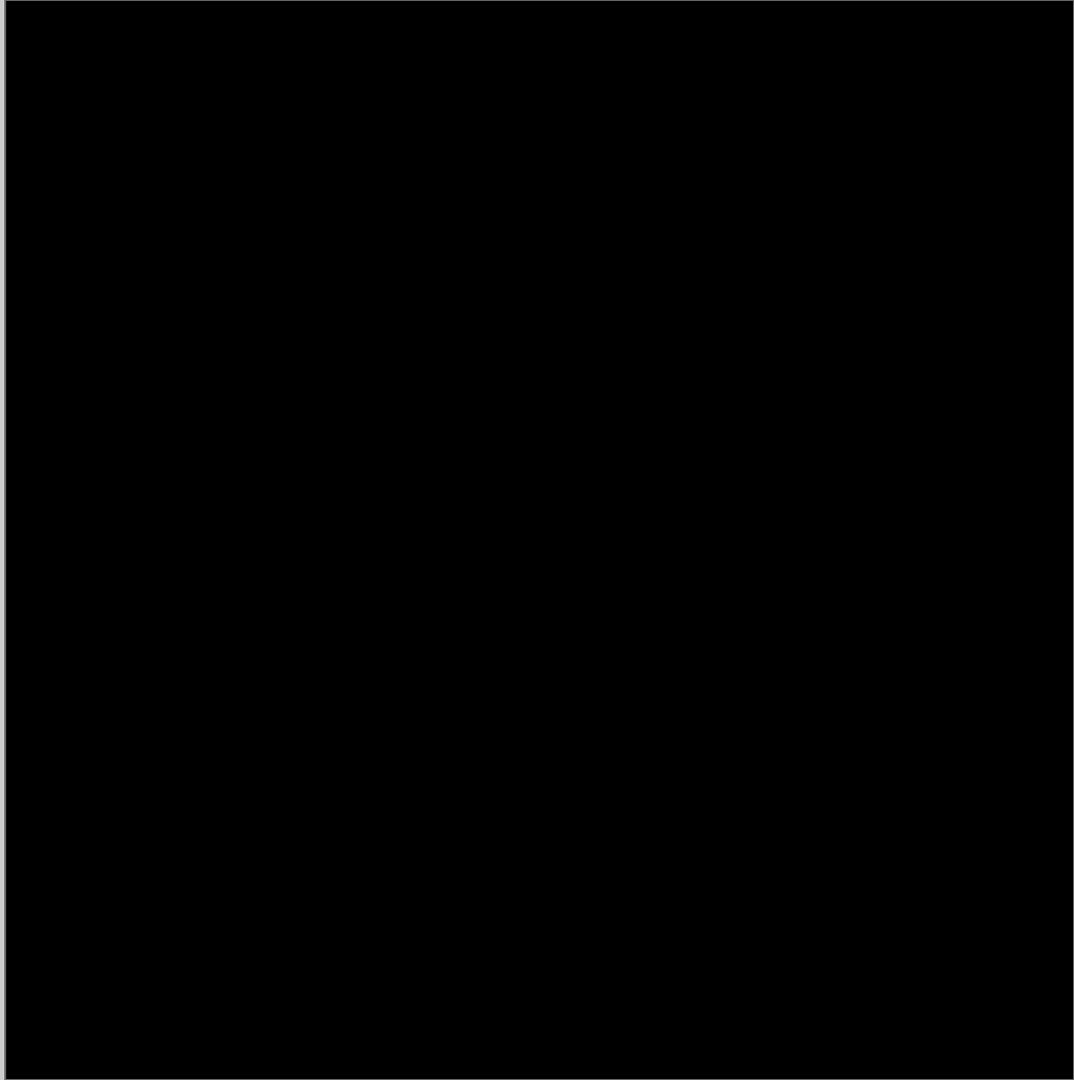

STARTALE
Web3 for Billions

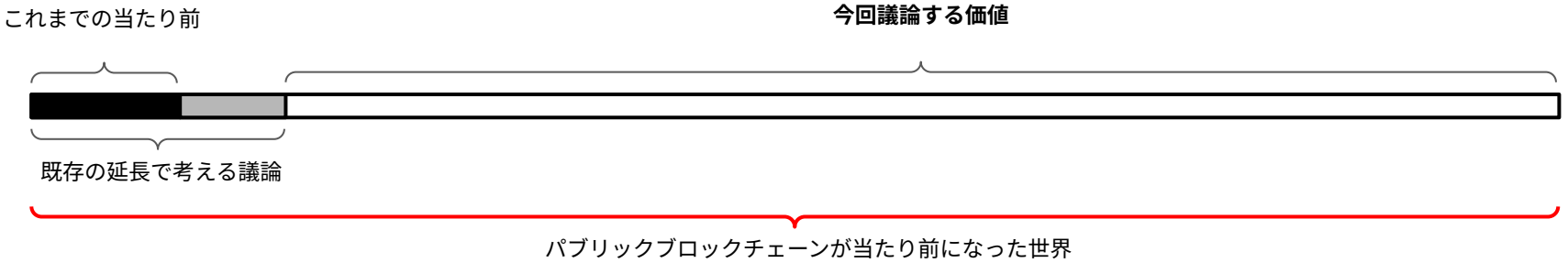
今回の趣旨



今回の発表でお伝えしたいこと

Startale Labs

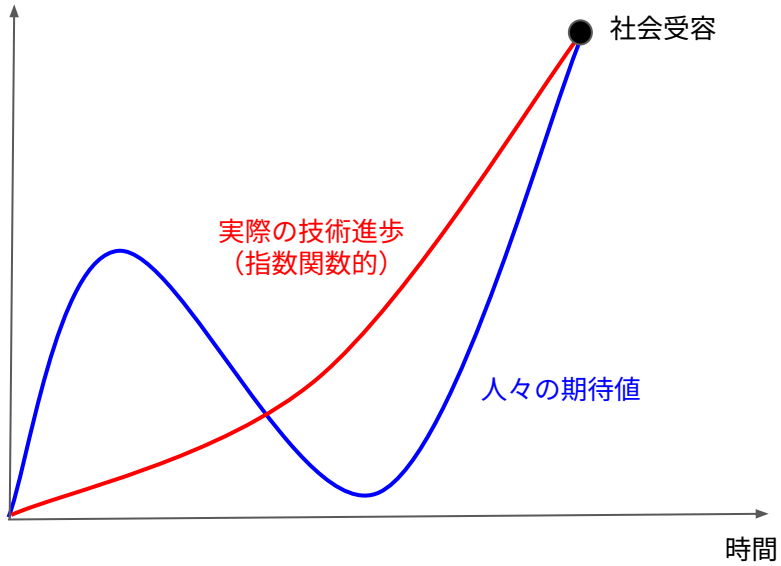
- 今回の発表はCBDCの発行をパブリックチェーン上で実施することを推奨するものではありません。
- 加速する技術革新の中で、20年、30年という単位で見据えた時に、あえて「これまでの当たり前」を良い意味で無視した議論をすることに大きな価値があるのではないか。
    - 30年前に、インターネットの上にここまで決済や証券市場、保険サービスなどが乗ってくることは「想定」されていなかった。
    - スマートフォンの普及でここまで決済のUXや金融アプリケーションが発展することは「想定」されていなかった。
- ブロックチェーンやAIなどの技術がより発展し日常生活で当たり前に使われるようになった世界でお金はどうあるべきかを考えることに意味があるのではないか。

