資料5

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

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）

2026 年 11 月 26 日

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

本資料は、同研究会第 1 回（2026 年 10 月 20 日）の討議において時間の制約上行えなかった技術的前提の整理を、書面により補足したものである。委員への事前配布を経て、第 3 回（2026 年 11 月 26 日）において公開のうえ説明する。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。その差を共有するため、技術的前提を、この資料のポイントとして整理する。

1 エグゼクティブサマリー

1.1 本資料の目的

金融庁が 2026 年 7 月 21 日に公表した「成長投資を促進するための金融戦略」は、AI 時代を見据え、「24 時間 365 日連続稼働」「商流・物流と繋がるプログラマビリティ」「決済基盤として信頼される安定性・安全性」を備えた、ブロックチェーン技術を基盤とする「オンチェーン金融」の推進を掲げ、既存の金融インフラ（オフチェーン金融）とのベストミックスを求めている [1]。同戦略のもと、環境整備に係る制度の在り方等を検討する場として、「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」（以下「本研究会」という。）が設置された [2]。戦略が求める三つの性質を、設計と実装がどこまで保証するかは、2.1 節で述べる。

本研究会第 1 回の事務局説明資料が掲げるステーブルコインおよび預金のトークン化、セキュリティトークン、分散型取引所（DEX）をはじめとする分散型金融（DeFi)、振替制度、証券決済の短縮化・高度化といったオンチェーン金融の各論は、いずれも重要であるものの、サービス概念・制度概念の側から置かれている [2]。しかし、概念の語が想起させる機能と、実際の技術が保証する範囲との間に乖離があることに目を向ける必要がある。

技術が引き受ける領域は性質の異なる二つの層に分かれ、ブロックチェーン（分散タイムスタンプ）は「順序と非改ざんの検証可能性」を、ERC の規格および実装は「署名鍵に紐づく残高・移転の状態遷移」をそれぞれ保証する。しかし、この二つを合わせても、金融サービスや法制度を支えるのに必要な要素のすべてには及ばない。偽造・二重使用の防止、帳簿の改ざん・不正の防止、および対抗要件との関係について、技術が満たす範囲と満たさない範囲は、2.2 節で述べる。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。つまり、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。このことについて認識を共有したい。

オンチェーン金融を推進すべきという議論は、従来の金融サービス API 連携の高度化だけでは越えられない限界があり、それを越える手段が現時点ではブロックチェーンを基盤とする方法に限られる、ということを前提とする。この前提の内容は 2.1 節で述べる。技術側から眺めれば、(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、監査において存在と非改ざんを説明する部分をタイムスタンプで置き換える構造と、ブロックチェーンおよび ERC が保証する範囲の切り分け。2.5 節)、(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移り得る点の長所と制限)、(3) 責任分界の考え方の変化（金融サービス・ブロックチェーン・ウォレットの障害を切り分ける必要性と、分散タイムスタンプにおける時刻認証基準の未達成および永続性の課題）に分解できる。オンチェーン金融の各論に入る前に、これらを押さえることで、オンチェーン金融を実現する設計と実装が保証する範囲を正確に捉えることができる。

1.2 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、という変化である。置き換わるのは記帳そのものではなく、監査において存在と非改ざんを説明する部分である（2.5 節)。本研究会が対象とするサービスの構成は、制度上の名称の違いを超えて、**ERC-20 に代表されるタイプの金融トークンのインターフェースと、発行体などに責任がある台帳に対するリンクトークンタイプタイムスタンプの組合せ**として整理できる。基本形は、パーミッションレス型ブロックチェーンの上に実装された ERC-20 である [3]。ステーブルコイン、預金のトークン化、セキュリティトークン、DEX を含む DeFi、許可型ブロックチェーンを利用した実装のうち署名鍵に金融取引の接点が移るものも、本資料ではこの分類に含める。台帳の正しさをタイムスタンプによって検証し得るという事実自体は、ブロックチェーンの登場以前から存在する技術と制度の延長線上にあり、それ単独では、制度の枠組みを変えるものではない。

なお、発行プラットフォーム外のウォレットへ移せず、ウォレット間で直接移転できない記録（市場データ事業者 RWA.xyz の用語では Represented Assets[10]）は、参加者間のメッセージに共有の時刻と順序を付す用途に近い。機能的には、口座の API 接続を高度化したものとほぼ同等であり、本資料では**部分利用タイプ（大分類 G5）**と呼び、他の大分類と同じ責任分界を当てない。

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移る変化である。具体的には、**顧客との取引の接点が、金融機関の口座単位から、顧客のウォレットが管理する署名鍵へ移り得**

ることである。この接点の移動が、イノベーションと規制上の検討の主な対象である。署名鍵を顧客のウォレットに移すことに利点が認められる場合と、認められない場合がある。デジタル庁の「令和 6 年度 DIW アドバイザリーボード報告書」[12] および「令和 7 年度　属性証明の課題整理に関する有識者会議　報告書」[13] は、Digital Identity Wallet（DIW）および Verifiable Credential（VC）について、定義、メリット、リスク要因、Wallet に求める要件、Issuer–Holder–Verifier（IHV）モデルを整理している。中心は、**すでに API ／バックオフィス連携で足りる領域は、あえて署名鍵ベースに置き換えない**こと、および**利用者を介した情報連携が必要になる場合に DIW を用いる**こと、という使い分けである（後述）。属性証明の文脈で書かれたこの場合分けは、金融における「口座 API の高度化（大分類 G5）」と「署名鍵に金融取引の接点が移るタイプ（大分類 G1）」の切り分けと同じである。金融への応用でも、この整理を参照する必要がある。

3. 責任分界の考え方の変化

オンチェーン金融の設計では、ブロックチェーンや他の事業者に、コストと責任の一部を委ねることがある。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。

帳簿に関する不正防止方法の変化で整理した、オープンな分散タイムスタンプとしてのブロックチェーンの機能について、**現在の時刻認証業務（単一のタイムスタンプ局）が満たしてきた信頼の基準から、分散タイムスタンプになったときに残る課題**を検討する必要がある。我が国では、総務大臣による時刻認証業務の認定制度（令和 3 年総務省告示第 146 号「時刻認証業務の認定に関する規程」[17]）およびその前身・並行である一般財団法人日本データ通信協会のタイムビジネス信頼・安心認定制度 [19] が、時刻源（UTC(NICT)）、精度（一秒以内）、設備、サイバーセキュリティ、情報開示、経理的基礎、休廃止時の終了計画等を求めている。国際的には、eIDAS 規則第 42 条 [20] および ETSI EN 319 421[21] 等が同種の要求を置いている。分散タイムスタンプでは、これらの要求を一つの認定事業者がまとめて引き受ける形にはならない。

さらに、**利用するブロックチェーン自体が、証券・決済に要する年数にわたって存続・稼働し続けるか**は自明ではない（検証への報酬や手数料の減衰、履歴改ざん耐性の低下、合意の一時停止、プロジェクトの放棄の判断等）。時刻のトレーサビリティ、停止と復旧、事業継続、**ブロックチェーンの永続**、暗号の危殆化への移行、検証者が依拠する情報の所在を、誰がどう保証するかを、金融インフラとして検討する必要がある。「ブロックチェーンだから安全／永続」かどうかではなく、現在の認定が求めていた基準を、誰がどのように満たすかを検討する。

1.3 研究会への論点（要約）

1. 各論（ステーブルコイン、セキュリティトークン、DeFi、振替、決済短縮）に入る前に、対象サービスを大分類（G0–G5）と詳細の分類に落とすこと。署名鍵に金融取引の接点

が移るタイプ（G1 等）と、部分利用タイプ（G5）および従来口座（G0）を分けること。付録の既存サービス対応表を参照すること。

2. 署名鍵に金融取引の接点が移るタイプについては、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、顧客に対する金融機関の責任を各層で切れる条件（運用条件と認証制度）を先に検討すること。ブロックチェーンに求められる要件はタイムスタンプサービスとしての適格性、ウォレットに求められる要件は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である。ウォレットの安全性には、流通経路の物理改変、署名 UI ／フロント改変（WYSIWYS の崩壊）、ソフトウェア依存（npm ／ CDN 等）、セキュアエレメント実装欠陥、開発者・運用者端末からの侵入を含めること（Bybit ／ Safe、Ledger 流通インプラント、Connect Kit、EUCLEAK 等の直近事例）。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こと。
3. オープンな分散タイムスタンプとしてのブロックチェーンについては、単一の時刻認証業務の認定要件から分散タイムスタンプにおける未達成を検討するための共通表を、事務局資料の前提とすること。あわせて、**利用するブロックチェーンの永続性**（検証への報酬や手数料、履歴の改ざん耐性、停止・再開、放棄の判断）を検討項目に含めること。
4. デジタル庁の DIW・属性証明に関する整理（API ／バックオフィス連携で足りる場合と、利用者を介した DIW が要る場合の使い分け）を、金融への応用における検討の参照として明示すること。

2 帳簿に関する不正防止方法の変化

2.1 推進の議論が置く前提

オンチェーン金融を推進する議論は、二つのことを前提にしている [1]。一つは、従来の金融サービス API 連携を高度化しても、機関の帳簿をまたいで第三者が検証できる順序と、署名鍵の間での転々流通は得られない、という限界である。もう一つは、この限界を越える技術的手段として、現時点ではブロックチェーンを基盤とする方法を超えるものが見当たらない、ということである。

この前提のもとでブロックチェーンに載せるのは、従来の API 連携だけでは足りない手続に限られる。あらかじめ契約した機関の間で、口座と API 連携によって責任と監査が閉じる領域は、あえて署名鍵に置き換えない。その切り分けは、サービスの接点の変化の視点から述べる。この前提が当てはまるのは、共有された検証可能な順序と、発行プラットフォームの外への移転が、そのサービスに不可欠な場合である。

金融戦略がオンチェーン金融に求める性質は、次の三つである。24 時間 365 日の連続稼働、商流・物流と繋がるプログラマビリティ、決済基盤として信頼される安定性・安全性である。同戦略は、これらを既存のオフチェーン金融とのベストミックスとして求めている [1]。

この三つは、金融戦略が期待する性質である。ブロックチェーンと ERC の設計と実装が、これらを自動的に保証するわけではない。連続稼働と安定性について、技術が保証できるのは、同一台帳上の順序と、ある時刻における存在、およびそれ以降の非改ざんまでである。チェーンが証券・決済に要する期間にわたって停止せず存続することまでは、この保証に含まれない。停止、再開、永続、および時刻認証の基準との差は、責任分界の考え方の変化の視点から扱う。プログラマビリティについて、ERC の規格が保証できるのは、署名鍵に紐づく残高と移転の状態遷移までである。商流・物流の上の権利の移転や、物の引渡しが完了することまでは、この保証に含まれない。これは、2.2 節で述べる対抗要件と、同じ境界である。既存のオフチェーン金融とのベストミックスを実現するには、API 連携で足りる領域と、署名鍵に接点が移る領域とを分けて検討する。

2.2 金融システムとして、帳簿に求められる要件

金融システムの帳簿に求めることは、二つの観点に分かれる。金銭としての観点では、偽造と二重使用を防ぐことである。会計および経済活動の観点では、金融サービスを管理する帳簿の改ざんと不正を防ぐことである。ブロックチェーンがこの二つをどこまで引き受けるかは、同じ台帳の内側で起きることと、台帳の外または法的な完結に属することとで異なる。

通常の要件について、ブロックチェーンが満たせるのは、同じ台帳の上での二重使用の防止と、ある時刻における記録の存在およびそれ以降の非改ざんである。満たせないのは、台帳の外で起きた二重譲渡と、窃取された署名鍵による移転である。記録が同一台帳上で正しく並び、後から改められないことは、台帳の外にある譲渡や、鍵そのものの盗用を無効には

しない。

第三者へ権利を主張する場面では、ブロックチェーンが示せるのは、前後関係と非改ざんという事実である。法令が、原簿への記録をもって対抗の要件を満たすと定めるときは、その記録の手段として使える。他方、移転の記録だけでは、民法第 467 条の確定日付のある通知・承諾にはならない。登記も引渡しも、台帳上に移転が残ったことだけでは法的には完結しない。社債、株式等の振替に関する法律が振替口座簿への記録に認めている対抗要件および権利の帰属も、暗号学的タイムスタンプが示す事実とは別の次元の問題である。

以下では、台帳側のタイムスタンプと金融サービス側の ERC が、この要件のどこまでを保証するかを示す。

2.3 何を整理しているか

本研究会の事務局説明資料が掲げる各論—ステーブルコインおよび預金のトークン化、セキュリティトークン、DEX・DeFi、振替制度、証券決済の短縮化・高度化 [2]—は、いずれも検討を要する。これを制度名のまま並列に議論すると、技術の骨格が共通であることが見えにくくなる。本資料が主張する整理は、次の二点である。

1. **発行体などに責任がある台帳に対するリンクトークンタイプタイムスタンプが、トランザクションの順序を付す：**原型は、Haber と Stornetta が 1990 年代に定式化し [5, 6]、のちに ISO/IEC 18014-3 として国際標準化されたリンクトークンタイプタイムスタンプである [7]。ここで発行されるのは**タイムスタンプトークン**である。ビットコインは、単一のタイムスタンプ局の運営を、ピア・ツー・ピアの計算による不特定多数のサーバによる順序の証明へ移したものである [9]。
2. **台帳の上で、金融トークンの残高と移転・承認の状態遷移が、署名鍵に紐付いて残る：**このインターフェースの代表が、Ethereum 上の ERC-20（EIP-20）である [3]。ERC-20 が規定するのは法的な資産の定義ではない。`totalSupply`、`balanceOf`、`transfer`、`transferFrom`、`approve`、`allowance` といったメソッドと、`Transfer`・`Approval` のイベントである。

