パブリックブロックチェーンの技術動向
～企業活用に向けた技術課題と現状～

2023年6月5日

株式会社日本総合研究所
先端技術ラボ

＜本件に関するお問い合わせ先＞ 渡邊 大喜（watanabe.hiroki@jri.co.jp）

はじめに

近年、NFTやWeb3.0といったブロックチェーン技術を基盤とした技術トレンドが発生している。

【IT動向リサーチ】NFT（Non-Fungible Token）に関する動向（2021年）
【先端技術リサーチ】Web3.0トレンドを俯瞰する ～ブロックチェーン技術が実現する次世代のインターネット～（2022年）

これまで企業におけるブロックチェーン基盤の活用においては、プライベート/コンソーシアム型のブロックチェーンを活用しての取り組みが中心であったが、上記技術トレンドによりパブリック型のブロックチェーンを活用した取り組みも増加している。

デジタル庁が開催する「Web3.0研究会」や経済産業省が公表した「Web3.0事業環境整備の考え方」においても、パブリックブロックチェーンの活用の重要性について言及されてきた。

一方で、パブリックブロックチェーンの企業活用を想定した際には、「スケーラビリティ」「セキュリティ」「プライバシー・機密性」「電力消費」といった技術課題が存在する。

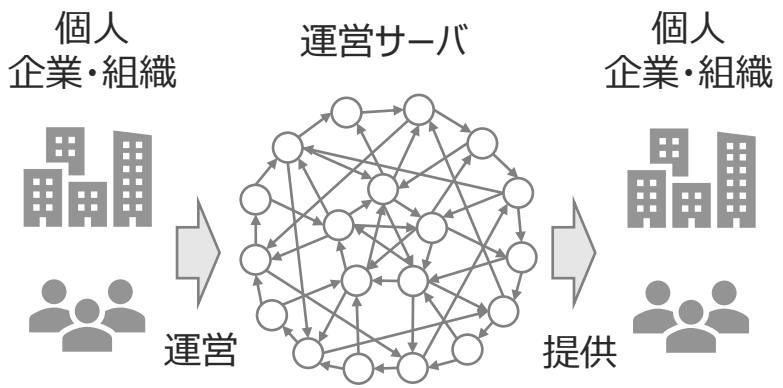
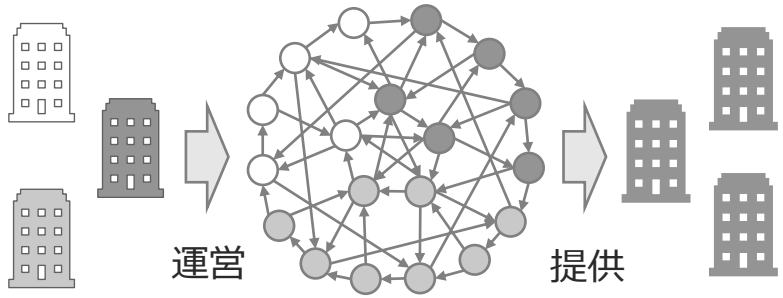
本レポートでは、2023年現在において、上記4つの観点での技術課題における現況を調査し、その解決策について整理した。本レポートが、パブリックブロックチェーンに関する技術の理解を促し、今後の活用に寄与するものになれば幸いである。

本レポートの主な想定読者：企業においてブロックチェーンを活用したシステム開発に携わっている方／検討している方

目次

1.1 パブリックブロックチェーンとは

- 誰もが自由にネットワークに参加が可能で、特定少数の管理者によらない運営がなされるブロックチェーンネットワークを「パブリックブロックチェーン」とよぶ。
- これまで、エンタープライズ用途ではコンソーシアム型のブロックチェーン利用が中心であり、パブリックブロックチェーンは主に暗号資産取引等を行う個人レベルのユーザによって利用されてきた。

	パブリックブロックチェーン	プライベートブロックチェーン／コンソーシアムブロックチェーン
運営／利用者	不特定多数の個人や組織 	単一／特定少数の企業や組織 
管理者	不在	存在（単一／特定少数）
データ	一般に公開されている	一部の参加者間でのみ共有
開発	オープンソースのため、誰でも参加できる	主となる開発企業が存在することが多い
例	• Bitcoin • Ethereum	• Corda • Hyperledger Fabric • Quorum

