



日本の Web3 戦略： ID・Privacy・Wallet が握る競争優位

石川 大紀 (TOKI Founder)

ブロックチェーンの再定義：次世代金融 OS へ

ビットコインは 2009 年、イーサリアムは 2015 年にローンチされ、それぞれ 17 年、10 年が経過した。その間、パブリックチェーンの本質的な価値は、そのパーミッションレスな性質に強く見出されてきた。誰もが検証ネットワークに参加でき、誰もがスマートコントラクトをデプロイでき、誰もがアプリケーションを通じて暗号資産をやりとりできるという性質である。

この根幹を支えるのは、分散化されたネットワークと分散した結果を一意に収束させる合意形成アルゴリズム、そしてトランザクション実行環境がもたらす、「改ざん耐性」、「検閲耐性」、「単一障害点の排除」である。信頼できる中央主体を介さずとも安全性が担保される点は、既存の金融インフラには全く想定しえない大きなパラダイムシフトであった。

誕生以来、このパーミッションレスという性質を基盤としたエコシステムは、量的・質的に成長を続け、特にステーブルコイン・Defi 領域の発展は顕著である。ステーブルコインの年間移転総額は年間 12 兆ドルを超え、主要カードネットワークに匹敵、あるいはそれを上回る水準に達したとされている¹。また、DeFi の TVL (Total Value Locked、Defi プロトコルに預けられている暗号資産総額) も数百億ドル規模を維持・拡大し、2025 年には 1000 億ドル台に達したとする報道もある²。

更に近年では、伝統的金融機関や大手資産運用会社による活用事例も増加している。例えば、BlackRock のトークン化ファンド「BUIDL」、J.P. Morgan による Deposit Token のパブリックチェーン展開、Franklin Templeton のオンチェーンファンドなどは、パブリックチェーンが実証実験段階を終え、実務インフラとしての位置づけを強めている象徴的な事例である。

ここで改めて注目すべきは、彼らが評価しているのは、パーミッションレスなネットワーク・エコシステムという側面だけではないということだ。パーミッションレスな性質を維持する過程で長年かけて形成された標準規格や共通インフラ、様々な暗号技術、そして複数主体が同一の「共有状態」を保つ技術であり、これに基づくアプリケーションの高い相互接続性やプログラマビリティである。共有状態を介した直接的な相互作用は、従来の個別 API 接続を前提とする閉域型インフラに比べ、相互運用に伴う摩擦を大幅に低減しうる。

その結果、資産の担保化、市場流動性の統合、クロスボーダ決済、証券決済、プログラム可能な状態依存型の配当や利払いといった金融サービスが 24 時間 365 日、即時かつシームレスに連動する。決済と投資の垣根は徐々に曖昧になり、従来では想像もつかなかった高度な金融サービスの実装が可能になる。AI エージェントが金融取引の主体となる未来においては、その重要性はさらに上がるだろう。

ブロックチェーンは今、単なる「共有台帳」の域を超え、次世代の「金融 OS」としての側面を強めているのだ。そして、金融 OS としてのブロックチェーン上に展開されるエコシステムの発展を加速させる鍵となるのが、「コンプライアンス」と「プライバシー」および、それらを統合的に管理する「ウォレット」の進化である。

次世代金融の鍵は ID・Privacy・Wallet

今後のエコシステムの発展を左右する鍵は、「コンプライアンスを遵守するための ID」、「共有台帳でも実現可能な Privacy」、「コントローラーとしての Wallet」の進化にある。日本の Web3 戦略を考察するうえで最も重要なファクターであり、なぜこれらが鍵であるかを以下で解説する。

① ID：規制適合性のオンチェーン接続

ID とは単なる本人確認情報ではなく、

- 法人属性
- 投資家区分
- 居住地
- 制裁対象該当性
- 資格要件

といった規制・契約上の属性情報を検証可能な形でオンチェーンに接続する仕組みである。これらは、ERC-3643 などを中心に標準化が進んでおり、今後エコシステムとしての実装が期待されている。

ERC-3643 等の標準化により、Allowlist 参照型（アドレスが OK か NG かを示すリストを参照して実行を判断するもの）から、Identity Registry/Compliance モジュール等を用い、「属性に基づく移転制約」をトークン標準側で実装する設計へと進化しつつある。これは、コンプライアンスをトークンロジックに内在化する試みである。

この仕組みが確立されることで、「許可された主体のみが特定資産へアクセス可能」という統制が、共有状態上でも実装可能となる。閉域ネットワークに依存せず、プログラマビリティと規制適合性を両立できる点に構造的意義がある。

