Discussion Purpose Only

託された未来をひらく
三井住友トラストグループ

CBDCフォーラムWG4

アセットトークナイゼーションの海外動向

2025年3月25日
デジタル企画部

三井住友信託銀行

目次

- 当資料は、CBDCフォーラムWG4で議論を行うための情報提供を目的として作成されたものです。
- 特定の金融商品の売買を推奨・勧誘するものではありません。
- 当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。

1 MMFトークン化の事例（BUIDL）

1. 金融機能からの見た特徴
2. スマートコントラクトから見た特徴

BUIDLとは

- BlackRock USD Institutional Digital Liquidityは2024年3月にEthereumで発行。
- 大手運用会社のMMFトークン化であり、ステーブルコインへの自動決済で注目を集めた。

BUIDLの特徴

- 米国の法律に基づく証券として発行。
- 運用内容は一般的なMMF（マネーマーケットファンド）。
- Ethereumで最初に発行され、その後複数のチェーンに展開。
- ステーブルコインUSDCへの即時換金機能を提供。
- 利息は通常のMMFの再投資と同様にBUIDLで月次分配。
  - 日次での分配にも現在は対応

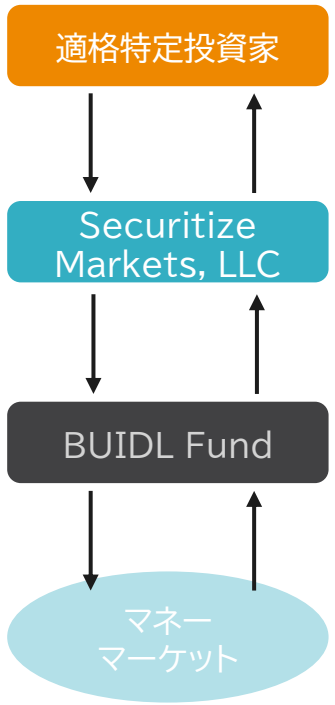
BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network

Investors can subscribe through Securitize Markets, LLC to participate in the fund. BlackRock invests in Securitize to drive transformation for digital assets infrastructure.

Mar 21, 2024

（出所）BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network -March 20, 2024 at 10:28 pm | MarketScreener

「証券」のスキーム概要



Securities Act Reg506（c）及びInvestment Company Act Section 3(c)に基づく。購入先は制限され、購入は500万米ドル～。

Securitizeのプラットフォームでトークン化し、販売を同プラットフォームで行う。

BlackRock Financial Management, Incが運用するMMF（Pooled Investment Fund Interests）

Bank of New York Melonがカストディアン、PwCがファンド監査を担当。

（出所）SEC FORM D

【ご参考】MMF（マネーマーケットファンドについて）

MMFとは、「国内外の公社債やCP（コマーシャルペーパー）、CD（譲渡性預金）等の短期の金融商品を中心に運用する、追加型公社債投資信託のこと。株式は一切組み入れず、リスクを少なくして安定した利回りを目標とするファンド。」（MMF｜投資の時間｜日本証券業協会）

A money market fund (MMF) is a type of mutual fund that invests in cash, cash equivalents and short-term debt securities. Think of MMFs as a cash management investment solution intended to offer portfolio diversification, liquidity and operational ease.（What are money market funds?｜BlackRock）

MMFトークン化のポイント

- 金融＝資金の融通には、金融商品には資金の性質を変換する役割
- 預金；家計の余剰資金を預かり、事業会社等の資金調達等へ
- MMFはホールセールファンディングとしての性格も（右記ご参照）
- MMFトークンの取組でMMFを単にトークン化しただけではなく、**資金の出し手に暗号資産あるいは分散型金融の主体を取り込んだこと**がポイント。（次頁）