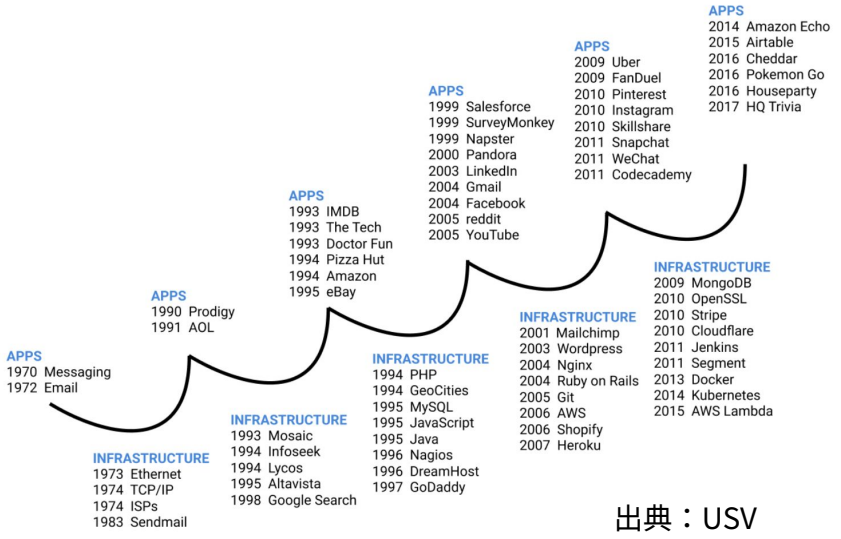


今回の発表でお伝えしたいこと

Startale Labs

- 新しい技術は往々にして最初は「おもちゃ」に見える。
- 実際の技術は指数関数的な進化だが、社会の期待は三次関数的な発展をたどる。そのため技術が過小評価されたり過大評価される。特に過小評価されている時に技術を正しく見積もるのは重要である。
- アプリがインフラを刺激し、インフラの成熟とともに新しいアプリが作られる。このサイクルで技術進化は進んでいる。（例：電球や飛行機、インターネットなど）





出典：USV

今回の発表でお伝えしたいこと

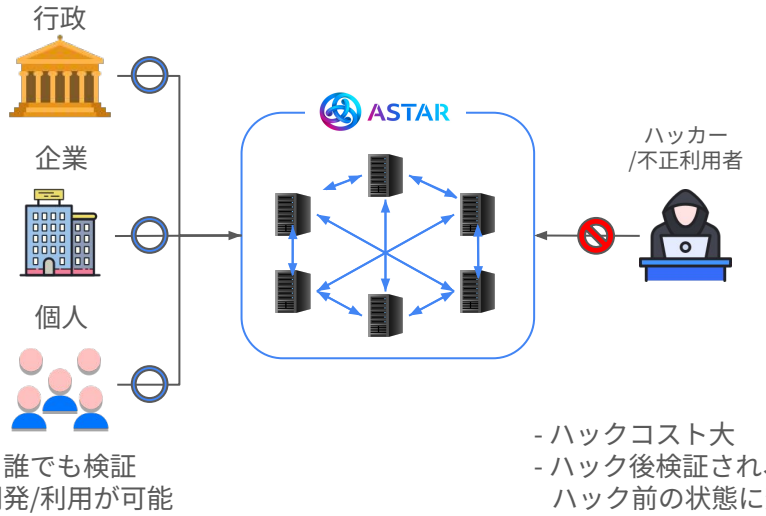
Startale Labs

- 新しい技術が出てきた時にその技術だからこそ可能になることが本質として残りビジネスの核となる。
  例：スマートフォン vs 電話。
- パブリックブロックチェーンの場合、比較対象は企業サーバーだが、サーバーに比べパブリックチェーンは 1) パーミッションレス 2) 検証可能性（透明性） 3) 不変性 (2重支払いの防止）などが考えられる。

