日本総研
The Japan Research Institute, Limited

変化する日本の規制環境下で再考するブロックチェーン技術と金融システム

～アセットトークナイゼーションから暗号資産・DeFiプロトコルまで～

(株)日本総合研究所
先端技術ラボ

2026年3月5日

本資料に関するお問い合わせ 市原紘平 (ichihara.kohei@jri.co.jp)

日本総研
The Japan Research Institute, Limited

サマリ（1of2） -変化する日本の規制環境下で再考するブロックチェーン技術と金融システム-

- 広義のDeFiと狭義のDeFi
  - ✓ 分散型金融(DeFi)について、伝統的金融機関等とブロックチェーンエンジニア等の専門家との間では、認識する内容に差異がある。
  - ✓ 後者は、パブリックブロックチェーンに保存されたプログラム(=スマートコントラクト)で実行される金融的機能を指す。(狭義のDeFi)
  - ✓ 一方、執筆時点(2026年3月)では、金融業界などでは上記の内容(狭義のDeFi)まではあまり意識されておらず、暗号資産そのものや、既存の金融商品のトークン化(アセットトークナイゼーション)の領域を主としてDeFiが認識されている。

- アセットトークナイゼーションにより加速する金融業務の標準化と効率化
  - ✓ アセットトークナイゼーションは、共通基盤(≒統合台帳)に様々な金融商品を載せるという点に新規性があり、以下のような技術的進展が見込まれている。
  - ✓ 金融機能のモジュール化：
    - ➢ 伝統的金融機関が重厚長大なシステムで一枚岩的に提供してきたサービス全体が、モジュール(小機能単位)に分解される。
  - ✓ 金融機能の標準化：
    - ➢ 同レイヤーのモジュール同士が競争や共通化を進めることでモジュールの機能が最適化・標準化される。
    - ➢ また、レイヤー間の連携方式についても標準化が進む。
    - ➢ 標準化技術の多くはしばしばオープン化され、新規プレーヤーの参入に繋がる。

日本総研
The Japan Research Institute, Limited

サマリ（2of2） -変化する日本の規制環境下で再考するブロックチェーン技術と金融システム-

- アセットトークナイゼーションへ取り組む伝統的金融業界へ向け
  - ✓ アセットトークナイゼーションの本質は金融機能のモジュール化・標準化であり、一過性の流行としてではなく、バックエンドを含めた業務の最適化・効率化の観点も持って取り組むことが肝要ではないか。
  - ✓ 金融機能のモジュール化・標準化こそが本質であると捉えた時、「ブロックチェーン上にトークンという形式で情報を記録する」という構成が最適ではない要件も発生し得ると考えられる。
  - ✓ 既に相当に効率的な金融システムを国内に抱える日本の伝統的金融機関としては、上記観点と新興技術への積極的なキャッチアップの両立に基づく判断が求められる。*

- 暗号資産へ取り組む伝統的金融業界へ向け
  - ✓ 足許、日本国内では暗号資産に関する規制の大幅な方針転換が進んでいる。
  - ✓ 暗号資産を巡っては対極的な意見が存在。社会的価値を意識した事業設計が中長期的信用の醸成に繋がる。

- トークン化(デジタル化)対象資産の拡大へ向け
  - ✓ 現行の法制下で紙の券面発行が前提となりデジタル化の障害となっているものについては、法改正等により解消されることが望まれる。(券面不発行や原簿への記録による第三者対抗要件の具備等)

*『すでに密集した状況にコンポーネントを追加することで、意図せず新たな複雑さをもたらす可能性』について「ASAP: デジタル資産プラットフォームの概念モデル」(p.19)でも指摘されている。

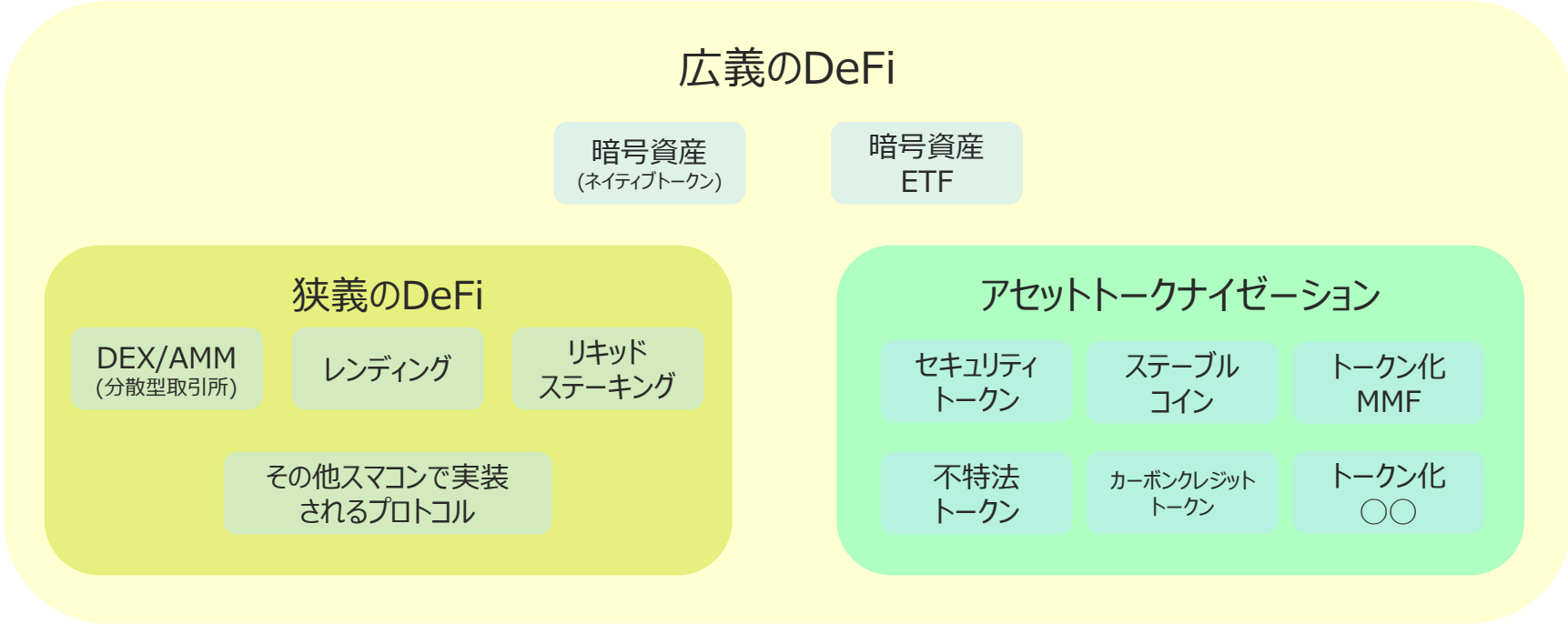
日本総研
The Japan Research Institute, Limited

目次 -変化する日本の規制環境下で再考するブロックチェーン技術と金融システム-

1章
分散型金融(DeFi)の登場と
既存の金融業務へのブロックチェーン技術導入の動き

1.1 広義のDeFiと狭義のDeFi

- ブロックチェーン技術自体が送金を目的としたビットコインと共に広まったものだが、これに加えスマートコントラクト(スマコン)、すなわち、ブロックチェーンに保存したプログラムを用いて様々な金融機能を実現しようとする動きとして分散型金融(DeFi)が登場した。
  - ブロックチェーンエンジニア等の観点では、スマコンによる種々の金融機能・プロトコルをDeFiと捉えることが多い。(狭義のDeFi)
- 一方、暗号資産には規制等もあり距離のあった既存金融事業者にも、効率化等を企図しブロックチェーンを導入する動きがある。
  - 既存金融事業者側は、暗号資産そのものや、ブロックチェーンを使って既存の金融商品等を「トークン化」するアセットトークナイゼーション(asset tokenization)も含めてDeFiを捉えることも多い。(広義のDeFi)



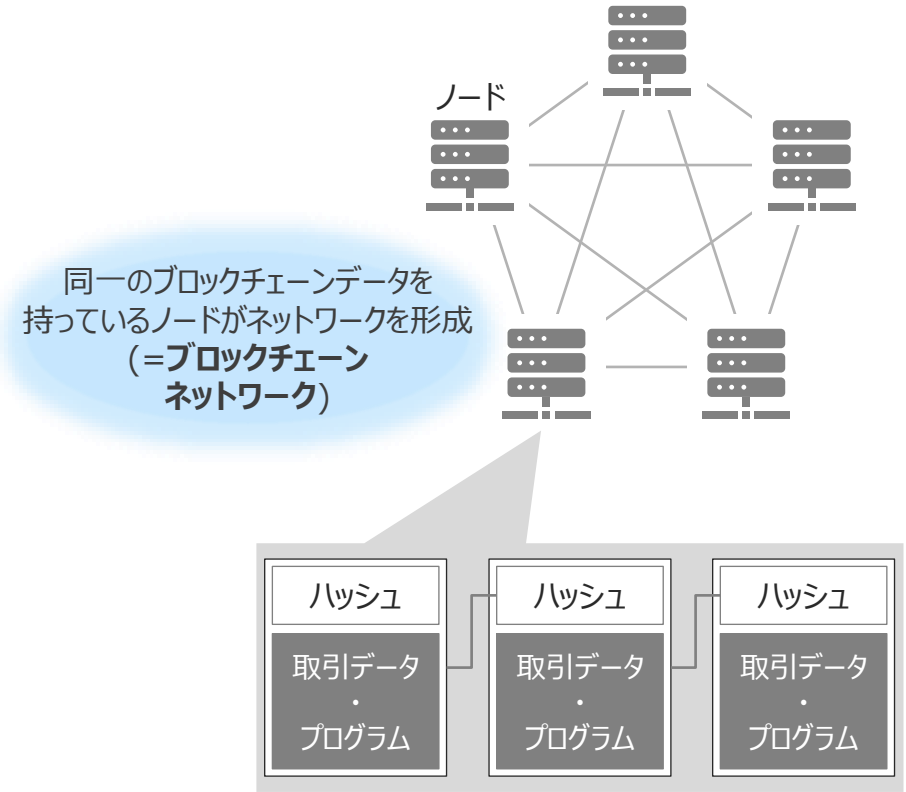
本レポートでは、ブロックチェーン技術(1章)、アセットトークナイゼーション(2章)、狭義のDeFi(3章)の順で解説する。