1.2 パブリックブロックチェーンの課題

- パブリックブロックチェーンでは従来、**①スケーラビリティ②セキュリティ③プライバシー・機密性④電力消費**といった技術課題が指摘されており、これらがエンタープライズ用途での利用の障壁となってきた。
- 一方で、着実な研究開発を経て、個々の課題については一部解消されつつある。

パブリックブロックチェーンの課題

経産省公表の資料[*1]では下記のように整理されている。

1. **スケーラビリティ**
   ブロックチェーンは既存の集中型処理システムと比較して処理速度が遅い。一方で解決の方向性が一定程度見えてきているとの声もある（L2レイヤー活用等）。
2. **セキュリティ**
   秘密鍵の管理方法等は課題。
3. **プライバシー・機密性**
   パブリックチェーン上の情報はすべて公開となるため、プライバシーが絡む情報や機密性が高い情報を載せることがそぐわない。ただし技術的解決が模索されつつある（ゼロ知識証明等）。
4. **電力消費問題**
   マイニングにあたって莫大な電力消費が必要に。
   ただし電力消費を抑えられる仕組み（Proof of Stake)への移行も進展。

課題へのアプローチ

スケーラビリティ P.8

- オフチェーンの取引基盤との連携（**レイヤー2**）
- ブロックチェーン同士を相互接続し**ブロックチェーン群**を構成。水平スケーリングを実現。
- **コンセンサスアルゴリズム**の改良。

セキュリティ P.19

- 秘密鍵の漏洩に備えた**ウォレット機能の改善・高機能化。**
- スマートコントラクトの**実装ガイドラインの利用。**
- **分散型オラクル**サービスの利用。

プライバシー P.28

- **ゼロ知識証明による**取引の秘匿化。
- マネーロンダリング対策との協調が必要。

電力消費 P.31

- **再生可能エネルギーや代替アルゴリズムへの転換。**
- Ethereumにおいては2022年9月にPoS（プルーフ・オブ・ステーク）へと移行し電力消費量が99.988%削減。[*2]

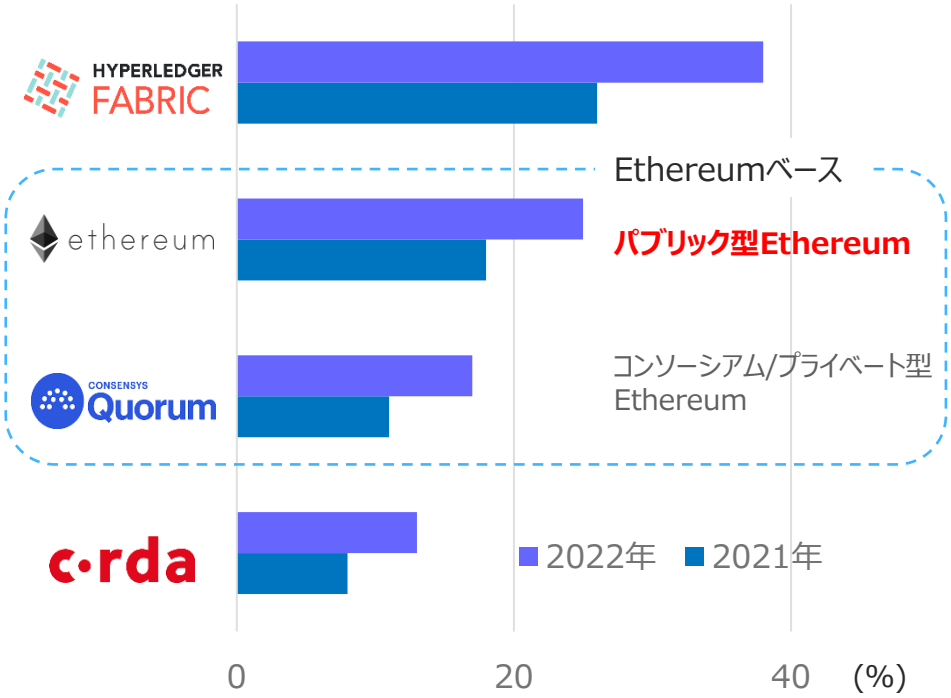
*1 経済産業省.「Web3.0事業環境整備の考え方−今後のトークン経済の成熟から、Society5.0への貢献可能性まで−」, pp.32, https://www.meti.go.jp/shingikai/sankoshin/shin_kijiku/pdf/010_03_01.pdf

