2024 年 3 月 6 日

各 位

株式会社大和証券グループ本社
大和証券株式会社
Fintertech 株式会社
株式会社 Ginco

大和証券グループと株式会社 Ginco による、国内初[1]のパブリックチェーン[2]におけるセキュリティトークンの発行及び発行プラットフォーム開発に向けた概念実証の検証結果について

株式会社大和証券グループ本社（本社：東京都千代田区、執行役社長 中田誠司、以下「大和証券グループ本社」）、大和証券株式会社（本社：東京都千代田区、代表取締役社長 中田誠司、以下「大和証券」）、Fintertech 株式会社（本社：東京都千代田区、代表取締役社長 相原一也、以下「Fintertech」）及び、株式会社 Ginco（本社：東京都中央区、代表者 森川夢佑斗、以下「Ginco」）は、国内初のパブリックチェーンにおけるセキュリティトークン（以下「ST」）の発行及び、発行プラットフォームの開発に向けて、概念実証（以下「本 POC」）を行いましたので、その検証結果についてご報告いたします。

1. 本 POC の概要

2023 年 11 月 30 日に公表しました通り、大和証券グループ本社及び大和証券、パブリックチェーンを活用した金融システム構築に精通する Fintertech 及び Ginco は協同し、下記の要領で本 POC を実施いたしました。

本 POC における各社の役割

参加企業	POC における役割
大和証券グループ本社	社債 ST の発行
大和証券	本 POC の統括、プランニング、検討内容の整理・確定
Fintertech	ソウルバウンドトークン[3]（以下 SBT）の発行 本 POC における技術的なアドバイス・検証
Ginco	本 POC におけるシステム環境の構築 本 POC における技術的なアドバイス・検証

[1]パブリックチェーン上で電子記録移転有価証券表示権利等が発行されたのは国内初

[2] 特定の管理主体を置かず、不特定多数の自由な参加者により合意形成を行うブロックチェーンであり、ビットコインやイーサリアムが代表例

[3] ソウルバウンドトークンとは譲渡不可能なトークン。保有する本人の証明等に活用されることを期待されている

① 本 POC に用いるスマートコントラクトの開発・公開

本 POC の実施に先立ち、Fintertech ならびに Ginco は、本 POC で利用する ST と SBT の発行を行う、スマートコントラクトを実装し、パブリックチェーンであるイーサリアム上に公開しました。

② SBT の付与

ST の発行に先立ち、Fintertech は、イーサリアム上に用意された投資家 2 名（以下「投資家 A」「投資家 B」）のアドレスに対して、SBT を付与しました。

③ ST の募集

2024 年 2 月 19 日に、大和証券グループ本社が ST の条件決定を行い、投資家 A に対して募集を行いました。翌 2 月 20 日を払込日・発行日として、イーサリアム上にて、ST を発行しています。

④ ST の移転

投資家 A は投資家 B に対して、ST の売却・移転を行いました。投資家 A 及び投資家 B のアドレスには、ともに SBT が付与されているため、投資家 A の指示に基づき、ST は投資家 B に移転されました。

⑤ ハッキング実験その 1

投資家 B の秘密鍵[4]がハッカーに盗まれたと仮定し、投資家 B の保有する ST について、別途用意したハッカー役のアドレスへの移転指示を行いました。ハッカー役のアドレスには SBT が付与されていないため、ST は移転されないことが確認できました。

⑥ ハッキング実験その 2

次に SBT の発行体である Fintertech の秘密鍵がハッカーに盗まれ、SBT コントラクトのオーナー権限[5]により、ハッカー役のアドレスへ SBT の付与を行うケースについて検証しました。

SBT の付与がオーナー権限で行われたことは Fintertech から確認できるため、Fintertech は自社の秘密鍵が盗まれている事実を認識することができます。