※筆者による肌感覚であり、定義を提案するものではない

1.2.1 ブロックチェーンとは？

- ブロックチェーンとは、データをブロックという単位でまとめてチェーン状につなげ、複数のノード*1で分散して保存する技術である。
  単一障害点を作らず、データの正しさを維持することができる。
- 現在では取引データ(数値の台帳上の付替え)のみならず、プログラムも保存できることが一般的。(「スマートコントラクト」と呼称)

ブロックチェーン・ネットワークのイメージと要素技術

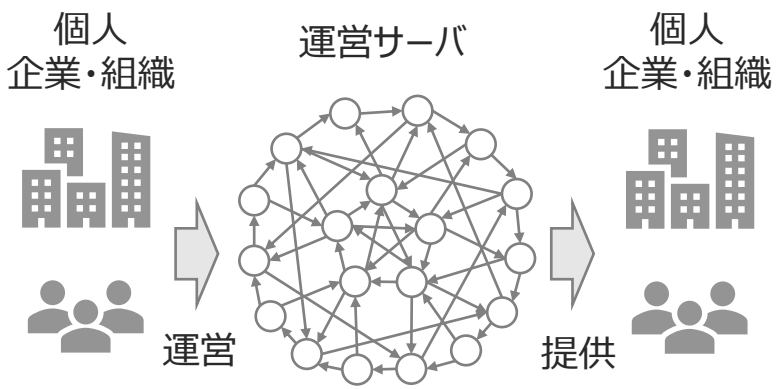
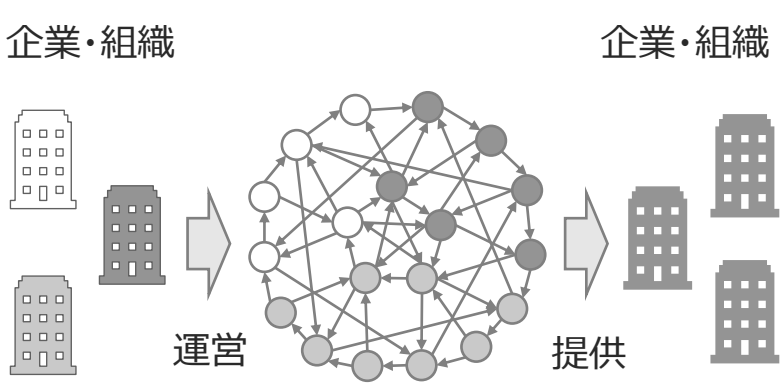


P2Pネットワーク (ネットワークの構造)	✓ 相互接続した複数のノードで、同じデータを共有。
電子署名、ハッシュ関数 (データの対改竄方式)	✓ 取引に用いる秘密鍵やアカウントアドレスは暗号学的に算出し、安全性を担保する。 ✓ ハッシュ値は小さなデータ容量となるため、軽量なデータで改竄されていないことを確認できる。
ハッシュチェーン (データの保存形式)	✓ データをブロックという単位にまとめ、過去のブロックに新しいブロックを追記する形式で保存する。 ✓ ブロックには前のブロックから固有に算出される値(ハッシュ値)を含める。過去データが変更されるとハッシュ値も変わるため、改竄が発覚する。 ✓ データの追加には全ノードの承認(コンセンサス)が必要なため、改竄が難しい。
コンセンサスアルゴリズム (データの正当性のルール) *2	✓ ノードが承認したデータをブロックチェーンに保存。 (*2:承認におけるルールこと)

*1 ブロックチェーンネットワークを構成するコンピュータやサーバ等。

1.2.2 パブリック型ブロックチェーンとプライベート型ブロックチェーン

- ビットコインなど、誰でも参加できる形で運用されているブロックチェーンをパブリック型ブロックチェーンという。
- 企業などでの用途に、参加者を制限した参加許可制のブロックチェーンをプライベート型 / コンソーシアム型ブロックチェーンという。
- 国内のセキュリティトークン(デジタル証券)は、プライベート型を利用。(運営企業の適切な運営に信頼を置くかたち。)

	パブリック型ブロックチェーン	プライベート型ブロックチェーン／コンソーシアム型ブロックチェーン
運営／利用者	不特定多数の個人や組織 	単一／特定少数の企業や組織 
データ	一般に公開されている	一部の参加者間でのみ共有
開発	オープンソースであり、誰でも参加できる	主となる開発企業が存在することが多い
例	• Bitcoin • Ethereum	• Quorum(クオラム) (Enterprise Ethereum) • Corda(コルダ) • Hyperledger Fabric

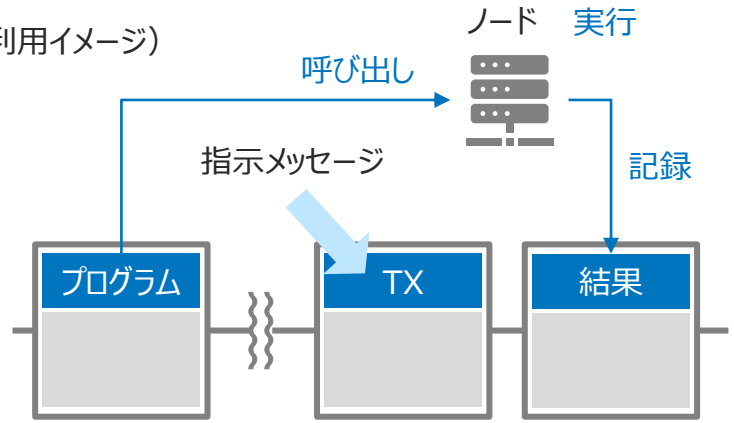
1.2.3 スマートコントラクトとは？

- ブロックチェーンにおけるスマートコントラクトとは、ブロックにプログラムを保存し、実行する技術。単にコントラクトやスマコンとも呼称。
- スマートコントラクトは「契約の自動執行」と誤訳されることがあるが、法的な契約を表すものではない。

概要

- ✓ スマートコントラクトとは、ブロックチェーンに保存されたプログラムを指す。
- ✓ 取引の指示などを記載したトランザクション(Tx)をブロックチェーンノードに送信し、プログラムを実行する。
- ✓ スマートコントラクトを利用してブロックチェーンにデータを記録するアプリを分散型アプリ(Dapp)と呼ぶ。
- ✓ スマートコントラクト機能をもつブロックチェーンの中ではEthereumの活用が最も進んでいる。(派生した各チェーン含む)

（利用イメージ）



メリット・デメリット

メリット

- ✓ スマートコントラクトの処理内容はブロックチェーンで確認できるため、公開されているソースコードと突合し、処理の正しさを検証できる。
- ✓ 取引データとトークン(暗号資産等)の残高を同時に制御でき、整合性を保ちやすい。

デメリット

- ✓ パブリックブロックチェーンでは、取引量の増加に伴い、手数料(Gas代)が高騰する場合がある。
- ✓ 原則、ブロックチェーンにアップロードされたスマートコントラクトは修正できない。

※注意

- ✓スマートコントラクトは「契約の自動執行」と誤訳されることがあるが、法的な契約を表すものではない。
- ✓例として、プログラムの実行によりトークンの移転が行われるが、これを以て直ちに権利が移転するわけではない。

1.2.4 ブロックチェーンにおけるアカウントとは？、トークンとは？

- ブロックチェーンでは、アカウントアドレスが口座番号に相当し、秘密鍵が暗証番号に相当する。
  ただし、国内のセキュリティトークンでは、秘密鍵を投資家や発行体が自己管理することはなく、証券会社等が預かる形となっている。
- トークンとは、ブロックチェーン上で保有者の移転を行えるデータだが、実態はあくまで持ち分(残高)の帳簿的記録であり、
  あるサーバから別のサーバへデータが転送されるようなものではない。

秘密鍵・公開鍵・アカウントアドレスの関係

秘密鍵 口座の暗証番号に相当

- 256bit長のランダム値(0~2の256乗-1までの数字のどれか)
- **秘密鍵を知っていれば、**アカウントの**トークン移転などが全て可能**
  (よって秘密鍵を資産とみなす)
- 他人に予測などされないよう、十分にランダムな値(乱数生成)を使用した上で厳格に管理することが必要。
- 16進数表記するため、見た目上64文字の英数字の並びとなる

一方向性のある関数にかける (*1)

公開鍵

- 秘密鍵から作られた512bitの値
- 「公開鍵」として扱う場合には、接頭辞"04"を付与する
- 16進数表記するので、見た目上128文字の文字が並んで見える
  (頭の04を含めると130文字)
- デジタル署名の検証に使用する

- 一方向性のある関数にかける (*2)
- 結果の256bit(32byte)から末尾160bit(20byte)を取り出す
- 頭に16進数であることを示す”0x”を接頭辞として付与する

アカウントアドレス(Ethereumアドレス) 口座番号に相当

- トークンの移転先やコントラクトを一意に定める値(アドレス)
- 16進数表記するので、見た目上42文字の文字が並んで見える
  (0x + 40文字)

トークンとその残高の実態

ブロックチェーン内のトークン残高情報更新のイメージ

秘密鍵

秘密鍵で**署名済みトランザクションを発行**することで残高を更新(送金)

ブロックチェーンデータ

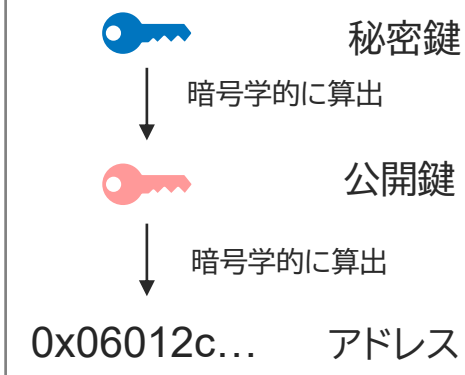
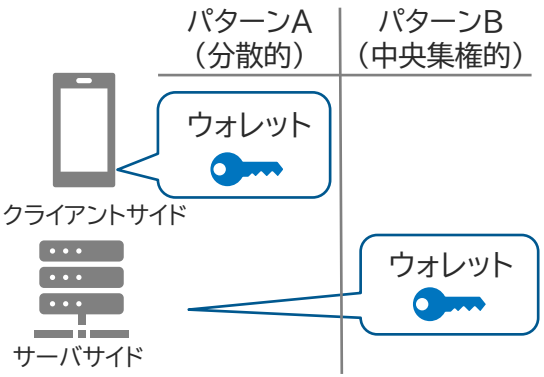
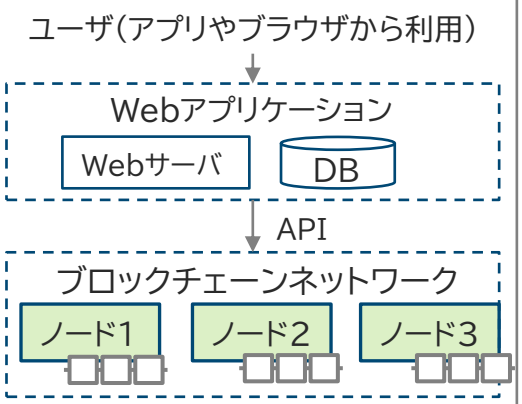
アカウント毎の残高情報を保有