この二つは、保証する内容が異なる。リンクトークンタイプタイムスタンプが引き受けるのは、トランザクションの順序と、それ以降の非改ざんを第三者が検証できることである。ERC-20 の規格と実装が引き受けるのは、署名鍵に紐づく残高と、移転・承認の状態遷移である。償還、準備資産の真実性、法的な権利の同一性は、いずれの層からも自動的には出てこない。概念の側でこれらを一続きに語ると、保証されていない性質を、技術が保証しているかのように扱うことになる。

基本形は、パーミッションレス型ブロックチェーンの上の ERC-20 である。許可型ブロックチェーンを利用した設計であっても、署名鍵に金融取引の接点が移り、発行プラットフォーム外のウォレットへ金融トークンを移し、ウォレット間で移転できるのであれば、同じタイプに入る。

2.4 台帳側：リンクトークンタイプタイムスタンプとタイムスタンプトークン

公証制度が、証書の作成、確定日付の付与、認証によって私的法律関係の明確化と安定を図ってきたのと同様に [23]、デジタルデータについても、ある時刻における存在と、それ以降の非改ざんを、第三者検証可能な形で示す要請がある。電子署名は、非改ざんの検証に加え、作り手の証明を行う。時刻の証明に絞って考案されたのが、暗号学的タイムスタンプである。

Haber と Stornetta の方式では、信頼できるタイムスタンプ局が文書のハッシュ値を受け取り、ハッシュの鎖（および後の改良では Merkle 木）を構成し、**タイムスタンプトークン**を返す [5, 6]。係争時には、タイムスタンプ局が第三者として証拠を提出する。局自身の正しさを示すため、定期的に鎖の先端を新聞等の信頼できる媒体に掲載する運用も、1990 年代から存在する。この方式は、ISO/IEC 18014-3 においてリンクトークンタイプタイムスタンプとして標準化された [7]。規格上の姉妹として、独立トークン方式のタイムスタンプ（ISO/IEC 18014-2）および時刻のトレーサビリティに関するプロトコル（ISO/IEC 18014-5）がある。インターネット上のプロトコルとしては、IETF RFC 3161 がある [8]。ここで確認するのは、**ハッシュ鎖の計算と構造は、現在のブロックチェーンで用いられているものと基本的に同じ**であること、および、1990 年時点での限界は、第三者検証可能な非改ざん検知のために信頼できるエンティティが必要であったことである [24]。台帳の正しさの検証自体は、ブロックチェーンを使うかどうかにかかわらず、タイムスタンプで行い得る。つまり、この部分では、制度の枠組みを変えるものではない。中央集権的タイムスタンプの弱点は、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ことである。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（責任分界の考え方の変化の視点から詳述する）。

2.5 タイムスタンプが置き換える人的運用

タイムスタンプが置き換える人的運用は、記帳そのものではなく、監査において存在と非改ざんを説明する部分である。ある時刻に記録が存在し、その後改められていないことを、担当者の説明や社内の突合によって監査に示す代わりに、第三者が検証できるタイムスタンプトークンで示す。帳簿を作り、取引を承認する作業は残る。監査のときに、存在と非改ざんを人手で説明する部分が、検証可能な証跡に置き換わる。電子帳簿保存等の実務で認定タイムスタンプが参照されてきたのも、この用法である。

この置き換えは、ブロックチェーンに固有ではない。前項のとおり、同じ証跡は単一の時刻認証業務でも出し得る。それ単独では、制度の枠組みを変えるものではない。変わるのは、その証跡を誰が、どの信頼モデルで出し続けるかである。一つの認定事業者がまとめて引き受けない形になったあと、監査に耐えうる証跡の責任を誰が負うかは、責任分界の考え方の変化の視点から扱う。

2.6 金融サービス側：ERC-20 トークンと署名鍵に紐づく残高

本研究会の各論で扱われるステーブルコイン、セキュリティトークン、トークン化預金、DeFi 上の残高などは、いずれも**金融トークン**である。その技術的な代表が ERC-20 である。ERC-20 は、アドレス（検証鍵に由来する識別子）ごとに残高を保持し、署名によって認可された移転と、第三者への引出し許可（`approve`/`transferFrom`）を状態遷移として記録する [3]。発行と移転の履歴が、開かれたタイムスタンプの上に、署名鍵へ紐付いて残る。口座簿との違いは、ここにある。顧客との接点が、口座管理機関の記録から、顧客が管理し得る署名鍵へ移り得る。

2.7 ERC-20：残高と移転のインターフェース

EIP-20 自体は発行体を定義しない [3]。金融サービスに載せるときは、供給、償還、契約管理の主体として発行体が付く。規格上、移転の条件は、呼び出し元の残高と、第三者移転のための許可（`allowance`）である。mint、停止、凍結などの発行体権限は、規格の外の拡張または運用として置く。顧客との接点は署名鍵のままである。発行体は、供給と、その実装が許す特権操作の主体である。

図 1 は、この関係を示す。保有者は署名鍵でトークン契約の `transfer` を呼ぶ。送金先は受取人のアドレスそのものではなく、トークン契約である。契約が残高を更新し、受取人のアドレスへ記帳する。

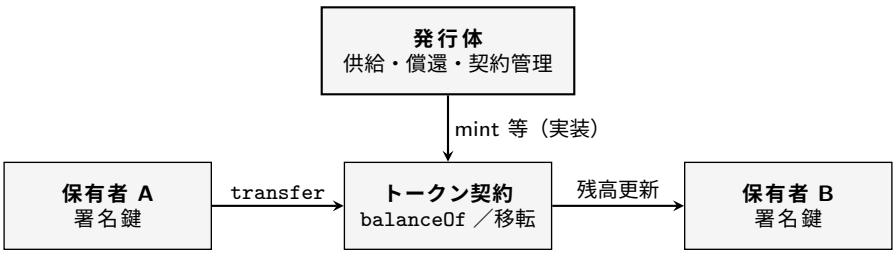


図 1　金融利用における ERC-20 の残高と移転。規格上、移転の条件は残高（と allowance）であり、発行体権限は拡張・運用で置く。顧客接点は署名鍵である。

2.8 ERC-20 と ERC-3643

ERC-3643（T-REX）は、ERC-20 互換の残高の上に、オンチェーンの身元検証と移転ルールを載せた規格である [4]。構成の詳細は付録 B に置く。ここでは、金融利用における差だけを示す。

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、発行体が移転を止め、または動かすための権限が、プロトコル仕様の中で実現されているか、規格の外の拡張・運用に置かれているか、である（図 2）。

ERC-20 を金融利用するときの移転は、署名のあと、残高（と allowance）を満たせば更新に至る。発行体は供給と償還等を担うが、規格上、移転の条件は残高である。停止、凍結、

適格性、適合性、強制移転は規格に含まれず、拡張または運用で置く。

ERC-3643 では、発行体（Owner）が Agent と規則を定める。署名のあと、トークンの停止・凍結を見、次いで適格性（Identity Registry の `isVerified`）と適合性（Compliance の `canTransfer`）を通過して、残高が更新される。適格・適合の判定と、強制移転等の Agent 権限は、規格の中に入る。

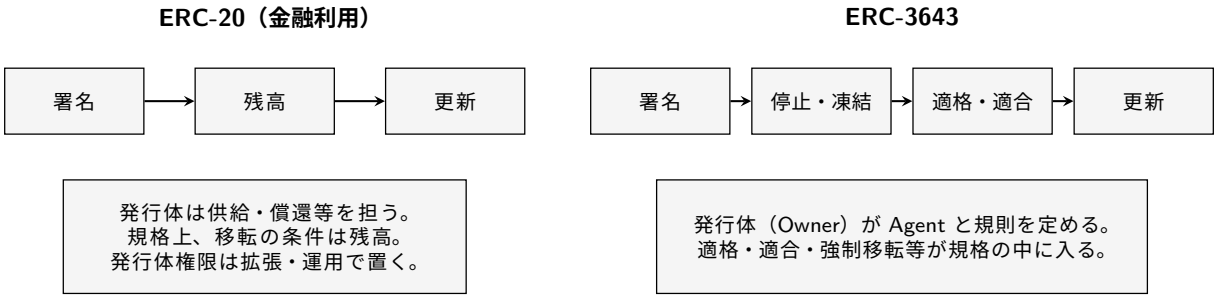


図 2　金融利用における ERC-20 と ERC-3643 の差。残高はいずれも署名鍵に紐づく。発行体が移転を制御する権限の置き場所が異なる。

2.9 ビットコインのイノベーションは「タイムスタンプ局の運営」の信頼モデルの変化である

Nakamoto（2008）は、ビットコインを次のように述べている [9]。

> 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.
>
> 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.

（日本語訳の一例：「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」「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」[25]。）

すなわち、ビットコインの論文が新しく提示したのは、データ構造そのものよりも、**信頼できる第三者機関を不要にするトラストモデル**であり、二重支払いを防ぐための分散タイムスタンプである。Haber らの論文は、同論文に引用されている。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、運営の分散化と報酬。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。

この構成が解いたのは、それ以前の電子マネーが転々流通をあきらめたことである。日銀

と NTT による電子現金は、現金に見立てたデータを利用者間で渡すことを目指した。しかし、通信上の障害によって帰属が曖昧になる問題を、信頼できるサーバを決済経路から外したまま解くことはできず、開いた転々流通は断念された。その後に普及した電子マネーは、店舗で使い、発行者の台帳へ戻す形となり、転々流通を前提としなくなった。ビットコインは、共有の帳簿と開かれたタイムスタンプによって、署名鍵の間で転々と渡すことを再び可能にした。

ERC-20 タイプの金融トークンは、この開かれたタイムスタンプの上に、発行者の主張する残高と移転の状態遷移を載せる。

2.10 許可型・コンソーシアム型ブロックチェーンの取り扱い

いわゆる許可型／コンソーシアム型ブロックチェーンは、リンクトークンタイプタイムスタンプのデータ構造の上に、決められたノードによる合意と、業務ロジックに応じた処理を加えたものとして理解できる。トラストモデルの意味では、単一または少数の運営主体に依存するタイムスタンプの延長（「タイムスタンプ 2.0」と呼んだ整理 [24]）に近い。スケーラビリティや確定性の面では扱いやすいが、**支え手の事業継続が大前提**である点で、単一の時刻認証業務が抱えてきた課題—赤字でも検証可能性を残せるか、事業譲渡後もサービスレベルが保たれるか—を解消してはいない。

他方、パーミッションレス型は、インセンティブ設計が機能する限りにおいて、一企業の収益判断から相対的に独立した持続を狙う。その代わり、合意の安全性、エネルギーまたはステークの集中、分岐、検閲、手数料市場といった、別の新たな成立条件・持続性の条件が発生する。

2.11 市場データの観察：Distributed と Represented

金融トークン化された資産の市場データ事業者である RWA.xyz は、次の二属性で当該資産を分類している [10, 11]。

- **External Wallet Mobility**：発行プラットフォーム外のウォレットへ移せるか（ホワイトリスト付きを含む）。
- **Peer-to-Peer Transferability**：ウォレット間で直接移転できるか（ホワイトリスト付きを含む）。

両方を満たすものを **Distributed Assets**、満たさないものを **Represented Assets** と呼ぶ。前者では、ブロックチェーンは資本形成と相互運用の経路として機能し、後者では、機関参加者の記録・突合の層として機能する、というのが同事業者の整理である。分類は静的ではなく、移せる・移転できるようになれば再分類される。

この分類は、本資料の大分類およびサービスの接点の変化と実質同じである。Distributed は「署名鍵に金融取引の接点が移り得るタイプ」、Represented は「口座間の共通タイムスタンプ／ API 高度化に近いタイプ」に対応する。市場データ上、Represented 側の残高の大部

分を Broadridge のレポ取引基盤（Canton ネットワーク）等が占める局面がある [62, 10]。日本の不動産セキュリティトークンにも、発行時条件によりセカンダリやチェーン間移動が制限され、Represented 側に寄る銘柄が相応にある。

Canton のように、サービス提供者の間のメッセージに共有のタイムスタンプと順序を付す実装は、機能的にはタイムスタンプの一部利用にとどまり、署名鍵に金融取引の接点が移るタイプではない。口座の API 接続を高度化したものと紙一重である、という第 1 回討議での整理 [26] は、この意味である。

2.12 研究会の対象を大分類と詳細の分類に落とす

制度名（ステーブルコイン、セキュリティトークン、DeFi 等）のまま並列すると、技術の骨格が共通であることが見えにくい。本資料は、まず**大分類 G0–G5** を設け、次に**詳細の分類（軸 A–H）**で整理する。既存サービスの対応は付録 D に置く。コードは公開情報に基づく類型割当であり、契約・ホワイトリストの設計により移動性（軸 F）等の位置は異なり得る。

2.12.1 大分類

二つの軸

1. x **軸（横）—顧客との取引の接点：**左＝金融機関の**口座**、右＝顧客の**署名鍵**。大分類を分ける主な違いは、管理の単位が口座か署名鍵か、である。
2. y **軸（縦）—タイムスタンプとしてのブロックチェーンを振替機能の実現のためにどこまで使うか：**下＝使わない、中＝骨格の一部だけ（順序・照合・W 等）、上＝残高移転の骨格に乗せる。