図表1　MMFのイメージ

図表2　MMFおよび商業銀行による資金融通*7

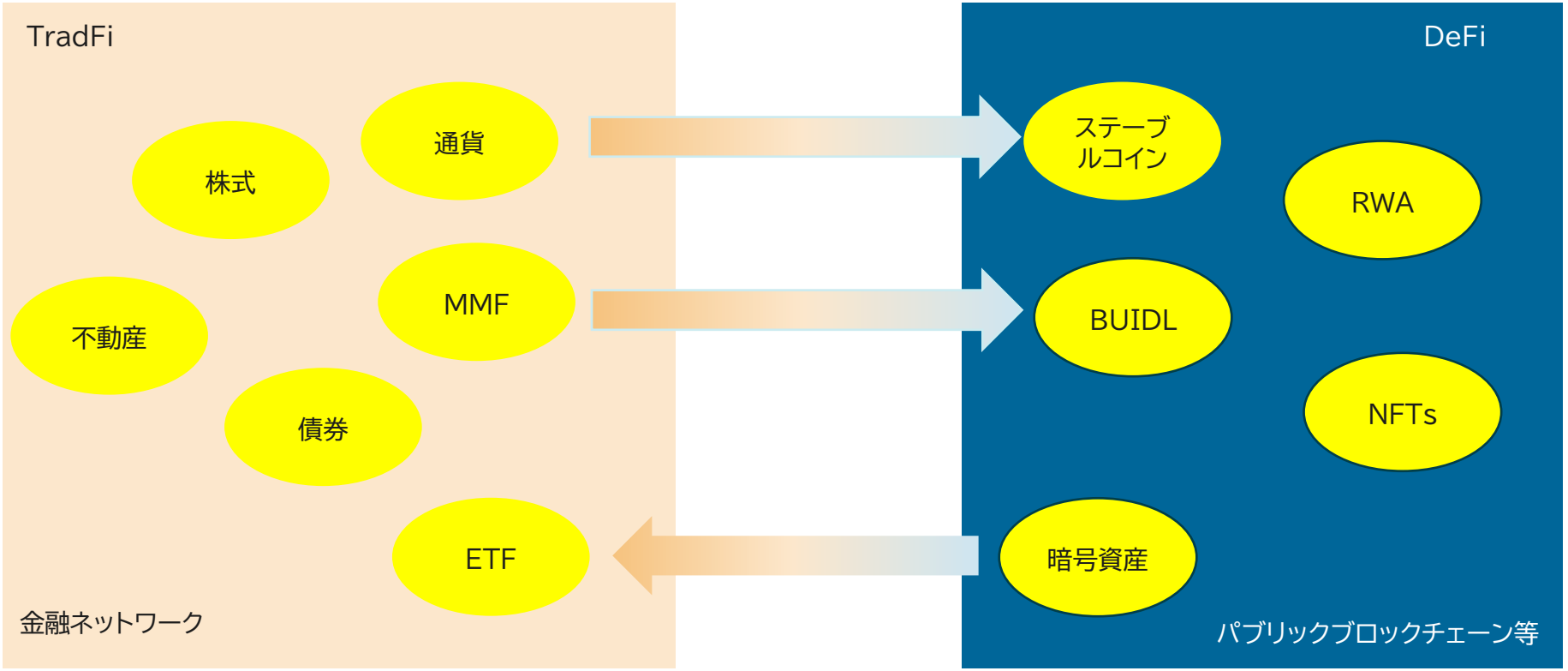
ホールセール・ファンディングのイメージ

リテール・ファンディングのイメージ

（出所）広報誌「ファイナンス」：米国MMF（マネー・マーケット・ファンド）入門

伝統金融(TradFi)と、分散金融(DeFi)の往来

- BUIDLは伝統金融商品を転用して暗号資産・分散型金融の経済圏の流動性をサポートするアセットを創出。
- ステーブルコインの需要が示すようにDeFiユーザーも法定通貨へのアクセスが必要。
- (米国等で取扱のある)暗号資産ETFは暗号資産へのアクセスを伝統金融の手法で提供するもの。

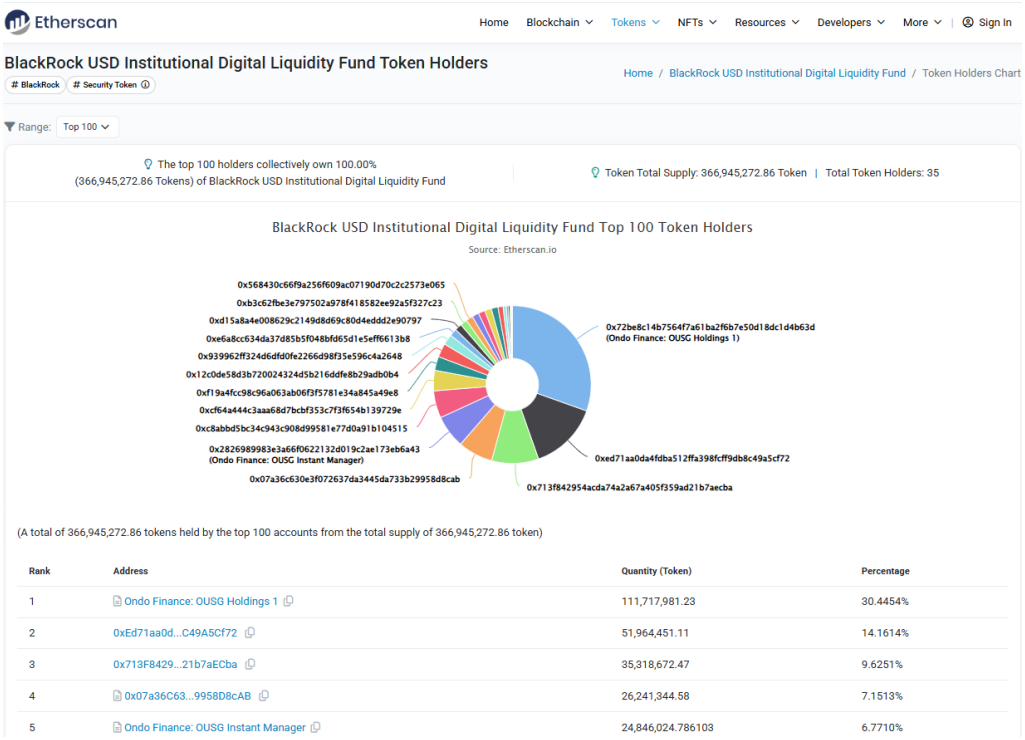


従来の投資家　　クリプトユーザー　　未来の金融？

BUIDLの保有者

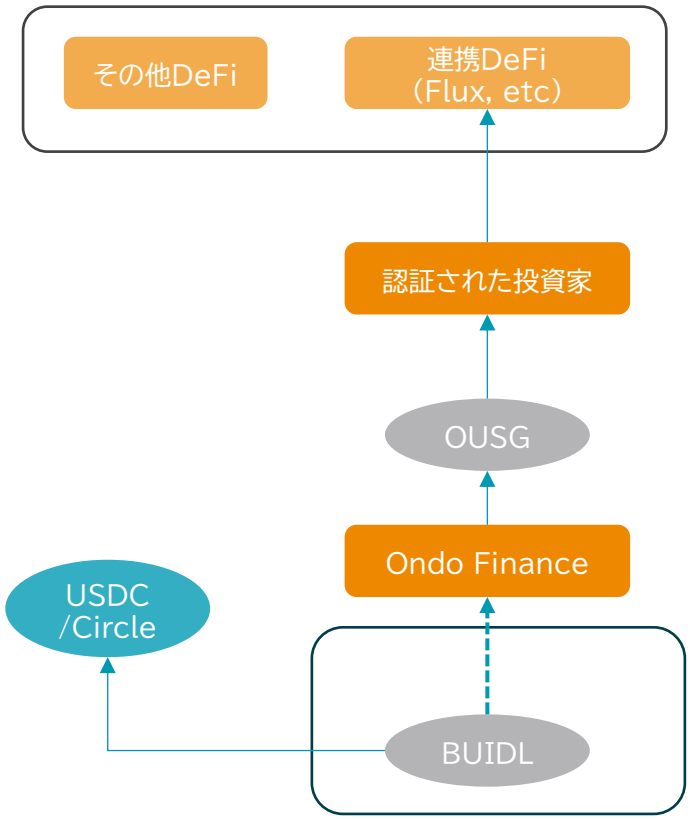
- BUIDLの最大保有者はOndo Finance社で、OUSGトークンに利用していることがうかがえる。
- OUSGはDeFi利用時の担保として活用され、DeFi取引の流動性の一端をBUIDLが担っていると理解できる。

Etherscanで見る上位保有者



(出所)EtherScan(2025/3/11アクセス)
BlackRock USD Institutional Digital Liquidity Fund Token Contract and Distribution Chart

BUIDLを通した流動性供給



認証されたDeFiプロトコルで利用され、流通トークンなどを通してDeFiへ(次頁)