こうした事実を把握した Fintertech は、オーナー権限により SBT コントラクトを無効

---

[4] 公開鍵暗号方式において、対応する公開鍵で暗号化された情報を復号する際に利用する文字列のこと。暗号資産の領域では、そのトークンの所有者であることを証明するデータを意味し、これを盗まれると自身のトークンが自由に移転されるリスクがある

[5] イーサリアム上での SBT の発行を管理するプログラム(いわゆるスマートコントラクト)を、ここでは「SBT コントラクト」としている。Fintertech は「SBT コントラクト」のオーナーであり、保有する秘密鍵によりオーナー権限がある。この POC では、その秘密鍵がハッカーに盗まれ、ハッカーがオーナー権限で SBT を付与している

化することができることを確認しました。そのうえで、新たな SBT コントラクトを用意し、当該新 SBT が移転可能なアドレスを表すものであることを、投資家及び発行体に周知したうえで、改めて投資家 A 及び投資家 B に当該新 SBT を付与できることを確認しました。

Fintertech からの連絡を受け、発行体である大和証券グループ本社はオーナー権限により、ST コントラクトにおける移転を可能とする SBT の一覧から、無効化された SBT を除くとともに、新 SBT を追加し、新 SBT を有する投資家のみが ST の売買が可能になるように変更を行えることを確認しました。

⑦ ハッキング実験その 3

投資家 B の秘密鍵を盗んだハッカーが、投資家 B の保有する ST について、投資家 A のアドレスへの移転指示を行うケースを検証しました。

投資家 A 及び投資家 B のアドレスにはハッキング実験その 2 で新たに付与された SBT があるため、ST は移転されました。

投資家 B は、保有する ST が移転されたことに気が付き、発行体である大和証券グループ本社へ連絡することで、大和証券グループ本社は、投資家 B の秘密鍵が盗まれている事実を認識しました。

そこで大和証券グループ本社はハッキングの事実を Fintertech へ連絡し、Fintertech は SBT コントラクトのオーナー権限により、投資家 B の SBT を無効化しました。

さらに、大和証券グループ本社は ST コントラクト[6]のオーナー権限により、不正に移転された ST について、投資家 A から投資家 B のアドレスに強制移転を行うことで、ハッキング前の状況に戻すことができることを確認しました。

なお、投資家 B の SBT を無効化後は、投資家 B からの ST の移転指示が反映されないことも確認しております。

⑧ ハッキング実験その 4

発行体である大和証券グループ本社の秘密鍵がハッカーに盗まれ、ST コントラクトのオーナー権限により、ST について、投資家 B から投資家 A への強制移転が行われたケースについて検証しました。

オーナー権限にて強制移転が行われたことは大和証券グループ本社から確認できるため、自社の秘密鍵が盗まれている事実を認識することができます。

こうした事実を把握した場合、大和証券グループ本社は、オーナー権限により ST コントラクトを無効化することができることを確認しました。さらに、新たな ST コントラクトを用意し、当該新 ST が社債の保有状況を表すものであることを投資家に周知し

[6] 注記 4 と同様に、イーサリアム上での ST の発行を管理するプログラムを、ここでは「ST コントラクト」としており、当該コントラクトのオーナーは発行体である大和証券グループ本社である。