G1 の内側では、さらに**発行プラットフォーム外への移動・ウォレット間移転を許すか**（軸 F）で、x 方向に「制限付き」と「移転自由」の位置の差が出る。図 3 では G1 制限と G1 移転自由の左右のずれとして示す。

平面上の位置と、平面外の切り分け

図 3 は**分類ごとの位置**を示すものである。G0・G5・G1・G2 は主平面上の点である（G2 は G1 と同象限だが、**誰が公式帳簿責任を負うか**が違う）。G3 は主平面の**上**（土台の上に乗る応用）、G4 は主平面の**外**（アドレスごとの残高として持たない非アドレス残高タイプ）に置く。

表 1 は、図 3 の各点・切り分けに対応する定義である。

同一ブランドでも、出庫可否・媒体・責任主体の設計が異なれば、図 3 上の位置が異なる（例：JPYSC の口座内提供とパブリック流通の設計差 [58]、Progmat の媒体差 [60]、JPM Coin の媒体差、DTCC の従来簿記と Tokenization[61]）。

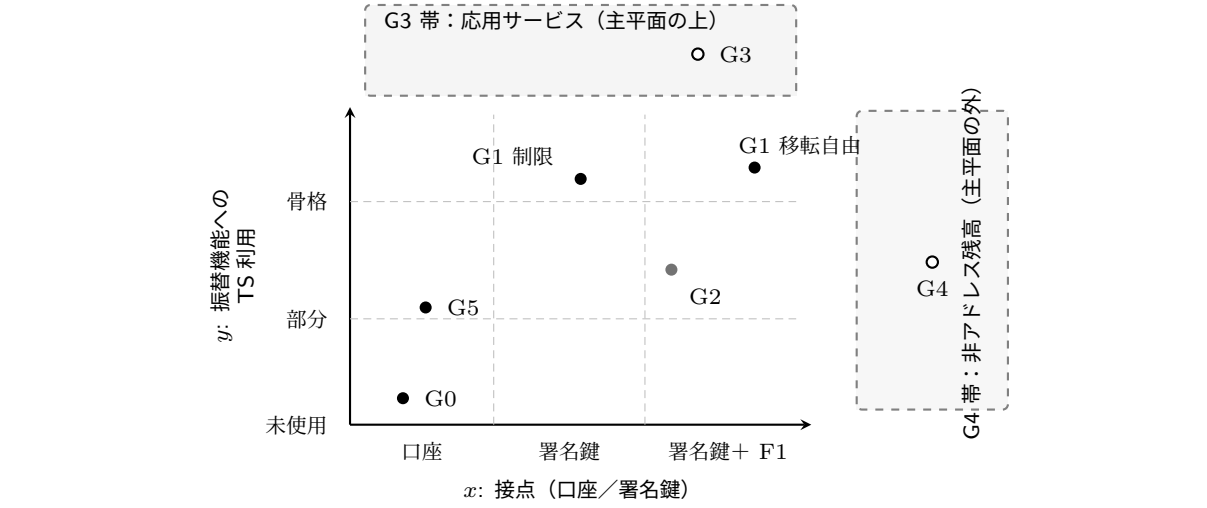


図 3　大分類の平面表示。主平面は x ＝接点、y ＝タイムスタンプとしてのブロックチェーンの振替への利用度。白抜き点の G3 は主平面の上、G4 は主平面の外に置く。

表 1　オンチェーン金融サービスの大分類—平面上の位置

記号	大分類	定義	平面上の位置
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）	(x, y) ＝口座・未使用
G5	部分利用タイプ	タイムスタンプ／取引順序の合意等の**骨格の一部だけ**を使う。顧客の署名鍵への金融トークン管理はない。口座 API 高度化と連続	口座 × 部分利用
G1	発行体付き金融トークンタイプ	発行体（または同等）があり、署名鍵／アドレス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	署名鍵 × 骨格。制限付き〜移転自由（軸 F）
G2	第三者帳簿責任者タイプ	証券の発行体ではなく、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	G1 と同象限だが**責任主体が違う**（振替論の中心）
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	主平面の**上**（G3 帯）
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	主平面の**外**（G4 帯）

2.12.2 詳細の分類の要点

詳細の分類は付録 C に定義を置く。

- **軸 B（帳簿の分解）：**経済・請求権（E）、法的名義・公式名簿（R）、移転台帳（T）、業務ワークフロー（W）を分け、責任主体を割り当てる。「帳簿の完全性＝発行体」は、通例、E（および名簿を合成する R）に限って成立する。**T の暗号完全性はブロックチェーン上の処理（タイムスタンプ層）が対象**であり、発行体の準備の真実性は対象外である。
- **軸 C（タイムスタンプ媒体）：**パーミッションレス（C1）、許可型だが第三者検証可能な取引順序の合意（C2）、古典的 TSA（C3）、コミットメントのみ公開（C4）、単一運営の私有 DB（C5）。
- **軸 D（インターフェース）：**本資料の「ERC-20 タイプ」は主に D1–D3（EIP-20 そのもの、互換拡張、他 VM の同種）。互換拡張の代表である ERC-3643 の構成は、付録 B に置く。
- **軸 E（署名鍵・カストディ）と軸 F（移動性）：**E5 かつ F2 は典型的 G5。F1（Distributed）でもホワイトリスト付きを含む。

2.12.3 事務局各論との対応

表 2 は、事務局資料の各論を大分類に再配置したものである。既存サービスの優先例は付録 D を参照されたい。

表 2　事務局各論と大分類・既存例（要約）

制度上の名称（事務局）	主な大分類	既存例（優先）
ステーブル・預金トークン化	G1（中心）、境界に G5 寄り	JPYC[57]、JPYSC[58]、3 メガ共同 SC[59]、USDC ／ USDT、JPM Coin、HSBC TDS、PIP 預金トークン
セキュリティトークン	G1	Progmat 銘柄群 [60]、ibet for Fin 銘柄群、SBI START 債、ODX START、BUIDL、BENJI
DEX・DeFi	G3 ＋土台は G1	Uniswap ／ Aave 等（応用）。土台は USDC 等。ibet Exchange ／ DvP
振替制度の DLT 化	G2、G1、G0、G5	ほふり（G0）、DTCC Tokenization（G2）[61]、issuer-sponsored ST（G1）。直接保有・機関口座の制約は接続の障害 [2]
証券決済の短縮化・高度化	（全大分類の**結果**）	類型の選択問題ではない。結果として扱う。
部分利用の説明	G5	Broadridge DLR[62]、強い Represented、Canton 上のワークフロー単体

証券保管振替機構（ほふり）が有する安全性と事業継続上の信頼に、このエコシステムが

匹敵するには、タイムスタンプとしての基準と、ウォレット層の基準の双方が必要となる。また、同じ名称の金融トークンが異なるチェーン上では別の契約として発行される点にも注意が必要である。一方で消却し他方で発行し直すか、橋渡しを使うかで技術的には移せるとしても、権利の同一性と裏付の引き当ては移転のたびに確認が必要で、実務上は極めて煩雑になり得る [26]。

3 サービスの接点の変化

3.1 何が制度変化の中心か

顧客との接点が口座から署名鍵へ移り得ることが、イノベーションと規制上の検討の主な対象である。

既存の振替制度において、顧客との接点は口座である。振替申請は口座管理機関を経由し、振替機関および各口座管理機関が振替口座簿を備える階層構造のもとで、記録と通知が行われる [2]。

ERC-20 タイプにおいては、移転の認可は署名鍵が持つ。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。顧客が自己管理する場合（いわゆるアンホステッド／セルフカストディ）、失念、相続、端末喪失、表示と署名対象の不一致（what-you-see-is-what-you-sign の欠如）が、そのまま権利の喪失や誤移転に直結し得る。

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。本研究会で最も優先すべき技術・制度の交差点は、「署名鍵に金融取引の接点が移ったときの振替の高度化」である [26]。切るべき層も分かれる。金融サービスの障害、ブロックチェーンの障害（停止、分岐、検閲、手数料市場の機能不全等）、署名画面を含むウォレットの障害は、別のものである。

3.2 デジタル庁における整理—引用の枠組み

筆者は、デジタル庁の DIW アドバイザリーボードおよび属性証明の課題整理に関する有識者会議の構成員を務めている。同庁が公開した報告書は、属性証明（身元・資格・属性等）の文脈で書かれているが、**署名鍵を単位とするウォレットの場合分け、リスク、求められる要件**は、金融への応用における検討の際にも参照し得る。以下、公開文書に即して要点を引く。

3.2.1 令和 6 年度 DIW アドバイザリーボード報告書

同報告書 [12] は、DIW を一意に定義してはいないが、「属性情報や資格情報等をスマートフォン等に保存し、利用者の操作を介して提示できるアプリケーション」が一般的に理解されている概念である、と整理する。Issuer（発行機関）が証明書等を DIW に発行し、Holder（利用者）が保存し、Verifier（サービス提供者）に提示する、という三者関係が基本図である。

同報告書は、「ウォレット」と呼ばれるサービスの多様性にも触れている。プラットフォー

ム事業者のウォレット、決済・金融系ウォレットに加え、**暗号資産／ NFT ウォレット**を例示し、「暗号資産/NFT にアクセスするための情報の管理や送金操作ができる。暗号化技術の活用やブロックチェーン技術との親和性等、機能面で DIW との類似点がある」と記している [12]。これは、属性証明の会議体自身が、金融資産ウォレットとの近接を認めた箇所である。

リスクについては、Issuer、Holder、Wallet ／ Wallet Provider、Verifier をステークホルダとし、少なくとも次のリスク要因を挙げている [12]。

a) 悪意ある Verifier

b) Verifier のなりすまし

c) 悪意ある Wallet Provider

d) Wallet の脆弱な実装（署名鍵管理等の実装が不適切な Wallet など）

e) 不適切な発行プロセス

f) 偽の Issuer

g) 悪意ある Holder

h) Holder の意図しない提示

個人の利用者にとってのリスクのまとめとしては、次が明示されている [12]。

- 偽の Verifier を見分けられず、フィッシングサイトにクレデンシャルを詐取される。
- 悪意ある Wallet Provider によって Wallet 内の情報に不正アクセスされる。
- 提示したクレデンシャルを第三者に再利用された場合、なりすましによる被害を受ける。
- 適切なバックアップ／リカバリの手段がないと、スマートフォンの紛失時にクレデンシャルを喪失する。
- Wallet サービスの終了によりクレデンシャルを喪失する。

行政機関・事業者側には、不正なクレデンシャルの受入れ、署名鍵管理不備によるなりすまし、ならびに**ビジネスモデルが成立せず Issuer や Wallet Provider が撤退する**という事業継続リスクが挙げられている [12]。

3.2.2 令和 7 年度　属性証明の課題整理に関する有識者会議　報告書

同報告書 [13] は、VC および DIW を次のように定義する（表 1.2-1 の要約）。

- **VC**：デジタル署名による真正性確保・改ざん防止等の機能を有する、「個人、法人、モノ等」の属性情報に関する汎用的で機械可読なデータ形式・データ流通の形態。期待されるメリットとして、真正性および非改ざん性の担保、署名等に基づくデータの信憑性に対する責任関係の明確化、機械可読性による事務処理の自動化を挙げる。
- **DIW**：個人・法人等が、自身の証明書 VC 等をスマートフォン等に保有・管理し、第三

者に提示するための仕組みおよびアプリケーション。期待されるメリットとして、VC と提示者の紐づけ、VC の発行先（Wallet の所有者）の確認、選択的開示によるプライバシー向上等を挙げる。

情報連携の基本形は、**IHV モデル**—発行者（Issuer）が発行した VC 等を利用者（Holder）が保持し、検証者（Verifier）に提示する形態—である [13]。官→民および民→官の組合せに焦点が置かれた。

短期的取組事項の一つとして、「官→民の Wallet に求める共通の要件の明確化」（A-2）が掲げられ、公的証明書 VC を格納する Wallet に求める要件として、**VC の発行・提示プロトコル、セキュリティ対策、署名鍵の管理方法、相互運用性など**を取りまとめることが提案されている [13]。EU の Architecture Reference Framework（ARF）のような包括的スコープではなく、行政機関が発行する VC を格納する Wallet に求める要件に絞る、との注記がある。民→官についても、行政機関が受け入れる Wallet の要件整理（C-2）が対応して置かれている。

同報告書はまた、リスク対策基準の検討に先立ち、用語の定義、ユースケースの精緻化、アーキテクチャとエコシステムの検討が先行して必要である、と記している [13]。これは、本研究会が各論に入る前に技術類型を共有すべきである、という本資料の主張と同じである。

3.2.3 API 連携・バックオフィス連携と DIW—いつウォレットを使うか

以下は、デジタル庁の整理のうち、サービスの接点をどこに置くかに関わる部分である。デジタル庁側の議論は、「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、あえて署名鍵ベースに置き換えない**こと、および**利用者を介した情報連携が必要になる領域で DIW を用いる**ことを、繰り返し確認している。

用語の区別（デジタル庁資料に即して）

属性証明の課題整理に関する有識者会議の事務局資料は、次を明示して区別する [14]。

- **バックオフィス連携**：ワンスオンリーを実現するため、マイナンバー制度等に基づき**行政機関同士**が内部事務として情報連携すること。情報システム用語の「バックエンド連携（サーバー間連携）」とは意味が異なる、との注記がある。
- **利用者を介した情報連携**：発行者（Issuer）が発行した VC 等を、利用者が DIW 等に保持し、検証者（Verifier）に提示する IHV モデル。行政機関間の連携に加え、**官民の間**で紙や PDF が残る領域をデジタル完結へ進めるための経路とする。