- トークンと言ってもデータの塊ではなく、あくまで実態は台帳上の残高の記録
- 個別のトークンはスマートコントラクト(プログラム)で発行量等が規定される
  ただし、証券としての詳細が記述されているものではない。
- 秘密鍵・公開鍵・アカウントアドレスは、定められた数理的関係で算出される
  どのEthereumネットワークでも共通(チェーンによって異なるものではない)
  (パブリックネットでも、その他のプライベートネットでも共通した数理的関係)

[用語]一方向性関数
元の値から結果を算出することは可能だが、その逆は非常に困難な関数
(秘密鍵から公開鍵を導くことは可能だが、その逆は実質的に不可能)
*1 楕円曲線(secp256k1)のスカラー倍算にかけ、その結果として得た座標(x, y)のx座標とy座標を繋げる。
*2 一方向性ハッシュ関数であるKeccak-256関数

[参考]ブロックチェーンに関する議論で混同されやすい用語

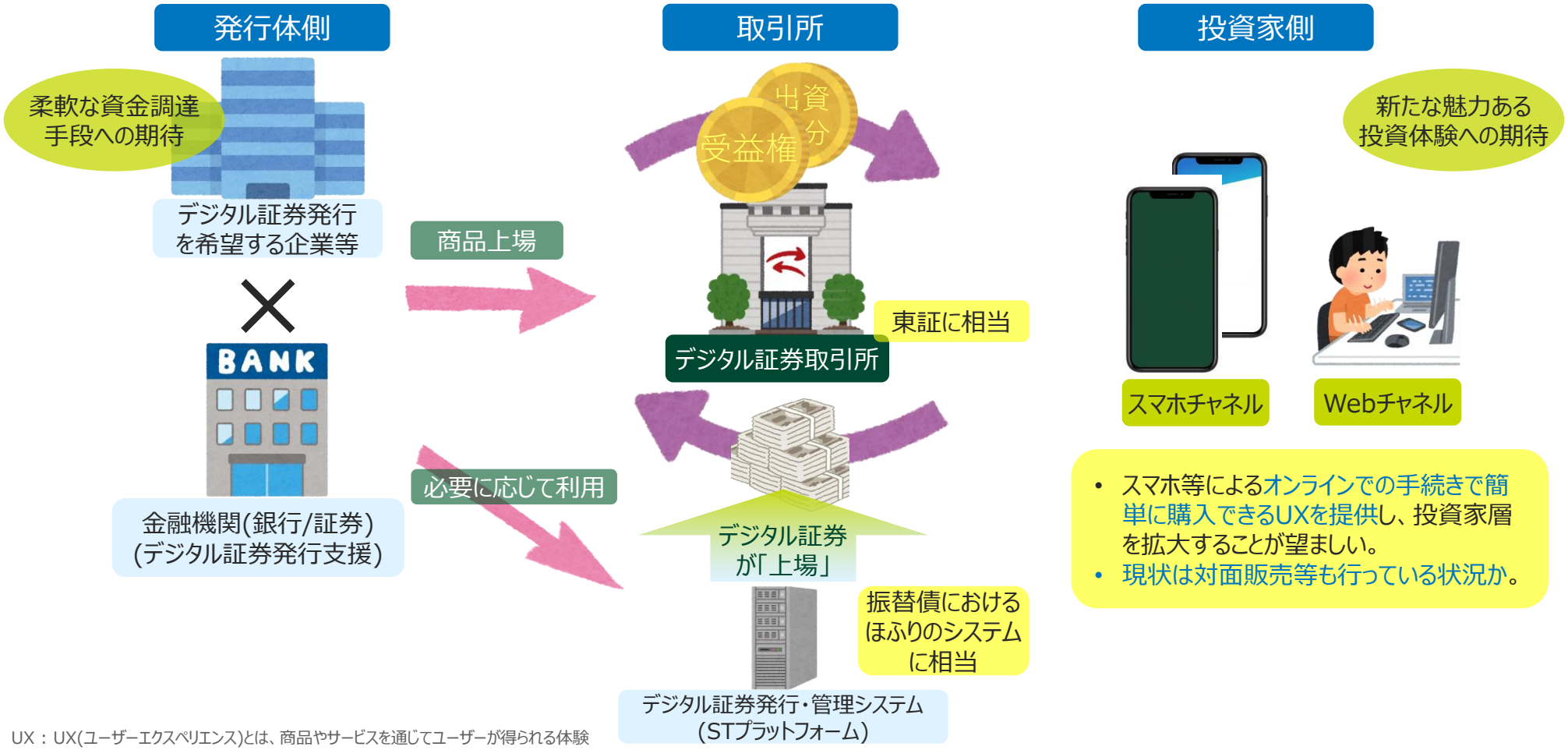
- Web3.0やブロックチェーンの活用の議論では、以下の用語の指す内容が参加者間で曖昧となり、認識齟齬が発生することがしばしばあるため注意されたい。
- 特にウォレットは、本来秘密鍵を管理するソフトウェアのことであり、複数の秘密鍵＝アカウントを管理できるものである点に注意。

	アドレス	ウォレット	ノード
意味	ブロックチェーン上のアカウントを示すための識別子。秘密鍵と対になり暗号学的に一意に定まる。(アカウントアドレスとも)	暗号資産やトークンの移転に必要な電子署名を生成するための秘密鍵を管理するソフトウェア。	ブロックチェーンネットワークを構成するコンピュータやサーバ等。
イメージ		サービスの運用形態によってウォレットが提供される場所が異なる。(検討が必要) 	
理解のポイント	• アドレスはブロックチェーン上の「口座番号」のようなもの（42桁の文字列） • アドレスに対して暗号資産やNFTトークンを送付する。	• 「ウォレット」（財布）という響きから暗号資産やトークンのデータ本体が格納されているイメージを持たれるが、実際は「秘密鍵」を保管・操作するためのソフトウェア。	• ノードは、ブロックチェーンのネットワークと直接つながっている。 • ユーザは、Webアプリケーションを介して、ブロックチェーンへの情報の読み書きを行うことが一般的。

2章
既存金融商品のトークン化
(アセットトークナイゼーション)

2.1.1 セキュリティトークン(デジタル証券)の全体像

- セキュリティトークン(ST, デジタル証券)とは、証券保管振替機構(ほふり)ではないシステムで電子的に発行、管理される有価証券
- すなわち、券面不発行の**非**振替債であり、主に以下2つの類型について期待され事例が積み上がっている。
  - ✓ 投資家に金銭以外のリターンも与えるような発行体の新たな資金調達手段 (例：社債セキュリティトークン)
  - ✓ キャッシュフローを生み出すアセットの証券化 (例：不動産の信託受益権を裏付けとするセキュリティトークン)



- スマホ等によるオンラインでの手続きで簡単に購入できるUXを提供し、投資家層を拡大することが望ましい。
- 現状は対面販売等も行っている状況か。

UX：UX(ユーザーエクスペリエンス)とは、商品やサービスを通じてユーザーが得られる体験

日本総研 The Japan Research Institute, Limited

2.1.2 セキュリティトークンの日本における法的整理

- 「セキュリティトークン」(ST)と「デジタル証券」は、国内でほぼ同義として使用され、各類型を指す法令用語、通称が存在する。
- デジタル証券は金融商品取引法(金商法)によって規制されており、下表の通り、開示規制や販売における業規制への準拠が必要。特に、第二項有価証券をトークン化した場合、第一項有価証券同等の規制への準拠が必要になる点に注意が必要。

元となる有価証券・権利 (トークンに表示される権利)	**トークン化した際の名称**	**開示規制の種別**	**業規制の登録種別**	**主な自主規制機関**
第一項有価証券 (社債、株式、国債・地方債等)	通称 **トークン化された有価証券表示権利**	第一項有価証券	第一種金融商品取引業	日本証券業協会
第二項有価証券 (信託受益権、集団投資スキーム等)	法令用語 **電子記録移転権利**	第一項有価証券 (トークン化により第一項有価証券同等の規制準拠が必要になる)	第一種金融商品取引業 (トークン化により第一項有価証券同等の規制準拠が必要になる)	日本 STO 協会
	通称 **適用除外電子記録移転権利** (内閣府令により、電子記録移転権利から除外されるもの)	第二項有価証券	第二種金融商品取引業	

上記を総称して「電子記録移転有価証券表示権利等」(法令用語)や「トークン化有価証券」(通称)と呼称

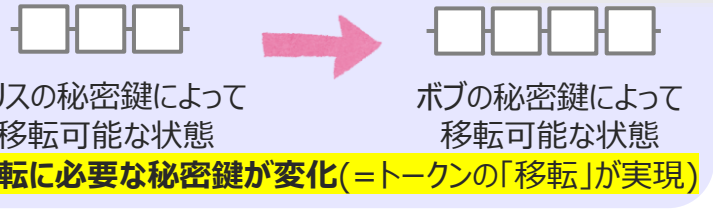
[表出典] 日本STO協会. “当協会について”. https://jstoa.or.jp/about/about/, (accessed on 2023-10-18)より弊社にて作成

2.1.3 セキュリティトークンのシステム概要 -トークンの移転と権利の移転の関係-

- デジタル証券(セキュリティトークン)形式での発行であっても、各証券の根拠法等の規定する対抗要件に変わりはない。
  このため、トークンの移転に連動して対抗要件が確実に具備される情報システムを構成する必要がある。[1]
- 社債、特定受益証券発行信託であればそれぞれ、社債原簿、受益権原簿への氏名、住所の記載が第三者対抗要件となる。
  このため、トークンの移転に連動して原簿が確実に更新される仕組みをとる必要があり、
  社債や特定受益証券発行信託のSTの発行事例があるSTプラットフォームであれば、基本的にこの連動の仕組みが整えられている。

トークンの移転と権利の移転の関係 (社債での例)

トークンの移転のイメージ



移転に必要な秘密鍵が変化(=トークンの「移転」が実現)