GPS x App

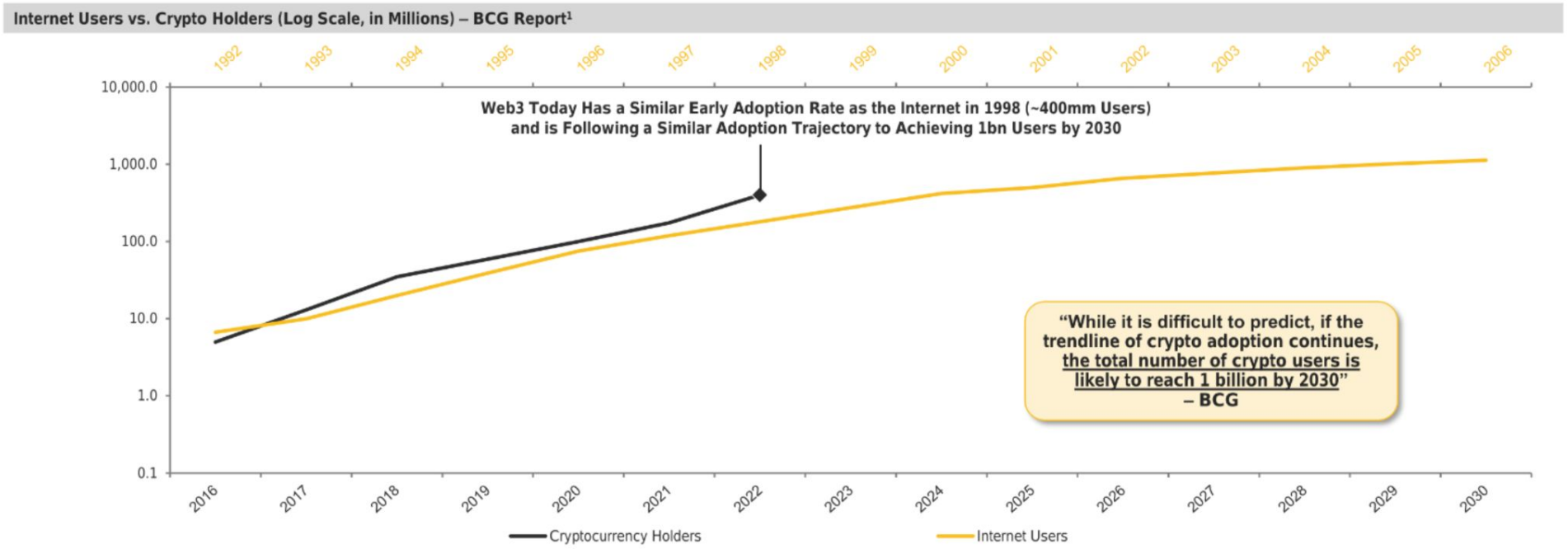
Photos x App

Uber



我々の現在地

2023年のWeb3ユーザー数はインターネットにおける1999年に相当する。
→ 今後5-6年で10億人のユーザー数を達成する。

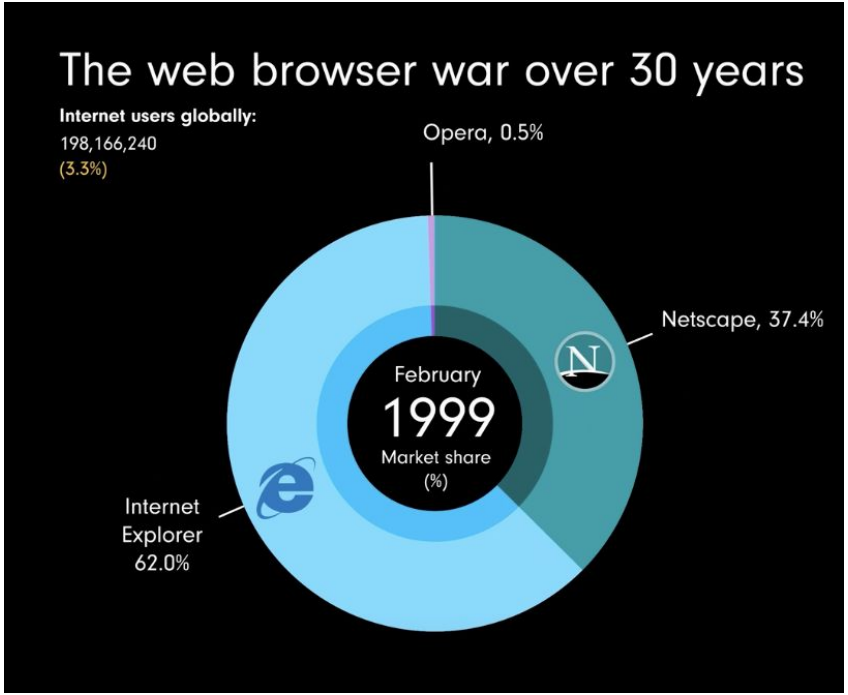


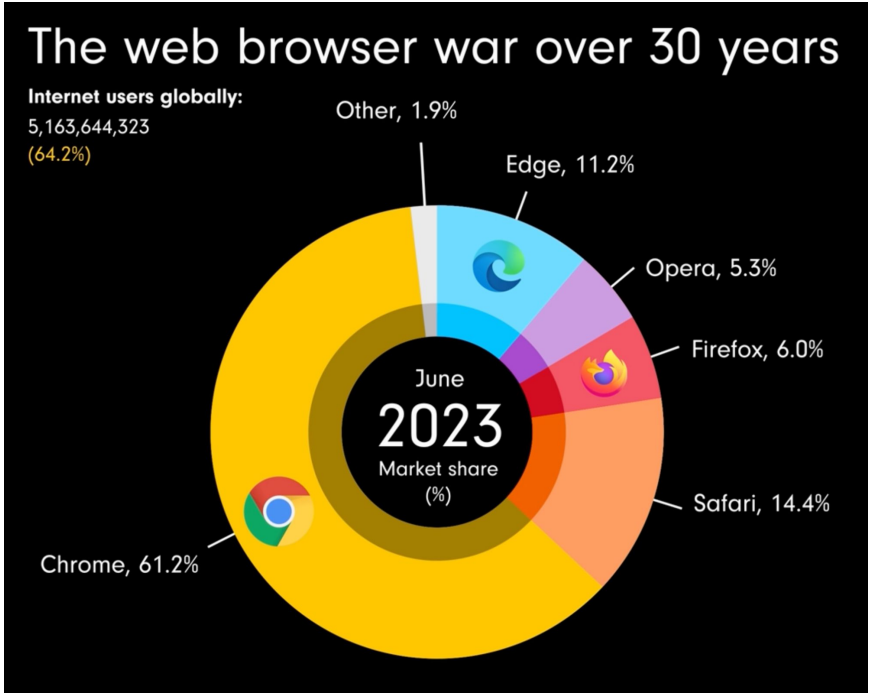
出典：ボストンコンサルティンググループ、CoinDesk

我々の現在地

Startale Labs

1999年のブラウザシェア率と2023年のブラウザシェア率
→ Web3も次の10-20年でさらなる技術革新の期待。メインプレイヤーはこれから生まれる。

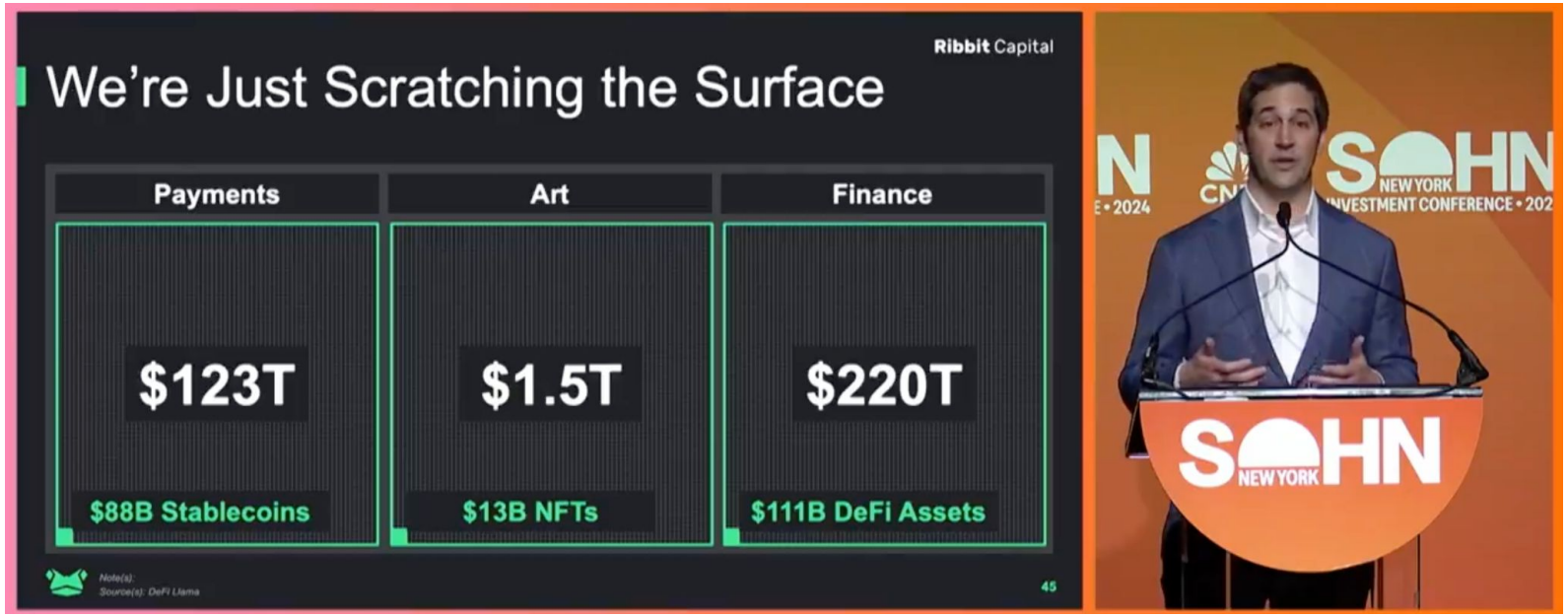




出典：EEAGLI

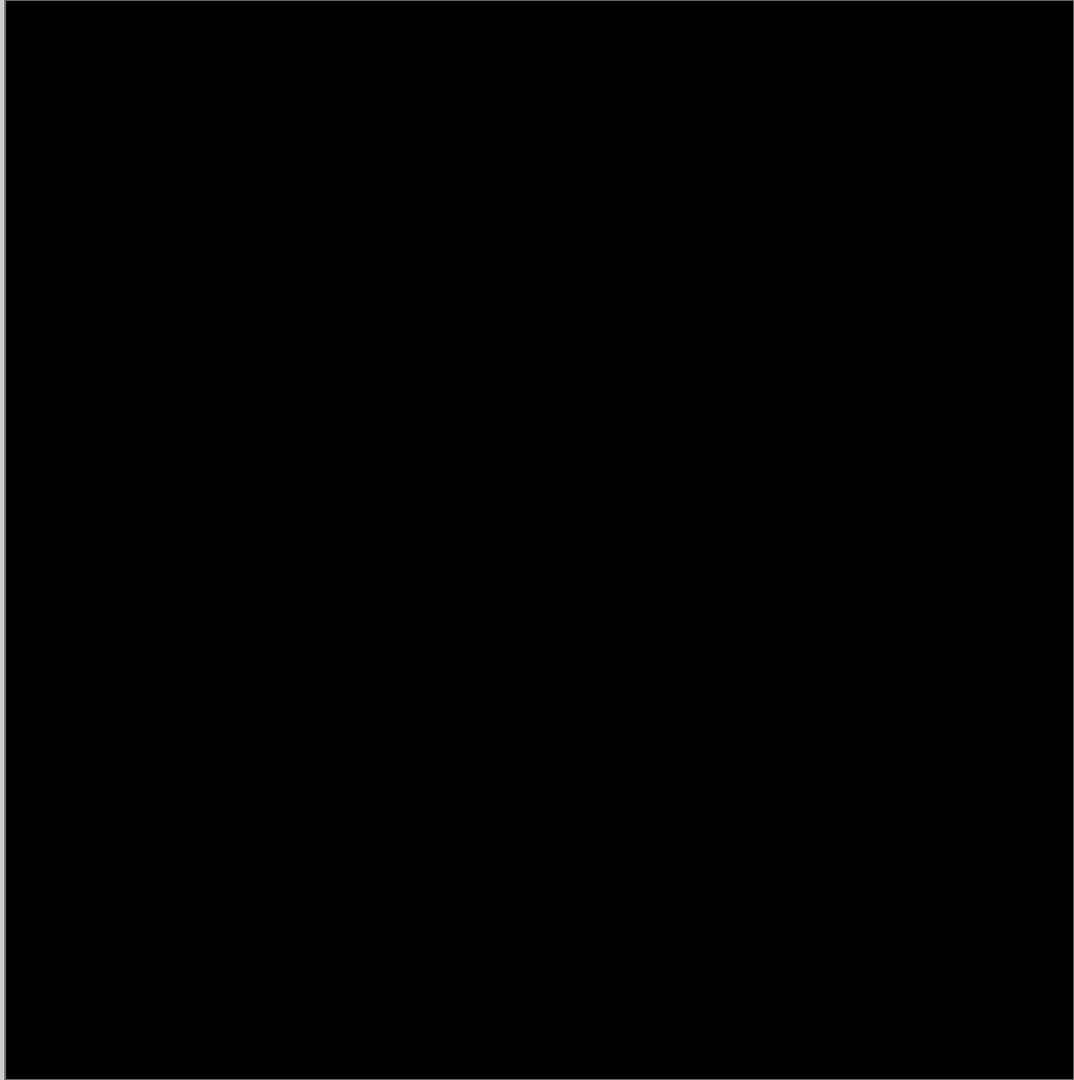
我々の現在地

いわゆるWeb3金融サービスを既存金融サービスと比較するとまだまだ黎明期に該当する。



出典：Ribbit Capital New York Investmenet Conference 2024

検討領域



ブロックチェーンの種類

Startale Labs

- ブロックチェーンの種類には大きく分けて３つあり、それぞれ異なる特徴を持つ。重要なのは「パーミッションレス」かどうか。
- StartaleはパブリックブロックチェーンのDevelopmentをしているため、パブリックチェーンを前提としたCBDCについて説明をする。

項目	パブリックチェーン	コンソーシアムチェーン	プライベートチェーン
ネットワーク検証者・参加者	誰でも参加が可能	複数の特定された機関・企業・団体・個人のみ参加可能	単一の機関・企業・団体・個人のみ検証可能
プライバシー	Txデータは公開され、誰でも確認可能	参加する組織間で情報が共有されるが、外部には公開されないことが多い	データをプライベートで管理し、特定の利害関係者のみがアクセス可能
セキュリティ	ノードが分散され、データの改ざんが難しい	パブリックチェーンとプライベートチェーンの間	ノードが分散されていないため、改ざんが比較的容易
スケーラビリティ	トランザクションの承認するための合意形成に時間がかかるため、低い	トランザクションの承認するための合意形成が短時間で済むため、高い	

検討事項

Startale Labs

CBDCをパブリックブロックチェーン上で発行する場合、少なくても以下の主要論点を考慮する必要があるのではないか。（既存のブロックチェーン運営にかかる主要論点を基に抽出した）

論点	詳細	課題	解決の方向性