*2: Crypto Carbon Ratings Institute「The Merge - Implications on the Electricity Consumption and Carbon Footprint of the Ethereum Network」 https://carbon-ratings.com/eth-report-2022

1.3 企業におけるパブリックブロックチェーン活用動向

- エンタープライズ分野においても、パブリック型ブロックチェーンの活用は年々増加している。
- 背景には、非金融セクターで生じたNFTやWeb3等の新たなムーブメントの発生がある。パブリック型ブロックチェーン技術課題の解決により、今後は、多様な事業領域においてパブリック型の採用事例が進む可能性がある。

時価総額TOP100企業のブロックチェーン基盤採用率*1

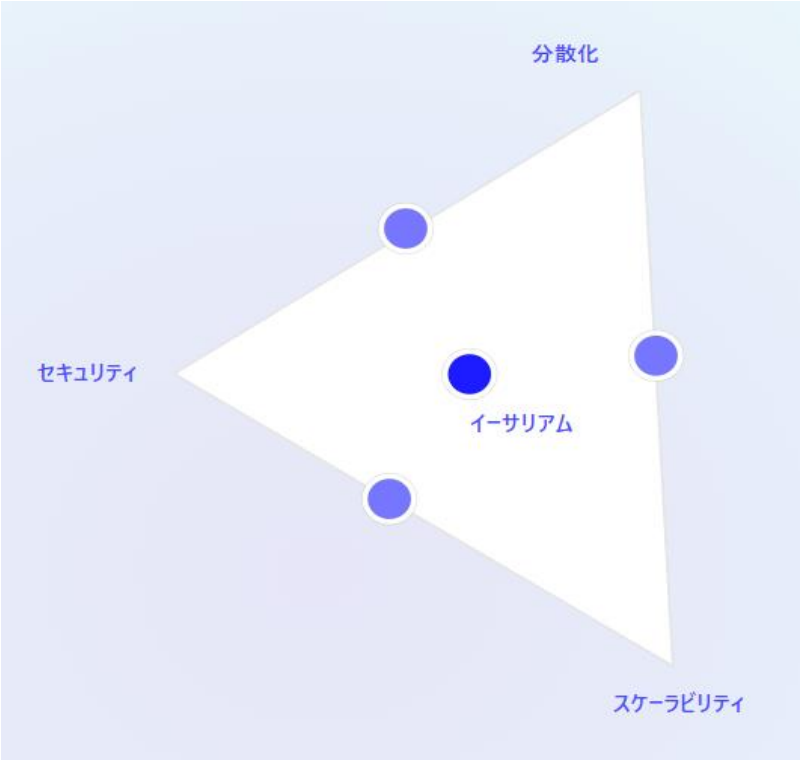


- 2022年において、時価総額に基づくグローバルTOP100企業*2のうち24%の企業がパブリック型Ethereumを利用している*1（BLOCKDATA社調査、2022年10月公表）。
- 2021年から2022年にかけて、上位４基盤の利用率はいずれも上昇しており、企業はパブリック型を含む複数基盤について利用推進している（パブリック型Ethereumの利用率は6ポイント上昇）。
- NFTを活用したデジタルマーケティングの文脈で、消費財・小売りセクターにおけるブロックチェーン戦略の公表も相次いでいる。
- NFTは二次流通可能な構造によりプライベート/コンソーシアム型よりも、パブリック型のブロックチェーン活用と相性が良く、同用途では活用が進むと思われる。

*1 BLOCKDATA社（CB Insight子会社）の下記レポートを元に日本総研作成
https://www.blockdata.tech/blog/general/the-state-of-enterprise-blockchain-in-2021,
https://www.blockdata.tech/blog/general/the-state-of-enterprise-blockchain-in-2022
*2 PwC「Global Top 100 companies - by market capitalisation」
https://www.pwc.com/gx/en/audit-services/publications/top100/pwc-global-top-100-companies-by-market-capitalisation-2022.pdf

[参考] ブロックチェーン技術のトリレンマ

- ブロックチェーン技術の発展において、同時に満たすことが難しい3つの特性「分散化」「スケーラビリティ」「セキュリティ」が存在する。
- パブリックブロックチェーンにおいては、3つの特性のバランスを鑑みて技術開発を行うことが重要である。