OUSGは認証されたユーザーのみ保有

Ondo Financeが発行するトークン
BUIDLが裏付資産

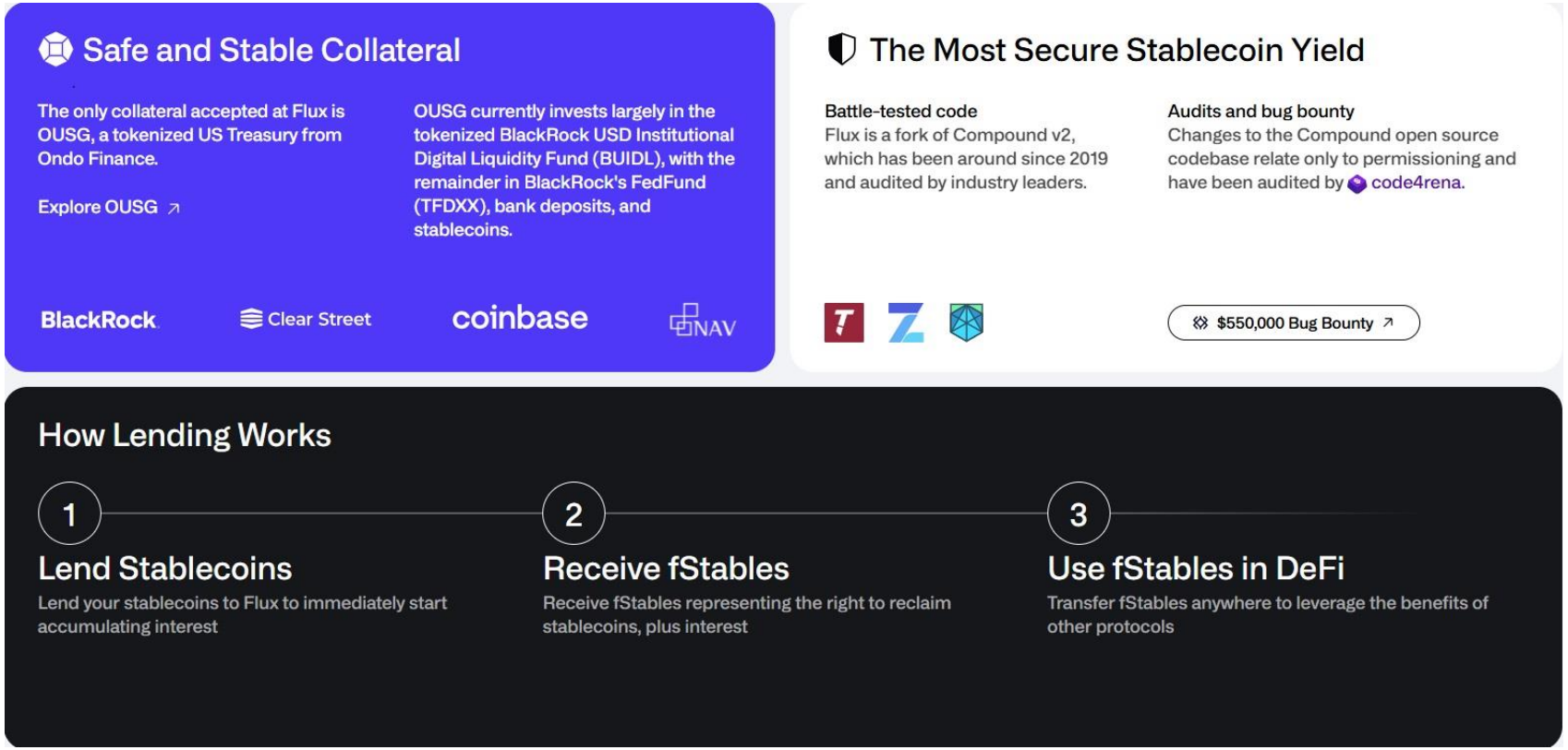
Ondo FinanceはBUIDLの一投資家

余剰が生じればUSDCに変換することも可能

(出所)BUIDL保有情報やOndo Finance/ Flux FinanceのHPを基に作成
Ondo Finance、fluxfinance.com

【参考】Flux；fluxfinance.com

- Flux FinanceではOUSGを担保にできる。
- OUSGを担保に得たアセットを活用して他のトークンを得るなどして、DeFiで取引をすることが可能になる。



（出所）Flux Financeホームページ（2025/03/11 アクセス、fluxfinance.com

MMFトークンから見るデジタルアセットの役割

- MMFトークンは伝統金融の流動性をDeFiへ持ち込む一手段となっている。
- 伝統金融でもトークンの利用が議論され始めており、今後のデジタルアセットの役割に注目が必要。

BUIDLが果たす機能とデジタルアセットの役割

- Ondo Financeはかつて裏付資産としてETFを保有していたが現在はBUIDLへ移行。
- 運用会社のオペレーション＋オンチェーンでの検証可能性がユーザーに安心を与えているか。
- オンチェーンの取扱の容易さからCFTCで店頭デリバティブでの担保利用についても議論。
- OUSGはMastercardが展開するMTNへ提供を進めるなど既存の金融ネットワークにも活用の幅を広げようとしている。

Use of BlackRock Tokens as Collateral Moves Closer to Mainstream

- CFTC subcommittee moved its recommendations to full committee
- The full committee is expected to vote on them later this year

By Olga Kharif and Muyao Shen
2024年10月3日 at 3:55 JST
Updated on 2024年10月3日 at 6:24 JST

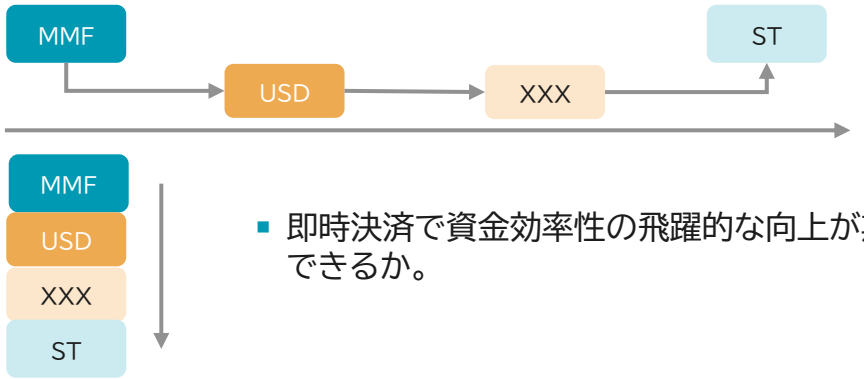
(出所)Use of BlackRock Tokens as Collateral Moves Closer to Mainstream - Bloomberg

Ondo Finance Brings Tokenized Real-World Assets to Mastercard's Multi-Token Network

(出所)Ondo Finance Brings Tokenized Real-World Assets to Mastercard's Multi-Token Network

