資料4

デジタル・分散型金融への対応のあり方等に関する研究会（第３回）

技術的設計を起点とした、本研究会における課題と論点整理の提案

松尾　真一郎
ジョージタウン大学研究教授／バージニア工科大学研究教授

2026 年 11 月 26 日

本日の目的

合わせたい認識

規制のあり方は、オンチェーン金融の概念ではなく、
それを実現する設計と実装が**保証する範囲**を対象にする必要がある。

1. 議論の多くは、ステーブルコイン、トークン化、定義の定まらない DeFi など、サービス概念・制度概念から始まっている。
2. しかし、オンチェーン金融の基盤をなすブロックチェーン技術および ERC の規格・実装が保証することと、金融サービスや法制度を支えるのに必要な要素の間には、かなりの差がある。
3. こうした技術的な設計と実装が保証する範囲を無視すると、保証されていない性質を前提にした不正確な制度論になり得る。
4. 従来の金融サービス API 連携によるイノベーションには限界があり、現時点では、オンチェーン金融の諸概念を実現する方法としてブロックチェーンを基盤とする方法を超えるものはない、ということがオンチェーン金融推進の議論の前提にある。
5. この前提をオンチェーン金融の基盤技術がもたらす変化の観点で分解し、技術的な長所、欠点、制限を共有することで設計と実装が保証する範囲を明らかにする。

この資料のポイント

1. 帳簿に関する不正防止方法の変化

企業の人的運用の一部をタイムスタンプで置き換える。

2. サービスの接点の変化

金融機関の口座管理から、ウォレットと署名鍵管理へ。

3. 責任分界の考え方の変化

ブロックチェーンや異なる事業者の組み合わせで、コストと責任の外注化を試みるが、トレードオフがある。

金融システムとして、帳簿に求められる要件

お金として見るとき：偽造と二重使用を防ぐ。

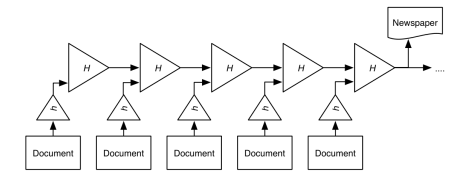
会計・経済活動として見るとき：金融サービスを管理する帳簿の改ざんと不正を防ぐ。

	ブロックチェーンで満たせること	ブロックチェーンで満たせないこと
通常の要件 偽造・二重使用 帳簿の改ざん	同じ台帳上の二重使用を防止する ある時刻における記録の存在と、それ以降の非改ざん	台帳の外で起きた二重譲渡 窃取された署名鍵による移転
対抗要件が必要な応用 第三者へ 権利を主張	前後関係と非改ざんという事実を示せる 法令が原簿への記録で足りると書くとき、その手段として使える	移転記録だけでは、確定日付のある通知・承諾にならない 登記も引渡しも法的には完結しない

暗号学的タイムスタンプ（1990）：公証人役場の電子化

ビットコインブロックチェーンで採用された方式。イベントの前後関係を暗号学的ハッシュ関数の連鎖で証明する。

1. タイムスタンプ事業者が、文書のハッシュを受け取る。
2. 受け取ったハッシュ値を用いて、ハッシュチェーンの次のノードを計算する。
3. ある時刻における文書の存在証明としてタイムスタンプトークンを返す。
4. 先端を新聞等に載せ、タイムスタンプ事業者自身も検証できる。



ISO/IEC 18014-3 のリンクトークンタイプタイムスタンプ（Haber and Stornetta, 1991）。

中央集権的タイムスタンプの弱点：長期保証を実現するため、赤字でも撤退できない民間では実施しにくいサービスであった。

日本では、この役割は**時刻認証業務**（総務大臣認定等の単一 TSA）として制度化されている。

ビットコインがしたこと

An electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party.
同意している二者が信頼できる第三者を必要とせず、直接取引が可能な、トラストの代わりに暗号的証明に依拠する電子支払いシステム。