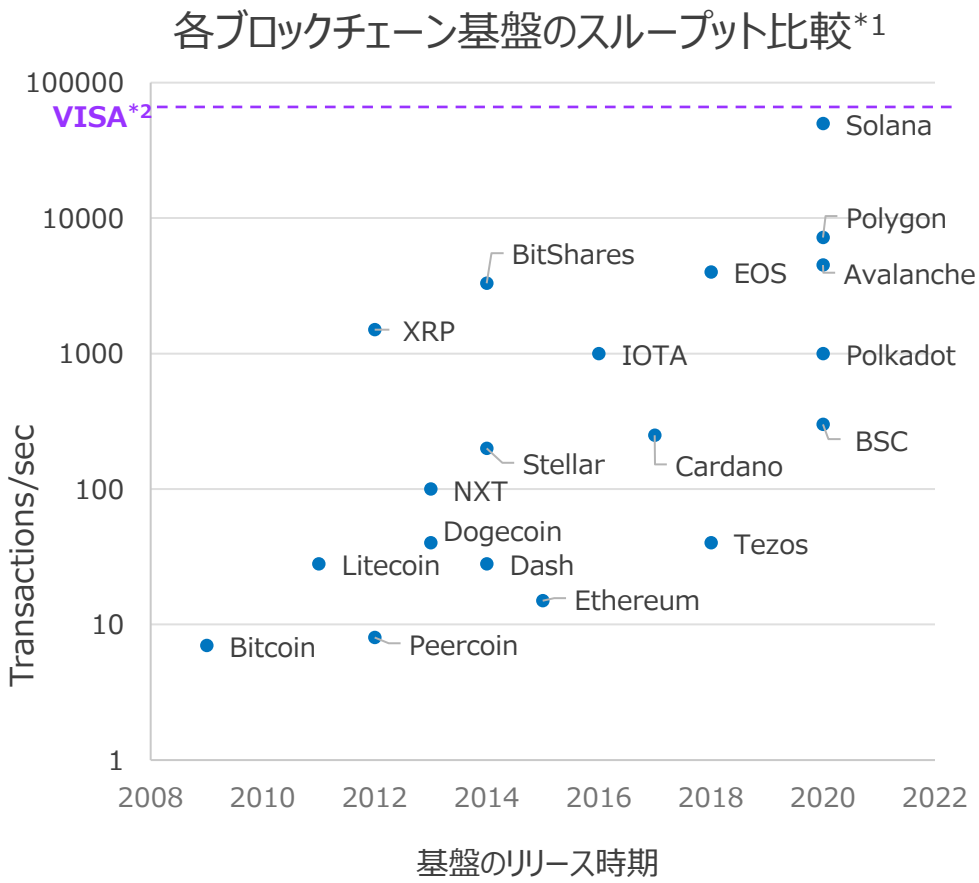
トリレンマの解決を目指すことをEthereumのビジョンに掲げている。
図出所： https://ethereum.org/ja/roadmap/vision/
（閲覧：2023.5.19）

- ブロックチェーンのトリレンマとは、Ethereumの共同創設者であるVitalik Buterinによって表明された概念[*1]。
- Ethereumでは次の3つの特性のバランスを維持しながらの技術開発を推奨している。
  - **分散化** - 特定のノードに権限が集中していない。
  - **スケーラビリティ** - トランザクションの増大に耐え得る。
  - **セキュリティ** - チェーンへの攻撃に抵抗することができる。
- Vitalik氏は、3つのうち一つを犠牲にして、他の2つの特性を強化することは「容易なソリューション」である主張している[*2]。
  - 例えば、クローズドなコンソーシアム型ブロックチェーンは、分散性を犠牲にして、セキュリティとスケーラビリティを向上している
- パブリックブロックチェーンにおいては、3つの特性をバランスを取りながら技術開発をしていくことは、技術的なチャレンジであり、イノベーションと見られている。

*1 https://vitalik.ca/general/2017/12/31/sharding_faq.html
*2 https://vitalik.ca/general/2021/04/07/sharding.html

2.1 スケーラビリティの現状

- Bitcoinなど最初期のブロックチェーンは、スケーラビリティ面に課題があるとされていたが、近年リリースされた基盤ではより高負荷な要求に対応できるなど、一定の技術向上が見られる。