マイナンバー制度に基づく行政機関間の情報連携には、法令上の利用範囲の制約があり、**官民の間ではそのまま使えない**。したがって、行政と民間の手続では紙・PDF の授受が残存する—これが、VC・DIW に取り組む現状課題として掲げられている [13, 14]。

DIW アドバイザリーボード報告書が示した三類型

令和 6 年度報告書は、行政が関わるユースケースで DIW の活用が期待できる類型を、次の三つに整理した [12]。

1. **証明書のスマホ搭載**：対面でもオンラインでも共通の UX で提示・検証できる（物理カード／紙の携帯からの脱却）。
2. **行政手続のデジタル化**：DIW による「利用者を介した情報連携」により、**バックオフィス連携が行き届かない領域**でもデジタル完結を推進する。確定申告の控除証明書、年末調整、罹災証明書、在外選挙人証、成績証明書の提示等が例示される。
3. **官民サービスでの選択的開示**：必要最小限の情報だけを開示する。物理カードや紙では実現しにくく、DIW を用いる場合の利点である。

類型 2 の図解は、バックオフィス連携でカバーできないため紙・PDF が残る現状を、利用者を介した提示で補完する、という構造である [12]。類型 3 は、プライバシーとデータ最小化の原則への寄与であり、「API で同じ属性を丸ごと渡す」こととは目的が異なる。

構成員意見・提言に現れる使い分けの原則

同報告書に記録された構成員意見および次年度提言には、使い分けの原則が、より端的に書かれている [12]。

- 「**官民をまたぐ連携で紙が発生する、それを DIW で解決するのはまず期待することではないか。API でできているところは置き換えられない。**」
- 「**本来は属性を連携させることが重要であり、DIW はその 1 つの手段として考えるべき。**」（マイナンバーの便利さの多くがバックオフィス連携に由来する、という対比つき）
- 「**DIW だけで解決するのではなく、バックオフィス連携やフェデレーションなども踏まえ現実的な解を考えるべき。**」
- 既存手段と DIW を利用者が使い分ける負担を背負わせる事態は避けるべき、という指摘も併記されている。

すなわち、政策の第一選択は「すでに信頼できる経路で API ／バックオフィス連携が成立している手続を、あえて DIW に載せ替える」ことではない。DIW が効くのは、**直接連携が法的・組織的・技術的に届かない**、または**利用者の意思・選択的開示・提示者の紐づけが本質的に要る**場面である。

令和 7 年度報告書・技術 WG が深めた論点

令和 7 年度報告書は、単一の証明書のやり取りであれば**フェデレーションによるデータ連携で大半は充足する**ため、VC の利活用の促進では**複数の VC をまとめて提示する**ユースケースの検討を進めるべきである、との委員意見を記録している [13]。あわせて、既存手法（署名付き PDF 等）との使い分けを認めつつ、機械可読性や選択的開示など VC・DIW の

特長が**どのような場合に役立つか**を広く理解させる必要がある、と述べる [13]。

技術ワーキンググループの議論概要では、就労証明書を題材に、次のような指摘が並ぶ [15]。

- 発行プラットフォームがあり、信頼できる経路で自治体へ直接データ連携できるなら、**VC 形式でなくとも足りる**のではないか（IHV モデルそのものが不要になり得る）。
- 他方、全国の会社と API 接続することの実現可能性、中小企業の署名鍵管理負担、様式差などの制約がある。
- 各社システムと共通 PF を API で結ぶ設計は、VC に期待していた「**API 連携が際限なく増えた際に手続が煩雑化する課題の解決**」と矛盾し得る。多数の発行主体から統一プロトコルで Wallet へ発行し、利用者が提示する形の方が、将来の汎用性が高い場合がある。
- 信頼できるエンティティと経路だけで完結するなら、伝達過程の改ざんは困難であり、署名・VC の要否自体を精査すべき、という指摘もある（再利用・なりすましリスクとの裏表）。

別紙の検討事項リスト（案）は、業務要件の洗い出し項目として、「**個人を介した情報連携を求めるか**（マイナンバー法の制約等で行政機関間の情報連携ができない証明書をデジタル化する場合など）」および「**そもそも Wallet は必要か**」を明示している [16]。導入判断の順序として、ユースケースの記述の後に、アーキテクチャの比較・選定を行う。

いつ DIW（ウォレット）を使うかの整理—デジタル庁資料からの抽出

デジタル庁資料が示す使い分けは、表 3 のとおりである。

3.3 金融への応用における検討のための対応

表 4 は、デジタル庁側の整理を、金融資産の ERC-20 タイプ管理への応用における検討のために対応づけたものである。

金融への応用における検討の際に参照すべきは、**署名鍵を単位とする場合分け、リスク、Wallet 要件、責任関係の明確化**、および表 3 の使い分けである。

3.4 署名鍵を顧客に移す場合・移さない場合

デジタル庁資料の使い分け（表 3）を金融への応用における検討に参照すると、次のようになる。

口座 API・機関間連携で足りやすい

- あらかじめ契約した機関同士の決済・照合・担保ワークフローであり、顧客の署名鍵を介さずとも責任分界と監査が閉じるもの（大分類 G5、強い Represented、Broadridge DLR タイプ）。

表 3　API ／バックオフィス連携と DIW（利用者を介した情報連携）の使い分け（デジタル庁資料に基づく整理）

API・バックオフィス連携・フェデレーションで足りやすい	DIW（利用者を介した提示）が効きやすい／要りやすい
行政機関同士で法令上バックオフィス連携が可能な手続	官民をまたぎ、バックオフィスが法令・制度上届かない手続（紙・PDF が残る領域）[12, 14]
発行者 – 検証者間に信頼できる直接経路があり、N×M の API が増えない設計	発行者・検証者が多数で、API が際限なく増える／接続不能な主体がある [15]
単一の属性・証明書を、あらかじめ合意した相手に渡すだけ	複数の VC をまとめて提示する、対面・オフラインでも同じ UX で提示する [13, 12]
検証者に渡す属性集合が固定で、丸ごと開示で足りる	選択的開示・データ最小化・発行者に提示先を知られないことが要件 [12]
利用者の意思確認が、既存の同意 UX や契約で足りる	提示者の紐づけ（Holder Binding）、利用者本人の操作を介した同意が本質 [13]
すでに API でできている領域	**わざわざ DIW に置き換えない** [12]

- 振替制度の階層口座のなかで、法令上の帳簿責任者が明確なまま、メッセージ連携を高度化すれば足りるもの（G0 の延長）。
- 単一のカストディアン網内、または少数の承認取引先間だけで完結し、N×M の接続が増えないもの（制限の強いトークン化預金の私有実装等）。

これらの実装がオンチェーンと称するものであっても、署名鍵に金融取引の接点が移るタイプ（G1）と同じ責任分界を当てるべきではない。すでに API やバックオフィス連携で足りる領域は、署名鍵に接点を移さない、という整理に対応する。

署名鍵／ウォレット側に移す利点が認められる場合

- **相手方が多数・未知・交代し得て**、都度の API 接続では際限なく煩雑になる（パーミッションレス上の流通、DEX・DeFi 上の二次利用、多数の検証者への提示）。デジタル庁技術 WG が指摘した「API が増え続ける問題」と同様である [15]。
- **発行プラットフォーム外**への持ち出しと P2P 移転が、商品の本質である（Distributed ／ F1。JPYC のノンカストディ明示、USDC 等）。
- **利用者の明示的操作と同意**、提示範囲の最小化、提示者の紐づけが要件である（属性証明の選択的開示・Holder Binding に対応）。金融では、委任・限度額・どの資産を動かすかの署名画面がこれに当たる。
- **対面・オフラインを含む共通 UX** や、複数の証明・残高をまとめて扱う必要がある（単一フェデレーションでは足りない、という令和 7 年度の整理 [13]）。

表 4　DIW・属性証明の整理と金融振替の対応

デジタル庁側の概念	金融（ERC-20 タイプ）への対応
Issuer	金融トークンの発行者、裏付資産の管理者、証券の発行体等
Holder ／ Wallet	顧客の署名鍵を管理するウォレット（自己管理またはカストディ）
Verifier	移転の相手方、取引所、DEX のフロント、カストディアン、検証を行う仲介者
Wallet Provider	ウォレットソフト／ハードの提供者、カストディ業者、回復サービス提供者
バックオフィス連携・信頼経路上の API	口座階層・振替機関間連携、全銀・RTGS、カストディ間メッセージ、G5 の取引順序の合意（Canton ワークフロー等）
利用者を介した情報連携（IHV ／ DIW）	署名鍵に金融取引の接点が移るタイプ（大分類 G1）。発行 PF 外への移動・P2P 移転
「API でできているところは置き換えない」	すでに機関間の API や口座連携で足りる決済・照合は、署名鍵に接点を移さない（G5 のまま残し得る）。
クレデンシャルの喪失・サービス終了	署名鍵の喪失、シード漏洩、業者退出による資産アクセス不能
表示と同意の形骸化	署名画面とオンチェーン上の実際の呼び出しの不一致（誤移転）
Wallet に求める要件（プロトコル、セキュリティ、署名鍵管理、相互運用）	金融資産ウォレットの認証・評価の参照枠
IHV モデル	発行・保有・移転先検証の責任分界の骨格

- 法制度上、従来の口座間・機関間の直接連携だけではカバーできない官民・異業種の接点に、金融トークンを載せる必要がある。

場合を分けるときは、少なくとも次の点を見る。

1. **誰が署名鍵を持つか：**顧客本人（自己管理＝軸 E1）、業者のカストディ（E2）、複数者の共同管理（E3）、機関同士のメッセージのみ（Represented ／ E5 = G5）。

2. **失念・相続・復旧を誰が負うか：**自己管理では、技術的には顧客に帰属しやすい。カストディでは、業者の義務と分別管理が中心になる。
3. **その署名鍵で何を証明し、何を認可するか：**属性の提示なのか、残高の移転なのか。後者は不可逆性が高く、前者と同一の UX・同一のリカバリ設計で足りるかは自明でない。
4. **発行プラットフォーム外への移動と P2P 移転を許すか：**許すなら Distributed（軸 F1）／大分類 G1 の移転自由。許さないなら、G5 または G1 の制限付き運用であり、責任の置き方も口座に近い側へ寄る。
5. **すでに信頼できる API ／バックオフィス相当で足りるか：**足りるなら、署名鍵に接点を移さない。

AI エージェントが金融取引を自動実行する局面では、エージェントのアイデンティティ検証と、エージェントが用いる署名鍵の管理が、さらに重なる [1, 13]。この局面では、属性証明側の DIW 議論（権限委譲・代理人）と、金融側のウォレット議論が重なる。

4 責任分界の考え方の変化

4.1 責任分界の考え方

責任分界では、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**。ブロックチェーンに求められる要件は、タイムスタンプサービスとしての適格性である。ウォレットに求められる要件は、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である。責任分界の選択肢と、それを考える場合の運用条件および認証制度を示す。

分界を可能にするには、ブロックチェーンとウォレットの双方について、性能上およびセキュリティ上の運用条件を定め、それを満たすことを認証する [26]。直近の事例が示すとおり、その「ウォレット」は端末チップに限らず、署名 UI、依存パッケージ、流通経路、運用者端末を含む。暗号資産ウォレット向けの Protection Profile（PP）が整備途上であることも、関連する技術コミュニティで共有されている [27]。**分界には認証が必要である**こと、認証の対象に**署名鍵管理装置とサプライチェーン**を含めること、およびデジタル庁側が Wallet 要件の明確化を既に検討事項としていること、を本研究会の前提に置く。

4.2 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。利用するブロックチェーンに何を要求するかは、金融インフラとしてのセキュリティ確保の基本的な検討項目である。ここでの問いは、概念が期待する安全性と永続を、分散タイムスタンプの設計と実装が保証しているかどうかである。「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。

4.3 現在の基準—我が国の時刻認証業務

4.3.1 総務大臣による認定制度

令和 3 年総務省告示第 146 号「時刻認証業務の認定に関する規程」[17] は、確実かつ安定的にタイムスタンプを発行する時刻認証業務を総務大臣が認定して奨励することにより、情報の信頼性を担保しながら電磁的流通を振興することを目的とする（第 1 条）。

同規程第 2 条は、「タイムスタンプ」を、電子データに付与される時刻情報等の総体であって、次の双方に該当するものと定義する。

1. 当該電子データがある時刻に存在していたことを示すためのものであること。
2. 当該電子データについて改変が行われていないかどうか確認することができるものであること。

