとなっています。しかし、その一方でこれらのトークンは、従来の金融商品とは異なる特性を持ち、新たなリスクも伴います。例えば、ハッキングによる盗難や、価格変動による損失などです。トークン型社会への移行は、企業にとって大きなチャンスであると同時に、大きなリスクを伴うのです。

このような背景の下、企業が直面する主要な課題は、これらの暗号資産を安全かつ効率的に管理する方法をいかに確立するかという点です。安全性と利便性を両立させた企業向けの WaaS（Wallet as a Service）の構築が急務となっており、それには先進的なセキュリティ対策とリスク管理戦略が求められます。トークン型の DX された社会では、暗号資産に関するセキュリティの重要性が一層強調され、企業がこれらの資産をどのように安全に管理し、高度なセキュリティ基準とプライバシー保護を確立することが必要不可欠になります。このような戦略を実施することで、トークンを活用する新しいビジネスモデルやサービスの可能性を最大限に引き出すことが可能となります。

トークン管理における課題

01 複数人に属するウォレットの管理の難しさ

企業が自社資産や顧客資産を管理する場合は、個人で暗号資産を管理する場合とは違い、その資産が複数人に属するという決定的な違いがあります。複数人に属するウォレットの管理においての単一秘密鍵での管理の問題のうち大きなものとして、秘密鍵の管理責任リスクと秘密鍵の保管リスクの 2 つが存在します。

1 つ目の管理責任リスクは、管理する資産の性質とその管理の手法との乖離に起因します。個人の場合ではウォレットの秘密鍵を本人が管理していればその管理責任は単にその個人が負うことになりますが、複数人に属する資産を単一の人間が管理することは管理責任的な観点から好ましくありません。単一秘密鍵で管理し、単一の人間がその資産を移動できるということは、その資産が複数人に属するものであるということを表現できていないとも言えます。その具体的なリスクとしては、一担当者による持ち逃げや担当者が不在の場合のオペレーションの停止などが挙げられます。

2 つ目の保管リスクにはハード面とソフト面の 2 種類があります。ハード面では秘密鍵を保管する端末（ハードウェアウォレット等）の故障・紛失・盗難リスク、ソフト面では保管端末に対するハッキングによる秘密鍵の流出リスクがあり、このどちらもが単一秘密鍵での管理の場合、一度で資産の流出や紛失を引き起こすこととなります。

このようなリスクを防げないことから単一秘密鍵での資産管理は複数人向けウォレットにおいては不適であり、秘密鍵管理をどう多元化・冗長化していくのかが重要となります。

02 従来の主流 マルチシグの問題点

単一秘密鍵管理問題に対する従来の解決策が、マルチシグという技術でした。

マルチシグは資産管理の各担当者が別々に作成した秘密鍵をもとにウォレットを作成し、決められた数の担当者（秘密鍵）の署名が集まって初めてそのウォレットから送金が行えるような仕組みです。例えば 3-of-4（全部で 4 つの秘密鍵が存在し、そのうちの 3 つの秘密鍵からの署名を組み合わせれば送金できる状態）のマルチシグでは、4 つの秘密鍵のうち 1 つの秘密鍵が紛失した場合でも送金は行え、4 つのうち 2 つまでの秘密鍵の流出であれば資産が盗まれる心配もありません。

このようにマルチシグは単一秘密鍵管理によるリスクを排除することには成功しましたが、それに伴い以下のようなデメリットも存在しました。

マルチシグのデメリット

デメリット 1 担当者の変更時に**毎回ウォレットアドレスの変更**が必要になる可能性がある

デメリット 2 **全てのブロックチェーンで対応されているわけではない**
（チェーンの種類によってはプロトコル依存となる）

デメリット 3 マルチシグの方式が**ブロックチェーンによって違う**

これらの利便性低下の問題の解決に使われるのが、 MPC という技術になります。

3. MPCとは

MPC は、簡易に訳すと、マルチパーティ計算といいます。MPC とは複数の主体がそれぞれの秘密情報をお互いと共有することなく共同で計算問題を解くことができるという技術です。対象となる計算問題自体は各自が単独で解くことはできない性質のものにもかかわらず、お互いの秘密情報を隠したまま協力して計算を行うことができます。

MPC の技術を署名に応用したものの 1 つに TSS (閾値署名) というマルチシグに性質が似た技術があります。

01 一部のキーシェアでの署名が行える TSS（閾値署名）

TSS は MPC の 1 種で、いくつかのキーシェア（Key shares, 鍵の断片のようなもの）のうち、決められた数のキーシェアによって作成された署名を組み合わせることにより、有効な署名を作成することができる技術です。これによってトランザクションの作成時に各キーシェアで作成した分散署名を組み合わせることによって、元の秘密鍵によって署名されたのと同等の署名を作成することができます。この時各々のキーシェアを一箇所に集めることなく、バラバラに分散署名を作成することができるため、署名時に秘密鍵自体が作成されることはありません。