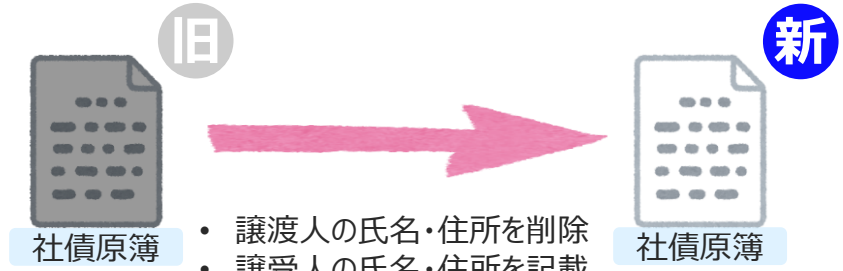
- ブロックチェーンでの「トークンの移転」とは、プログラムによってデータ更新の権限設定が切り替わることである。
- データの塊がある端末から別の端末へ送信されるようなものではない。

**トークンの移転によって
表示されている権利
そのものが移転する訳ではない**

確実な
連動が
必要

権利の移転

- 権利そのものの移転は証券類型ごとの根拠法等によって規定される。
  (社債の場合は社債原簿への氏名・住所の記載が対抗要件)



- 譲渡人の氏名・住所を削除
- 譲受人の氏名・住所を記載

**社債原簿の更新によって
権利の移転が成立**

[用語]対抗要件
権利関係を当事者以外の第三者に対して主張するための法律要件。

[1] 市原紘平. “証券へのブロックチェーン技術適用に関する検討 -日本の法制度下での社債を事例に-”. 信学技報, vol. 120, no. 380, SITE2020-40, pp. 7-14. 2021/3/1. https://www.ieice.org/ken/paper/20210301hC2E/, (accessed on 2023-10-18)

[参考]セキュリティトークンシステムにおいてブロックチェーンに保存される情報

- スマートコントラクト(プログラム)では、トークンの名称や総発行量等、あくまで数値データとしての振る舞いのみ定義するのが一般的。
  トークンのスマコンは以下のような関数を持ち、これらを使用して所望の機能(残高更新等)を実行。(Webアプリ等のUIを介して行う)
  - ✓ function totalSupply() …トークンの総発行量を返す。
  - ✓ function balanceOf(address account) …入力したアカウントアドレス("account")の持っているトークンの量を返す。
  - ✓ function transfer(address to, uint256 value) …入力したアカウントアドレス("to")へ指定量("value")のトークンを送る。
- 一方、社債を例にすれば、法令上対抗要件となる社債原簿に記載が必要な情報は「氏名・住所」とされている。(会社法第681条)
  よって、トークンの情報とは別に権者の情報を管理する必要がある。また社債要項のような情報もブロックチェーンとは別管理が普通。
  ブロックチェーンでは過去データを消去することができないため、個人情報を記録するのは望ましくなく、
  情報の消去が可能なデータベース(RDB等)で別途管理することが望ましいと考えられる。[1]

トークンのコントラクトの記載内容例

ERC20.sol

contracts > token > ERC20 > ERC20.sol

```
38  abstract contract ERC20 is Context, IERC20, IERC20Metadata, IERC20Errors {
39      mapping(address => uint256) private _balances;
40
41      mapping(address => mapping(address => uint256)) private _allowances;
42
43      uint256 private _totalSupply;
44
45      string private _name;
46      string private _symbol;
47
```

総供給量(_totalSupply)や
トークン名(_name)の定義部

```
118     function transfer(address to, uint256 value) public virtual returns (bool) {
119         address owner = _msgSender();
120         _transfer(owner, to, value);
121         return true;
122     }
```

transfer関数の定義部

ブロックチェーンとは別のデータベースも必要

ブロックチェーンデータ

アカウント毎の残高情報を保有

以下のような情報はブロックチェーンとは別の
データベース(RDB等)で管理するのが望ましい。
- 社債要項(発行要項)等、証券としての情報
- 権者の個人情報(氏名・住所) (原簿情報)
- 権者とそのアカウントアドレスの対応付け

[1] 市原紘平. “証券へのブロックチェーン技術適用に関する検討 -日本の法制度下での社債を事例に-”. 信学技報, vol. 120, no. 380, SITE2020-40, pp. 7-14. 2021/3/1. https://www.ieice.org/ken/paper/20210301hC2E/, (accessed on 2023-10-18)

日本総研 The Japan Research Institute, Limited

発行済みレポート引用

[参考]セキュリティトークンシステムの設計上の考慮点

- 証券を構成するために必要十分な情報はブロックチェーン外の別のサブシステムで管理し、その証券がどのContract(トークン)に対応しているのかという情報を管理する必要が生じると考えられる。
- 権利者の個人情報についてもブロックチェーン外の別のサブシステムで管理することが、セキュリティ上(個人情報保護等の観点から)望ましいと考えられる。

Ethereumを用いたセキュリティトークンシステムの構成例

フロントエンド
(Webサーバ等)

ユーザ入力の処理
(HTTPリクエストの処理等)

バックエンド
(Appサーバ)

業務ロジック処理

JSON-RPCによる利用

トークン持分量読み取り等

Ethereum
クライアントの
稼働するサーバ

- ブロックチェーンデータ本体を保管
- ブロックチェーンデータからアドレス毎のトークン持分量を読み取り
- トークン移転トランザクション等の発行

ブロックチェーンデータ

ブロック生成・受取

トランザクション発行

証券情報DB

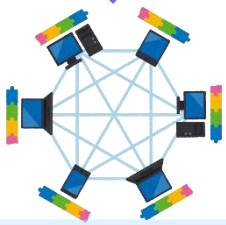
- 証券に関する情報を保管
- 証券とContractの対応付けを記録

- トークンのContract自体に証券の内容をある程度持たせることはできるが十分と言えるか。
- 別途DBで証券として十分な情報を管理すべきではないか。

権利者DB

権利者の個人
情報を保管

- 権利者の個人情報もブロックチェーンに保存する構成もあり得る。
- しかし、セキュリティやプライバシー保護の観点から望ましくないのではないか。



ブロックチェーンネットワーク

[出典] 日本総合研究所. “セキュリティトークンの概説と動向”. https://www.jri.co.jp/page.jsp?id=38970, (accessed on 2023-10-18)

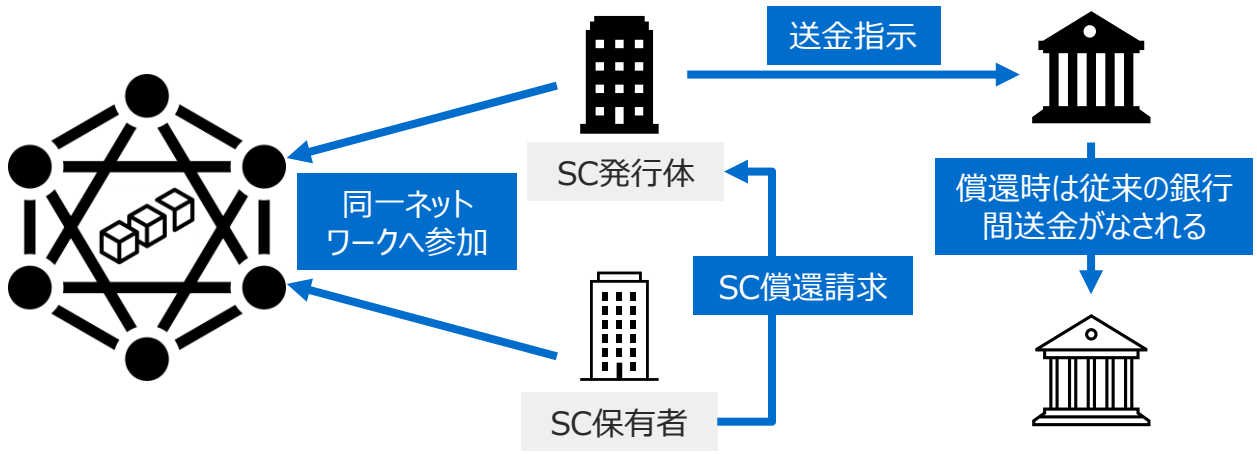
日本総研 The Japan Research Institute, Limited

2.2 ステーブルコイン(SC)

- ブロックチェーンに発行される、1トークン=1ドルの様に定額レートでの法定通貨との交換を保証するトークンをステーブルコイン(SC)という。発行にあたり、同額を法定通貨や短期国債等の安定資産で裏付けることで交換レートを保証する。(信託等のスキームを使用)
- 単一台帳を共有するブロックチェーンネットワーク上の口座同士のSC送金では、全口座が1つのネットワーク上に集約されているため、送金は早期に完了する。(ただし、銀行預金への償還まで行う場合は、従来同様の銀行間送金システムが使用される)
- このため国際送金用途で早期に着金するSCを使用し、必要に応じて銀行預金に戻すといった用途は有望視される。
- また、セキュリティトークン(ST)が発行されているブロックチェーン上に発行したSCでSTの決済をする場合、単一台帳(単一ブロックチェーン)上での数値の付け替えとなるため、処理が早期に完了できることが期待される。

SC送金の概要

- ✓ SC送金は「単一台帳を共有する単一ネットワーク」の参加者同士の送金。
- ✓ このため、更新する台帳が1つであり、同一銀行内の送金同様に簡潔に完了する。



SC償還時の概要

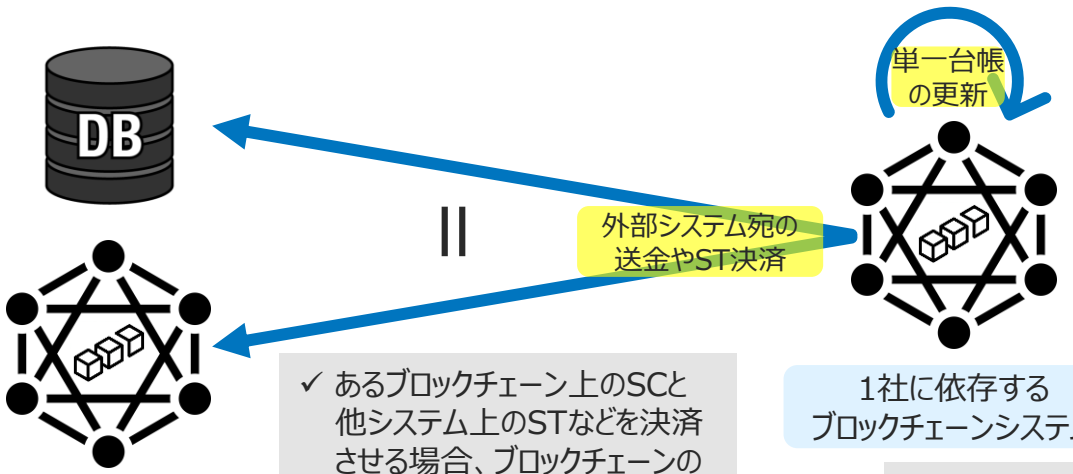
- ✓ SCを法定通貨に戻す際には、SC発行体の銀行口座からSC保有者の銀行口座へ、従来通り銀行間の送金ネットワークによる送金が行われる。