- 安易な連想ではあるが、オンチェーンのTreasuryやCBDCが現れるとこの役割は代替できるか？
- MMFからSCへの変換がT+0で即時実行できることで、MMFの資金化に数日要することとの差異。
- 実質マネーマーケットを通して中銀の流動性にアクセスが可能であることを踏まえると民間の取組で十分か？
- BISのレポートではステーブルコインはクリプトマーケットのショックとは関係なく、金融政策からの影響の方が強いという指摘も。(参考; Stablecoins, money market funds and monetary policy)

即時決済とcomposability



- 即時決済で資金効率性の飛躍的な向上が期待できるか。

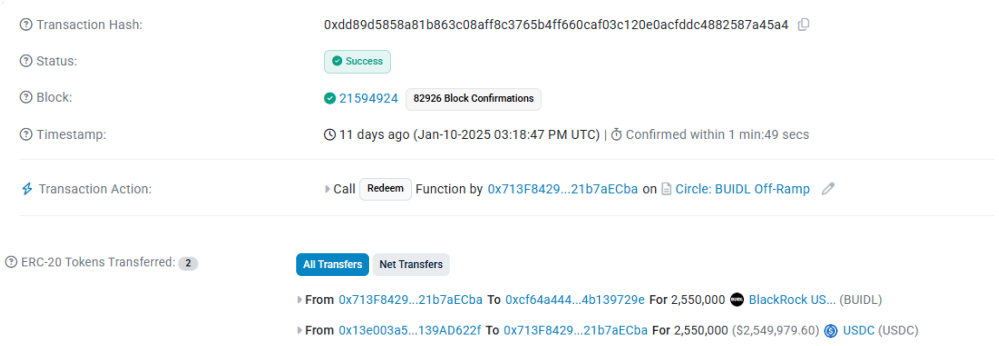
BUIDLの技術的特徴

- BUIDLはUSDC（米Circle社が発行するステーブルコイン）へ即時換金が可能。
- 配当は一つのブロックチェーン上で一つのトランザクションとして分配が可能。