In this paper, we propose a solution to the double-spending problem using a peer-to-peer distributed timestamp server to generate computational proof of the chronological order of transactions.
分散されたピア・ツー・ピアのタイムスタンプサーバーを使って、トランザクションの時間的順序の計算機的証明を生成することによる、二重支払い問題を解決するシステム。

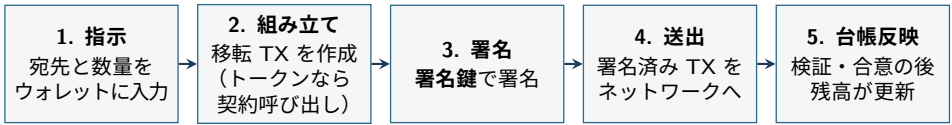
Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008。日本語訳は松尾ほか『ブロックチェーン技術の未解決問題』所収、崎村夏彦訳。

技術的な構成は、次の二つである。

1. タイムスタンプによる、帳簿の**非改ざん**の保証。
2. そのタイムスタンプサービスを**永続**させるための、運営の分散化とリワード。

帳簿の中身は、**署名鍵の間のトランザクションの累積**として表される。やり取りしているデータが、お金を表象しているように認識できるのは、このためである。

署名鍵を用いた暗号資産・トークン移転の手順



ネイティブ資産（例：ETH）

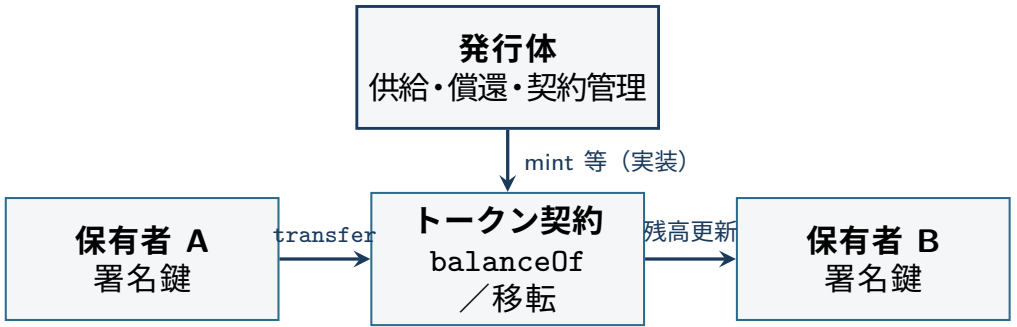
送金先アドレスへ、数量そのものを載せる。

金融トークン（例：ERC-20）

送金先は**トークン契約**。
呼び出しデータに、受取アドレスと数量を入れる。

自己管理でもカストディでも、技術上の接点は署名鍵である。

ERC-20：残高と移転のインターフェース

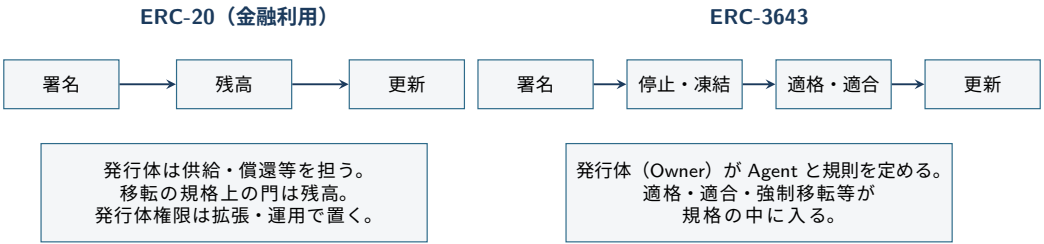


規格

上の移転ゲートは残高（と allowance）。発行体権限は拡張・運用で置く。

顧客接点は署名鍵。発行体は供給と、実装が許す特権操作の主体である。

ERC-20 と ERC-3643



どちらも、金融利用では発行体があり、残高は署名鍵に紐づく。差は、発行体の止める・動かすための権限がプロトコル仕様で実現されているか、運用側にあるかの違いである。

何が制度変化の中心か

イノベーションと規制上の変化の大部分は、
顧客との接点が**口座**から**署名鍵**へ移り得る点に集中する。

- 既存：接点は口座。申請は口座管理機関経由。
- ERC-20 タイプ：移転の認可は署名鍵（カストディでも技術上の接点は鍵）。
- 自己管理では、失念・端末喪失・表示と署名対象の不一致が権利喪失に直結し得る。