基盤のスケーラビリティは年々向上

- スケーラビリティとは、システムが高負荷な状況に対応できる度合いのこと。
- 最初期からのブロックチェーン基盤（Bitcoin、Ethereum等）において、毎秒に処理できるトランザクション数（TPS）は10のオーダーであり、高性能が要求されるエンタープライズ領域への適用においては課題となっていた。
- 近年リリースされた基盤では、より高負荷（1000TPS以上）な要求に対しても、対処可能であるなど技術向上が見られる。

*1 リリース当時に公表・推論された理論上限値を元に日本総研作成。データはリリース当時のものをプロットしており、リリース後に性能アップデートが行われた場合は値が異なる可能性あり。
*2 クレジットカード決済大手VISAのシステムは6.5万TPSのキャパシティがあると公表（2017.8 時点）
https://www.visa.co.uk/dam/VCOM/download/corporate/media/visanet-technology/aboutvisafactsheet.pdf

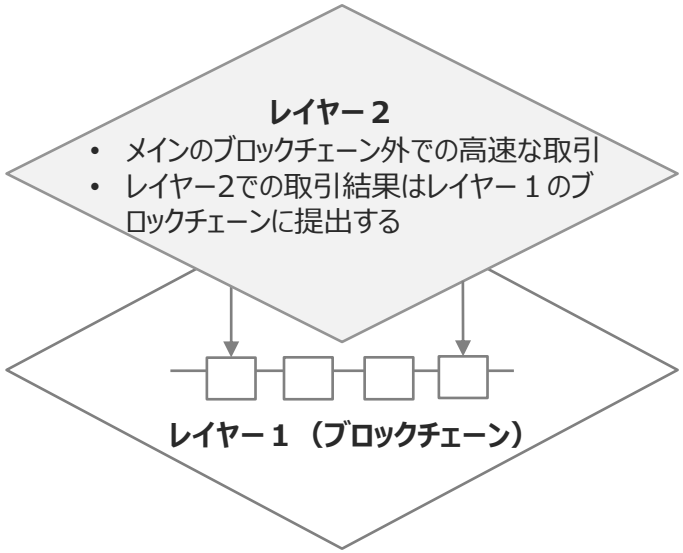
2.2 スケーラビリティ向上のアプローチ

- ブロックチェーンの処理能力を向上させるために**「レイヤー2プラットフォームの活用」「ブロックチェーン群による水平スケーリング」「コンセンサスアルゴリズムの改良」**の３つのアプローチが主流。
- それぞれブロックチェーンのトリレンマのバランスを取りながら技術開発が行われる。

アプローチ	概要	特徴	プロダクト例
レイヤー2プラットフォームの活用	ブロックチェーンを第一層（レイヤー1）として上層のオフチェーン領域（レイヤー2）でトランザクション処理を行い、一括まとめて第一層へ結果を提出する。	• スマートコントラクト基盤として最大のシェアを持つEthereumを第一層としたエコシステム。 • 実装方式がサイドチェーンやzkRollupなど複数存在し、開発競争が激しい。	Polygon PoS, Optimism, zkSync
ブロックチェーン群による水平スケーリング	相互運用性のある複数のブロックチェーンを運用し、系全体として処理できるトランザクション数を向上させる。	• ブロックチェーン群には様々なアプリケーションに特化した独自のブロックチェーンが存在する。 • ビジネス要件や規制に合わせてブロックチェーンをカスタマイズ可能。	Polkadot, Avalanche, Cosmos
コンセンサスアルゴリズムの改良	ブロックチェーン技術の中核である合意形成に用いられるアルゴリズムを改良し、垂直スケーリングの性能を向上。	• 初期のブロックチェーン（Bitcoin等）に実装されたコンセンサスProof-of-Work以来、長年の研究開発を経て様々な手法が提案されてきた。	Solana, EOS

2.3 レイヤー2プラットフォーム

- レイヤー2とは、メインとなるブロックチェーンを第一層（レイヤー１）とし、そのブロックチェーンの外部で取引（レイヤー２）を行う技術の総称。
- レイヤー２で行った取引や計算処理の最終結果のみがレイヤー１のブロックチェーンに書き込まれる。