トランザクションの処理性能 (TPS/スケーラビリティ)	大量のトランザクションの処理が可能なのか	大量のトランザクション量を処理することができるようにする	下位レイヤーのチェーンを作成
プライバシー	ユーザーのトランザクション履歴等が確認できてしまう	ユーザー情報とトランザクション情報が紐付けされないされないようにする	ゼロ知識証明など
セキュリティ	不正なトランザクションやハッキングが起きる可能性がある	ハッキングがされにくい仕組みを作る	バリデータの分散化 コンセンサスアルゴリズム改善
障害体制	サーバーがダウンした時のCBDCの運用はどうなるか	サーバーがダウンしてもCBDCの運用が止まらない仕組みを作る	バリデーター・ノードの分散化
分散性	パブリックチェーンのため、チェーンの所有者・意思決定者はどうなるか	ネットワーク自体のガバナンスを日銀主導で、管理できるようにする	オンチェーン、オフチェーンの使い分け
ユーザーエクスペリエンス	ユーザーにとってわかりづらく、使いづらい仕様になっている	Web2同様もしくは近しいユーザーエクスペリエンスの提供をする	Account Abstractionなど
インターオペラビリティ (相互運用性)	他のチェーンでのアセットの利用ができない or 難しい	他のチェーンでもCBDCが利用されるようにする	CCIP, CCTPなど

スケーラビリティ

- パブリックブロックチェーンは前提として、分散性、スケーラビリティ、セキュリティにトレードオフが存在している。（パブリックブロックチェーンのトリレンマ）
- このトリレンマの中でスケーラビリティに特化したSolanaのようなAlt L1や分散性を重視したEthereum L1などが複数のブロックチェーンが存在している。
- 現在最大のスマートコントラクトL1であるEthereumではL2の開発が進んでおり一定のスケーラビリティの改善が見られるが、現状CBDCに求められる水準 (10万TPS)には至っていない (理論値では1万TPSを超えるものもある)。

各チェーンのスケーラビリティの比較表

レイヤー	**L1**		**L2**			
ブロックチェーン	**Ethereum**	**Solana**	**Optimism**	**Arbitrum**	**Polygon zkEVM**	**Astar zkEVM**
実測TPS **(1秒あたりのTX処理数)**	13.60	339.10	6.50	20.30	0.20	1
平均手数料 per TX	$2.403	$0.018	$0.067	$0.007	$0.138	$0.018

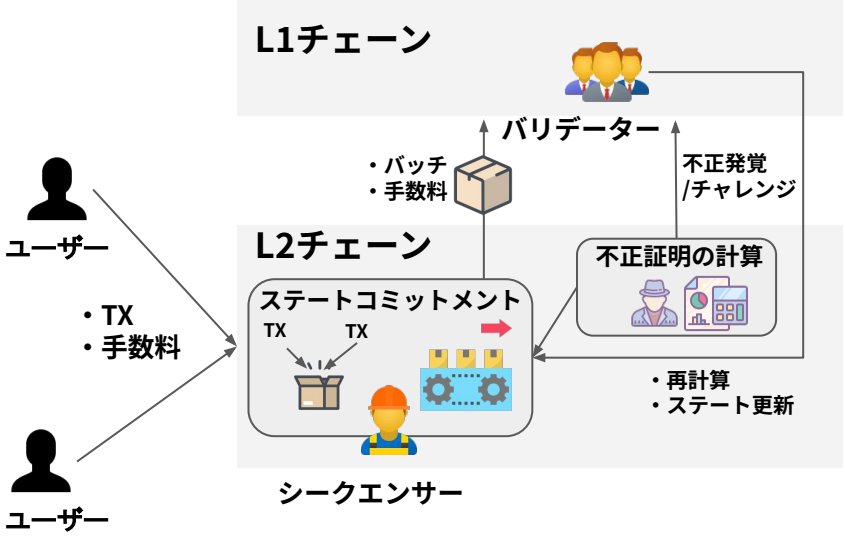
※2024/05/06時点の実測値データ from Dune (TPSと**平均手数料 per TXは日々変動**)
※参考までに、Avalancheは実測値で3.5TPS（C-chain）as of 15th Apr.