USDCへの換金

Etherscan上での確認

- 関数”Redeem”を呼び出して換金を実行
  - 呼び出し元のアドレスからBUIDLを送り出し
  - 同アドレスでUSDCを受取。

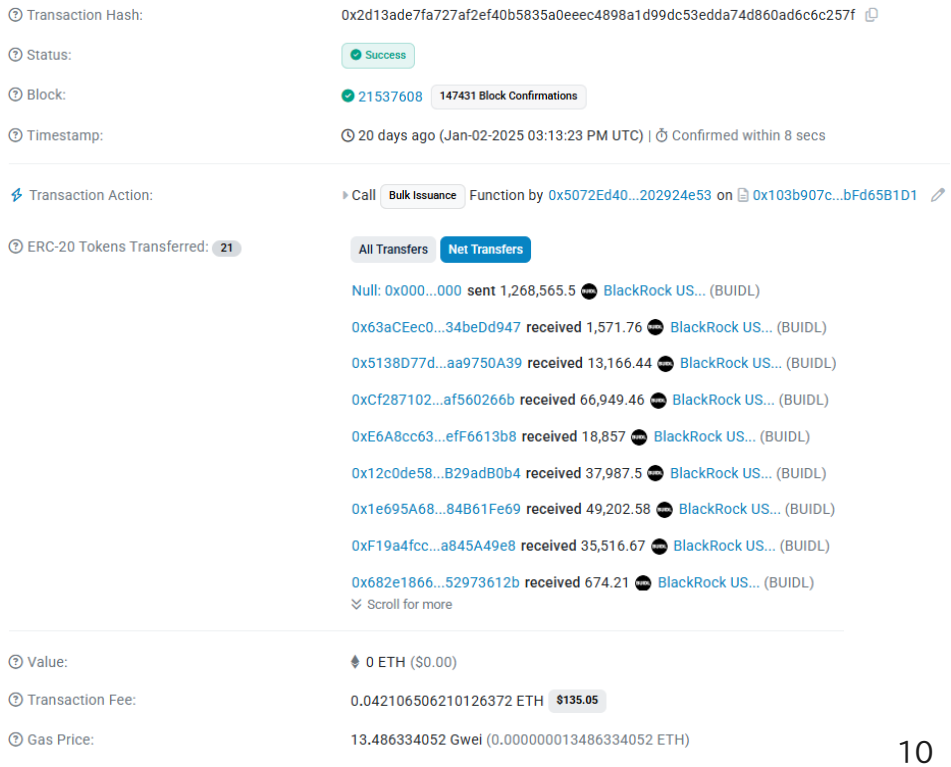


（出所）Etherscan

一括での分配金

Etherscan上での確認

- 関数”BulkIssuance”を呼び出して換金を実行
  - 合計1,268,565.5のBUIDLを分配
  - 投資家向けの分配内容はその下段で確認

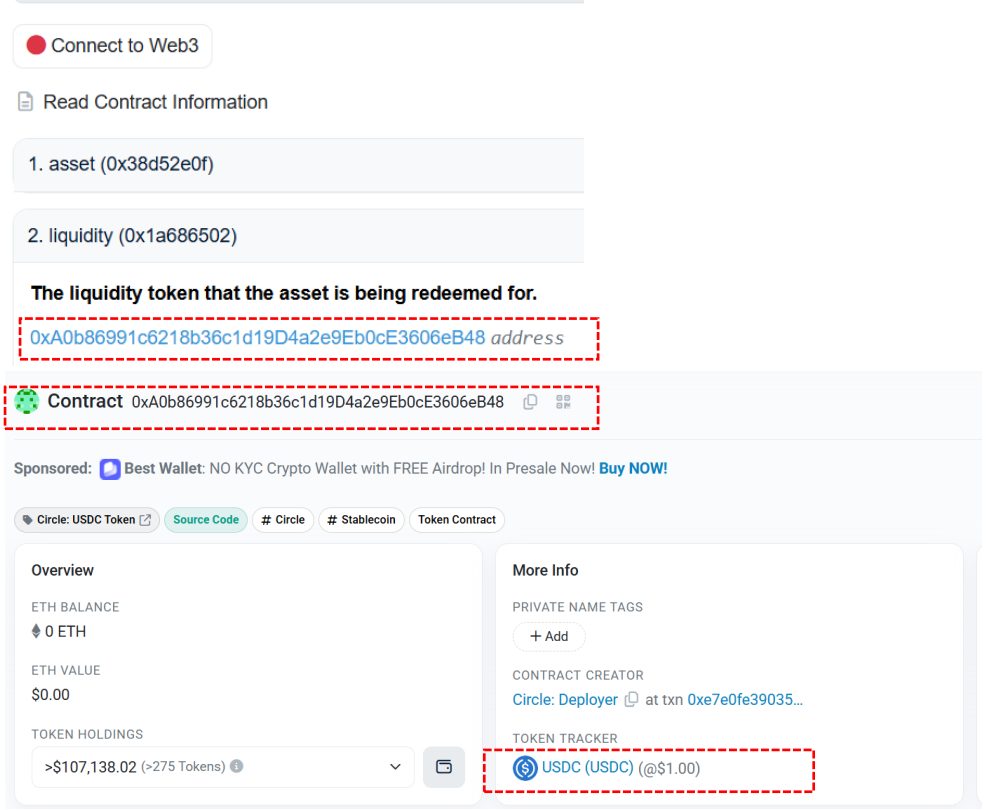


コントラクトでの確認：USDCへの変換“redeem”

```
function redeem(
    uint256 amount
) external override whenNotPaused onlyAssetHolder {
    address recipient = settlement.recipient();

    // Transfer asset
    IERC20(asset).safeTransferFrom(msg.sender,
                                   recipient, amount);

    // Checkpoint liquidity balance before
    uint256 redeemerBalanceBefore =
            IERC20(liquidity).balanceOf(msg.sender);
    // Notify settlement
    settlement.redeem(msg.sender, amount);

    // Require liquidity balance increase by amount (1:1)
    require(
        IERC20(liquidity).balanceOf(msg.sender) -
                        redeemerBalanceBefore == amount,
                        "Liquidity transfer failed");
}
```

Circle: BUIDL Off-Ramp (0x31d3f59ad4aac0eee2247c65ebe8bf6e9e470a53) | Address 0x31d3f59ad4aac0eee2247c65ebe8bf6e9e470a53 | Etherscan

- スマートコントラクトのコードがEtherscanなどで確認が可能。
- これにより予め挙動を確認できる。



Circle: USDC Token (0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48) | Address 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48 | Etherscan

- 引出トークンはスマートコントラクトのアドレスで確認ができる。
- 該当アドレスをさらに確認するとUSDCであることがわかる。

コントラクトでの確認：一括分配“bulkIssuance”

```
    function bulkIssuance(uint256 value, uint256 issuanceTime,
                          uint256 totalInvestors, uint256 accreditedInvestors,
                          uint256 usAccreditedInvestors, uint256 usTotalInvestors,
                          uint256 jpTotalInvestors, bytes32[] memory euRetailCountries,
                          uint256[] memory euRetailCountryCounts)
                          public override onlyIssuerOrAbove
        {
        require(euRetailCountries.length == euRetailCountryCounts.length,
                'EU Retail countries arrays do not match');
        // Issue tokens
        getToken().issueTokensCustom(omnibusWallet, value, issuanceTime, 0, '', 0);
        addToCounters(totalInvestors, accreditedInvestors, usAccreditedInvestors,
                      usTotalInvestors, jpTotalInvestors, euRetailCountries, euRetailCountryCounts, true);
        emitTBEOperationEvent(totalInvestors, accreditedInvestors,
                     usAccreditedInvestors, usTotalInvestors, jpTotalInvestors, true);
    }
```

DSToken | Address 0x603Bb6909Be14f83282E03632280D91bE7fB83b2 | Etherscan

- Redeemと比較して複雑に見えている。
- コードによる検証は可能であるが、挙動を確認することは(専門的知識がないと)難しい。
- BUIDLに関していえば、一定水準以上の投資家限定。
- 保有者を拡大して類似の商品を検討する場合には、技術的に検証可能であることに加え、想定ユーザーが安心して活用できる環境を整備していくことが望ましい。

2 実証実験事例とプライバシー関連技術（RSN、EPIC、etc）

1. Regulated Settlement Network
2. プライバシー強化技術（PET）関連のプロジェクト
3. その他トピックス

Regulated Settlement Network（RSN）について

- 米国金融機関がSIFMA、Swiftらと取り組んだ実証実験。NY連銀のInnovation centerもオブザーバ参加。
- 異なる資産間あるいは異なるネットワーク間の決済を検証

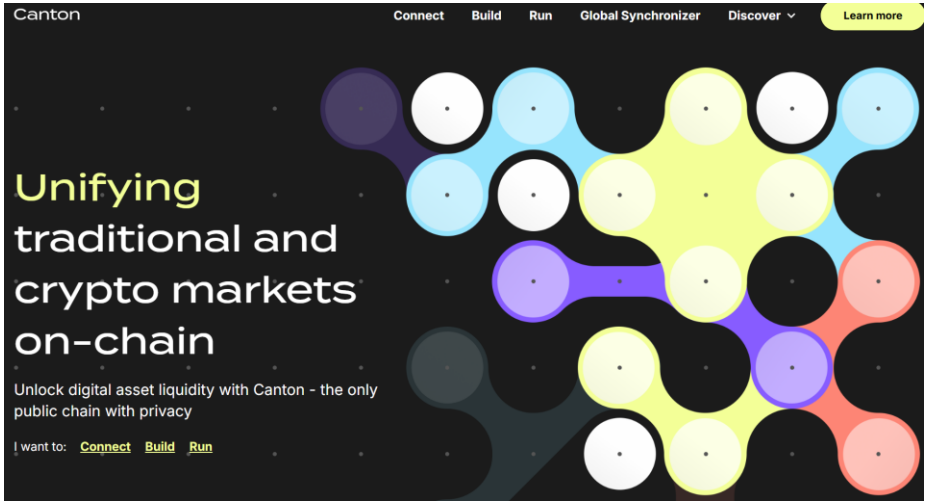
RSNの実証実験

- 金融機関からはJPMorgan,Citi,Visa,Mastercard、らが参加。
- 複数のプラットフォーム間で決済を行う将来を想定して実験。

（出所）BlackRock Launches Its First Tokenized Fund, BUIDL, on the Ethereum Network -March 20, 2024 at 10:28 pm | MarketScreener

金融用のDLT“Canton Network”も利用

- Canton Networkは2023年にDigital Asset社が開発した“DAML”をベースに開発された分散台帳。
- 金融機関での利用をターゲットに設計されている。



（出所）①Introducing the Canton Network

RSN:インターオペラビリティについて

- 既存の銀行システム(Fedwire、CHIPS、ACHなど)との統合を視野に入れて設計。
- DLTベースの決済システムを 従来の金融インフラとスムーズに統合 できるようにする。