署名鍵に接点が移ったとき、**チェーン層**と**ウォレット層**で、
顧客に対する金融機関の責任を切れるか。切れないなら参入は事実上起きない。

本研究会で優先すべきは、署名鍵に接点が移ったときの**振替の高度化**である。

ウォレット（署名鍵）ベースが有効な条件

デジタル庁報告書からの学び [1]

「すべてをウォレットにせよ」ではない。
すでに API ／バックオフィス連携で足りる領域は、わざわざ署名鍵ベースに置き換えない。

API 等で足りやすい	署名鍵が効きやすい
機関同士で閉じる決済・照合	相手方が多数・未知で API が増え続ける
階層口座のメッセージ高度化	発行 PF 外への持ち出し・P2P が本質
すでに信頼経路がある手続	本人操作・提示範囲の最小化が要件

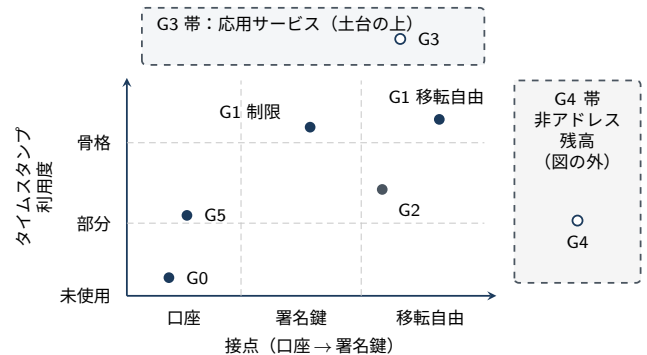
[1] デジタル庁「令和 6 年度 DIW アドバイザリーボード報告書」（2025 年 3 月 27 日）。

大分類 G0–G5

記号	大分類	定義	例
G0	現在の金融システム	従来の階層口座振替。署名鍵なし、共有タイムスタンプなし。	ほふり、銀行勘定
G5	部分利用タイプ	タイムスタンプ等の骨格の一部だけを使う。署名鍵への金融トークン管理はない。	Broadridge DLR、Canton ワークフロー
G1	発行体付き金融トークンタイプ	発行体があり、署名鍵に紐づく残高がタイムスタンプ付き台帳上で移転し得る。	JPYC、USDC、Progmat、ibet
G2	第三者帳簿責任者タイプ	預託・振替機関等が entitlement 等をトークン化し、公式帳簿責任を負う。	DTCC Tokenization
G3	応用サービスタイプ	DEX ／ AMM ／レンディング等。土台の金融トークンは G1 等。	Uniswap、Aave
G4	非アドレス残高タイプ	アドレスごとの残高として持たない。UTXO や、検証がクライアント側にあるものなど。	RGB、Taproot Assets

G0–G5 の見取り図

横軸＝接点（口座／署名鍵）。縦軸＝振替へのタイムスタンプ利用度。**G1 と G5 を同じ「オンチェーン」で論じない。**
G1 の左右差（初出）：**制限**＝発行 PF 外・P2P に制約あり。**移転自由**＝外への持ち出し・ウォレット間移転を許す。



G1 と G5——ここが制度論の分岐点

G1（接点＝署名鍵）

- 残高が鍵／アドレスに紐づき移転し得る
- 外部への移転可能・P2P 可（ホワイトリスト付き含む）
- 例：JPYC、USDC、多くのセキュリティトークン

G5（部分利用・口座寄り）

- タイムスタンプ／順序の**一部**のみ
- 顧客の署名鍵管理はない
- 口座 API 高度化と連続
- 例：Broadridge DLR タイプ

各論に入る前に、対象を G1 か G5（または G0 ／ G2）かに落とす。
同じ「オンチェーン」でも、**同じ責任分界を当てない**。詳細は文書版の大分類表・対応表。