「時刻認証業務」とは、電子データに係る情報にタイムスタンプを付与する役務を提供する業務である（第 2 条第 2 項）。

総務大臣が認定できる要件は、第 3 条第 1 項各号に列挙されている。以下は、**告示の号順に従った**要約である（条文番号の対応は付録を参照）。

1. **デジタル署名方式**（信頼できる認証事業者から発行を受けた電子証明書に基づく、当該業務専用の利用者署名符号を用いて時刻情報等にデジタル署名を施す方式）を用いること（第一号）。
2. 日本標準時通報機関である国立研究開発法人情報通信研究機構が生成する協定世界時（UTC(NICT)）を時刻源とし、当該時刻源との時刻差が**一秒以内**となるよう、時刻の品質を管理および証明する措置を講ずること（第二号）。
3. 認定業務であることを一意に特定できる情報を含み、自らが改ざんされた際にこれを検知する手段を有するタイムスタンプを、有効である間十分な安全性を有する暗号技術や装置等を用いて堅実に生成すること（第三号）。
4. 電気通信システムに十分なサイバーセキュリティ対策を講ずること（第四号）。
5. 設備を含む建築物について、震災、風水害、落雷、火災等の被害を容易に受けない措置および十分な防犯対策を講ずること（第五号）。
6. 利用者および検証者に対し、改ざん等に関する検証を適切に行うに当たり必要な情報を提供すること（第六号）。
7. 継続的に安定して遂行するに足りる**経理的基礎および技術的能力**その他の能力を有すること（第七号）。
8. 欠格事由に該当しないこと（第八号）。
9. 利用者および検証者に、必要に応じて関連情報を提供すること（第九号）。

10. その他、確実かつ安定的に発行するために必要な措置を講ずること（第十号）。

加えて、認定の有効期間は二年ごとの更新を要する（第 4 条）。認定事業者は、休止または廃止しようとするとき、検証に必要な情報の継続的提供その他の利用者・検証者保護に十分な内容を含む**終了計画または再開計画**を併せて届け出なければならない（第 5 条第 3 項）。運用規程の策定・公表（第 6 条）、個人情報等の適正取扱い（第 7 条）、毎年の監査と総務大臣への報告（第 8 条）、認定の取消し（第 9 条）、事業の承継（第 10 条）も定められている。指定調査機関として、一般財団法人日本データ通信協会が指定されている [18]。

4.3.2 タイムビジネス信頼・安心認定制度（日本データ通信協会）

総務大臣認定の前から、日本データ通信協会は「タイムビジネス信頼・安心認定制度」を運用してきた [19]。適合性評価の観点は、技術基準、運用基準、ファシリティの基準、システム安全性の基準、情報開示の基準の五つである。時刻認証の技術方式として、デジタル署名を用いる方式、リンキング方式、アーカイビング方式が区別される。時刻配信業務認定事業者（TAA）と時刻認証業務認定事業者（TSA）が分離され、TSA の時刻は認定 TAA からの配信・監査を受け、UTC(NICT) に対し ±1 秒以内であること等が求められてきた [19]。電子帳簿保存法等の実務では、認定タイムスタンプの利用が広く参照されてきた。

4.4 国際的な比較

- **ISO/IEC 18014** シリーズ：独立トークン方式のタイムスタンプ、リンクトークンタイプタイムスタンプ、トレーサビリティ等（いずれもタイムスタンプトークンの枠組みであり、金融トークンではない）[7]。
- **IETF RFC 3161**：Time-Stamp Protocol[8]。
- **eIDAS 規則第 42 条**：適格電子タイムスタンプは、(a) 日時をデータに、検知不能な改変を合理的に排除する形で結合すること、(b) 協定世界時にリンクした正確な時刻源に基づくこと、(c) 適格トラストサービス提供者の高度電子署名もしくは高度電子シール、または同等の方法によること、を求める [20]。
- **ETSI EN 319 421**：タイムスタンプを発行するトラストサービス提供者のポリシーおよびセキュリティ要求。Best practices Time-Stamp Policy（BTSP）として、公開鍵証明書に支えられ、精度一秒以内等を含む [21]。プロトコルとプロファイルは EN 319 422。

我が国の総務大臣認定は、デジタル署名方式に寄せた制度設計であり、リンキング方式（リンクトークンタイプタイムスタンプの系譜）はデ協の民間認定側に残る、といった整理が従来なされてきた [22]。分散台帳がリンクトークンタイプタイムスタンプの系譜にあることを踏まえると、**制度がどの方式を「タイムスタンプ」として認めるか**自体が、オンチェーン金融の接続点になる。ここでも、認められるのは時刻認証としてのタイムスタンプ（およびそれが返すタイムスタンプトークン）であり、金融トークンの適法性とは別の問いである。

4.5 従来のタイムスタンプサービスとの違い

単一の TSA が引き受けていたことと、分散タイムスタンプで起きることとを対比すると、表 5 のようになる。

表 5　従来のタイムスタンプサービスとの違い（単一 TSA と分散タイムスタンプ）

単一 TSA が引き受けていたこと	分散タイムスタンプで起きること	論点
認定事業者が時刻品質を管理・証明（UTC(NICT)、一秒以内）	多数のノード／バリデータ／マイナー	誰の時計を、どの手順で UTC に結び付けるか。結び付けない設計なら、何を「時刻」と呼ぶか
設備・防犯・サイバーの認定対象が明確	運営主体が拡散し、匿名に近い場合もある	調査・監査の入口はどこか
休廃止時の終了計画、検証者への情報提供	チェーンは存続しても、単一の事業者は残らない／分岐する	クライアント、過去状態、チェックポイント等、検証に必要な情報の保管義務は誰か
経理的基礎・技術的能力	手数料市場やステークに依存	赤字でも検証可能性を残す仕組みはあるか（ほふり水準の事業継続）
事業体の存続・終了計画	**ブロックチェーン永続が未保証**（後述）	ブロックチェーンプロジェクトが停止したときの対応
暗号アルゴリズム更新を事業者が計画	ハードフォークやウォレット移行が必要	危殆化時の移行責任と、顧客資産の扱い（量子計算機リスクを含む [1]）
タイムスタンプの法令上の依拠（電子帳簿保存等）	分散台帳の記録が同じ法的地位を持つかは未整理	どの記録を、どの法令の「タイムスタンプ」とみなすか
表示規制（認定業務である旨の表示）	「オンチェーンだから公証に相当」等の標榜	誤認防止の規律は何か

許可型で運営主体が明確な実装には、既存の時刻認証業務の基準をほぼそのまま当てられる場合がある。パーミッションレスには、当て直した基準表が要る。いずれの場合も、ERC-20 タイプは分散タイムスタンプを**利用する**側であるから、利用するブロックチェーンの選定・モニタリング・障害時の顧客対応を、誰の義務とするかを、責任分界と一体で設計する必要がある。

4.6 ブロックチェーンの永続性の課題

総務大臣認定は、認定事業者に**継続的に安定して遂行するに足りる経理的基礎**と、休廃止時の**終了計画**を求める [17]。分散タイムスタンプでは一つの事業者がまとめて引き受ける形にはならないが、「ブロックチェーンが消えてよい」ことにはならない。オンチェーン金融が利用するのは、第三者が検証可能な**順序付き台帳の継続的生成**である。したがって責任分界

の考え方としては、暗号と時刻源に加え、**利用するブロックチェーンが、証券・決済・償還に要する期間にわたって存続し、検証可能な状態を保つか**を検討する必要がある。「ブロックチェーンだから永続する」は、公開されている経験則にも、主要ネットワークに関する研究にも、裏付けられていない。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である。

モニタリング項目への分解

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**（ネットワークが止まり続けないか）。
2. **履歴の改ざん耐性の維持**（過去の確定を覆すコストが、保護すべき価値に対して十分か）。
3. **検証可能性の継続**（過去のタイムスタンプトークン相当・状態を、何年後でも第三者が検証できるか。ノード・スナップショット・チェックポイントの供給を含む）。
4. **エコシステムの継続**（クライアント実装、ブリッジ、カストディ接続、法的エンティティの存続）。チェーンが「動いて」いても、利用者が資産を動かせなければ、金融インフラとして機能していない。

（1）検証への報酬や手数料—最大級のチェーンでも未解決

パーミッションレス型の安全性は、多くが**報酬で買う計算／ステーク**に依存する。その予算が長期に維持されるかは、設計上の仮定であって観測事実ではない。

Bitcoin：ブロック補助金は約四年ごとに半減し、最終的にはゼロへ向かう。ケンブリッジ大学オルタナティブ・ファイナンス・センター（CCAF）は、手数料が補助金を置き換えるという想定に対し、実績上の手数料収入が今日のセキュリティ水準を維持するには遠く及ばないこと、手数料が極めて揮発的であること、補助金のドル価値を維持するには大幅な価格上昇が要ること等を整理している [42, 43]。一例として、2026 年 10 月近傍の 90 日間では、手数料がマイナー収入に占める割合は約 0.67% にすぎず、歴史的にも多くの期間で 5% 未満にとどまる、との報告がある [42]。攻撃費用は「ネットワークの時価総額」ではなく**マイナー収入に連動して下がる**、という整理も同報告の論点である。他方、攻撃の総費用（TCA）を推計し、現行では攻撃が経済的に非現実的である、補助金減衰とセキュリティの単純な線形関係は成り立たない、とする研究もある [44]。**結論が割れていることは、金融インフラの前提としては不十分である。**

Ethereum：実行を L2 へ移すロードマップの下で、L1 のベースフィーが大きく減少し、L2 が L1 に払う blob ／データ可用性フィーが長期の価値捕捉の中心になる、との議論がある [45]。L2 からの L1 への支払いが一時的に急減した局面も観察されており、L1 の検証への報酬や手数料を誰が長期に賄うかは未確定である [46]。さらに、バリデータの収益が ETH 建てである一方コストは法定通貨建てであるため、価格の持続的下落が退出を誘い、極端に

は合意が止まる、という「下方スパイラル」懸念も政策・研究の場で論じられている [47]。これは「スマートコントラクトが安全か」とは別の、**ブロックチェーンの稼働そのもの**の問題である。

（2）検証への報酬や手数料が足りないときの現実—履歴の書き換え

Ethereum Classic は、2020 年夏に複数回の 51% 攻撃を受け、数千ブロック規模の再編成と数百万米ドル規模の二重支払いが発生したと報告されている [48, 49]。ハッシュレートの低下が攻撃費用を下げ、流動性のある上場が攻撃誘因を高める、という組み合わせである。事後に MESS 等の対策が導入されたが、「**一度乗ったチェーンが、常に同じ改ざん耐性を持つ」わけではない**ことを示す。パーミッションレスに金融トークンを載せる制度は、利用するブロックチェーンの検証への報酬や手数料のモニタリングと、閾値を下回ったときの顧客・業者の行動（確認待ちの延長、入出金停止、退避）を、あらかじめ設計しなければ、タイムスタンプとしての完全性を前提にできない。

（3）停止と「社会的」再開—永続と可用性は別

Solana は、2022 年に複数回、数時間規模でブロック生成が停止し、バリデータ協調による再起動で復旧したと公式に報告している（例：2022 年 9 月約 6 時間 19 分、2022 年 6 月約 4.5 時間、2024 年 2 月約 4 時間 46 分）[50, 51]。資金の消失はなかったとされるが、**合意の継続は、コードだけでなくオペレータ集団の協調に依存する**。ほふりや認定 TSA が求める計画停止・障害対応・終了計画と比べれば、「誰が再起動を決め、誰が顧客に説明するか」が分散環境では曖昧になる。許可型・コンソーシアム型でも、ブロックプロデューサや API 事業者が報酬不足で退出する事例があり [52]、運営主体の経理的基礎の問題が形を変えて残る。

（4）プロジェクトの放棄の判断・分岐・名目上の残存

暗号資産プロジェクトの多数が短命であることは、業界報告でも繰り返し指摘される（例：2020–2021 年のプロジェクトの多くが開発放棄、平均ライフサイクルが市場サイクルより短い、等の整理 [53]）。Steem から Hive へのコミュニティ分岐 [54]、Terra ／ LUNA 崩壊に伴うチェーン停止と Terra Classic への分離 [55] は、「記録が一つの正史として残る」ことが保証されない例である。時価総額だけが残り、検証に耐える稼働が続いていないチェーンも観察され [56]、**名目上の存続と、検証可能な金融インフラとしての存続は一致しない**。

責任分界の考え方：検討項目

以上を、総務大臣認定が求めてきた項目に対応づけると、表 6 のようになる。検証への報酬や手数料・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である。

表 6　ブロックチェーン永続性に関する検討項目（タイムスタンプ媒体として）

認定 TSA 側の類比	分散／許可型台帳で問うこと
経理的基礎	検証への報酬や手数料（補助金＋手数料／ステーク報酬）の水準とトレンド。閾値を誰が監視するか
終了計画・再開計画	チェーン停止、分岐、クライアント終了、ブリッジ不通時に、検証データと資産退避をどう残すか
設備・運用の継続	バリデータ／ BP の退出、プール集中、再起動の社会的手続きの明示
検証者への情報提供	アーカイブノード、チェックポイント、状態証明の長期供給者は誰か
事業承継	ガバナンス攻撃・財団解散・許可型運営者の事業譲渡後も、同じ媒体とみなせるか

制度論としての帰結は、次である。

1. 大分類の基本形（パーミッションレス上の ERC-20 タイプ）を採用するほど、**利用するブロックチェーンの永続リスク**を顧客・業者・監督が引き受けることになる。G5 や許可型（C2）は、運営主体の終了計画を書きやすい代わりに、単一／少数主体の経理リスクが残る。
2.「主要なチェーンだから永続する」は、Bitcoin ／ Ethereum ですら研究・政策議論が継続中の命題である [42, 45]。銘柄選定のチェックリストではなく、**モニタリング指標と閾値超過時の行動**を、発行体・カストディ・振替接続の契約と監督に落とす必要がある。
3. ほふり水準と比較するとき問うのは、ハッシュレートや TVL の大きさではなく、**赤字・退出のあとに検証と権利移転が残るか**である。