プラットフォーム間でのDvP決済を検証

- トークン化された商業銀行預金、米国債券などの複数の資産クラスを分散台帳上で取扱。
- 他の分散台帳システムや既存システム間とも決済インフラの断片化や決済プロセスの不確実性といった課題を解消する可能性を示唆。

Figure 3: Cross-network DvP settlement high-level design

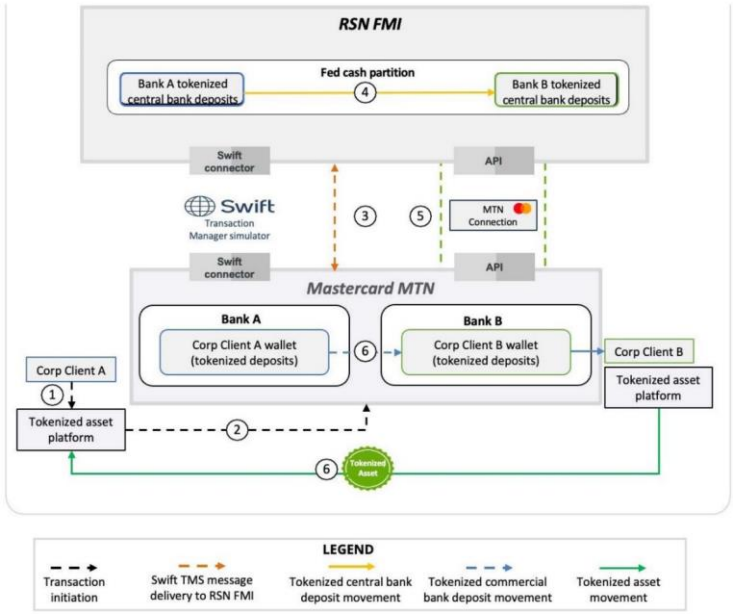
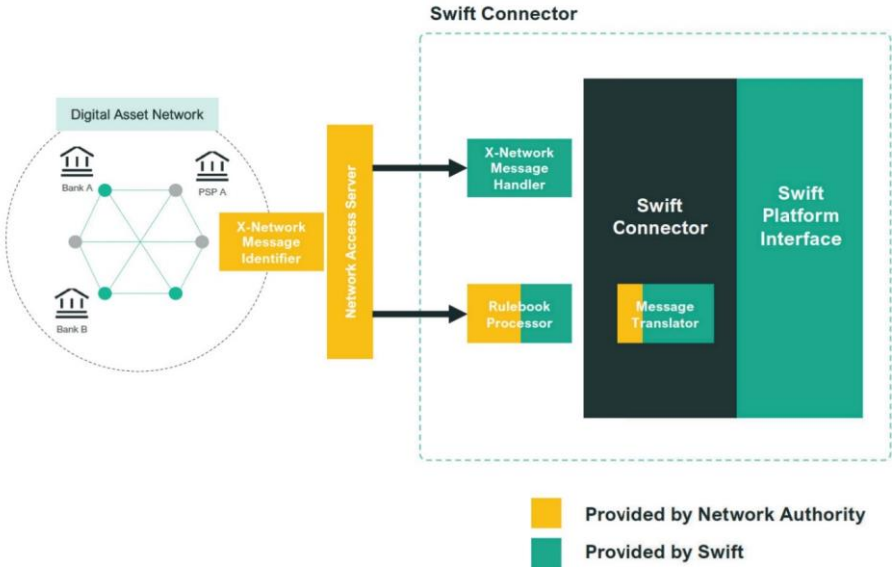


Figure 4: Swift Connector Integration Model



(出所)Regulated Settlement Network Proof-of-Concept - SIFMA - Regulated Settlement Network Proof-of-Concept - SIFMA

Canton Networkについて

- プログラミング言語DAMLをベースに開発。「当事者間」でのみ取引内容を共有するDLT。
- UTXOに類似した「contract」を中心に取引を表現

DAMLのContractについて

- Contractに関係者を定義して閲覧権限をコントロール
- 契約には(consuming/non-consuming)の違いがあり、consmingを使用後はarchiveを行い再利用できないよう変換。
  - 情報の参照等はnon-consumingとして取扱

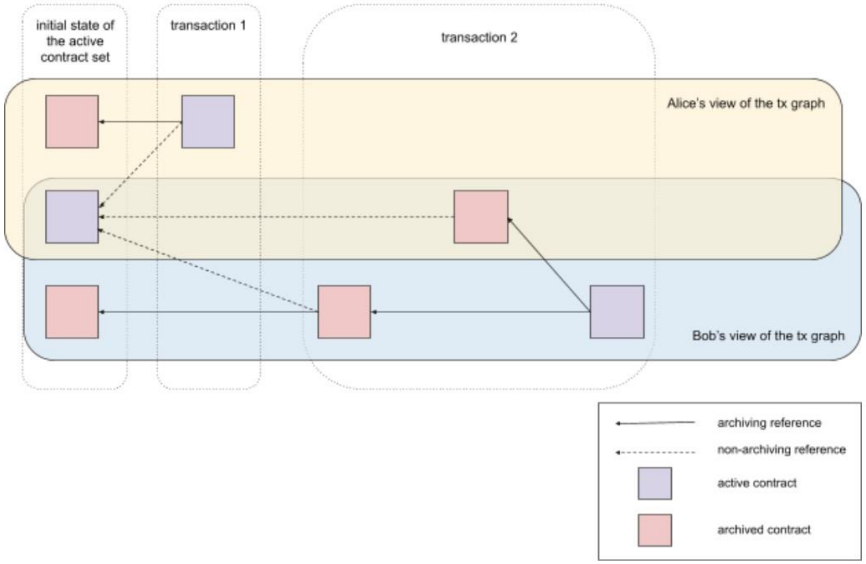


Figure 1: Example transaction graph with sub-transaction privacy. Alice and Bob each have only a partial view of the full transaction graph. Initially there are three active contracts, each party sees only two of them. Transactions 1 and 2, submitted by Alice and Bob respectively, evolve the Active Contract Set (ACS), archiving two of the initial contracts, creating two new active contracts, and