スケーラビリティ

- 今回はEthereum L2で使用することを想定する。
- Ethereum L2では大きく分けてOptimistice RollupsとZk Rollups が存在する。

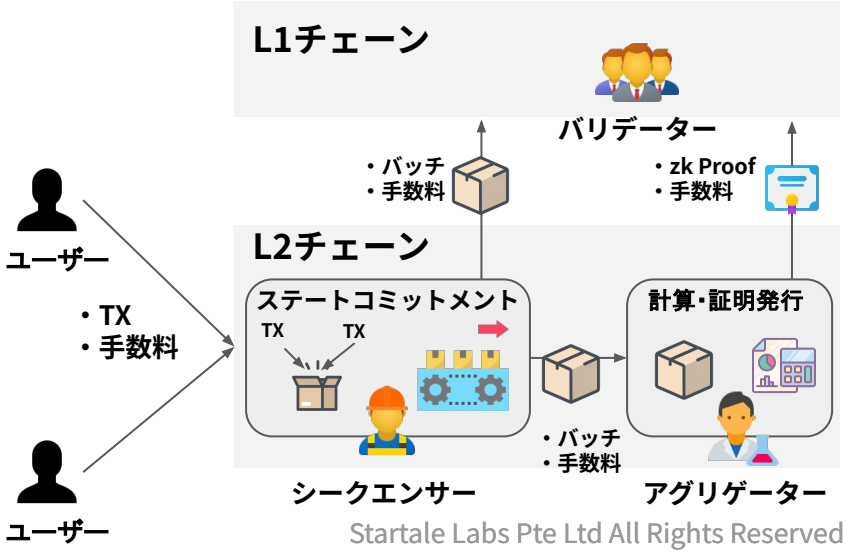
Optimistic Rollups

Optimistic Rollupsではシークエンサーが複数のTXをバッチし、それをL1へと送信する。送信された後、一定期間TXに対するチャレンジ期間を設け、その間にTXに対する異議申し立てがない場合、TXが正しいとして承認される。



zk Rollups

zk Rollupsではシークエンサーが複数のTXをバッチし、それをL1へと送信し、アグリゲーターがプルーバーを介してTX共有することなしに、L1へTXの正当性を証明する。



スケーラビリティ

Startale Labs

- Ethereum L2では大きく分けてOptimistic RollupsとZk Rollupsが存在する。

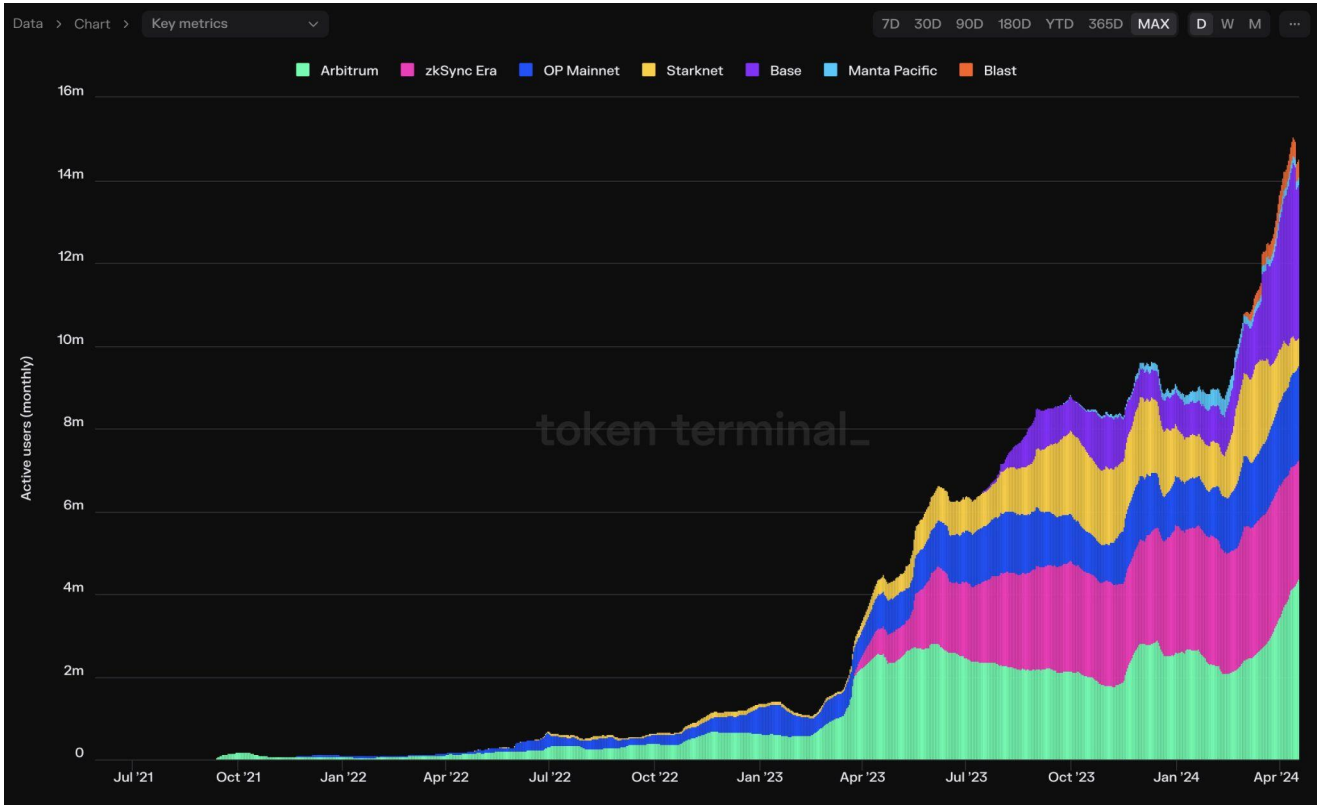
比較表

項目	Optimistic Rollups	zk Rollups
理論値: 最大TPS	✖ 500	○ 2,000
シークエンスあたりのガスコスト	○ ~40,000	✖ ~500,000
収益	○ 計算式や変数、報酬量はチェーン側で設定可能	△ 計算式や変数、報酬量はチェーン側で設定可能
ファイナリティー	✖ 7日間	○ 数分以内
セキュリティー	✖ Froud Proofにより能動的なチャレンジがないとTXが検証されない	○ Zk Proofにより全てのTXが毎回検証される
成熟度	○ Optimism, Arbitrum, Base等の有名なチェーンで利用されている	○ Polygon, ZkSync Era, Astar等の有名なチェーンで利用されている
EVM互換性	○ 高い (同じEVMを使用)	○ ZK EVMであれば互換性高い

スケーラビリティ

Startale Labs

- 現在、Ethereum L2の月間アクティブユーザーは合計1500万人ほど。



出典：Token Terminal

- EIP4844以降L2の手数料は$0.01-$0.1ほどに低下している。

Layer-2 average transaction fees – March 14 | Source: Dune

出典：Dune

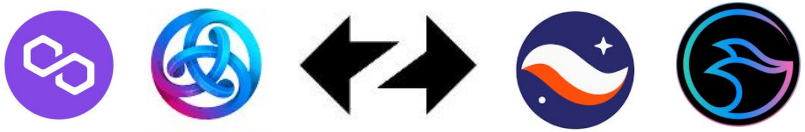
- 巷で言われる批判：ブロックチェーンにはプライバシーがない。
- ゼロ知識証明（ZKP）が注目を集めているが、CBDC運用においてプライバシーをどこまで求めるかは要検討

ゼロ知識証明とは

公開できる情報と秘密にしたい情報に対して、ある者が確かに秘密情報を持っていることを、秘密情報自体を相手に開示することなく証明をする。

例：お酒を買う時に、相手に年齢、名前などを開示せずに、確かに20才以上であることを証明する。

現在ブロックチェーン界隈で盛んに研究開発とアプリケーションの開発が行われている。



パブリックチェーン上でできるようになること

- パブリックブロックチェーンでは全ての情報が公開されると認識されがちだが、取引の正当性を参加者全員で合意することをデータの秘匿性を保ったまま可能にする。
- AMLやKYC、GDPRなどにかかる情報取得がよりプログラマブルになる。
    - プログラマブル・プライバシー
- スマートコントラクトの特定ロジックの秘匿化（ビジネスロジックの機密性を保ちつつスマートコントラクトの条件が適切に実行されていることを保証する）
- 従来はプライバシーの懸念から実現が困難であったアプリが可能になる。例えば、投票や個人情報確認など。
- ZKPはプライバシーだけではなく、スケーラビリティやインターオペラビリティにも有力。

