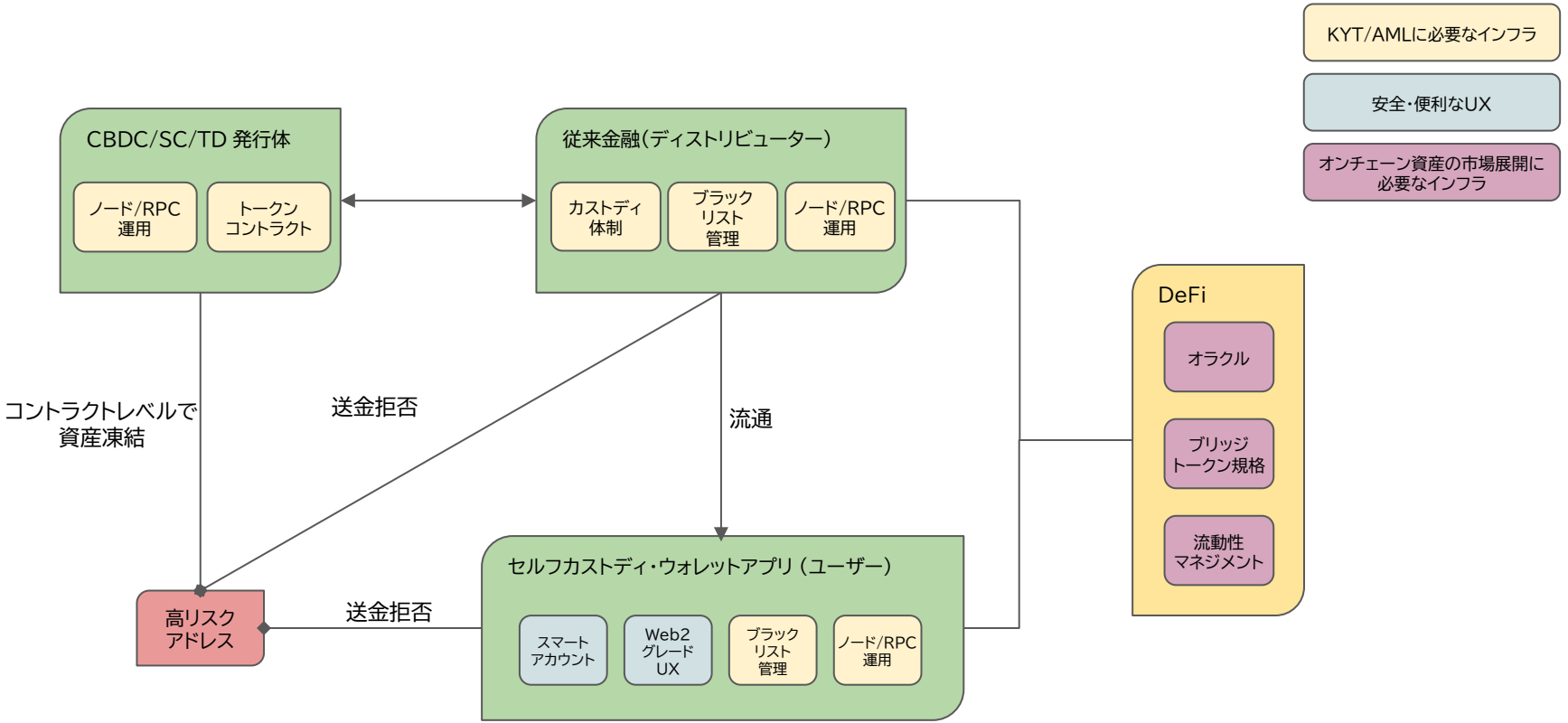
STARTALE

Web2とWeb3の垣根がない
信頼されるインターネットインフラ構築に向けて

CBDC/SC/TDをパーミッションレスブロックチェーンで展開する上で必要なインフラ



STARTALE Bringing Billions Onchain

Know-Your-Transaction（KYT）/ AML

高リスクアドレスに送金させない
高リスクコントラクトをコールさせない

トークンコントラクト	トークンをミント・バーンするスマートコントラクト自体に、コントラクトオーナーが任意のアドレス上のトークンを凍結できる機能を設ける。
ノード/RPC運用	各SPが送金tx等を実行する際、ブラックリストを参照して該当アドレスへの送金をプロトコルレベルでシャットアウトできる機能を設ける。 またUX側の必要に応じて、Readデータをインデックスしやすい形で取得できるようにする。
ブラックリスト管理	当局からの要請やOFAC制裁等に対応したブラックリストを管理（委託）し、コントラクト/RPC/エンドUIレベルでのフィルタリングに利用。
発行体	コントラクトレベルでの凍結権限の管理・行使。*マルチチェーン展開の徹底（Wrapped-to-native）*。 各トークンコントラクトのコード監査の徹底。
従来金融 ディストリビューター	ブラックリストの管理。高リスクアドレスへのディストリビューションの拒否。
ウォレットアプリ	同様の送金先制限に加え、必要に応じてオンチェーンデータを規制に準拠した形で取得・整形する （例：高リスクアドレスやコントラクトをエンドUIで非表示にする）。