- ✓ SC発行業者は独自のSC専用ネットワークを立ち上げる動きを見せている。(Tempo, Stable, Arc等)
  しかし、特定業者によるインフラ運営ではブロックチェーンの意義は薄れる。
- ✓ SCを仲介する暗号資産交換所は、SC流通量を増やしたいSC発行体からレベニューシェアを受け、一部を「報酬」としてSC保有者に与えている。
  対して米銀のロビー団体などは、実質的な利息の提供による預金流出やそれに伴う融資減少を懸念し、禁止するよう働きかけている。

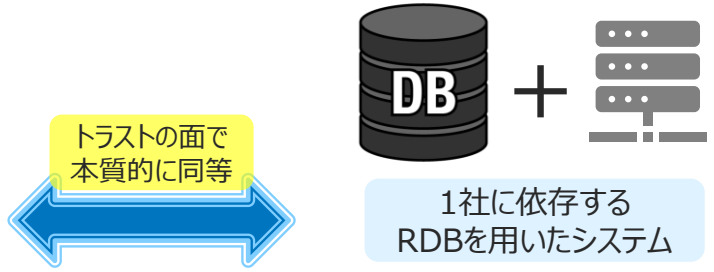
詳細は日本総研発行「X金融未来Tech No.4 ステーブルコインの卓越性に関する考察」参照。また、法的な裏付け資産を持たずアルゴリズム等によって価格安定を目指すの暗号資産もステーブルコインと称される場合があるが本頁では割愛

[考察]トークナイゼーションのシステム構成 ～単一台帳でのみ生じる効率性～

- 同一ブロックチェーンネット上のアカウント間のSC送金やSCとSTの決済が効率的なのは、更新する台帳が1つであることによる。
  - ➢ このため、SCとSTが別のブロックチェーン上に発行されている場合などは、一般的なシステム連携と同等以上の効率性とはならない。
- また、日本で使用されるSTのシステム基盤は多くがプライベートチェーンであり、1法人(または複数法人によるコンソーシアム)が運営の責任を負う。これは責任の所在が明確になるメリットの反面、システムへの信任(トラスト)は運営者たる1法人(またはコンソーシアム)への信任と同じとなる。
  - ➢ こうした構成ではパブリック型ブロックチェーンの持つ透明性は活かされないため、1社による運営の、より簡潔なシステム構成としてRDB*1を用いたシステム構成についても検討の価値があると考えられる。



更新する台帳が1つである以下の場合に効率的な処理が可能
- ✓ 送金元と送金先のアカウントが同一ブロックチェーンネット上にある
- ✓ SCとSTが同一ブロックチェーンに発行されている



- ✓ あるブロックチェーン上のSCと他システム上のSTなどを決済させる場合、ブロックチェーンの持つトークン交換の原子性*2や効率性が活かせない。
- ✓ 外部システム接続となる限り、接続先がブロックチェーンでもRDBでも、同等の効率性・確実性となる。

- ✓ ブロックチェーンを用いたシステムでも個人情報などは権限管理されたRBDに記録することが望ましく、元々RDBも用いる必要がある。(p.14)
- ✓ スマコンを用いると、サービス内容に関わるプログラム(スマコン)と取引の実行データが不可分なブロックチェーンに保存されるが、RDB+Appサーバの構成であればプログラムとデータは別々に整理できる上、プログラムのアップデートも容易である。
- ✓ 一方、パブリックチェーンには誰もがプログラムを公開できるという特徴がある。

*1 リレーショナルデータベース(RDB)：複数のテーブルを関連付けて複雑なデータ操作を高速・正確に処理する、最も主流なデータベース方式
*2 原子性：データベースの処理において、一連の操作が「すべて実行される(Commit)」か「一つも実行されない(Rollback)」のいずれかの状態になること。トークン交換の原子性とはトークン同士のDvPが確実に実現すること。

日本総研 The Japan Research Institute, Limited

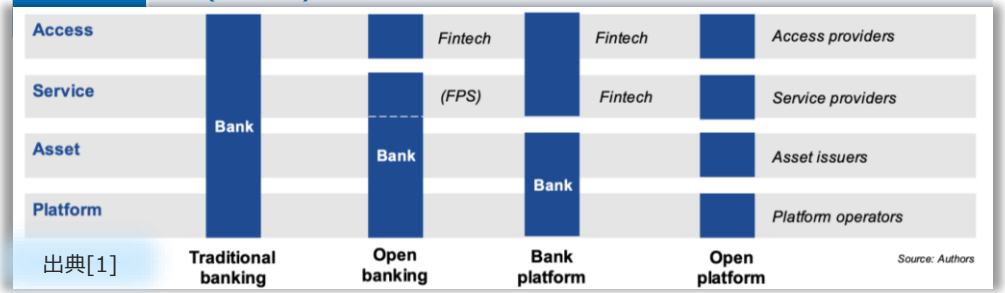
[参考]統合台帳(プラットフォーム)による効率化についての指摘論考

- 前頁で述べた単一の台帳(統合台帳; Unified Ledger)による効率化の可能性が、IMFやBISのペーパーでも指摘されている。

IMF(International Monetary Fund); 国際通貨基金, BIS(Bank for International Settlements); 国際決済銀行

IMFによるワーキングペーパー

タイトル	ASAP: デジタル資産プラットフォームの概念モデル (ASAP: A Conceptual Model for Digital Asset Platforms)[1]
著者	Victor Budau*1 & Herve Tourpe (*1元仏中銀の"Enterprise Architect & Blockchain expert")
公開日	2024/2/2 (IMF Working Paper)
要点	✓ デジタル資産プラットフォーム(DAP)のための、ASAP(アクセス、サービス、資産、プラットフォーム)という概念モデルを紹介。統合プラットフォームを通じた市場構造の簡素化に注目する。 ✓ ASAPの各層をブロックチェーンシステムで例示すれば、アクセス(Wallet)、サービス(DeFiプロトコル)、資産(各種トークン)、プラットフォーム(ブロックチェーン)となる。 ✓ 同モデルでは資産とプラットフォーム(PF)が分離される(下図)。すなわち、銀行が勘定系システム(PF)で預金(Asset)を管理しているのに対し、パブリックチェーンを用いたシステムでは、チェーン(PF)は記録等の基本機能に専念、そこにはトークン(Asset)が自由に発行されていると指摘する。



出典[1]

BISによるワーキングペーパー

タイトル	Finternet: 未来の金融システム (Finternet: the financial system for the future)[2]
著者	Agustín Carstens*2 & Nandan Nilekani (*2:元メキシコ中銀総裁)
公開日	2024/4/15 (BIS Working Papers)
要点	✓ トークン化された中央銀行通貨、商業銀行預金、企業株、社債、国債等の複数の金融資産市場を、共通のプログラム可能なプラットフォーム上で統合するデジタルプラットフォームとして「統合台帳」(unified ledgers)を定義。 ✓ トークン化のメリットを最大限に引き出すには、堅牢なガバナンスと規制の枠組みに支えられた、複数のトークン化された資産を共通のプラットフォームに統合する必要がある。(ただし、各法域のニーズに応じて、複数の台帳が共存することも可能) ✓ 煩雑な手作業によるワークフローと複雑な法的・規制的枠組みを持つ資産と、既に合理化されたプロセスと明確な法的・規制的枠組みを備えデジタルでほぼ自動化されたシステムにある金融資産を区別し、前者はトークン化の難易度が高い一方で得られる効果も高く、後者はその逆となる点を指摘。 ✓ パブリックチェーンによる統合台帳を用いた場合、ユーザは資産に対して比類のないコントロール権を得る。一方で、無記名トークン(Bearer tokens)と記名トークン(Non-bearer tokens)に対する望ましい規制の違いを認識し、後者では登録証券などのセキュリティと規制遵守が強化されるべきとする。

[1]Victor Budau & Herve Tourpe, "ASAP: A Conceptual Model for Digital Asset Platforms", International Monetary Fund;, 2024/2/2, https://www.imf.org/en/publications/wp/issues/2024/02/02/asap-a-conceptual-model-for-digital-asset-platforms-544387 (accessed on 2026/2/20)
[2]Agustín Carstens & Nandan Nilekani, "Finternet: the financial system for the future", Bank for International Settlements, 2024/4/15, https://www.bis.org/publ/work1178.htm (accessed on 2026/2/20)

日本総研 The Japan Research Institute, Limited

2.3 トークン化対象拡大の議論

- 社債や特定受益証券発行信託のSTに加え、地方債やMMF(Money Market Fund*)のトークン化についても議論が隆盛している。
- しかし、上記を含むいくつかのアセットについては法制上、(紙による)券面の不発行を認める規定が無いことなどから、完全なデジタル化ができない、もしくは複雑なスキームを用いる必要がある状況となってしまっている。
  - 例えば、MMF(投資信託の一種)のデジタル化(トークン化)を考える時、投資信託の受益権については受益証券の発行義務があり、譲渡と対抗要件の成立には券面の交付が必要である。
  - このため、①発行時に「券面不所持の申出」を投資家から受け付け、②譲渡時には「一部解約/償還」という構成をとる、といったスキームでの実現が検討されている。[1]

*MMF：格付けの高い国債や社債などの短期金融資産で運用される公社債投資信託

- 券面不発行や原簿への記録による第三者対抗要件の具備を幅広に認め、デジタルで完結する処理が可能となる法改正が望まれる。

券面発行を前提とした「アナログ規制」の残る主な証券類[2]

	券面の全部不発行	譲渡時のデジタル完結化	第三者対抗要件のデジタル化
地方債	×：券面発行前提 不発行を認める規定無し	×：券面交付前提 譲渡効力発生には券面交付要	×：券面所持/交付前提 対抗要件として券面所持/交付要
投資信託の受益権	×：券面発行前提 受益証券の発行義務		
特定目的会社(TMK)の優先出資証券	×：券面発行前提 優先出資証券の発行義務		