- Zkを用いたチェーン基盤にはzk SyncやAstar zkEVMなどがあるが、現状スケーリング耐性が十分ではなく実際の社会受容を満たすことは困難である。

Name	Send ETH	Swap tokens
Boba Network	< $0.01	< $0.01
Optimism	< $0.01	< $0.01
Arbitrum One	< $0.01	< $0.01
zkSync Era	< $0.01	-
Polygon zkEVM	< $0.01	$0.10
Loopring	$0.01	$0.78
zkSync Lite	$0.02	$0.04
Metis Network	$0.02	$0.10
DeGate	$0.04	$0.17
Ethereum	$0.92	$4.61

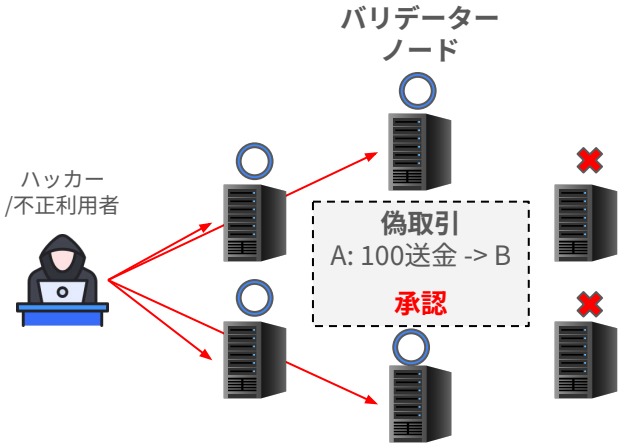
#	NAME	PAST DAY TPS
1	Base	28.08
2	Degen Chain	25.15
3	Arbitrum One	15.05
4	Ethereum	13.46
5	zkSync Era	9.88
6	Blast	8.05
7	OP Mainnet	5.52
8	Scroll	4.74
9	Mantle	3.91

セキュリティ・障害体制

Startale Labs

- ブロックチェーンは改ざんが不可能なのではなく、改ざんが現実的に極めて困難である仕組みである。
- 低い分散性、暗号化技術の脆弱性、コンセンサスアルゴリズムの脆弱性、ネットワーク攻撃への脆弱性（51%攻撃、Sybil攻撃、ダブルスペンディング攻撃など）、スマートコントラクトの脆弱性などが考えられる。
- 一方で、Bitcoinをはじめ、誰でも24時間365日アクセス可能なシステムが過去にダウンタイム0かつブロックチェーン自体の改ざんがされていないのは驚くべきことである。

51%攻撃の事例



コンセンサスアルゴリズム

例	説明
PoW	複雑な数学問題に取り組み、最初に問題の解を見つけたマイナーが新しいブロックを生成する
PoS	バリデータはトークンの保有量に応じて選ばれ、ブロックを生成する
PoA	特定の信頼できるノードがトランザクションを承認し、ブロックを生成する
DPoS	トークンホルダーが確率によって限られた数の「代表者」を選出し、代表者がトランザクションを承認し、新しいブロックを生成する

分散性（ガバナンス）

Startale Labs

- パブリックブロックチェーン上のCBDCでは、ガバナンスの問題が重要になる。
- ブロックチェーンのプロトコル変更やハードフォーク、アップグレードをどのように意思決定するか、ステークホルダー間の利害対立をどのように調整するかなど、様々なガバナンス上の課題を意思決定をし実行する必要がある。
- CBDCのガバナンスにおける中央銀行の役割や、国際的な協調も検討する必要がある。

ブロックチェーンにおけるガバナンスの種類

項目	オンチェーンガバナンス	オフチェーンガバナンス
ガバナンス参加者	トークン保有者	トークン保有に限らず、設定可能
決定プロセス	ブロックチェーン上での投票	ブロックチェーン外での提案・議論・投票で決定
投票権	トークン保有量に基づく	トークン保有量に限らず、設定可能
透明性	ブロックチェーン上に記録されるため、透明性が高い	ブロックチェーン上への記録が求められない
分散性	トークン保有者による意思決定のため、分散性が比較的高いとされている	限られた参加者によって意思決定がされるため、分散性が低い

ユーザーエクスペリエンス

Startale Labs

- 巷で言われる批判：ブロックチェーンはUXが良くない。
- Account AbstructionやChain Abstructionなどの技術が登場している。

UXが良くない具体例

- 秘密鍵・シードフレーズの管理 (無くすと資産が永遠に引き出せない)
- Walletに十分なネイティブトークンがないとトランザクションが起こせない
- 間違ったアドレスに送金をしてしまう
- 毎回のトランザクションの際に手数料の支払いと署名をしなければならない
- チェーンごとにユースケースが異なり、チェーンごとにアカウントを作成する必要がある
- ユースケースごとに指定のトークンを保有していないと利用できない
- etc

Account Abstraction

ユーザーアカウントとコントラクトアカウントの差異を抽象化(Abstraction)し、UXを向上させる。

これまでは、Externally Owned Account (EOA)と呼ばれる外部所有アカウントが秘密鍵を使用してTxを作成する。AAを用いるとスマートコントラクト自体がTxを認証する役割を果たすのでマルチシグやソーシャルリカバリーなど様々なロジックを容易に組み込むことができる。

また、スマートコントラクトは秘密鍵がないので、ユーザーが単一で鍵を管理する必要がない。

Chain Abstraction

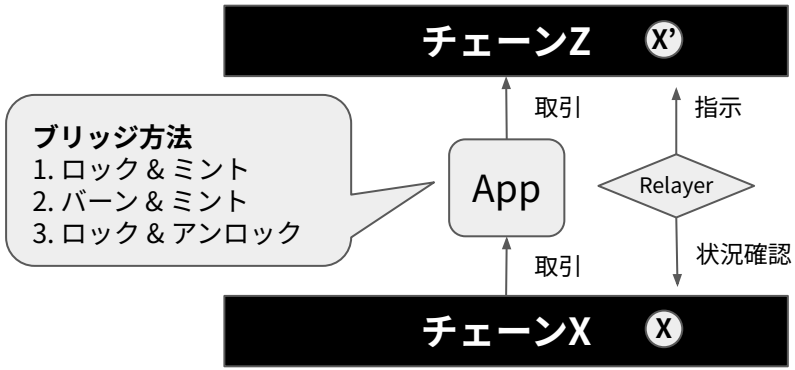
チェーン自体の差異を抽象化(Abstraction)し、UXを向上させる。

ユーザは複数のブロックチェーンを使っていることを認識せずに、自身の持つアセットとユースケースに関わらず、一つのアカウントからブロックチェーンを切り替えることなく、トランザクションを起こすことができる。

インターオペラビリティ

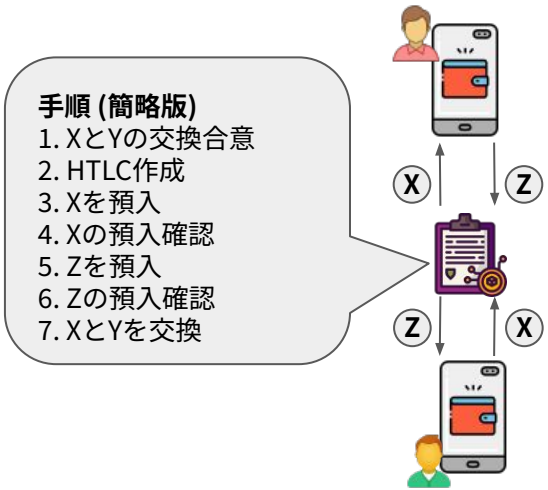
- CBDCが広く普及するためには、他のブロックチェーンやデジタル通貨との相互運用性が重要。
- 異なるブロックチェーン間でCBDCを円滑に移動できるようにすることで、利便性が向上し、ネットワーク効果を高めることができる。
- ブロックチェーンブリッジやアトミックスワップなどの技術を活用し、インターオペラビリティを確保する必要がある。