セルフカストディ・ウォレットアプリ（エンドUI）

従来金融・Web2グレードの利便性とUX
Web3特有リスクの排除と喚起

スマート アカウント

スマートコントラクトウォレットを活用し、安全な資産管理とWeb2サービスに匹敵する利便性を実現。

Web2 グレード UX

- セキュアMPC
  - サービスの仕組みやセキュリティレベルやリカバリニーズに応じて柔軟にキーを生成・削除できる。
  - セットアップ例：各SSOのセッションキー、SP保管キー、ユーザーのクラウドバックアップキーでの2-of-3。
- Gas Abstraction
  - Gasのスポンサリングやネイティブトークン以外での支払い（例：ステーブルコイン）を可能にすることで、送金やスワップ等の利用手数料を細かく設定できる。
- Chain Abstraction
  - チェーンの垣根を意識させないUX（Unified Account）。ブリッジやスワップを必要に応じてバックグラウンドで実行。
- サブアカウント
  - 親アカウントに紐づき、利用アプリ毎に生成されるスマートアカウント。利用アプリ側にspend権限を託すことで、都度ユーザーapprovalを必要としないUXや、料金の引き落とし機能等を実装できる。
- DAppハブ
  - ウォレットアプリ内から特定dAppsへの誘導や、in-appで動くdAppフレームワークの活用およびSDKの提供。

パーミッションレスBC + Chain-abstraction文脈で必要なインフラ

インターオペラビリティ

トークン コントラクト

ノード/RPC 運用

トークン規格

トークン規格の選定または開発。考慮すべきポイントとして、

- ベースとなるメカニズムの処理速度が効率的で、
  各ブリッジレーン間の処理を実行するノードやリレーヤーの数と質の担保。
- 「KYT/AML」で言及した凍結機能等の効力がどの対応チェーン上でも及ぶこと。
- 対応チェーンの数が多く、新規チェーンへの対応が早いこと。
- 安全性が実証されているもの。十分なコード監査を受けているもの。オープンソース（ベース）のもの。

DeFi分野での有用性

オラクル

流動性 マネジメント

ブリッジ

核となるユースケースは、分散型金融市場へのアクセスである。そのために必要となるのが、

- 流動性プール（LP）。各SPのKYT/AMLポリシーの精査が必要かも検討する。
  - LPの仕様や、十分な参加者が集まっているかといった事項を鑑みた効率的な流動性マネジメントが必要。
- 複数のオープンマーケットを加味した価格オラクル。
  - 自発的なセットアップが必要。ユースケースに応じてプッシュ・プル・オフチェーンオラクルを使い分ける。
- ステーブルコインがクロスチェーンアセットとして機能するためには、多数のブリッジを幅広くカバーすべきである。
  - ネイティブ：大元となるチェーンやトークン規格に依存するブリッジ。
  - インテント：オンチェーンエージェント（ソルバーやフィラーなど）がP2Pオーダーマッチングを行うブリッジ。
  - リクイディティ：主にLPを介するブリッジ。

インフラサービス活用における注意点

Web3では、障害発生時の素早い原因特定に特有のナレッジが必要
リスクを網羅的に把握・最小化し、定期的な予行演習や監査をすべき

1. ベンダー依存によるオペレーションリスク
    - サービスの安定性
        - ノード/RPC運用
            - セキュリティの重要度に応じて、ベアメタルでのホスティングを検討。
            - 複数プロバイダ（クラウド上でのセルフホスト含む）の活用。
            - 地理的分散（ブリッジやウォレットの運用時）とバックアップ + バランサーの実装。
        - インデクサー（Web3 API）とWeb2 APIサービス
            - 活用を検討する際は、SLA指定の徹底や障害の原因を素早くキャッチするシステムが必要。
    - ビジネスのライフサイクル
        - 近年、より包括的なサービスを展開するベンダー（ウォレット等）に買収され
          サービスを停止するケースが多く見受けられる。

2. セキュリティリスク
    - 自社開発のものも含め、オンチェーンの部分は複数のセキュリティベンダーからコード監査を受ける、
      また受けているものを選ぶ。

ディスカッション

Web2とWeb3の垣根とは？
垣根をなくすにはどのような技術的アプローチが必要か？
規制面や性能面、利便性でどのようなトレードオフが考えられるか？

STARTALE