[1]齊藤達哉, "【速攻解説】「トークン化MMF」と「トークン化法」で、ステーブルコイン×デジタル証券の"理想形"へ！日本と海外のギャップと解決に向けた道筋とは", note, 2025/10/2, https://note.com/tatsu_s123/n/na345deba4ac2 (accessed on 2026/2/20)
[2][1]内の図表より筆者作成

[参考]「コントロール可能な電子記録(CER)」 ~「記録の支配」の概念の登場~

- 以下の様に、電子的な記録に対する物権的な「支配」の概念が法律に登場している。
  - ✓ 背景には、無体のデジタル資産としてのブロックチェーン上のトークンと秘密鍵によるトークン移転(本稿p.13で解説)や、貿易業務効率化の分野で、紙の船荷証券の代替として電子化された船荷証券が登場してきたことがある。
  - ✓ なお、欧州各国でも具体的な立法は行われており、分散台帳技術(DLT)を用いた場合でも、証券台帳に記録される保有名義人の記録をもって権利関係を規律している。[1]
- UCC (Uniform Commercial Code; 統一商事法典) 第12編が新設 (2022年 米国)[1]
  - ✓ 「コントロール可能な電子記録」(CER; Controllable Electronic Record)の概念が導入された。
  - ✓ 本新設の目的は、無体のデジタル資産における財産権の移転を規定すること。
  - ✓ CERのコントロールは、以下要件が全て満たされる場合に認められる(§12-105)
    - I. CER から生じる実質的に全ての利益を享受する権限(power)
    - II. そのような享受を他者に妨害されない排他的権限
    - III. 記録の移転の結果としてコントロールを他者へ移転できる排他的権限
    - IV. 以上の権限が自らに属することを何らかの方法で容易に示すことができる
- 「商法（船荷証券等関係）等の改正に関する要綱」の採択 (2024年 日本)
  - ✓ 「記録の提供」といった概念によって、一定の要件を満たすシステムに記録される電子記録に私法上の効力を認める考え方を採用。
  - ✓ 『一定の資格を有する記録機関を必要とせずに、電子的な記録に私法上の効力を認める法制度は、既存のものとは異なる画期的な制度であると評価』[2]との意見もある。
  - ✓ 米国と違い、現状では「電子船荷証券記録」以外の電子的な記録に関する法案提出には至っていない。

[1]奥山太雅、杉村和俊, “トークン化された資産の権利関係―スイス・ドイツ・フランス・米国の法整備からの示唆―”, 日本銀行ワーキングペーパーシリーズ, 2025/7/18, https://www.boj.or.jp/research/wps_rev/wps_2025/wp25j10.htm (accessed on 2026/2/20)
[2]有吉尚哉, “船荷証券の電子化から「トークン法」への期待”, N&Aニューズレター, 2024/9/13, https://www.nishimura.com/ja/knowledge/newsletters/finance_law_240913 (accessed on 2026/2/20)

日本総研 The Japan Research Institute, Limited

[参考]その他のトークン化アセット

- 既存の金融商品のトークン化の他に、実物の貴重品や利用権を「トークン化」した事例存在。(弊社発行「デジタル証券とRWAトークンの動向」に詳述)

トークン化対象	サービス事例	分類	詳細	補足
貴金属	● 三井物産デジタルコモディティーズ ジパングコイン(ZPG)	● 日本の資金決済法において暗号資産	● 金の市場価格に連動するように構成されたトークン(コイン) ● 価格連動の仕組みは以下の通り(創・佐藤法律事務所より引用[1]) ① 『三井物産デジタルコモディティーズ社(以下「発行者」といいます。)がZPGを発行する場合、ZPGの移転と同時に、(利用者に代わってZPGを購入した)デジタルアセットマーケッツ社のために、ZPGの数量と同等の金現物を、調達資金を用いて三井物産社から購入』 ② 『当該購入した金現物は、デジタルアセットマーケッツ社へ販売すると同時に、デジタルアセットマーケット社から発行者が消費寄託を受ける』 ③ 『ZPGは金現物の消費寄託に関する引渡請求権を表象するが、ユーザーはZPGを持っていても現物の金の引渡しを請求できない』 ④ 『しかし、マーケットメーカーであるデジタルアセットマーケッツ社が金の市場価格に近似した価格でZPGを購入することを約束している(なお、かかる請求権には銀行保証が付される)』 ⑤ 『デジタルマーケッツ社がZPGを有する場合、発行者にZPGと同数の金現物の引渡しを要求できる』	● トークン(コイン)はプライベートチェーン上に発行される[2] ● 金同様、銀やプラチナの市場価格に連動するジパングコインシルバー、ジパングコインプラチナも発行。[3]
実物アート作品	● Freeport(米国)	● 米国において証券(セキュリティトークン)	● Freeport社は実物のアート作品を「分割・トークン化」して販売する。 ● 米証券取引委員会(SEC)の規制に準拠しており、証券(セキュリティトークン)の一種として販売している。 ● 「分割・トークン化」の法的な詳細や、投資家に保証される権利についてはSECの公開情報に記載[4]がある。主な内容は以下の通り。 ✓ 有限責任会社の一種(対象アート作品ごとの"series LLC")が実物のアート作品の所有権を保持。 ✓ 投資家はトークンに投資すると、投資したシリーズの有限責任会社の持分("shares")を受け取る。シリーズが所有するアート作品の直接の所有権を受け取るわけではない。(トークン自体は投資家に権利を与えるものではなく、シリーズの利益を表現する。)	● アート作品は不動産など程安定的にキャッシュフローを生むわけでは無いが、展示会・美術館などへの貸出で生むケースがあり得る。 ● Ethereum上に発行[4]

[1]斎藤創, 今成和樹, "現実資産(RWA)のトークン化と日本法", 創・佐藤法律事務所, 2023/9/1, https://innovationlaw.jp/rwa-token/ (accessed on 2023/10/11)
[2]三井物産デジタルコモディティーズ, "Zipangcoin White Paper Version 4.0", 三井物産デジタルコモディティーズ, 2023/6/30, https://www.mitsuidc.com/zpg-whitepaper (accessed on 2023/10/11)
[3]三井物産デジタルコモディティーズ, "ジパングコインシルバーおよびジパングコインプラチナ発行のお知らせ", 三井物産デジタルコモディティーズ, 2023/6/30, https://www.mitsuidc.com/230630-pressrelease (accessed on 2023/10/11)
[4]U.S. Securities and Exchange Commission, "freeportholdings_253g2", U.S. Securities and Exchange Commission, 2023/5/8, https://www.sec.gov/Archives/edgar/data/1946910/000182912623003143/freeportholdings_253g2.htm (accessed on 2023/10/11)

日本総研 The Japan Research Institute, Limited

[参考]その他のトークン化アセット

- 既存の金融商品のトークン化の他に、実物の貴重品や利用権を「トークン化」した事例存在。(弊社発行「デジタル証券とRWAトークンの動向」に詳述)

トークン化対象	サービス事例	分類	詳細	補足
酒類	● UniCask(日本) Cask NFT	● 現物償還型(NFT) (引渡請求権を表象か)	● UniCaskは熟成樽の中のウイスキーを「分割・トークン化」して販売する。 ● 「分割・トークン化」の詳細は以下の通り。 『NFTの所有者は、樽をボトリングした際に、その結果（ボトル詰めされたウイスキー）を引き受けることができます。』[1] (『Cask NFTを使った樽引き渡し請求』[2]) ● 酒類販売免許を保持(麹法第3778号)[3] ● ウイスキーなどの酒類は時間が経過し熟成が進む程価値が高まるためNFTの価値も高まる可能性がある。(ただし購入時より高額となるかは、初期販売時の値付け等に依るものと考えられる。)	● 設立間もない資本の薄い蒸留所などが、将来の酒の引渡請求権をトークン化し熟成前に販売することで、キャッシュを先に得られるといった活用の可能性が考えられる。
宿泊施設の利用権	● NOT A HOTEL (日本)	● 利用権型(NFT) 自家型前払式支払手段[4]	● NOT A HOTELは、優れたデザインの別荘物件の共有持分(貸借件の準共有持分を含む)を販売。オーナーたちは保有口数に応じて年間所定の日数物件を利用することができる。 ● 同社は上記とは別に「メンバーシップNFT」も販売、同NFT保有者は1年のうちランダムで決められた日に毎年物件を利用することができる。(年間1~3連泊の3種のNFTがある。)[4] ● メンバーシップNFTの有効期間は47年間で、物件利用の際の鍵となるNFT「THE KEY」がメンバーシップNFT保有者に毎年エアドロップ(発行)される。[4] ● 物件を利用できる日はNFTごとに決まっており、NFTのReveal(購入したNFTの詳細が確定される処理)時にランダムで決定される。[4] ● NFTはEthereum上に発行されており、「メンバーシップNFT」「THE KEY」ともに自由に譲渡が可能。[4]	● NOT A HOTELは自社が管理する物件を利用できる権利として、自家型前払式支払手段と整理して提供。[4] ● 他事例として、ラグジュアリーホテルの宿泊権のNFT化の検討をHashPortらが発表している。[5]

[1]UniCask Co., Ltd., “Genesis Cask Springbank 1991”, UniCask Co., Ltd., 2021/12/15, https://unicask.jp/products/nft/01-cask-springbank-1991-320.php (accessed on 2023/10/11)
[2]UniCask Co., Ltd., “実物資産 x NFT Whiskey Cask NFT”, Japan Blockchain Association, 2021/9/14, https://jba-web.jp/cms/wp-content/uploads/2021/10/UniCask-whisky-x-NFT.pdf (accessed on 2023/10/11)
[3]UniCask Co., Ltd., “特定商取引法に基づく表記”, UniCask Co., Ltd., 2021/12/8, https://www.unicask.com/static/public/pdf/%E7%89%B9%E5%AE%9A%E5%95%86%E5%8F%96%E5%BC%95%E6%B3%95%E3%81%AB%E5%9F%BA%E3%81%A5%E3%81%8F%E8%A1%A8%E8%A8%98_UniCask.pdf (accessed on 2023/10/11)
[4]NOT A HOTEL Inc., “NOT A HOTEL MEMBERSHIP NFT”, NOT A HOTEL Inc., 2022/8/1, https://notahotel.com/nft (accessed on 2023/10/11)
[5]HashPort Inc., “HashPortとウェルス・マネジメント、現実資産（RWA）のNFT化に関する業務委託契約を締結”, PR TIMES, 2023/10/3, https://prtimes.jp/main/html/rd/p/000000069.000046288.html (accessed on 2023/10/11)