また、Fireblocks の MPC-CMP では最初のキーシェアの作成時に元々存在する秘密鍵からキーシェアを分割するのではなく、各キーシェアをバラバラに作成してからアドレスを作成します。つまりキーシェアの作成時からトランザクションの署名までのどのタイミングにおいても秘密鍵自体が生成されることがないため安全性が高いと言えます。

02 マルチシグと比べた MPCの 3つの利点

マルチシグと比べた MPC の利点の 1 つとしては、運用上の柔軟性が高いことがあります。マルチシグでは署名に使用する秘密鍵を変更したい時（ウォレット管理の担当者が異動になった時など）に毎回アドレスを再生成する必要があります。その一方 MPC では、元のアドレスを変更することなく新しいキーシェアを作成することが可能です。何らかの運用上の変更があった場合に毎回アドレスが変更されてしまうのは運用自体をより煩雑にするため、このような MPC の特徴は大きな利点といえます。

2 つ目の利点はプロトコルに依存しないことです。MPC ではトランザクションの署名の作成自体をオフチェーンで分散的に行えるため、ブロックチェーンによって対応できないということが起こりません。例えば Fireblocks の MPC は ECDSA および EdDSA 署名に対応しているため、現状存在するブロックチェーンのほぼ全てに対応していることになります。

3 つ目の利点としてはトランザクション手数料が安くなることがあります。多くのマルチシグ署名においては各々の秘密鍵がオンチェーンで署名を行うため、通常のアドレス（シングルシグ）における署名に比べてトランザクション手数料が高くなります。MPC の場合は署名の作成はオフチェーンで行われるため、通常の署名と変わらない手数料でトランザクションを発行することができます。

4. Fireblocksの紹介

Fireblocks は、 MPC-CMP という暗号技術と多層のセキュリティ施策によって、 安全性と利便性を兼ね備えた企業向けセミカストディアルウォレット（顧客の管理方法によってカストディアルにもノンカストディアルにもなり得るウォレット）を提供しています。

Fireblocks におけるセキュリティは複数の層によって構成されており、主なものとしては以下の 3 つの項目があります。

01 **MPC-CMP での単一障害点の排除**

02 **TEE を利用した鍵管理や権限システムのハードウェアレベルでの分離**

03 **トランザクション作成時の権限管理システム (Automated Policy Engine)**

01 MPC-CMP での単一障害点の排除

Fireblocks で利用されている MPC-CMP は 2020 年に Fireblocks の研究開発チームにより開発されたオープンソースの MPC プロトコルです。トランザクションを署名する際にキーシェアの間で 6 ～ 9 周の通信が必要だった従来の MPC に比べて、この技術では 1 周分の通信で良いことから（厳密には 4 周の通信が必要ですが、3 周分は事前処理が可能）発表当時で従来の 8 倍程度の速度向上が行われました。

Fireblocks では 3-of-3 のキーシェア（3 つ存在するキーシェアの全ての署名を組み合わせることによって有効な署名の作成が可能）を用いてウォレットを作成します。具体的には 3 つのキーシェアのうちの 2 つが Fireblocks 管理下のクラウド上の TEE（信頼された実行環境 , 詳細は後述）内に存在し、残りの一つはユーザーが管理を行います（SaaS モデルの場合）。

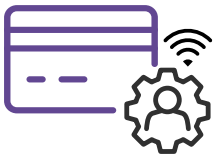
前述の通り、ウォレットの生成時やトランザクションの署名時において 3 つの鍵が一箇所に存在することなくバラバラに秘密計算を行うため、通常の運用時に秘密鍵が生成され単一障害点となることはありません。

また、3 つのキーシェアのうちの一つはユーザー側のみにしか存在しないため、Fireblocks が単独で顧客資産を引き出すことは不可能な仕組みとなっています（一方ユーザー側には秘密計算を用いて生成されたキーシェアのバックアップは用意されるため、ユーザーのみが実際にウォレットにアクセスすることができます）。 Fireblocks 管理下の 2 つ

のキーシェアはクラウド上にありホット環境に存在しますが、３つ目のユーザー管理のキーシェアについては以下のようにユーザーが管理方法をカスタマイズすることでウォレット全体の性質を変更することができます。

ホットウォレット

インターネット接続下にあり送金などが自動化されたウォレット



ウォームウォレット

インターネット接続下にあるが送金に人間が介入するウォレット

コールドウォレット

インターネットに接続されていない環境で管理されるウォレット

例：https://www.macnica.co.jp/business/security/solution/web3security/

ユーザーと Fireblocks の 2 者でキーシェアを管理する運用体制によってキーシェアの管理が多様化し、外部からの攻撃に対する耐性が増していると言えます（キーシェアの地理的分散やユーザー側では難しい TEE 下でのキーシェアの運用が可能になる）。