4.7 長期保証—技術と事業継続

タイムスタンプ（およびそれが返すタイムスタンプトークン）が、通貨・証券・資産を表す**金融トークンの記録**に結び付くとき、有効期間の短さは通常許容されない。暗号の危殆化は、タイミングの正確な予測は難しいが、標準暗号の経験では数十年単位で問題になり得る。技術的課題と同等に重要なのが、**事業継続**および直前節の**ブロックチェーンの永続**である。単一のタイムスタンプ局モデルでは、収益性が悪化しても、顧客が依拠している検証を継続しなければならない、という状態に陥り得る [24]。分散タイムスタンプは、この点をインセンティブ設計で緩和し得る一方、表 5・表 6 の未達成を残す。証券保管振替機構が有する安全性と事業継続上の信頼に匹敵させるための要求項目は、この対比表の金融版として、本研究会で埋める必要がある。検討項目は、次のとおりである。

- 停止と復旧（計画停止、障害、攻撃、合意の一時停止と再起動）。

- オペレータが退出しても検証が残ること（アーカイブとチェックポイント）。
- 検証への報酬や手数料の監視と、閾値を下回ったときの入出金・確認ポリシー。
- チェーン分岐・プロジェクトの放棄の判断時の正史の扱いと顧客資産の退避。
- 誤記録の取消しと損失の帰属。
- 暗号の危殆化への移行手順と責任。
- 顧客資産の移転不能時の救済（署名鍵喪失を含む）の限界の明示。

4.8 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。署名鍵に金融取引の接点が移るタイプ（大分類 G1）および業者カストディ（軸 E2）を制度の中心に据えるなら、**ブロックチェーン層の正しさだけでは足りない**。直近の公開事例は、Secure Element やハードウェア自体が侵害された場合だけでなく、**流通経路・署名 UI・依存パッケージ・開発者端末**が侵害された場合にも、顧客資産や機関カストディが失われることを示している。

（1）流通経路の物理改変

2026 年 10 月、ハードウェアウォレット製造事業者 Ledger は、東南アジア等の再販経路で流通した真正デバイスに、セットアップ時の 24 語リカバリフレーズを画面から読み取り LTE ／ eSIM で外部送信する**ハードウェアインプラント**が仕込まれた事案を確認した、と公表した [28, 29]。同社によれば、Secure Element や OS、取引署名ロジック自体は改変されておらず、したがって端末の自己完全性検査では検知しにくい。流通停止要請や再販ルールの強化が行われ、同業の Trezor も再販網の見直しを発表した [30]。

検討項目：自己管理（E1）を推奨する前提として、「正規流通・開封検知・再販禁止・端末認証」をどこまで監督・業界慣行・顧客説明の対象とするか。カストディ業者（E2）が顧客資産を預からない場合でも、顧客が用いる端末の流通リスクをどこまで顧客の自己責任とするか。

（2）署名 UI ／フロント改変（WYSIWYS の崩壊）

2025 年 2 月 21 日、暗号資産取引所 Bybit の Ethereum コールドウォレット（マルチシグ）から、公表ベースで約 15 億米ドル規模の資産が不正移転された [31]。第三者フォレンジック（Sygnia 等）および Safe{Wallet}側の整理によれば、Bybit のインフラ自体より、**Safe{Wallet}のフロントエンド（AWS S3 上等で配信される JavaScript）**に改変が入り、署名者の画面上は正当な移転に見える一方で、実際の署名対象が悪意あるコントラクト更新等にすり替わった、とされる [32, 33]。FBI は北朝鮮系の TraderTraitor ／ Lazarus に帰属すると公表した [34]。CEO 説明では、Ledger 等のハードウェアに表示された内容と画面表示の不一致が欺瞞の一部であった、との技術解説もある [35]。

これは、署名鍵そのものの抽出ではなく、**what-you-see-is-what-you-sign**

（WYSIWYS）の崩壊である。マルチシグとハードウェア署名があっても、署名 UI のサプライチェーンが侵害されれば足りる。

検討項目：カストディ・マルチシグ・ハードウェア署名を「署名鍵管理が堅牢である」と認める条件に、**署名ペイロードの独立検証（クリアサイニング、オフライン検証、複数経路の突合）**を含めるか。第三者の署名 UI ／ウォレット SaaS を使う場合の責任分界（発行体・取引所・UI 提供者・顧客）をどう切るか。

（3）ソフトウェア依存（npm ／ CDN 等）

2023 年 12 月、Ledger Connect Kit の npm パッケージが、元従業員アカウントのフィッシング等を契機に悪意ある版へ差し替えられ、当該キットを動的読込していた多数の dApp 利用者の署名が資産流出につながった [36]。ハードウェアは無傷でも、**接続ライブラリの CDN ／パッケージ供給**が侵害されれば足りる。

検討項目：金融資産ウォレットおよび業者フロントの SBOM、依存の固定化、署名付き配布、動的 CDN 更新の禁止／制限を、認証・監督上の運用条件に含めるか。

（4）セキュアエレメント実装欠陥

2024 年、Infineon の ECDSA 実装における非定数時間の剰余逆元に起因するサイドチャネル攻撃（EUCLEAK）が報告され、YubiKey 5 系列（ファームウェア 5.7 未満）および YubiHSM 2（2.4.0 未満）等への影響が Yubico のアドバイザリにまとめられた [37, 38]。攻撃には物理近接と専用機材が要るが、Common Criteria 等の高い評価を経たセキュアエレメントでも、**サプライチェーン上の暗号ライブラリ依存**が長期間見落とされ得ることを示す。Yubico は自社ライブラリへの移行により Infineon 依存を減らすと述べている [38]。機関向け HSM についても、物理近接で改ざん証跡を残さず内部にアクセスし得る、といった製品アドバイザリが公開されている例がある [39]。

検討項目：金融インフラが依拠する HSM ／セキュアエレメントの、アルゴリズム実装・ファームウェア世代・サプライヤ依存のインベントリと、危殆化時の署名鍵移行・再発行手順を、暗号移行論と接続して求めるか。

（5）開発者・運用者端末からの侵入

北朝鮮系と目される活動では、偽の求人・コーディング課題等で取引所・カストディ周辺の開発者端末に侵入し、署名鍵・資格情報・クラウドセッションを窃取する手法が繰り返されている。例として、Ginco 経由で DMM Bitcoin から約 4,503 BTC が流出した事案（2024 年）[40]、Rain 取引所からの約 1,600 万米ドル規模の流出 [41]、上記 Bybit 事案における Safe 開発者マシン／ AWS セッションの侵害 [33] がある。

検討項目：「署名鍵は HSM に閉じている」と言いながら、署名承認・デプロイ・クラウド配信の権限が開発者ノート PC に残っていないか。職務分離、ハードウェア認証、セッショ

ンの短寿命化、本番署名のエアギャップを、カストディ規制・検査項目にどう落とすか。

ウォレットの安全性：検討項目の要約

以上より、ウォレットの安全性における検討項目は、次を含む。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。

1. **署名鍵の所在**だけでなく、**署名内容の真正な表示と検証**（WYSIWYS）を、責任分界の条件に含めること。
2. **端末・HSM のチップ完全性**に加え、**流通・再販・開封、署名 UI ／ CDN ／ npm、開発者端末・クラウド資格情報**を、サプライチェーン評価の対象に含めること。
3. 自己管理（E1）と業者カストディ（E2）で、上記リスクの**負担者と説明義務**が異なることを、制度上明示すること。E1 では顧客が流通・開封を確認しきれない現実と、業者・製造者・再販者の役割を整理する必要がある。
4. デジタル庁が Wallet 要件（プロトコル、セキュリティ、署名鍵管理、相互運用）を検討事項としていること [13] と、暗号資産ウォレット向け PP 整備 [27] を、金融資産ウォレットの認証枠に接続すること。
5.「すでに API ／バックオフィス連携で足りる領域は、署名鍵に接点を移さない」（表 3）判断と対応させて、**署名鍵に移すと決めた領域**では、上記サプライチェーン項目を満たさない限り責任を切れない、とすること。

5 研究会への論点

本節の項目は、規制の対象をサービス概念ではなく、設計と実装が保証する範囲に置くための共通前提である。各論に入る前に、設計と実装が保証する範囲、その長所、欠点、制限を示したうえで、次の事項を事務局資料に記載する。

1. **対象サービスの類型化：**各論の前に、表 1・表 2 および付録 D に倣い、大分類 G0–G5（署名鍵に金融取引の接点が移る G1 と部分利用の G5 を含む）を分ける事務局資料を作成する。RWA.xyz の Distributed ／ Represented は補助線として用いてよいが、一次の制度判断は我が国の法令と監督の言葉で行うこと。
2. **デジタル庁整理との参照：**DIW アドバイザリーボード報告書および属性証明の課題整理に関する有識者会議報告書の、**API ／バックオフィス連携と利用者を介した DIW の使い分け**（表 3）、リスク要因、Wallet 要件を、金融への応用における検討のための参照表として、関係省庁の協力のもと整備する。「すでに API ／バックオフィス連携で足りる領域は、署名鍵に接点を移さない」原則を、事務局資料の前提とする。
3. **タイムスタンプ基準の対比表：**総務大臣認定の要件と、分散タイムスタンプにおける未達成（表 5）、および**利用するブロックチェーンの永続性**（表 6：検証への報酬や手数料、履歴の改ざん耐性、停止・再開、放棄の判断）を、共通前提として次回資料に掲げる。

4. **責任分界の選択肢：**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したうえで、金融機関が顧客に対する責任を切る／切らないの選択肢と、責任分界を考える場合の運用条件・認証制度を提示する。ウォレット層の条件には、WYSIWYS（署名内容の独立検証）、HSM／セキュアエレメントの実装世代、流通・再販、署名 UI／依存パッケージのサプライチェーン、運用者端末の職務分離を含めること。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こと。
5. **決済短縮は結果として扱う：**T+1 化等の是非は、振替の高度化とタイムスタンプ層の信頼が回った後の帰結として扱う。

付録 A　ERC-20（EIP-20）の状態遷移—要約

本付録は、法的な資産定義ではない。インターフェースの要約である [3]。

必須に近いメソッド（仕様上の扱いは EIP-20 本文に従う）：

- `totalSupply()`：総供給量。
- `balanceOf(address _owner)`：残高。
- `transfer(address _to, uint256 _value)`：呼び出し元から移転。`Transfer` イベント。
- `transferFrom(address _from, address _to, uint256 _value)`：許可に基づく引出し。`Transfer` イベント。
- `approve(address _spender, uint256 _value)`：引出し許可。`Approval` イベント。
- `allowance(address _owner, address _spender)`：残許可額。

任意のメタデータ：`name`、`symbol`、`decimals`。

事前条件・事後条件の直感：`transfer` は、呼び出し元残高が十分であること（仕様上は不足時に throw すべきとされる）を前提に、送信側残高を減じ、受信側残高を増す。`approve`/`transferFrom` は、第三者契約が代理で移転するための許可フローを与える。ゼロ値の移転も通常の移転として扱いイベントを発火する、等の細部は EIP-20 に従う。

付録 B　ERC-3643：適合性付き移転の構成

ERC-3643 は、ERC-20 互換の残高インターフェースに、オンチェーンの身元検証と移転ルールを組み合わせた規格である [4]。ERC-20 の `transfer` 等は呼べる。実装上の移転は、関係者の身元の適格性と、トークンに課した規則への適合性を両方満たすことを条件とする。発行体（Owner）が、規則の設定と Agent の任命を行う。本文の対比は図 2、ここでの構成は図 4 である。

- **Token**：ERC-20 面の残高と移転に、pause と freeze を加える。
- **Identity Registry**：アドレスに紐づくオンチェーン身元が検証済みか（`isVerified`）を返す。適格性の門である。
- **Compliance**：その移転が発行体の定めた規則を満たすか（`canTransfer`）を返す。適合性の門である。
- **Agent**：発行体が任命する。freeze、強制移転、鍵喪失時の recovery を行う。
- **Claim と Trusted Issuers（ONCHAINID）**：身元に付された主張と、それを発行してよい主体の登録である。Identity Registry が適格性を判定するときの参照になる。

保有者の操作の接点は署名鍵である。発行体は、適格性と適合性のチェックをどう置くか、および Agent 権限を誰に与えるかを決める主体である。両方の門を通過した移転だけ

が、台帳上の残高更新として記録される。

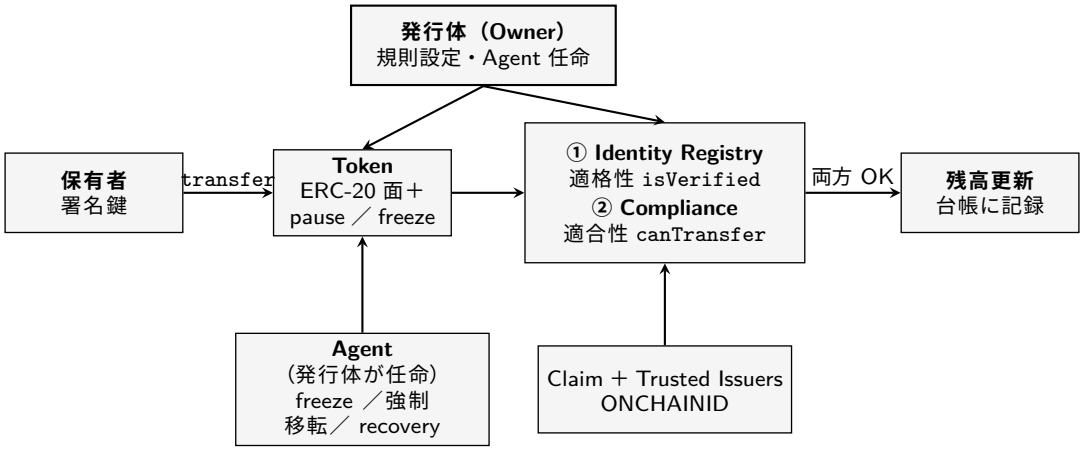


図 4　ERC-3643 の適合性付き移転。保有者の `transfer` は、停止・凍結のあと、適格性と適合性を両方満たして残高が更新される。

付録 C　詳細の分類—軸 A–H の定義

大分類（表 1）のうえで、各軸は独立に選ぶ。類型コードは**大分類** | `A` | `B-pattern` | `C` | `D` | `E` | `F` | `G-*` | `H` の形で書く。空欄は未設計／複合とする。