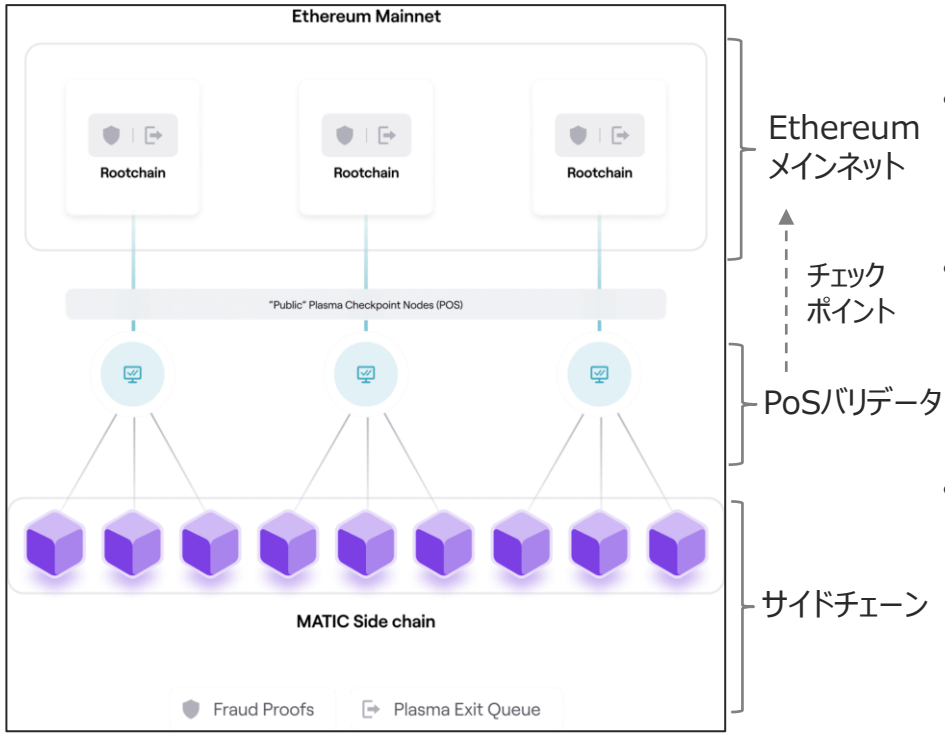
プロダクト例	レイヤー1	特徴
Lightning Network	Bitcoin	P2PでBitcoinの支払いチャネルを構築する。
Optimistic Ethereum	Ethereum	レイヤー2技術Optimistic Rollupを実装
Polygon	Ethereum	多様なレイヤー2技術を利用するためのフレームワーク群。レイヤー2のサイドチェーンのネットワークである「Polygon PoS」が主力。

実用化が進むレイヤー2

- レイヤー２とは、メインとなるブロックチェーン（Bitcoin、Ethereum）を第一層（レイヤー１）として扱い、トランザクションをブロックチェーンの外部、即ち第二層（レイヤー２）で安全に処理する技術。
- 具体的には、最終の取引結果に至るまでのトランザクションや計算処理をブロックチェーン外のネットワークで行い、ある時点の最終の取引結果のみをブロックチェーン（レイヤー1）に記録する。これにより、**第一層のブロックチェーンのスケーラビリティや手数料コストに縛られず、より高速かつ安価にレイヤー２で取引が可能。**
- レイヤー2のネットワークに独立したブロックチェーン「サイドチェーン」を用いるケースもある（Polygon PoS等）。レイヤー2のセキュリティは第一層となるブロックチェーン側に大きく依存している。
- Ethereumにおいては、2016年頃から研究開発が始まっており、近年実用化が進んでいる。

2.3.1 レイヤー2プラットフォーム例①　Polygon PoS

- レイヤー1をEthereumとするも、レイヤー2は独自の暗号資産（MATIC）を持つPoSブロックチェーン（サイドチェーン）で構成されている。
- ナイキ、ディズニー等の大手エンタープライズが提携を表明しており、近年注目が集まる。



Polygon PoSのアーキテクチャ。
図出所：https://polygon.technology/solutions/polygon-pos
（閲覧：2023.3.20）