クロスチェーンブリッジ概略図



※ロック　　：トークンをスマートコントラクトに預入をし、流通しないようにする
※アンロック: スマートコントラクトに預入されたトークンを引き出す
※ミント　　：トークンもしくはトークンの債権を発行する
※バーン　　：トークンを出金ができないアドレスに預入、永久に出金できないようにする

アトミックスワップ概略図



第三者を介さない、
Peer to Peerの取引が可能

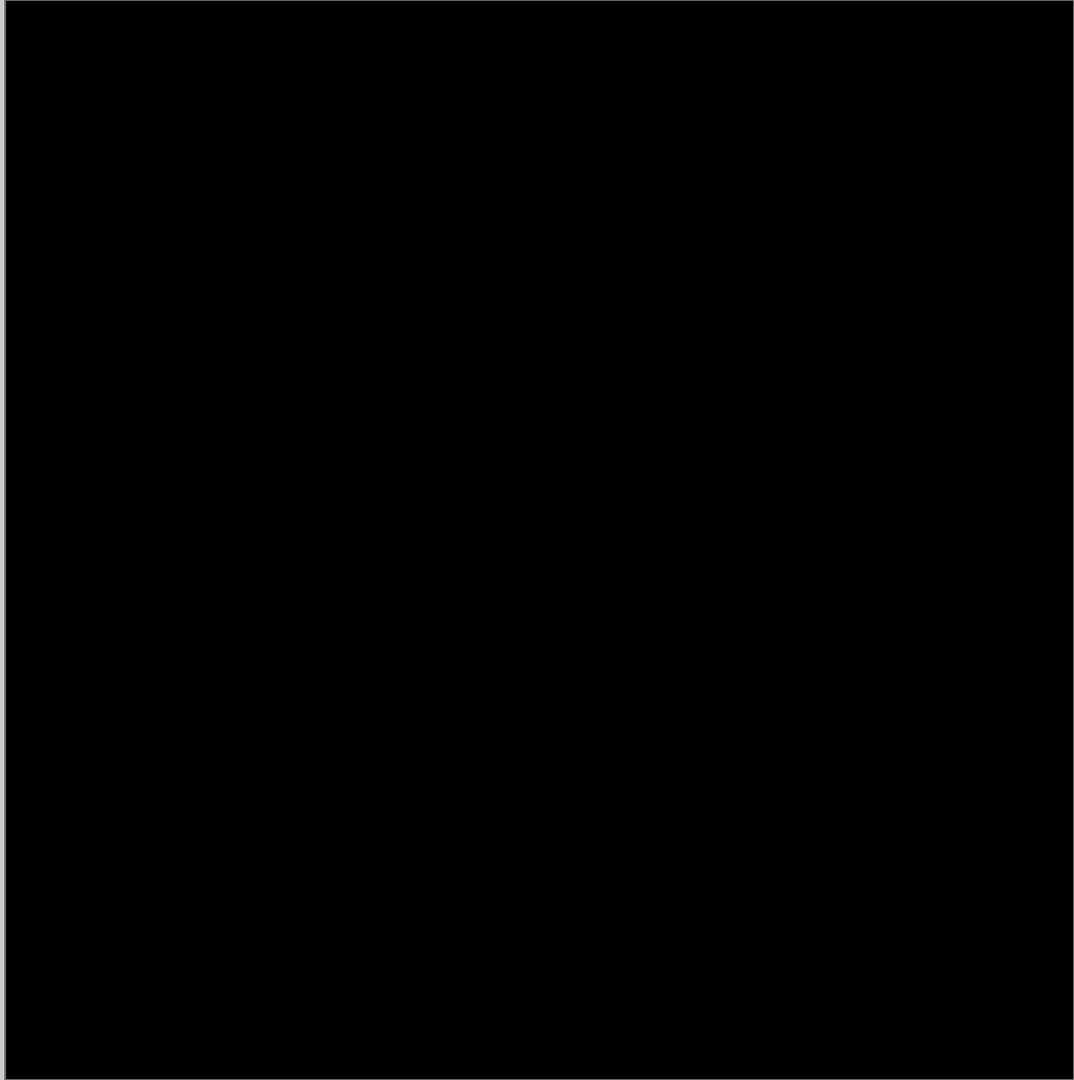
パブリックブロックチェーンにおけるCBDC

Startale Labs

- 現在のパブリックチェーンとパブリックチェーン上でのCBDCの発行はスケーラビリティ観点において、難しいことが想定される。

論点	課題	解決の方向性	評価
トランザクションの処理性能 (TPS/スケーラビリティ)	大量のトランザクション量を処理することができるようにする	下位レイヤーのチェーンを作成	✖ L2施策では、必要とされるTPSを満たすことができない
プライバシー	ユーザー情報とトランザクション情報が紐付けされないされないようにする	ゼロ知識証明など	○ CBDCで活用可能
セキュリティ	ハッキングがされにくい仕組みを作る	バリデータの分散化 コンセンサスアルゴリズム改善	○ CBDCで活用可能
障害体制	サーバーがダウンしてもCBDCの運用が止まらない仕組みを作る	バリデーター・ノードの分散化	○ CBDCで活用可能
分散性	ネットワーク自体のガバナンスを日銀主導で、管理できるようにする	オンチェーン、オフチェーンの使い分け	△ ガバナンスで決まったことが受け入れられない場合にハードフォークの可能性がある
ユーザーエクスペリエンス	Web2同様もしくは近しいユーザーエクスペリエンスの提供をする	Account Abstractionなど	○ CBDCで活用可能
インターオペラビリティ (相互運用性)	他のチェーンでもCBDCが利用されるようにする	CCIP, CCTPなど	○ CBDCで活用可能