軸 A　供給・発行の主体

- A1：単一の営利発行体（Circle、JPYC 社、銀行単体等）
- A2：発行体＋振替代理人／カストディアン分担（BUIDL ＋ Securitize タイプ）
- A3：預託・振替インフラが entitlement を発行（DTCC Factory タイプ）＝ G2
- A4：複数発行／共同発行（コンソーシアム銀行 SC 等）
- A5：プロトコル／ DAO 主導の供給（DAI 的）。G3 寄り
- A0：供給主体なし（ワークフローのみ）＝ G5 寄り

軸 B　帳簿層の責任配置

帳簿は次の四層に分解する。**E** 経済・請求権（準備、預金、信託財産、償還義務 ↔ 流通量）、**R** 法的名義・公式名簿、**T** 移転台帳（残高写像と Transfer の順序・非改ざん）、**W** 業務ワークフロー（合意・担保凍結・現金レール連携）。責任者の記号例：Iss（発行体）、TA（振替代理人等）、CSD（預託・振替機関）、Chain（チェーン／合意）、Cust、Plat、User、n/a。

典タイプパターン：

- **B-α**：E=Iss、R=Iss（または Iss ＋オフチェーン）、T=Chain。例：USDT ／ USDC、JPYC（償還ゲートは Iss）。
- **B-β**：E=Iss、R=TA が T ＋ PII を合成、T=Chain（公式名簿の一部）。例：BUIDL

／ Securitize。

- **B-γ**：R=CSD（DTC の公式帳簿。LedgerScan 等で追跡）、T=Chain + CSD が公式化。例：DTCC Tokenization。
- **B-δ**：R=Iss +コンソーシアム規則、T=許可型の取引順序の合意。例：ibet、旧 Progmat。
- **B-ε**：W が主、T は弱または表象のみ。例：Broadridge DLR。
- **B-ζ**：プロトコル／担保契約。無発行体 DeFi 脚。

軸 C　タイムスタンプ媒体

C1：パーミッションレス L1 ／ L2。C2：許可型だが第三者検証可能な取引順序の合意（ibet、許可 Avalanche L1、Canton synchronizer 等）。C3：古典的時刻認証を自帳簿に押す。C4：コミットメントのみ公開・状態はクライアント側（RGB）。C5：単一運営者の私有 DB +薄い順序。

軸 D　金融トークンのインターフェースタイプ

D1：EIP-20 そのもの。D2：ERC-20 互換+拡張（ERC-3643、freeze 等。構成は付録 B）。D3：他 VM の同種（SPL、TRC-20、ibet 標準、CIP 等）。D4：UTXO ／契約オブジェクトタイプ。D5：クライアント側状態。D0：金融トークンなし（W のみ）。本文の「ERC-20 タイプ」＝主に D1–D3。基本形＝ G1×C1×D1×E1×F1。

軸 E　署名鍵・カストディ

E1：顧客自己管理（ノンカストディ）。E2：業者カストディ。E3：共同管理／ MPC ／スマートコントラクトウォレット。E4：機関の登録ウォレットのみ。E5：署名鍵に金融取引の接点が移らない（口座・メッセージのみ）＝ G5 の定義的特徴。

軸 F　移動性（RWA.xyz と同趣旨）

F1：Distributed（発行 PF 外へ移せ、P2P 可。ホワイトリスト付きを含む）。F2：Represented（外に出せない／ P2P 不可）。F3：ハイブリッド（条件付きで F1 へ移行中）。

軸 G（移転制約）・軸 H（償還ゲート）

移転制約の置き場所：G-a（制約なし）、G-b（オフチェーンのみ）、G-c（オンチェーン許可）、G-d（pause ／ freeze ／強制移転）、G-e（登録ウォレット間のみ）。償還：H1（常時パー償還・KYC）、H2（限定顧客）、H3（償還なし／二次のみ）、H4（デトークン化で従来口座へ）、H5（プロトコル清算）、H0（該当なし）。H1 でも、発行体は各人残高の正本管理者である必要はない。要るのは顧客 $\leftrightarrow$ アドレス対応、償還時に必要量がゲートに渡ったことの検証（T を読む）、E の総量整合である。

責任分界チェックリスト（コードから読む）

1. E の失敗（準備不足・償還不能）→ 通例 Iss。タイムスタンプはチェックしない。
2. R の失敗（誤名義・KYC 紐付け誤り）→Iss ／ TA ／ CSD。
3. T の失敗（再編成・検閲・停止等）→Chain。
4. T 上の特権操作（不正 mint、不当 freeze）→ 見えるのは Chain のチェック機能。抑止は権限設計・監督。
5. 署名鍵の失敗（E1 の喪失、E2 の業者事故）→ 軸 E。ウォレット認証。
6. W の失敗（DLR 等）→G5。G1 の分界論を持ち込まない。

付録 D　既存サービス対応表

公開プレス・公式資料に基づく類型割当である。凡例：大分類｜ A ｜ B ｜ C ｜ D ｜ E ｜ F ｜制約｜ H。

G0　現在の金融システム

ほふり振替制度、日銀当座・国債振替（従来）、DTC 従来簿記、銀行勘定系・全銀ネット等。G1 ／ G2 の接続相手であり、事務局資料 D の出発点。

G1　発行体付き金融トークンタイプ

ステーブル／電子決済手段（日本）

サービス	コード要約	メモ
JPYC（1 号、JPYC 社）	G1 ｜ A1 ｜ B-α ｜ C1 ｜ D1 ｜ E1 ｜ F1 ｜ H1	2025-10-27 発行開始 [57]。Avalanche ／ ETH ／ Polygon ／ Kaia（Kaia は 2026-05 追加）。JPYC EX ＝ノンカストディ明示。P2P 制限なし。発行・償還は KYC。発行上限は当初「1 日あたり 100 万円」、2026-05 以降は「1 回あたり 100 万円」（連続申請制限あり）
JPYSC（3 号、SBI 新生信託 ×Startale）	G1 制限極｜ A1 ｜ B-α ｜ C1 準備｜ D1 様｜ E2 ｜**現状 F2** ｜ H2	2026-06-24 国内初の信託タイプ円 SC[58]。VC トレード口座内のみ・出庫不可。法令整理後にパブリック流通へ移行予定（同一商品の移動例）

サービス	コード要約	メモ
3 メガ共同発行 SC	G1 ｜ A4 ｜ B-α/δ ｜ C2 寄り ｜ D3 様｜ E2 ｜ F2 寄り ｜ H2	みずほ・MUFG・SMBC、受託 MUTB、TISI 基盤。特定信託受益権。2026-07 実証、2026 年度中の実取引開始めざす [59]。銀行 KYC 済み利用者間
Progmat Coin 等	G1 ｜ A2/A4 ｜ B-α/δ ｜ C2 寄り ｜ E2 ｜ F2 寄り	信託タイプ 3 号の系統。媒体・移転条件は銘柄・時期により異なる

ステーブル（海外・主要）

USDC、USDT、PYUSD、RLUSD 等：概ね `G1` ｜ `A1` ｜ `B-`α ｜ `C1` ｜ `D1/D3` ｜ `E1/E2` ｜ `F1` ｜ `H1/H2`。DAI ／ USDS は A5・B-ζ 寄り（担保契約タイプ）。USDe は準備の性質が預金タイプと異なる。

トークン化預金

- **JPM Coin ／ JPMD**（Ethereum、Base）：G1 ｜ A1 ｜ B-α ｜ C1 ｜ D1 ｜ E2/E4 ｜承認先間の F1 ｜ H2。Canton ネイティブ計画では C2・D3 へ（同一商品・媒体変更）。
- **HSBC Tokenized Deposit Service**：私有チェーンのみなら G5 寄り／ G1 制限極（C5・F2）。Canton DvP パイロットは G1 接続への移行例。
- 国内 PIP・トークン化預金実証（ディーカレット DCP×GMO あおぞら等）：G1 ｜ C2 ｜ E2 ｜ F2 寄り。

トークン化国債・MMF・ファンド（海外）

BUIDL（BlackRock ／ Securitize）：`G1` ｜ `A2` ｜ `B-`β ｜ `C1` ｜ `D1/D2` ｜ `E1` ｜ `F1 (WL)` ｜ `H2`—公式名簿＝ Token ledger ＋ PII の合成。BENJI ／ FOBXX、WTGXX、USDY ／ OUSG、USTB、USYC、PAXG ／ XAUT 等も G1 に属する。

セキュリティトークン（日本）

- **Progmat** 上の不動産 ST 等：G1 ｜ B-$\delta\to\beta$ 寄り｜ **C2**（専用 Avalanche L1 ／ AvaCloud）｜ D2/D3 ｜ E2 中心｜ F2〜条件付き F1。2026-07 に全 ST（4,520 億円超）が Corda5 から移行完了 [60]。
- **ibet for Fin**（BOOSTRY）：G1 ｜ B-δ ｜ C2 ｜ D2/D3。不動産 ST 多数（例：川崎・商業／オルタナ信託）。**SBI START 債**（2026-03、100 億円、社債 ST）は ibet ＋ ODX

START 上場。

- **ODX START**：G3 寄り（市場）。約定は PTS、土台 ST は G1。

G2　第三者帳簿責任者タイプ

DTCC Tokenization Services（DTC）：`G2` ｜ `A3` ｜ `B-`γ ｜ `C1+C2` ｜ `E4` ｜ `Registered Wallet` 間の `F1` ｜ `G-e` ｜ `H4`。公式の帳簿・記録は DTC に残り、ComposerX LedgerScan 等がチェーン上の移転を追跡して記録する設計（NAL 等の整理）。Digital Omnibus ＋ミント。2026-07 選別参加者での本番取引、2026-10 に市場向け提供が予定・展開 [61]。起動時ネットワーク例：Canton および Besu。原証券名義は Cede & Co.。日本の振替法との差分が論点。Euroclear 等の CSD 実証は同種の国際比較用。

G3　応用サービスタイプ

Uniswap、Sushi、Curve、Aave、Compound 等：土台の金融トークン（USDC 等）は別行の G1。ibet Exchange ／ DvP ／ Escrow はコンソーシアム上の応用。暗号資産取引所のオフチェーン照合＋オンチェーン出庫は G3 ／ G0 混合。

G4　非アドレス残高タイプ

RGB ／ Taproot Assets（C4・D5）、Canton Coin（D4 UTXO、CIP 上の金融トークンとは別）、Liquid Network 発行資産の一部。

G5　部分利用タイプ

- **Broadridge DLR**（Canton）：`G5` ｜ `A0` ｜ `B-`ε ｜ `C2` ｜ `D0` ｜ `E5` ｜ `F2`。レポ合意・執行・担保所有の同期。現金は従来決済レール。RWA.xyz の Represented（Canton）の大部分 [62, 10]。
- Canton 上の機関ワークフロー単体（金融トークン未載）：同じネットワーク名に G1（CIP ／ JPMD）が同居し得るため、**ネットワーク名で切らない**。
- 強い Represented、HSBC 私有 TDS（外部移転なし）、従来口座＋ API 突合のみ。

同一ブランドの移動例（再掲）

JPM Coin（ETH ／ Base→Canton）、Progmat（Corda→Avalanche L1）、HSBC TDS（私有 →Canton DvP）、JPYSC（口座内のみ → パブリック出庫予定）、DTCC（従来簿記 G0→Tokenization G2）。

付録 E　用語一覧

本資料は、「トークン」を単独では用いない。時刻認証側と金融サービス側を次のとおり書き分ける。

本資料の用語	意味・注意
タイムスタンプトークン	時刻認証が返すデータ。ISO/IEC 18014 等。存在時刻と非改ざんの検証に用いる。金融トークンではない
リンクトークンタイプタイムスタンプ	ISO/IEC 18014-3 の方式名。「リンクトークン」は規格用語であり、金融トークンを指さない
金融トークン	金融サービス上の残高・権利を表すもの。ERC-20 トークン、セキュリティトークン、ステーブルコイン、トークン化預金等を含む総称
ERC-20 トークン／ ERC-20 タイプ	EIP-20 インターフェースに代表される、署名鍵に紐づく残高と移転の状態遷移。他チェーンの類似規格を含む便宜的総称（軸 D1–D3）
ERC-3643	ERC-20 互換の残高に、オンチェーンの適格性（Identity Registry）と適合性（Compliance）、および発行体が任命する Agent の権限を規格として載せたもの。構成は付録 B
大分類 G0–G5	本資料の大分類。G0 現在の金融システム、G1 発行体付き金融トークンタイプ、G2 第三者帳簿責任者タイプ、G3 応用サービスタイプ、G4 非アドレス残高タイプ、G5 部分利用タイプ
E ／ R ／ T ／ W	軸 B の帳簿四層（経済、名義、移転台帳、ワークフロー）
セキュリティトークン、ステーブルコイン、トークン化預金	制度・市場で定着した金融トークンの固有名詞。本資料でもこの語を用いる
分散タイムスタンプ	Nakamoto の用語法に近い。単一 TSA の不在。返すものは依然として時刻順序の証明であり、金融トークンそのものではない
Distributed / Represented	RWA.xyz の金融トークン化資産の分類。本資料では軸 F および G1 ／ G5 の補助線
DIW	デジタル庁報告書の Digital Identity Wallet。暗号資産ウォレットと同一視しない
利用者を介した情報連携	Issuer が発行した VC 等を Holder が保持し Verifier に提示する経路（IHV）。バックオフィス連携の補完

本資料の用語	意味・注意
バックオフィス連携	デジタル庁資料では、マイナンバー制度等に基づく**行政機関同士**の情報連携。サーバー間 API 一般とは別義
IHV	Issuer–Holder–Verifier
時刻認証業務／ TSA	総務省告示・デ協認定の文脈。分散台帳のバリデータ集合とは同一でない

付録 F　時刻認証業務の認定要件—条文番号の対応

本文第 III 部の要約に対応する、令和 3 年総務省告示第 146 号の条文番号は次のとおりである。

- 定義：第 2 条（タイムスタンプ、時刻認証業務）
- 認定要件：第 3 条第 1 項第一号〜第十号
- 更新：第 4 条
- 変更・休廃止と終了計画：第 5 条
- 運用規程：第 6 条
- 監査報告：第 8 条

参考文献

[1] 金融庁,「成長投資を促進するための金融戦略」, 2026 年 7 月 21 日.