レイヤー2として動作するPoSブロックチェーン*1

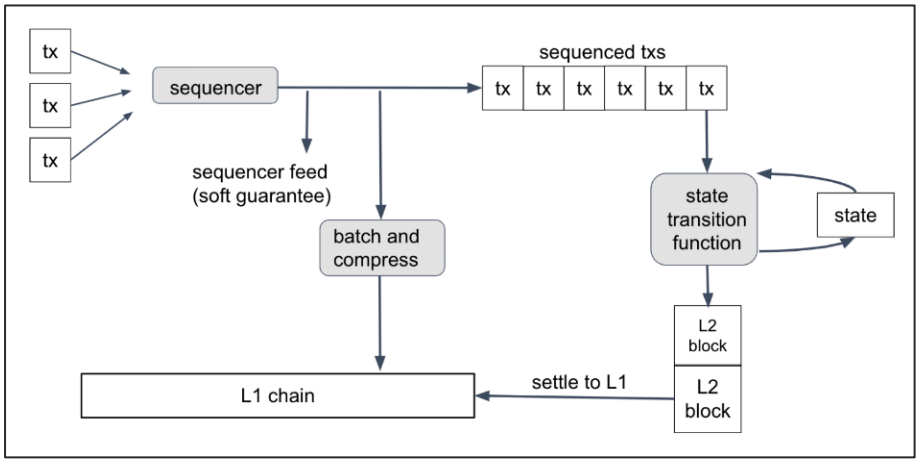
- Polygon PoSはPolygon Labsが開発するレイヤー2ソリューション。（元々Matic Networkという名称で知られており、2021年にリブランディング。）
- レイヤー1にEthereum。レイヤー2ネットワークには、MATICという暗号資産を発行した異なるブロックチェーン（サイドチェーン）を利用。「低コスト」「高スループット」「EVM*2互換」を強みにユーザを集める。
- **近年、NFT用途でのエンタープライズ利用例（米ナイキ、米ウォルト・ディズニー等）が増えており注目を集める。**

観点	特徴
スループット	PoSコンセンサスにより、約7,000TPSが可能 (2020年時点でのテストネットでの計測値)
分散性	チェックポイントのブロックを生成する検証ノード数は100。検証ノードになるには、暗号資産MATICのステーキングが必要。
セキュリティ	Polygon PoSでの取引結果をまとめたチェックポイントをレイヤー1のEthereumに提出することでファイナリティを確保。また、チェックポイントに不正がある場合、証拠を提出することで検証ノードがステーキングしているMATICが没収される。

*1 PoSとは、Proof-of-Stakeの略。PoSはブロックチェーンのコンセンサスの一種で暗号資産の保有量に応じてブロック生成者を選出する方式。
*2 EVMとは、Ethereum Virtual Machineの略。Ethereum上のスマートコントラクトの実行環境のこと。Polygon PoSはEthereumのスマートコントラクトと互換性がある。

2.3.2 レイヤー2プラットフォーム例②　Arbitrum One

- Ethereumコミュニティにて提案されたレイヤー2プロトコルOptimistic Rollup（次頁参照）を実装している。今後のEthereum発展に伴いレイヤー1とレイヤー2の連携が強固となると見られている。
- DeFiやNFT関連のプロダクトが展開されており、L2レイヤーの中では最も利用されている*。



Arbitrum Oneの最新アップデート「Nitro」のトランザクション処理フロー。
図出所：https://developer.arbitrum.io/inside-arbitrum-nitro/
（閲覧：2023.4.24）

1．「シーケンサー」と呼ばれるノードがトランザクション（tx）の順番付けを行い、複数トランザクションを圧縮したデータをレイヤー1チェーン（Ethereum）に提出する。
2．同時に順位付けされた複数トランザクションを実行して、ブロックチェーンの台帳を更新。
3．レイヤー2ブロックを作成し、最新の台帳状態を持つL2のブロックチェーンに追加する。

* レイヤー2などブロックチェーン上のプロダクトの利用度合いはTVL（Total Value Locked）で計測されることが多い。TVLはあるプロトコルへの「預かり資産」の総数を示す。2023年4月時点ではレイヤー2のプロトコルではArbitrumが66%のシェアを占める。