責任分界の考え方

金融サービスの障害、ブロックチェーンの障害、ウォレットの障害を
切り分けられるようにする必要がある。

ブロックチェーンに求められる要件	ウォレットに求められる要件
タイムスタンプサービスとしての適格性	金融サービス提供者が管理しない 顧客との接点としての安全性

責任分界の選択肢を提示し、責任分界を考える場合の運用条件と認証制度の検討が必要。

タイムスタンプとしてのブロックチェーンと時刻認証制度

ERC-20 タイプは時刻認証業務の認定を自ら受けるのではない。
ブロックチェーンを分散タイムスタンプとして利用するため、従来のタイムスタンプサービスとの違いを認識し、同じ要件を満たしえるのかを検討する必要がある。

現行の単一 TSA（総務大臣認定等）が引き受けてきた骨格の例：

- 時刻源（UTC(NICT)）・一秒以内
- 設備・サイバー・情報開示
- 経理的基礎・休廃止時の終了計画・検証者への情報提供

「ブロックチェーンを使う」と書くだけでは、どれが満たされどれが未達成かは分からない。

従来のタイムスタンプサービスとの違い

単一 TSA	分散 TS で起きること	論点
時刻品質の管理・証明	多数ノード／バリデータ	誰の時計を UTC に結ぶか
設備・監査対象が明確	運営主体が拡散	調査・監査の入口はどこか
終了計画・情報提供	事業者消滅／分岐	検証情報の保管義務は誰か
経理的基礎	手数料・ステーク依存	赤字でも検証は残るか
事業体の存続	**ブロックチェーン永続が未保証**	ブロックチェーンプロジェクトが停止したときの対応

ブロックチェーンの永続性の課題

「ブロックチェーンだから永続する」は、経験則にも主要研究にも支えられていない。
ほふり水準と比較するとき問うのは、**赤字・退出のあとに検証と権利移転が残るか**。

少なくとも次の項目を分けてモニタリング項目にする。

1. ブロック／状態遷移の継続生成
2. 履歴の改ざん耐性の維持
3. 検証可能性の継続（アーカイブ・チェックポイント）
4. エコシステムの継続（クライアント、接続、法的エンティティ）

維持のための予算等・停止再開・放棄の判断を、発行・カストディ・監督の**モニタリング指標と閾値超過時の行動**に関する議論が必要。

ウォレットの安全性

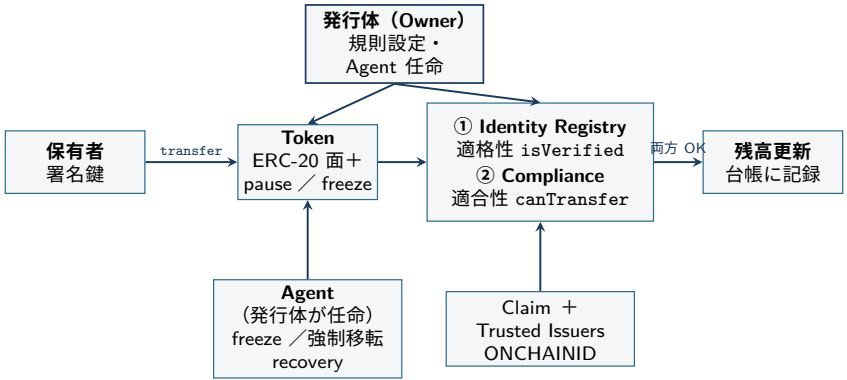
「ウォレット」には、少なくとも次を含めて検討項目にする。

1. 流通経路の物理改変
2. 署名 UI ／フロント改変（WYSIWYS の崩壊）
3. ソフトウェア依存（npm ／ CDN 等）
4. セキュアエレメント実装欠陥
5. 開発者・運用者端末からの侵入

認証対象に署名鍵管理装置とサプライチェーンを含める（文書版第 II 部）。

参考

参考：ERC-3643：適合性付き移転の構成



保有者の操作の接点は署名鍵である。発行体は、適格性・適合性のチェックと Agent 権限のあり方を決める主体である。