たうえで、改めて投資家 B に当該新 ST を付与できることを確認しました。

⑨ 新たな SBT 下での、新たな ST の移転

⑦で入れ替えた新たな ST、SBT を用いた移転が可能かを確認するため、投資家 B は投資家 A に対して ST の売却・移転を行いました。

⑩ 償還

2024 年 2 月 28 日に ST は償還されたため、発行体である大和証券グループ本社は、オーナー権限により ST コントラクトを無効化しました

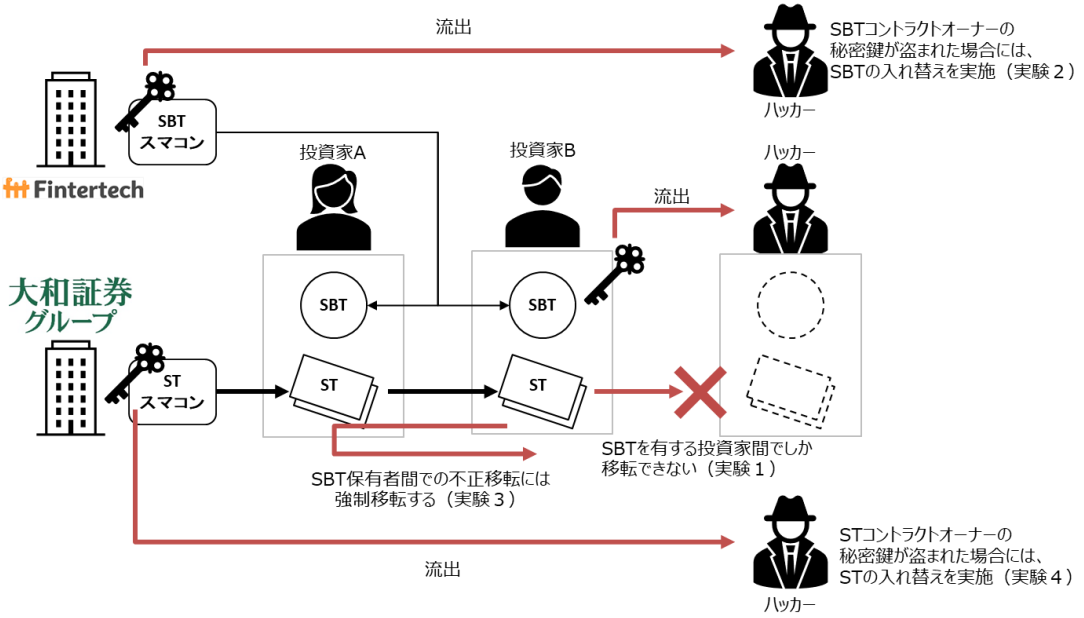
本 POC で利用した ST 及び SBT のスマートコントラクトは以下になります。

	スマートコントラクトのアドレス
当初発行 ST	0x28C7f48f5eafd3C95fb475192eCEd4AAa62B3Ed0
入替後の 新 ST	0x295b14EaCb0110368Af4d8DE0c7556dA4Ca592F8
当初発行 SBT	0x6f17f8DE8f1B8a0fb5513B4ca513093F1C1d56eE
入替後の 新 SBT	0xF0CB3B45F3a5C2E49ad9FAEb65Df79Db890554Ea

2. 本 POC による成果

本 POC において、ST は SBT が付与された投資家間でしか移転できない設計とし、これによってハッキングによる秘密鍵の流出時にも ST の不正な移転ができない設計としました。そのうえで、下記のハッキング実験を行っています。

	盗まれた秘密鍵	実験により確認したこと
ハッキング実験その 1	投資家の秘密鍵	不正な移転を SBT で制限することが可能か
ハッキング実験その 2	SBT 発行体の秘密鍵	SBT のオーナー権限で SBT を不正に付与された時に、ハッキング前の状況に回復可能か
ハッキング実験その 3	投資家の秘密鍵	SBT を保有している同士で不正な移転が起きたときにハッキング前の状況に回復可能か
ハッキング実験その 4	発行体の秘密鍵	ST のオーナー権限で ST を不正に付与された時にハッキング前の状況に回復可能か



ハッキング実験その 1 を行った結果、SBT の活用がハッキングによる不正移転防止に、一定の有効性を持つことを確認できたと言えます。

ハッキング実験その 2 では、SBT コントラクトのオーナーの秘密鍵がハッキングされ、ハッカーのアカウントに SBT が付与されるケースにおいても、その SBT コントラクトを無効化し、新たな SBT を付与することで、ハッキング前の状況に戻すことが可能であることを示すことができました。