Canton Networkの“ノード”について

- ネットワーク参加者はノードをプロバイダ(Canton Service Provider)に接続して取引を行う。

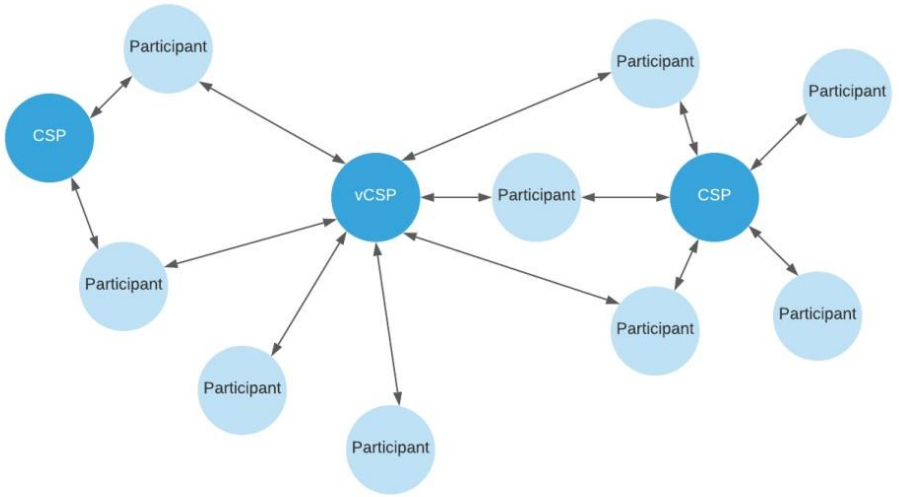


Figure 3: Canton Network topology. Participants connect to each other via Canton Service Providers (CSPs) or consortium vCSPs. Parties can transact if their participant nodes are connected to a common CSP or vCSP. No single node processes all network transactions.

(出所)Canton Network - White Paper - Jan 2024

プライバシー技術に関する動向紹介

- プライバシー管理は金融取引において非常に重要な要素
- PET（Privacy Enhancing Technology）は実務

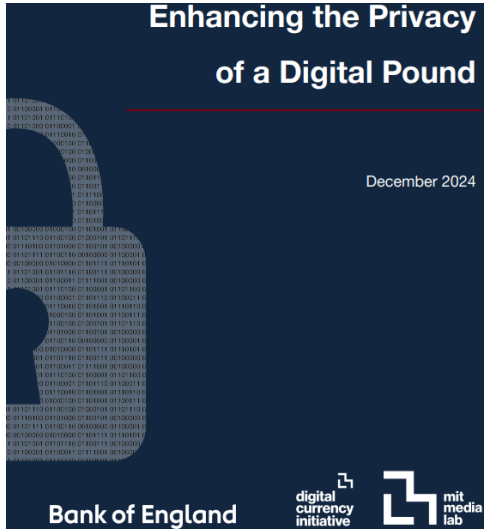
JP Morgan Kinexys Project EPIC

- 2024/12にJP Morgan/Kinexysからレポートが公開
- ファンドのトークン化を事例にプライバシーやアイデンティティの管理においてPETを検証
- 具体的には投資家のオンボーディング、アトミックスワップを利用した効率的な資金管理さらにはセカンダリ取引のプライバシー保護に取り組んだ。

（出所）JPMC-Kinexys-Project-Epic-Whitepaper-2024.pdf

イングランド銀行とMIT DCI

- 2024/12にイングランド銀行とMITからプライバシー強化について共同研究を行ったレポートを公開。
- 秘匿化、ゼロ知識証明そしてMPCなどの技術を検証。



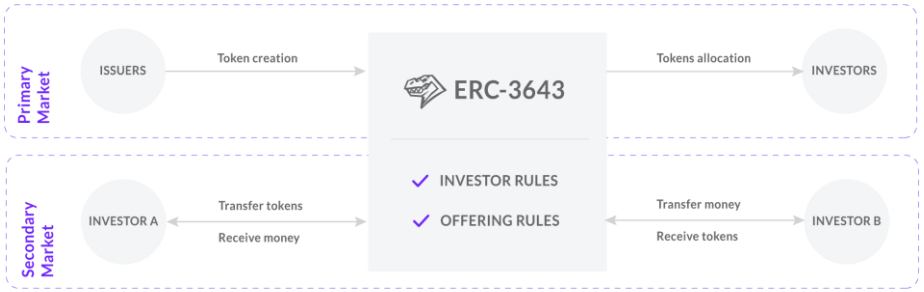
（出所）Enhancing the Privacy of a Digital Pound

トークン規格への組込

- トークン規格にアイデンティティ管理等プライバシー管理を取り込んだものも検討されている

ERC-3643（Permissioned Tokens）

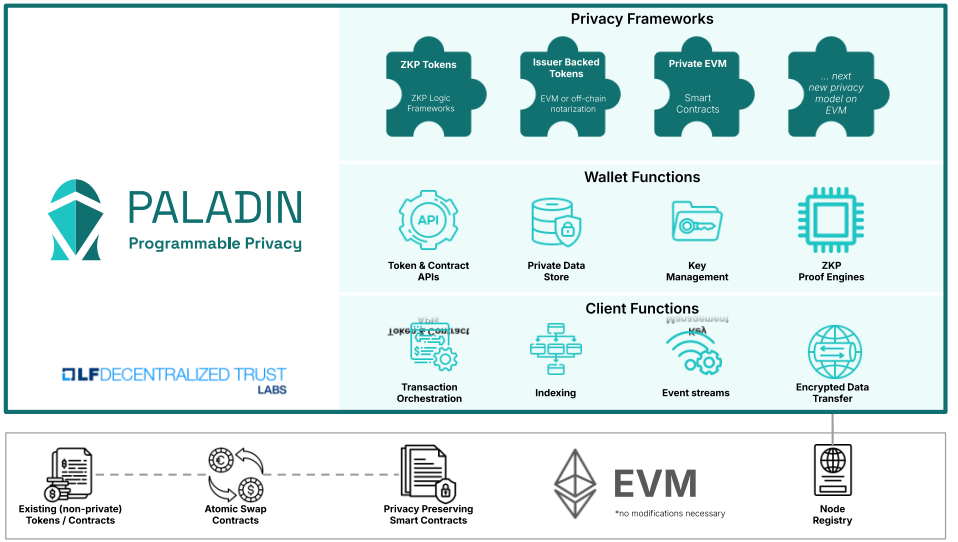
- ERC-3643はTokeny社による開発で、T-REX（Token for Regulated Exchange）と呼ばれており、金融規制の順守を目的の一つにしている。
- ABN AMRO銀行が同規格を利用して、2023年9月にPolygon上でグリーンボンドを5百万ユーロ発行。



（出所）ERC-3643: The Official Smart Contract Standard for Permissioned Tokens

Paladin（LF Decentralized Trust）

- LF Decentralized Trust傘下のOSSプロジェクト。
- ゼロ知識証明を利用して数学的に設計されたZETOトークンや発行体に信用を置いて発行するissuer backed トークンなどを取扱。