いただきたいフィードバック



論点

Startale Labs

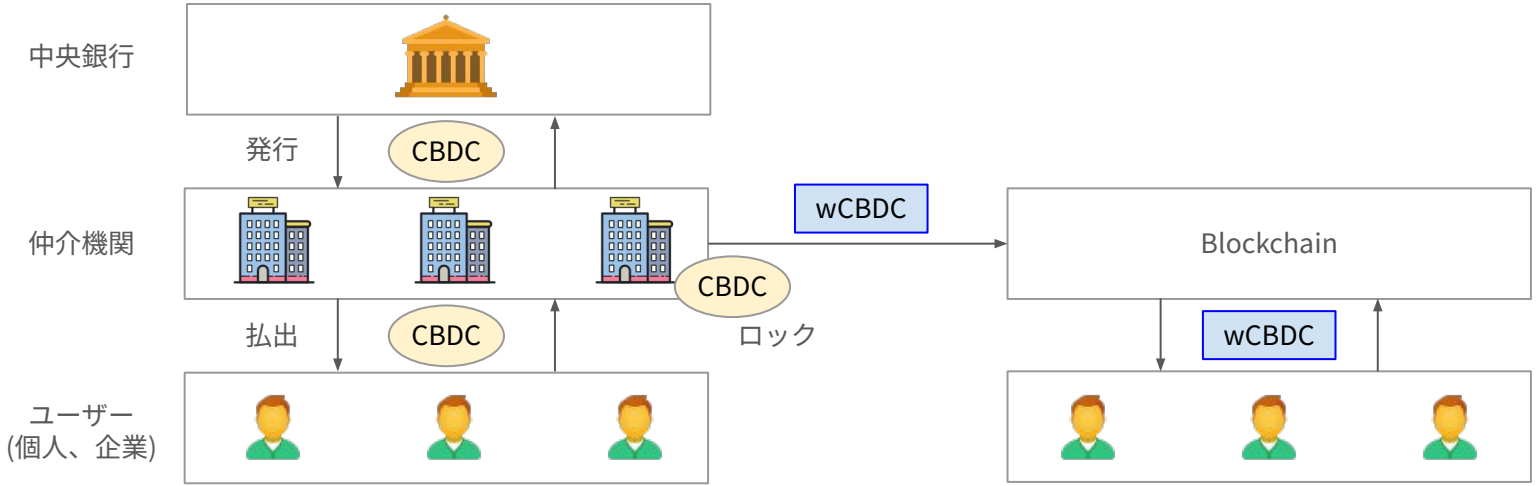
- 上記検討項目以外にどのような主要検討項目が考えられるか？

ブロックチェーンとCBDCの未来（完全に私見）

パブリックチェーンの活用路線

Startale Labs

- パブリックチェーン上に直接CBDCを発行することのハードルは高い。
- CBDCプラットフォームで発行されたCBDCをロックし、wCBDC（wapped CBDC）としてパブリックチェーン上に発行することは考えられるが、実態としての動きについては要検討

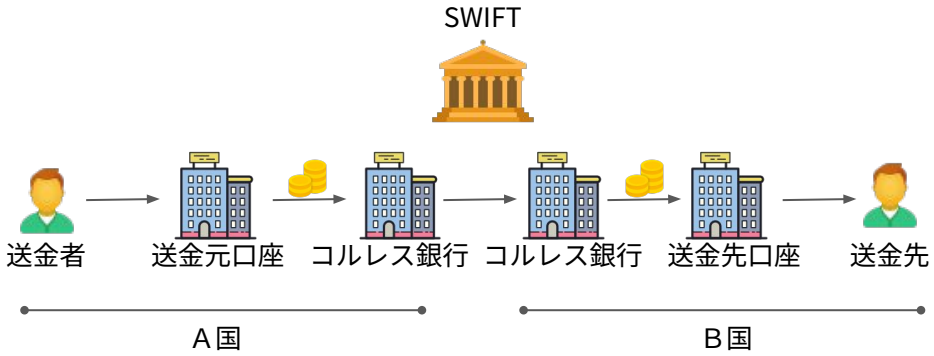


・CBDCは従来式またはPrivateブロックチェーンで発行されることを想定
・中銀がCBDC発行・償還を担い、仲介機関経由でCBDCがロックされwCBDCを発行
・wCBDCの移転制御のために、ウォレットやスマコンのホワイトリスト登録が考えられる

国際送金の革新

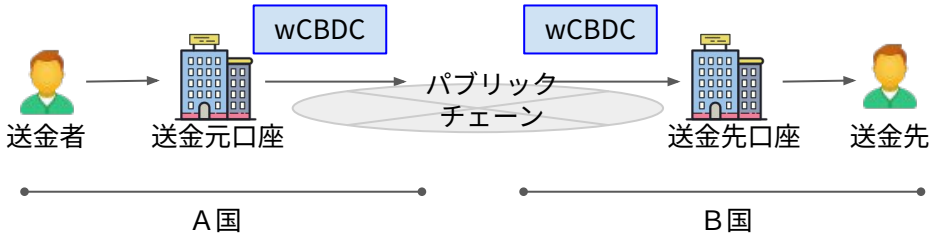
- CBDCがブロックチェーン上で流通することで、国際送金が簡素化される。
- 現在の国際送金は、コルレス銀行を経由するため、時間とコストがかかる。
- ブロックチェーンを活用したホールセールCBDCでは、24時間365日リアルタイムで送金が可能となり、送金手数料も削減されうる。

現状



- 決済機関を複数経由するために手数料とリードタイムがかかる

BC活用



- ブロックチェーンを活用することで中間機関を削減しDvPを実現
- パブリックチェーンの場合は送金者国でwCBDCを発行し送金先に着金（FXが混ざる場合はAMMの仕組み等が必要）

プログラマブルマネーの実現と透明性向上

Startale Labs

- CBDCがブロックチェーン上で流通されることで、プログラマブルマネーが実現する。
- プログラマブルマネーとは、スマートコントラクトなどによって自動的に実行される資金の流れを指す。
- 例えば、人の手を介さず特定の条件が満たされた場合にのみ支払いが実行されるなど、柔軟な資金管理が24時間可能になる。
- これにより、エスクローサービスや複雑な金融取引の自動化が実現し、効率性と透明性が向上する。

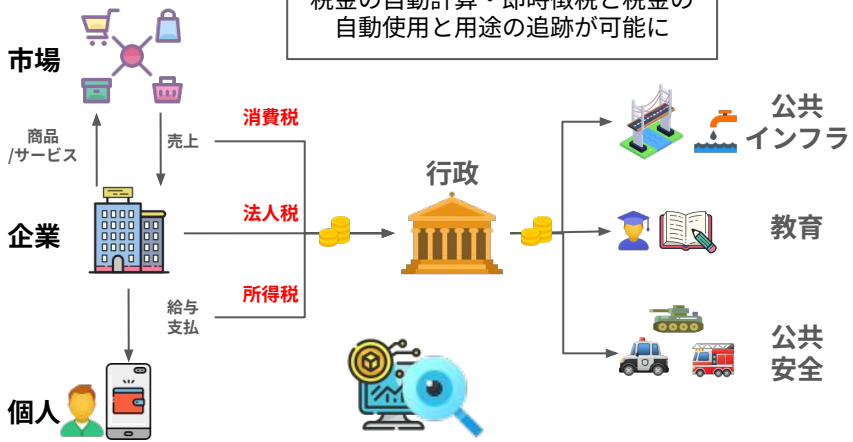
個人での金融サービス提供概略図

第三者を介さず、自動で借り手の残高から
スマートコントラクトで定義された条件に従って、
貸し手に返済が可能に

スマートコントラクトでの条件例
返済期間: 30日
利息率: 10%
ペナルティ: 毎日0.1%増加

計算・徴税の自動化と使用用途の追跡概略図

税金の自動計算・即時徴税と税金の
自動使用と用途の追跡が可能に



トークン経済の発展

Startale Labs

- CBDCがブロックチェーン上で流通することで、トークン経済が発展する。
- トークン経済とは、デジタルトークンを用いた経済活動を指す。
- CBDCをベースとして、様々なデジタルトークンが創出される。例えば、有形・無形資産がトークン化され、今まで取引されていないものまでにも価値が生まれる。
- さらに、一円未満での決済も可能となることで、新しい経済活動のユースケースが生まれる可能性がある。

トークン化資産例

資産	詳細
株式・債券	金融商品の小口化により、今までリーチできなかった層のリーチと流動性の向上
不動産	不動産をトークン化することで、一般の人が所有権の一部を得ることでできる、また流動性の向上
サービス権利	サブスクリプションや公共サービスの使用権をトークン化することで、利用者間での取引が可能に。
個人情報	個人情報や医療データをトークン化することで、データの管理とアクセス権利個別に管理可能。また　個人情報の売買が可能に。

マイクロペイメント例

音楽

サブスクリプションの契約ではなく、特定の曲を一回だけ聞きたいときに、特定の曲を聞いた回数分だけ支払う。

健康データ

ヘルスケア企業等に自分の健康データの一部だけ提供した見返りに報酬を受け取る。

記事

100ページ以上ある記事の特定の記事のみ閲覧したい場合に、その1ページの閲覧にのみに対して支払う。

論点

Startale Labs

- CBDCがパブリックブロックチェーン上で流通されることによってどのようなことが可能になりますか？

EOF