[2] 金融庁,「事務局説明資料」, 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（令和 8 事務年度第 1 回）, 2026 年 10 月 20 日.

[3] F. Vogelsteller and V. Buterin, “ERC-20: Token Standard,” Ethereum Improvement Proposals, no. 20, 2015. `https://eips.ethereum.org/EIPS/eip-20`

[4] J. Lebrun, T. Malghem, K. Thizy, L. Falempin and A. Boudjemaa, “ERC-3643: T-REX — Token for Regulated EXchanges,” Ethereum Improvement Proposals, no. 3643, 2021. `https://eips.ethereum.org/EIPS/eip-3643`

[5] S. Haber and W. S. Stornetta, “How to time-stamp a digital document,” *Journal of Cryptology*, vol. 3, no. 2, pp. 99–111, 1991.

[6] D. Bayer, S. Haber and W. S. Stornetta, “Improving the efficiency and reliability of digital time-stamping,” in *Sequences II*, Springer, 1993, pp. 329–334.

[7] ISO/IEC 18014-3, *Information technology — Security techniques — Time-stamping services — Part 3: Mechanisms producing linked tokens.*

[8] C. Adams, P. Cain, D. Pinkas and R. Zuccherato, “Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP),” IETF RFC 3161, 2001.

[9] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008.

[10] RWA.xyz, “A New Framework for Tokenized Assets: Distributed & Represented,” `https://app.rwa.xyz/blog/a-new-framework-for-tokenized-assets-distributed-and-represented`

[11] RWA.xyz Documentation, “Tokenization Type,” `https://docs.rwa.xyz/frameworks/tokenization-type`

[12] 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. `https://www.digital.go.jp/policies/trust`

[13] デジタル庁,「令和 7 年度　属性証明の課題整理に関する有識者会議　報告書」, 2026 年 4 月. `https://www.digital.go.jp/councils/vc-diw-governance`

[14] デジタル庁,「事務局説明資料」, 属性証明の課題整理に関する有識者会議（第 2 回）, 2026 年 2 月 26 日. `https://www.digital.go.jp/councils/vc-diw-governance`

[15] デジタル庁,「令和 7 年度　属性証明の課題整理に関する有識者会議　技術ワーキンググループ　議論の概要」, 2026 年 2 月 26 日.
https://www.digital.go.jp/councils/vc-diw-governance

[16] デジタル庁,「別紙 3　行政機関における VC・DIW の活用にあたる検討事項リスト（案)」, 令和 7 年度属性証明の課題整理に関する有識者会議報告書別紙, 2026 年 4 月.
https://www.digital.go.jp/councils/vc-diw-governance

[17] 総務省,「時刻認証業務の認定に関する規程」, 令和 3 年総務省告示第 146 号.
https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

[18] 総務省,「タイムスタンプについて」,
https://www.soumu.go.jp/main_sosiki/joho_tsusin/top/ninshou-law/timestamp.html

[19] 一般財団法人日本データ通信協会,「タイムビジネス信頼・安心認定制度について」, 総務省提出資料. https://www.soumu.go.jp/main_content/000679657.pdf

[20] Regulation (EU) No 910/2014 (eIDAS), Article 42 (Requirements for qualified electronic time stamps).

[21] ETSI EN 319 421, *Electronic Signatures and Trust Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.*

[22] 日本トラストテクノロジー協議会,「我が国のタイムスタンプサービスについて」.
https://www.soumu.go.jp/main_content/000603325.pdf

[23] 法務省,「公証制度について」, https://www.moj.go.jp/MINJI/minji30.html

[24] 松尾真一郎,「タイムスタンプの再発見と『いわゆるブロックチェーン』」.

[25] 松尾真一郎ほか,『ブロックチェーン技術の未解決問題』（該当箇所は崎村夏彦訳）.

[26] 松尾真一郎,「第 1 回コメントスクリプト」, 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 1 回, 2026 年 10 月 20 日.

[27] BGIN Cyber Security Working Group, discussions on Protection Profiles for cryptoasset wallets (work in progress).

[28] Ledger, “Ledger’s Response to the Hardware Implant Attack,” 2026 年 10 月 15 日.
https://www.ledger.com/blog-response-hardware-implant-attack

[29] B. Toulas, “Ledger confirms spy chip implant behind wallet crypto thefts,” BleepingComputer, 2026 年 10 月.

https://www.bleepingcomputer.com/news/security/ledger-confirms-hardware-wallet-spy-implant-behind-crypto-thefts/

[30] B. Toulas, “Ledger asks sellers across Asia to halt sales after supply-chain attack,” BleepingComputer, 2026 年 10 月 14 日. https://www.bleepingcomputer.com/news/security/ledger-asks-sellers-across-asia-to-halt-sales-after-supply-chain-attack/

[31] Bybit, “Bybit Security Incident: Timeline of Events and FAQs,” 2025 年 2 月. https://www.bybit.com/en/learn/this-week-in-bybit/bybit-security-incident-timeline

[32] Sygnia, “Sygnia’s Investigation into the Bybit Hack: What We Know So Far,” 2025 年. https://www.sygnia.co/blog/sygnia-investigation-bybit-hack/

[33] Safe Ecosystem Foundation, “February 28th, 2025: Statement by the Safe Ecosystem Foundation,” 2025 年 2 月 28 日. https://safefoundation.org/blog/safe-ecosystem-foundation-statement

[34] Federal Bureau of Investigation, “North Korea Responsible for $1.5 Billion Bybit Hack,” 2025 年 2 月. https://www.fbi.gov/investigate/cyber/alerts/2025/north-korea-responsible-for-1-5-billion-bybit-hack

[35] CertiK, “Bybit Incident Technical Analysis,” 2025 年 2 月. https://www.certik.com/blog/bybit-incident-technical-analysis

[36] Ledger, “Security Incident Report” (Ledger Connect Kit / npm), 2023 年 12 月 20 日. https://www.ledger.com/blog/security-incident-report

[37] T. Roche et al., “EUCLEAK,” IACR Cryptology ePrint Archive 2024/1380, 2024 年. https://eprint.iacr.org/2024/1380

[38] Yubico, “Security Advisory YSA-2024-03: Infineon ECDSA Private Key Recovery,” 2024 年 9 月 3 日. CVE-2024-45678. https://www.yubico.com/support/security-advisories/ysa-2024-03/

[39] CVE-2025-59703, Entrust nShield Connect XC / 5c / HSMi, 2025 年. https://github.com/advisories/ghsa-h78c-68qv-3qg9

[40] Wiz, “TraderTraitor: Deep Dive,” 2025 年. https://www.wiz.io/blog/north-korean-tradertraitor-crypto-heist

[41] T. Brewster, “How North Korean Hackers Pilfered $16 Million From A Crypto Exchange Via LinkedIn,” Forbes, 2024 年 12 月 4 日.

https://www.forbes.com/sites/thomasbrewster/2024/12/04/north-korean-hackers-stole-16-million-from-a-crypto-exchange-through-linkedin/

[42] W. Wu, A. Neumueller and C. Wang, “Funding Bitcoin’s Future: Paying for Security as the Block Subsidy Fades,” Cambridge Centre for Alternative Finance (CCAF), Cambridge Judge Business School, 2026 年. https://www.jbs.cam.ac.uk/faculty-research/centres/alternative-finance/publications/funding-bitcoins-future-paying-for-security-as-the-block-subsidy-fades/

[43] Cambridge Centre for Alternative Finance, “Cambridge Digital Mining Industry Report,” 2025 年 4 月. https://www.jbs.cam.ac.uk/wp-content/uploads/2025/04/2025-04-cambridge-digital-mining-industry-report.pdf

[44] L. Nuzzi, K. Waters and M. Andrade, “Breaking BFT: Quantifying the Cost to Attack Bitcoin and Ethereum,” SSRN, 2024 年 2 月 15 日. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4727999

[45] The DeFi Report, “Are ‘blob fees’ the only thing that matters long-term for Ethereum?,” https://thedefireport.io/research/blob-fees-ethereum

[46] Bitcoin.com News, “L2 Scaling Challenges May Undermine Ethereum and Bitcoin’s Long-Term Security,” 2024 年. https://news.bitcoin.com/l2-scaling-challenges-may-undermine-ethereum-and-bitcoins-long-term-security/

[47] CryptoSlate, “Ethereum’s hidden death spiral mechanic could freeze $800 billion in assets regardless of their safety rating,” https://cryptoslate.com/ethereums-hidden-death-spiral-mechanic-could-freeze-800-billion-in-assets-regardless-of-their-safety-rating/

[48] Documentation of August 2020 Ethereum Classic 51% attacks. https://meowsbits.github.io/51-percent-docs/

[49] N. De, “Ethereum Classic Labs Plans ‘Defensive Mining’ Strategy as Hashrate Plummets,” CoinDesk, 2020 年 8 月 21 日. https://www.coindesk.com/markets/2020/08/21/ethereum-classic-labs-plans-defensive-mining-strategy-as-hashrate-plummets

[50] Solana Foundation, “09-30-22 Solana Mainnet Beta Outage Report,” 2022 年. https://solana.com/news/09-30-22-solana-mainnet-beta-outage-report

[51] Solana Foundation, “02-06-24 Solana Mainnet Beta Outage Report,” 2024 年 2 月. https://solana.com/news/02-06-24-solana-mainnet-beta-outage-report

[52] EOS Sweden, announcement regarding end of block producer / public API operations, 2023 年 6 月. https://eossweden.org/

[53] A. Iwanicki, “Reasons for Public Blockchain Stagnation,” Onchain Economy Conference materials, 2025 年.

[54] “Hive Hard Fork is Successful, STEEM Crashes Back to Earth,” Investing.com, 2020 年 3 月 20 日. https://www.investing.com/news/cryptocurrency-news/hive-hard-fork-is-successful-steem-crashes-back-to-earth-2117369

[55] Wikipedia, “Terra (blockchain),” https://en.wikipedia.org/wiki/Terra_(blockchain)

[56] Unchained, “Why Many ‘Zombie Blockchains’ Still Have Market Caps in the Billions of Dollars,” 2024 年. https://unchainedcrypto.com/why-many-zombie-blockchains-are-still-worth-billions-of-dollars/

[57] JPYC 株式会社,「【国内初】日本円ステーブルコイン『JPYC』および発行・償還プラットフォーム『JPYC EX』を正式リリース」, 2025 年 10 月 24 日. https://prtimes.jp/main/html/rd/p/000000283.000054018.html

[58] SBI ホールディングスほか,「国内初の信託タイプ円建てステーブルコイン『JPYSC』の提供開始に関するお知らせ」, 2026 年 6 月 24 日. https://startale.com/ja/blog/jpysc-launch

[59] みずほ銀行・三菱 UFJ 銀行・三井住友銀行・三菱 UFJ 信託銀行・TISI,「複数銀行によるステーブルコイン共同発行およびクロスボーダー決済高度化に関する実証実験を実施」, 2026 年 10 月 16 日.

[60] Progmat, Inc. / Avalanche,「Progmat 基盤の Avalanche 連携完了について」（Project Keystone）, 2026 年 7 月 13 日. https://progmat.co.jp/

[61] DTCC, “DTCC Turns Tokenization into Reality,” 2026 年 7 月 15 日; SEC Staff No-Action Letter to DTC (Tokenization Services), 2025 年 12 月 11 日. https://www.dtcc.com/

[62] Broadridge, “Distributed Ledger Repo (DLR),” https://www.broadridge.com/capability/middle-and-back-office-solutions/post-trade-processing/distributed-ledger-repo-solutions