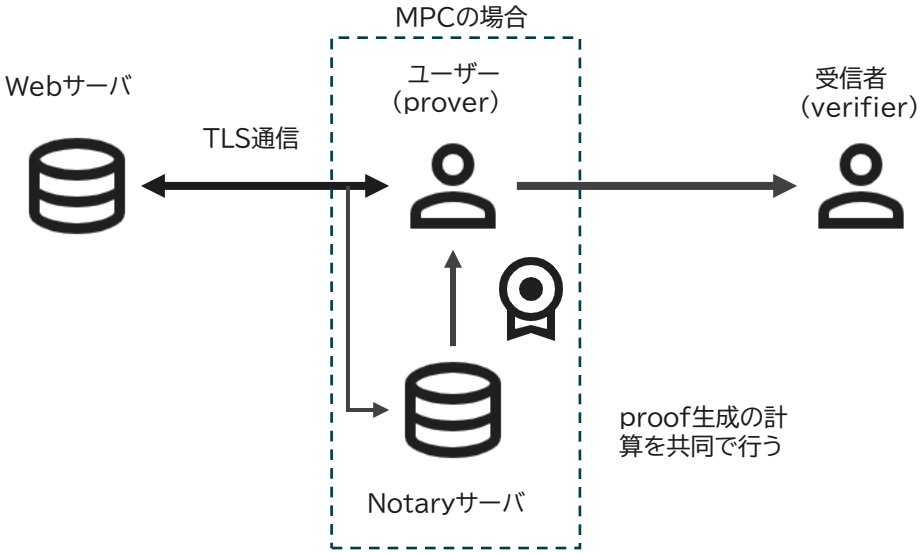
（出所）Paladin Programmable Privacy for EVM

【トピックス】WEB PROOF

- WEB Proofはwebで取得したデータを第三者へ正当なものであると証明すること。
- TLS通信とゼロ知識証明関連技術を組合わせたものがzkTLSと呼ばれている。

zkTLSによるWeb Proof

- TLS通信はhttpsで利用されているオンライン通信を安全に行う規格。
- 通信は安全に行われるが、その内容を第三者に証明することは容易ではない。
  - 画面キャプチャは合成画像かもしれない。
  - アクセスしている画面で見てもHTML情報をコピーした偽サイトかもしれない。
- TrustPointを設定して効率的かつ安全な情報連携を目指すもの。
  - MPC、TEE、Proxyなどのプロトコルを利用してTLS通信内容（ウェブ画面の内容等）を第三者にその正当性を検証可能にする。
  - 情報のポータビリティを活用した取組について模索中。



Web Proofのユースケース	
資格情報	個人データを第三者に証明
整合性	データの正確性と信頼性向上
ポータビリティ	プラットフォーム間でデータを移動
資産化	データの収益化

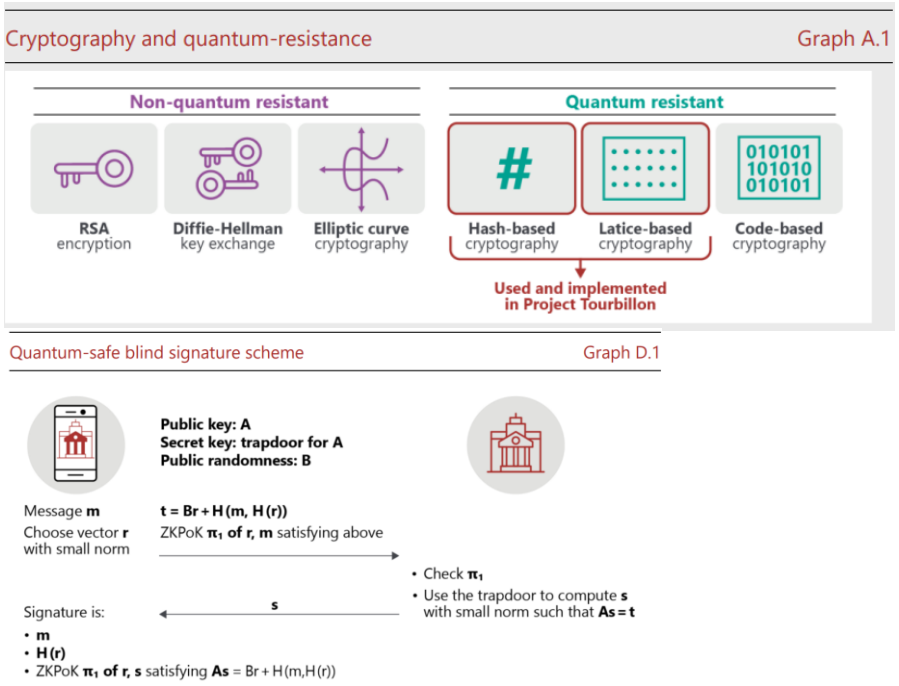
（出所）What will the verifiable web look like?

【トピックス】量子コンピュータ、耐量子暗号

- 量子コンピュータの実用化が意識され、公開鍵暗号の危殆化リスクが指摘されている。
- 「2030年問題」が注目を集め、国内金融機関でも対応が議論。

CBDCと耐量子暗号の検討

- Project Tourbillionはプライバシーやセキュリティに焦点を当てたBISによるプロジェクト
- セキュリティに関しては量子耐性のある暗号について検証



(出所)Project Tourbillon: exploring privacy, security and scalability for CBDCs

「2030年問題」と暗号方式の入替

- 米国NISTからは2030年には2048bitの暗号鍵長の公開鍵暗号は破られる可能性を指摘
- 国内でも暗号方式の移行などビジネスの影響を検討

Table 4: Security strength time frames

Security Strength		Through 2030	2031 and Beyond
< 112	Applying protection	Disallowed	
	Processing	Legacy use	
112	Applying protection	Acceptable	Disallowed
	Processing		Legacy use
128	Applying protection and processing information that is already protected	Acceptable	Acceptable
192		Acceptable	Acceptable
256		Acceptable	Acceptable

(出所)SP 800-57 Part 1 Rev. 5, Recommendation for Key Management: Part 1 – General | CSRC

令和６年７月４日
金融庁

「預金取扱金融機関の耐量子計算機暗号への対応に関する検討会」の開催について

(出所)「預金取扱金融機関の耐量子計算機暗号への対応に関する 検討会」の開催について：金融庁

Disclaimer

- 当資料は、CBDCフォーラムWG4で議論を行うための情報提供を目的として作成されたものです。
- 特定の金融商品の売買を推奨・勧誘するものではありません。
- 当資料は当社が信頼性が高いと判断した情報等に基づき作成しておりますが、その正確性・完全性を保証するものではありません。