② Privacy：完全な秘匿性と制御可能性

実務上重要なのは、単なる匿名性ではない。求められるのは、「必要な主体に対して、必要な情報のみを開示できる制御可能な開示構造」である。

ゼロ知識証明等の暗号技術を活用することで、

- 第三者に対する秘匿性（匿名性・機密性・非リンカビリティ）の完全な確保
- 規制当局等に対する選択的開示
- 取引の検証可能性の維持

を同時に実現する設計が可能となる。

さらに重要なのは、プログラマビリティを損なわないことである。情報の秘匿技術はその特性上、実行可能なロジックや相互接続性に制約を生じさせる傾向がある。したがって、秘匿性を確保しながらも、共有状態上で高度な金融ロジックを実装できる構造を維持することが極めて重要となる。2025 年はプライバシーテックのグローバルな競争が本格的に始まった年であり、その技術革新や実装を巡る競争は加速している。

また、かつての Tornado Cash に代表されるような、追跡を拒絶することに集中するあまり選択的開示が不可能になってしまうような仕組みは、法的コンプライアンスの観点から実務への導入は困難である。次世代のデジタル金融インフラにおいては、プライバシーの保護と AML/CFT 等の規制要件への適応というトレードオフに陥りがちな機能要件を、高度な暗号技術によって統合的に解決するアプローチが不可欠である。

③ Wallet：金融 OS の統治レイヤー

Wallet はもはや単なる秘密鍵管理ツールではない。ID と Privacy を束ね、金融 OS 上での参加資格・実行権限・情報開示範囲を横断的に管理する「統治レイヤー」である。

トークンはオンチェーン上で最終的な実行可否を判定し、条件を満たさない場合には取引を拒否する。一方、Wallet は「誰が、どの属性で、どの条件のもとで実行するのか」を事前に統治する。すなわち、オンチェーンでの判断履行（Enforcement）と、サービス横断的な事前統治（Governance）を分離し、エコシステム全体のガバナンス構造を形成する役割を担う。

Wallet の統治機能は、主に以下の四層から構成される。

① ID・Claim 統治

オンチェーン ID および Claim（属性証明）の保持・更新・失効対応を担い、ID ネットワークや発行体と接続することで、属性に基づくアクセス制御を横断的に管理する。これにより、単一サービス単位ではなく、エコシステム全体で一貫した統治が可能となる。

② ポリシー適用と事前統制

ポリシーエンジンを内包し、トランザクションの事前審査、取引条件の制御、不正検知、監査ログ生成などを通じて内部統制を実装する。機関投資家や企業が求めるコンプライアンス要件は、この層で横断的に適用される。

③ 実行機能の統合

トークン管理、取引指示、スワップ、レンディング等の金融機能は、これらの統治条件のもとで実行される。Wallet は実行の起点であると同時に、統治された条件の下での実行を保証する。

④ 外部システム接続

ERP、貿易金融システム、給与支払い等の既存業務フローとの接続を担うことで、Wallet は既存金融システムとのインターフェースとなる。

重要なのは、Wallet が単なる UI や実行ツールではなく、ID ネットワーク、ポリシー、制度要件を横断的に統合する統治基盤である点である。企業は Wallet を通じて、複雑な基盤を意識することなく、統治された状態で共有状態経済圏に参加できる。

この統治レイヤーを握る主体こそが、次世代デジタル金融における構造的競争優位を確立する。

日本の Web3 戦略

本邦において、Web3 起点の金融プレイヤー層は依然として限定的である。しかし、今後の競争軸が「ID の標準化」、「Privacy 実装力」、「Wallet を軸としたエコシステム構築」に本格的に移る中で、後発である日本にも勝機はある。

日本の現状を展望すると、Web3 という新興マーケットで成長し力をつけた国外のインフラをまずは活用するという風潮が強い。ウォレット、オラクル、ブロックチェーン開発キットなど重要なインフラは全て国外で成長・発展してきたものが優先的に検討されている。企業の戦略としては当然の選択肢であり、まずはそこからスピーディにビジネスを立ち上げようとなるのは理解できる。

しかし、基盤ソフトウェアを国外に依存し、アプリケーション層のみを担う構造は、Web2 で繰り返されてきた構図である。次世代金融において同じ轍を踏まないためには、制御レイヤーの主導権を確保する視点が不可欠である。

日本には依然として十分な投資体力はある。既存金融と技術スタートアップの実装力を融合させ、グローバルなエコシステムに接続可能な ID・プライバシー・Wallet を開発・統合することで世界と戦っていくことができるかどうか、中長期での我々のポジションを左右する。

¹ リテール決済用のクレジットカードと直接比較できるものではないが、金額イメージを掴むことができる。

² <https://www.coindesk.com/business/2025/09/18/defi-tvl-rebounds-to-usd170b-erasing-terra-era-bear-market-losses>