3章
暗号資産(ネイティブトークン)と狭義のDeFi

3.1 暗号資産(ネイティブトークン)

3.1.1 暗号資産に関する国内動向

3.1.2 暗号資産に関する議論

3.2 代表的なDeFiプロトコル

3.2.1 狭義のDeFi

3.2.2 分散型取引所(DEX / AMM)

3.2.3 レンディング

3.2.4 分散型ステーブルコイン

3.2.5 リキッドステーキング

3.1.1 暗号資産に関する国内動向 ～金商法への移行・申告分離課税・ETF解禁へ～

- 2025年12月以降、日本国内の暗号資産に対する規制動向は大きな転換点にある。
  - ✓ 20%の申告分離課税へ：「令和8年度与党税制改正大綱」にて、申告分離課税20%と3年間の損失繰越控除が明記
  - ✓ 根拠法が金商法へ移行：投資/投機対象としての実態から金融審議会「暗号資産制度に関するワーキンググループ」報告で明記
  - ✓ 暗号資産ETF承認への動き：前掲の「税制改正大綱」の中で、分離課税の対象として「暗号資産を対象とするETF」が明記

2025年末以降の日本国内での暗号資産規制動向

	従来	今後
根拠法令	資金決済法	金融商品取引法 (金融庁は2026年中に国会へ 金商法の改正案を提出する予定)
基本的な位置づけ	電子マネーに近い「決済手段・送金手段」	株式や投資信託のような「投資性のある金融商品」
取引所の扱い	暗号資産交換業者(登録制)	証券会社同等の「第一種金融商品取引業」 に準ずる厳しい業規制
不公正取引の防止	法的な罰則規定が限定的	インサイダー取引規制や 相場操縦に対する厳罰化(課徴金等)
情報開示 (ディスクロージャー)	業界団体の自主規制に基づく説明	発行体に関する厳格な法定情報開示義務の導入
税制	総合課税 税率:15%~約55%(最大,累進課税)	申告分離課税 税率:一律20.315%

日本総研 The Japan Research Institute, Limited

3.1.2 暗号資産に関する議論

● 暗号資産を巡っては、肯定派と否定派で対極的な意見がある。否定派だった有力者が肯定派へと転向した例も見られる。

否定派
「内在的価値の欠如」、「犯罪利用のリスク」を根拠に厳しい評価

肯定派
国家管理の通貨システムの脆弱性を指摘、
干渉を受けない「新しいデジタル基盤」としての価値を強調。

ジェイミー・ダイモン氏 (JPMorgan Chase CEO)
- 「詐欺」「ペットの石」「分散型ポンジスキーム」
- インフラとしてのブロックチェーンは評価するが、ビットコイン自体は内在価値がなく、マネーロンダリングや脱税、犯罪に利用されていると批判。

ヴィタリック・ブテリン氏 (Ethereum共同創設者)
- 「分散型ワールドコンピュータ」「金融の民主化」
- 単なる通貨ではなく、スマコンによって「仲介者なし」で金融サービス(DeFi)を動かせる、透明性の高いインフラとしての価値を重視。

ウォーレン・バフェット氏 (Berkshire Hathaway会長)
- 「何も生み出さない」
- 農地やアパートのようにキャッシュフローを生む「生産的資産」ではなく、次に高く買ってくれる人を待つだけの投機対象に過ぎないと批判。

マイケル・セイラー氏 (MicroStrategy会長)
- 「デジタル・ゴールド」「富の保存における最高戦略」
- 法定通貨はインフレで価値が溶け出す「溶ける氷」であり、発行上限が2100万枚と決まっているビットコインは、究極の希少資産と主張。

【転向】ラリー・フィンク氏 (BlackRock CEO)
- 【2017年】「マネーロンダリングの指標に過ぎない」
- 【現在】ビットコインを「恐怖の資産(Asset of Fear)」、つまり経済的不安や地政学的リスクに対する避難先(Flight to Quality)として認め、現物ETFの提供を主導。また、金融インフラの未来は「トークン化(Tokenization)」にあると予言。

技術的評価

◯ 金融機能のモジュール化・オープン化、統合化(c.f. p18統合台帳)、暗号技術高度化のきっかけとなっている。
◯ 仮に今後AI需要が細り、データセンタ設備が過剰となった場合、マイニングが有効な活用方法として受け止められる可能性。
◯ グローバル展開されたアクセスフリーな金融インフラ(=パブリックチェーン)は、高度な決済システムがない途上国にとって利用価値がある可能性。
✕ AI需要などで計算資源が枯渇する予測もある中、今後暗号資産への社会的受容が変化するリスク。(マイニング会社のAIデータセンタ進出の実例)
✕ 社会に対してゼロサムまたはマイナスサム(エネルギー消費・計算資源消費を考慮)のゲームが、暗号資産取引として繰り返されている。
✕ L1(ブロックチェーンと暗号資産自体)の開発を行い暗号資産販売で収益を得ることばかりが繰り返され、社会的意義のあるサービスが見られない。

日本総研 The Japan Research Institute, Limited

3.2.1 狭義のDeFi

- (狭義の)DeFi(Decentralized Finance; 分散型金融)とは、パブリックチェーンのスマートコントラクトによって提供される金融サービス。
  - ブロックチェーンエンジニア等の専門家は、単にDeFiと言えば狭義のDeFiを想起するが、p.4で整理したように非専門家などは暗号資産そのものやアセットトークナイゼーションも含めてDeFiと認識する傾向がある。*
- 開発したプログラム(スマコン)をパブリックチェーンで公開することで、誰もが開発したサービスを実際の暗号資産取引で活用できる。
- 特定の企業などが所有・利用するサーバーではなく、パブリックブロックチェーンネットワークを形成する無数のノードでプログラムが実行され、サービスが提供されるため、規制の対象となる組織・団体などを特定することが難しい。
  - ただし、複雑な処理を行う多くのDeFiプロトコルには、開発を行っている企業がある。

代表的なDeFiのプロトコル

分野	概要	代表的なサービス名
分散型取引所 (DEX / AMM)	ユーザー同士がスマートコントラクトの流動性プールを介してトークンを交換する基盤。	Uniswap Curve Finance
レンディング (貸借プロトコル)	スマートコントラクト上で暗号資産の過剰担保型貸借を自動化するプロトコル。	Aave Compound
分散型ステーブルコイン(SC) (アルゴリズム型SC)	中央集権的な発行体を持たず、暗号資産を担保としたスマートコントラクトによってアルゴリズムで価値を安定させるSC。	MakerDAO (現Sky)
リキッドステーキング	PoS(Proof of Stake)ブロックチェーンのステーキング機能と、DeFiの流動性を結びつけるサービス。	Lido

*筆者による肌感覚であり、定義を提案するものではない

3.2.2 分散型取引所(DEX / AMM)

- 分散型取引所(DEX; Decentralized Exchange)では、一般的な取引所*のように、買手と売手の注文をマッチングさせる板(オーダーブック)方式を採るのではなく、プログラム(スマートコントラクト)が自動で価格決定し、取引相手となることが特徴。
  - ➢ この自動価格決定の仕組みのことをAMM(Automated Market Maker; 自動マーケットメイカー)という。

*CEX(Centralized Exchange);中央集権型取引所ともいう

代表的なAMMプロトコル

	仕組み・特徴等
Uniswap AMMの始祖	✓ **仕組み:** 「流動性プール」と呼ばれるプログラム(スマコン)で作られた「金庫」に、例えばETHとUSDCを1:1の価値になるようにペアで入れる。ユーザーがこのプールで「ETH*をUSDCに交換したい」場合、プール内のETHが増え、USDCが減る。 ✓ **価格(レート)の決まり方:** Uniswapでは「プール内のETHの枚数 × USDCの枚数 = 常に一定(K)」というシンプルな数式(定数積フォーミュラ)で価格が自動計算される。ETHがプールに増えるほど、ETHの価格(USDC建て)は自動的に下がる。(なお、簡略化しているが、実際にはプロトコルが徴収する手数料分も含めて計算される) ✓ **革新性:** 誰でもこのプールに資金を提供でき、代わりに取引手数料を稼げる(=流動性マイニング)というモデルを最初に作った。コードのフォーク(派生)元としても多く採用され、後続のPancakeSwapやSushiSwapの元である。
Curve Finance SC特化AMM	✓ **仕組み:** Uniswapと同様のプール型だが、USDCとUSDT(両者とも著名なドル建てSC)のように「本来同じ価値(1ドル)であるべきペア」に特化。 ✓ **価格(レート)の決まり方:** Uniswapの数式では、少し大きな金額を交換しただけで価格が大幅に動き(スリッページ)、損をしてしまう。Curveは独自の数理モデル(StableSwap)によりスリッページを極小化し、プール内の比率が多少偏っても、なるべく1:1の価格を維持するように設計されている。 ✓ **革新性:** 上記仕組みにより、大口の資金でも安心してステーブルコイン同士を両替できる。

*ETH:Ethereumブロックチェーンの暗号資産(ネイティブユーティリティトークン), USDC:著名なドル建てステーブルコイン

3.2.3 レンディング

- レンディングのプロトコルでは、スマートコントラクトが「貸出」と「借入」の仲介を行う。
  - 貸手(プールへ資産を預け入れる側)の利用理由：プロトコルによって決定される金利に基づいた利息を受け取れるため。
  - 借手(プールから資産を借り入れる側)の利用理由：借りた暗号資産でレバレッジ取引や空売りを行い、儲けを狙うため。*

*他DeFiプロトコルでの運用も含み、同手法で高金利を得ることをイールドファーミングという。

代表的なレンディングプロトコル

	仕組み・特徴等
Compound アルゴリズムによる 自動金利調整の古株	✓ **仕組み:** 貸手は様々な暗号資産を1つの大きなプール(スマコン)に預け入れ、借り手はそのプールから借りる。 借りるためには借入額よりも価値の高い別の資産を「担保」として預ける必要がある(過剰担保)。 ✓ **金利の決まり方:** プール内の資金の「利用率」によってプログラムが自動で金利を変動させる。 借りる人が多くプールの資金が減ると金利が上がり、プール資金の枯渇を抑制する。 逆に借りる人が少なければ金利は下がる(借り入れを促し、プールの資金効率を高める)。 貸出金利と貸手が受け取る金利には差があり、コントラクトが差分を得る(プロトコルが徴収する手数料)。 この需給バランスによる自動金利調整モデルをCompoundが確立した。
Aave フラッシュローンが特徴	✓ **仕組み:** Compoundと同様の「プール型レンディング」。 ✓ **金利の決まり方:** 基本的にはCompoundと同様、「資金利用率(Utilization Rate)」に基づいて自動的に金利を決定する「アルゴリズム型金利モデル」。 ✓ **革新性:** フラッシュローン(瞬間的な無担保借入)は、Aaveの特徴な機能。 「1つのトランザクション(ブロックチェーン上の1回の記録)の中で、借りて、何かに使い、全額＋手数料を返す」という条件であれば、無担保でいくらでも資金を借りることができる。 もし返せなければ、そのトランザクション自体が最初から無かったことになるため、Aave側に貸し倒れリスクはない。 主に価格差を利用したサヤ抜き(アービトラージ)などに使われる。