ハッキング実験その 3 では、不正な移転先が SBT を有する場合には、SBT のみでは不正な移転を防ぐことはできないことも確認いたしました。こうした場合においても、オーナー権限による SBT の無効化及び、ST の強制移転によりハッキング前の状況に戻すことが

可能であることも確認できました。

ハッキング実験その４では、STコントラクトのオーナーの秘密鍵がハッキングされ、ハッカーにより ST の強制移転が行われるケースを検討しましたが、こうした場合においても、そのSTコントラクトを無効化したうえで、新たなSTを付与することで、ハッキング前の状況に戻すことが可能であることを示すことができました。

ビットコインやイーサリアムといった暗号資産では中央集権的な管理組織が存在しないことから、ハッキングによる不正な移転が行われた際に元の状況に戻すことは非常に困難です。

しかし、ST においては発行会社や証券会社、SBT の付与者等が連携し、スマートコントラクト等を用いて管理することで、不正な移転が行われたとしても、ハッキング前の状況に戻すことが可能であることを示せたと言えます。

3. パブリックチェーンとパーミッションドチェーン[7]との比較

現時点で、国内で発行された ST は、主にパーミッションドチェーン上で発行されています。こうしたパーミッションドチェーンと今回の POC で利用したパブリックチェーンを比較すると以下のようになります。

	パーミッションドチェーン	パブリックチェーン
代表例	Progmat、ibet	ビットコイン、イーサリアム
スケーラビリティ（処理速度）	一般にパブリックチェーン対比で処理速度は速い	一般にパーミッションドチェーン対比で処理速度は遅い
ガス代[8]	一般に、パブリックチェーン対比でガス代は安い	一般にパーミッションドチェーン対比でガス代は割高になる
プライバシー	外部に公開されていないため、プライバシーが保たれる	透明性が高く、取引状況等が公開される
セキュリティ	限定された管理者に対し攻撃すれば足りるため、パブリックチェーン対比で、セキュリティのリスクは高いとされる	攻撃には、攻撃者が相当のリソースを持つ必要があり、パーミッションドチェーン対比でセキュリティが堅固とされる
インターオペラビリティ	パブリックチェーンとの連携にはクロスチェーン技術[9]を利用	同一のパブリックチェーン内であれば、クロスチェーン技術は不要

[7] あらかじめ限定された参加者により合意形成を行うブロックチェーンのこと

[8] ブロックチェーンにおいて、取引の実行やブロックチェーン上のプログラムに処理時に必要となる手数料のこと

[9] 異なるブロックチェーン同士を接続する技術のこと

パーミッションドチェーンは、パブリックチェーンと比較し、スケーラビリティやガス代、プライバシーなど利点があります。

一方、パブリックチェーンは、セキュリティ面が堅固である他、暗号資産やNFTといった既存のパブリックチェーン上に存在するトークンとの相互運用性が高いと言えます。そのため、パブリックチェーンにおいて日々進化するエコシステムの活用が容易であり、そのダイナミズムを取りこみやすい点が利点であると言えます。

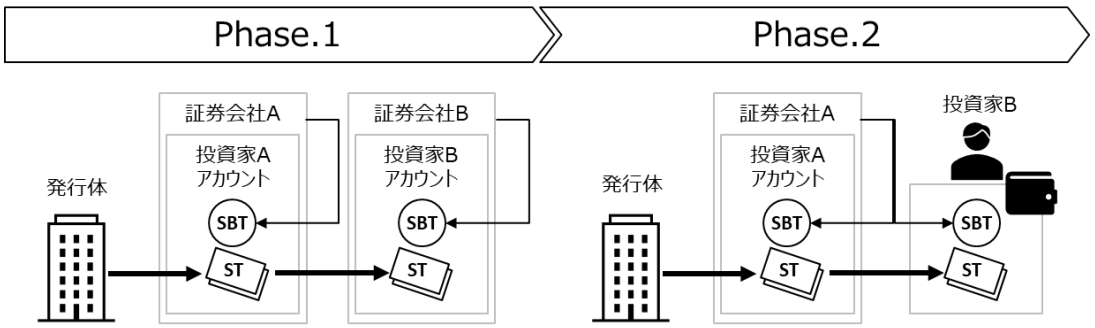
例えば、パブリックチェーン上に発行された ST の保有者に対し、利払いや優待としてパブリックチェーン上で発行されたステーブルコインやNFTを付与するケースを考えてみると、付与されたステーブルコインやNFTもパブリックチェーン上に存在するため、パブリックチェーン上のサービスにおいて、直接利用することが可能です。