02 TEEを利用した鍵管理や権限システムのハードウェアレベルでの分離

TEE とは内部のプログラムや記録が外部から読み取ったり改竄したりできないような性質（耐タンパ性）を持った、システムから隔離された実行環境のことです。TEE 内ではあらかじめ定められたアルゴリズムによる処理を外部から観測されることなく行うことができ、内部の機密情報が流出することもありません。

Fireblocks におけるクラウド管理の 2 つのキーシェアは TEE 内部に保存されているため、万が一ハッキングなどのクラウド内部への侵入があったとしてもキーシェア自体は盗まれません。これはクラウドサービスの管理者や Fireblocks の従業員に関しても同様となります。キーシェアだけではなくユーザーの権限やトランザクションの管理システムも TEE 内部に存在しており、クラウド内の OS からは権限やアルゴリズムの書き換えは不可となっています（ただし厳密に言うと TEE 自体を信頼できた上での話となります）。

03 トランザクション作成時の権限管理システム (Automated Policy Engine)

キーシェアと同様に TEE 内部に存在しているトランザクション発行時の権限管理システムでは、ユーザー側に複数の役割が存在します。

トランザクションの **開始者**	トランザクションの **承認者**	トランザクションの **署名者**
発行したい TX を **提案するユーザー**	提案された TX を **承認するユーザー**	ユーザー側のキーシェアを 保持し実際に部分署名を **作成するユーザー**

これら 3 つの役割の管理者がトランザクションの作成時に多重に審査を行うことで、1 人の管理者でトランザクションの作成が行えないような仕組みになっています（トランザクションの開始者と承認者は Fireblocks 管理下のキーシェアを間接的にコントロールしていると言えます）。また、複数存在する署名権限を持ったメンバーのキーシェアは全て別々のものとなっており、各自がキーシェアを紛失した場合でも秘密計算を用いて新たなキーシェアを作成することが可能です（暗号化されたバックアップも Fireblocks のクラウド上に存在されます）。

このような機能向上によって、数分単位でのキーシェアの自動更新やコールド環境下での署名といった機能も追加されました。中でも MPC を使ったコールド環境下での署名は各国のカストディ規制下においても重要な機能と考えられます。

5. まとめ

複数人管理のウォレットの重要性が増す中、従来のマルチシグではなく MPC という技術を利用することにより Fireblocks は柔軟性や冗長性の高いウォレットシステムを提供しています。

MPC だけではなく TEE などの多層のセキュリティによって資産の安全性を高める Fireblocks は、MPC-CMP 技術のオープンソース化や内部システムの監査（SOC 2 の取得や定期的な侵入テスト）を通してサービスの透明化と信頼性の向上にも努めています。

企業向けの他にも Fireblocks は to C 向けのノンカストディアルウォレットを提供するサービスの展開を開始しており今後に注目です。

また秘密鍵を分散しかつそれぞれを 1 箇所に集めることなく署名を行い、鍵の一部を紛失した場合にも復旧が比較的簡易な MPC という技術は暗号資産やプライバシー技術の発展により、今後ますます使われていくことになるでしょう。

参考文献

- **Fireblocks Direct Custody Principles | Fireblocks**
  https://www.fireblocks.com/principles/
- **MPC vs. Multi-sig | Fireblocks Blog**
  https://www.fireblocks.com/blog/mpc-vs-multi-sig/
- **Introducing MPC-CMP: Pushing MPC Wallet Signing Speeds 8X | Fireblocks Blog**
  https://www.fireblocks.com/blog/pushing-mpc-wallet-signing-speeds-8x-with-mpc-cmp-9/
- **Fireblocks' MPC-CMP code is Open-Source | Fireblocks Blog**
  https://www.fireblocks.com/blog/fireblocks-mpc-cmp-code-is-open-source/
- **秘密分散 /MPC, TSS 等 | questryio**
  https://scrapbox.io/questryio/ 秘密分散 %2FMPC,_TSS 等
- **違いは何？ HSM, TPM, セキュアエンクレーブ , セキュアエレメント | wolfSSL**
  https://wolfssl.jp/wolfblog/2022/03/08/difference-hsm-tpm-secure-enclave-secure-element-hardware-root-trust/

- **ETHERSECURITY PACIFIC HOLDINGS PTE. LTD.**（本社:シンガポール、代表取締役:加門昭平）及びその 100%子会社である株式会社イーサセキュリティ（本社：東京都渋谷区、代表取締役：加門昭平、紫竹佑騎）の協力にて作成

お問い合わせ

株式会社マクニカ
合同会社　暗号屋

add-venture@macnica.

https://www.macnica.co.jp/business/security/solution/

- 本ホワイトペーパーに掲載されております社名および製品名は、各社の商標および登録商標です。
- 本資料は、出典元が記載されている資料、画像等を除き、弊社が著作権を有しています。
- 著作権法上認められた「私的利用のための複製」や「引用」などの場合を除き、本資料の全部または一部について、無断で複製・転用等することを禁じます。・本資料は作成日現在における情報を元に作成されておりますが、その正確性、完全性を保証するものではありません。