3.2.4 分散型ステーブルコイン

- 法定通貨等を裏付けにするのではなく、暗号資産を担保にプログラムで「1ドル」の価値に安定する暗号資産を作ることを目指すもの。

代表的な分散型ステーブルコインプロトコル

	仕組み・特徴等
MakerDAO* 暗号資産を質草とするスマコンによる質屋	✓ **仕組み:** ユーザーはETHなどの価格変動のある暗号資産を、Makerのスマートコントラクト(Vault=金庫)に担保としてロックする。 すると、その担保価値の一定割合まで、米ドルに連動したステーブルコイン「DAI」を新規に「発行(借入)」できる。 貸し出されるDAIが担保価値の一定割合に抑えられている(過剰担保)のは、価格変動によりETHの市場価値が下がった際、貸し出したDAIを回収できない(債務超過)となり1ドルの価値が保てなくなる(デペッグする)のを防ぐため。 DAIの借入中は金利(Stability Fee)がかかり、精算時に支払う。(プロトコルの収益源) ✓ **価値の維持:** DAIの信用(1DAI = 1ドル)は、「システム全体で、発行されているDAI以上の価値の担保が常に存在する」ことによって成り立つ。これを維持するための安全装置として、以下のような「強制清算」の仕組みがある。 担保にしているETHの価格が暴落し、DAIの貸出額に対して担保ETHが危険な水準に達する(最低担保率を下回る)と、スマートコントラクトが自動的に担保のETHを没収して市場で売却、DAIを取得してユーザーへの貸出分のDAIと相殺する。 これにより、常にシステム全体で「発行されているDAI以上の価値を持つ担保」が存在することが保証され、1DAI = 1ドルが維持される。

*なお、2024年8月にプロジェクト名を「Sky」へリブランディングしており、ステーブルコイン(DAI)についても現名称は「USDS」

3.2.5 リキッドステーキング

- リキッドステーキングは、ステーキング(PoSでのブロック承認作業への参加)による「資金ロック」のデメリットを解消する仕組み。
- PoS(Proof of Stake)とは、PoW(Proof of Work)における演算能力の代わりに、
  保有する資産の量をもって取引(ブロック)の正当性を担保する合意形成手法。
  - 「このブロックチェーンの暗号資産を多量保有し、ネットワークに預け入れている(Stakeしている)人ほど、
    そのネットワークを攻撃して価値を毀損する動機がないだろう。
    だから、預け入れている資産の量と期間に応じて、ブロックを追加する権利と報酬を与えよう」という考え方に基づく。

代表的な分散型ステーブルコインプロトコル

	仕組み・特徴等
Lido ステーキングの預かり証* (*LST; Liquid Staking Token)	✓ **仕組み:** ETHをステーキングすると、本来はネットワークに資金が長期間ロックされ、その間は他の取引に使えなくなる。 Lidoは、ユーザーから集めたETHをまとめてステーキングのプロ(バリデーター)に委任する。 ✓ **預かり証トークン:** 上記の見返りとして、Lidoのプログラム(コントラクト)は預かったETHと1:1の価値を持つ預かり証トークン「stETH」をユーザーに発行する。(stETHは、stakedETH、または「エスティース」と読む) ユーザーはstETHを持っていればステーキング報酬を受け取れ、かつそのstETHをAave等で担保に入れたり、Uniswapで売買したりと、DeFiのプロトコルで自由に運用することができる。 (預り証トークンのことをLST; Liquid Staking Tokenという)

4章 まとめ

4.1 まとめ (冒頭サマリと同内容)

日本総研
The Japan Research Institute, Limited

4.1 まとめ (冒頭サマリと同内容)

- 広義のDeFiと狭義のDeFi
  - ✓ 分散型金融(DeFi)について、伝統的金融機関等とブロックチェーンエンジニア等の専門家との間では、認識する内容に差異がある。
  - ✓ 後者は、パブリックブロックチェーンに保存されたプログラム(=スマートコントラクト)で実行される金融的機能を指す。(狭義のDeFi)
  - ✓ 一方、執筆時点(2026年3月)では、金融業界などでは上記の内容(狭義のDeFi)まではあまり意識されておらず、暗号資産そのものや、既存の金融商品のトークン化(アセットトークナイゼーション)の領域を主としてDeFiが認識されている。

- アセットトークナイゼーションにより加速する金融業務の標準化と効率化
  - ✓ アセットトークナイゼーションは、共通基盤(≒統合台帳)に様々な金融商品を載せるという点に新規性があり、以下のような技術的進展が見込まれている。
  - ✓ 金融機能のモジュール化：
    - ➢ 伝統的金融機関が重厚長大なシステムで一枚岩的に提供してきたサービス全体が、モジュール(小機能単位)に分解される。
  - ✓ 金融機能の標準化：
    - ➢ 同レイヤーのモジュール同士が競争や共通化を進めることでモジュールの機能が最適化・標準化される。
    - ➢ また、レイヤー間の連携方式についても標準化が進む。
    - ➢ 標準化技術の多くはしばしばオープン化され、新規プレーヤーの参入に繋がる。

日本総研
The Japan Research Institute, Limited

4.1 まとめ (冒頭サマリと同内容)

- アセットトークナイゼーションへ取り組む伝統的金融業界へ向け
  - ✓ アセットトークナイゼーションの本質は金融機能のモジュール化・標準化であり、一過性の流行としてではなく、バックエンドを含めた業務の最適化・効率化の観点も持って取り組むことが肝要ではないか。
  - ✓ 金融機能のモジュール化・標準化こそが本質であると捉えた時、「ブロックチェーン上にトークンという形式で情報を記録する」という構成が最適ではない要件も発生し得ると考えられる。
  - ✓ 既に相当に効率的な金融システムを国内に抱える日本の伝統的金融機関としては、上記観点と新興技術への積極的なキャッチアップの両立に基づく判断が求められる。*

- 暗号資産へ取り組む伝統的金融業界へ向け
  - ✓ 足許、日本国内では暗号資産に関する規制の大幅な方針転換が進んでいる。
  - ✓ 暗号資産を巡っては対極的な意見が存在。社会的価値を意識した事業設計が中長期的信用の醸成に繋がる。

- トークン化(デジタル化)対象資産の拡大へ向け
  - ✓ 現行の法制下で紙の券面発行が前提となりデジタル化の障害となっているものについては、法改正等により解消されることが望まれる。(券面不発行や原簿への記録による第三者対抗要件の具備等)

*『すでに密集した状況にコンポーネントを追加することで、意図せず新たな複雑さをもたらす可能性』について「ASAP: デジタル資産プラットフォームの概念モデル」(p.19)でも指摘されている。

執筆者・先端技術ラボのご紹介

執筆者

市原 紘平
Ichihara　Kohei

シニア・リサーチャー
Senior Researcher

Web3研究に取り組み、2018年からセキュリティトークン等をSMBCグループ内で啓蒙。現在、事業企画への生成AI活用に興味。

■ 執筆レポート

- デジタルアイデンティティの動向と展望
- AI駆動開発とSysEngへのAI適用研究の動向
- EAの活用動向とArchiMateの概説
- デジタル証券とRWAトークンの動向　他

■ 学術論文

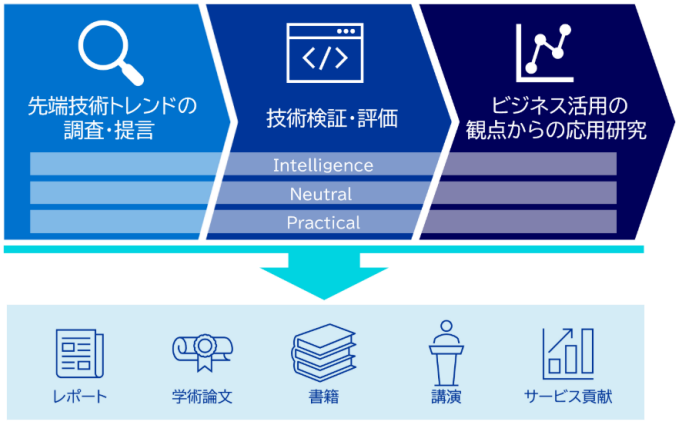
- Automation of Node Redundancy for Stable Operation of Various Types of Blockchain Nodes. (IEEE ICCE 2025) 他

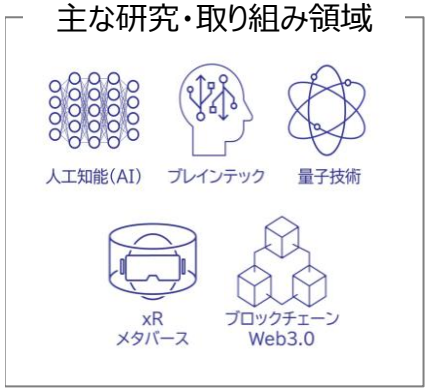
■ 専門委員活動 他

- ISO/TC 68委員会 委員、ISO/TC 68/JWG 1（デジタル通貨） エキスパート

先端技術ラボ

先端技術を活用したITサービスの創出に向けた技術の目利き役として、
「先端技術トレンドの調査・提言」、「技術検証・評価」、
「ビジネス活用の観点からの応用研究」に取り組んでいます。





弊社ホームページの **特集サイト** では、IT分野における先端技術の調査レポート、及び所属する部員のプロフィール詳細がご覧いただけますので、ぜひご参照ください。

本レポート執筆者へのメディア取材や講演などに関するご相談につきましては、当社ホームページの **問い合わせフォーム** よりご連絡ください。

株式会社日本総合研究所

日本総研は、シンクタンク・コンサルティング・ITソリューションの3つの機能を有するSMBCグループの総合情報サービス企業です。

東京本社　〒141-0022　東京都品川区東五反田2丁目18番1号　大崎フォレストビルディング
大阪本社　〒550-0001　大阪市西区土佐堀2丁目2番4号