しかし、パーミッションドチェーンで同様の行為を行うと、付与されたステーブルコインやNFTはパーミッションドチェーン内にとどまるため、パブリックチェーンに広がるエコシステムに直接的に接続することは難しいと言えます。

4. 残された課題・今後の展望

本 POC では、発行体である大和証券グループ本社が投資家を勧誘し、証券会社による私募の取扱い・媒介等は行わず、保護預かりも行わない形式としました。今後、投資家の利便性を考え、証券会社による募集の取扱い、媒介、保護預かり等が可能な体制を整えることを検討しています（Phase1）。

また、将来的には、投資家のアンホステッドウォレット[10]の利用を認める場合（Phase２）についても検討していく方針です。Phase２では、証券会社保護預かりの口座から、アンホステッドウォレットに移転する際に、犯罪による収益の移転防止に関する法律における取引時確認を適切に実施できるかが論点となります。こうした際にどのような対応が考えられるかは、ステーブルコインの移転を行う電子決済事業者等取引業者において求められる措置などを参考にしながら、法制度の整備も含め、業界全体で検討していく必要があるものと考えます。



[10] 秘密鍵を、証券会社等に預けず、自身でウォレットアプリなどを用いて保管すること

Fintertech 株式会社について

Fintertech は、大和証券グループ及びクレディセゾンがそれぞれ創業来培ってきた金融ビジネスのノウハウを礎としながら、最先端のテクノロジーの活用や外部企業との連携により次世代金融サービスを機動的にかつ柔軟に創出することを目指しています。

主な事業として、暗号資産を活用した「デジタルアセット担保ローン」及び「デジタルアセットステーク（消費貸借）」、クラウド型応援金サービスの「KASSAI」、「未来をわかちあう投資」を提供する貸付型クラウドファンディングサービス「Funvest」を展開しています。

会社名	Fintertech 株式会社
所在地：	東京都千代田区一番町 5 番地アトラスビル 6 階
代表者	相原 一也
設　立	2018 年 4 月 2 日
事業内容	次世代金融領域における新たな金融サービスの創出、運営
企業 URL	https://fintertech.jp/

株式会社 Ginco について

Ginco は、「経済のめぐりを変えていく」をビジョンに掲げ、ブロックチェーン技術を活用し、企業の Web3 事業を支援する Web3 Development Company です。

2017 年の創業から Web3 業界の総合ディベロッパーとして、より早く、より安全に、より費用対効果高くブロックチェーンを活用するためのインフラを提供してまいりました。

Web3 サービス開発のための API&SDK サービス「Web3 Cloud」や、業務用暗号資産ウォレットを中心とする「Web3 SaaS」、コンサルティングなどのプロフェッショナルサービスなどの B2B 事業に加え、個人向けモバイルウォレットアプリ「Ginco」を提供するなど、Web3 の社会実装に向けて多角的に取り組んでいます。

会社名	株式会社 Ginco
所在地：	〒104－0032 東京都中央区八丁堀三丁目 27-4
代表者	森川夢佑斗
設　立	2017 年 12 月 21 日
事業内容	クラウド型ブロックチェーンインフラおよび、同インフラを利用した各種エンタープライズサービスの開発・運営・提供
企業 URL	https://ginco.co.jp/

以 上