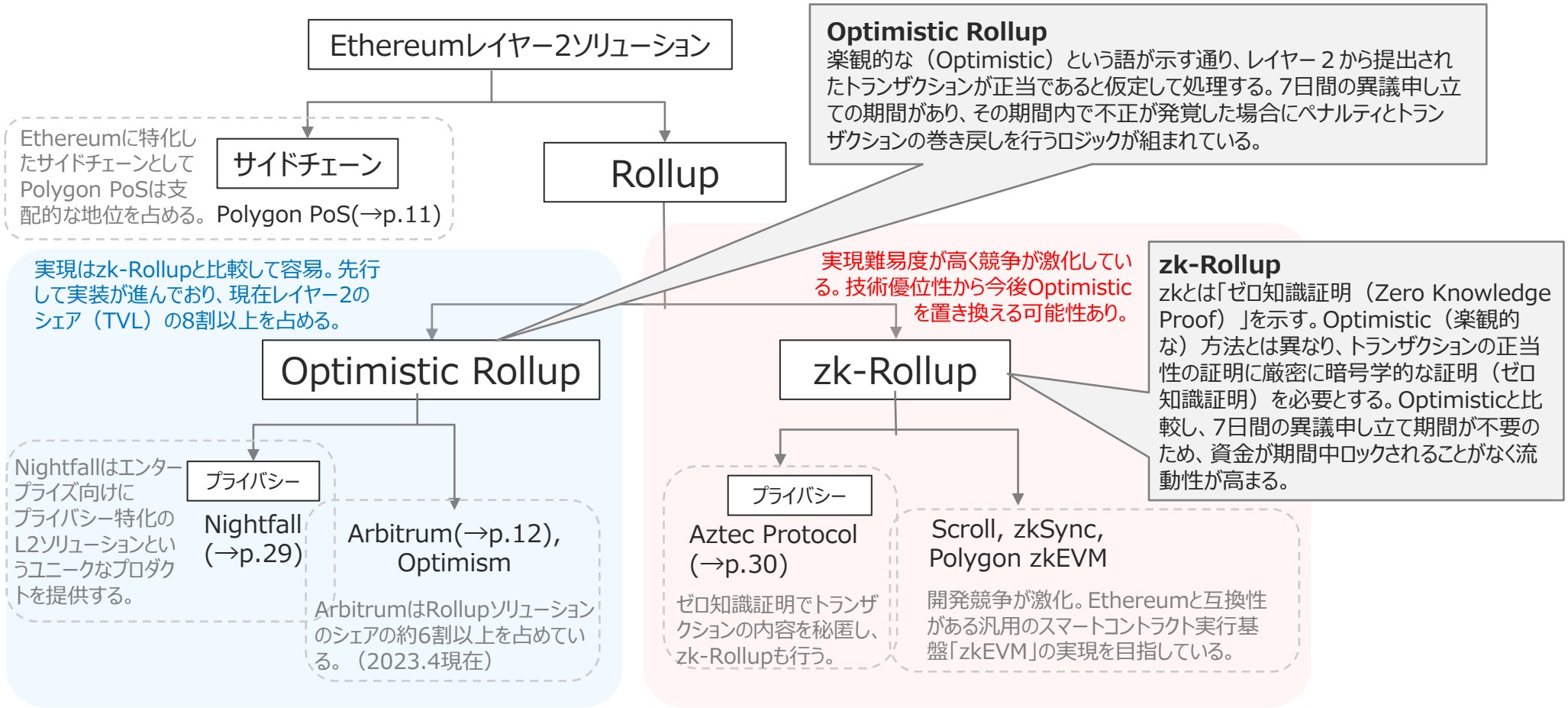
Ethereum互換のレイヤー2プロトコル

- Arbitrum OneはOffchain Labsが開発するレイヤー2ソリューション。
- レイヤー1はEthereum。レイヤー2では、Ethereumコミュニティにて提案されたレイヤー2プロトコルOptimistic Rollupを実装し、レイヤー1と協調する。ユーザはレイヤー1にてETHをデポジットすると、レイヤー2でETHが使用可能になる。
- **現在、DeFiやWeb3プロジェクトを中心に利用されており、レイヤー2において最大のTVL*を持つ。**

観点	特徴
スループット	約40,000TPSと見られている。（注：非公式値）
分散性	メインネットベータ版では、検証ノードはOffchain Labsによって管理されている。集権化された運営であったが、2023年3月に独自トークンARBの発行とDAOへの移行を発表。
セキュリティ	複数トランザクションの圧縮データをL1に提出することでファイナリティを確保。不正防止にペナルティの仕組みを持つ。Ethereumの開発ロードマップと連携しており、プロトコルレベルでより強固なL1/L2連携が進むとみられる。

[参考] 過熱するRollup技術開発

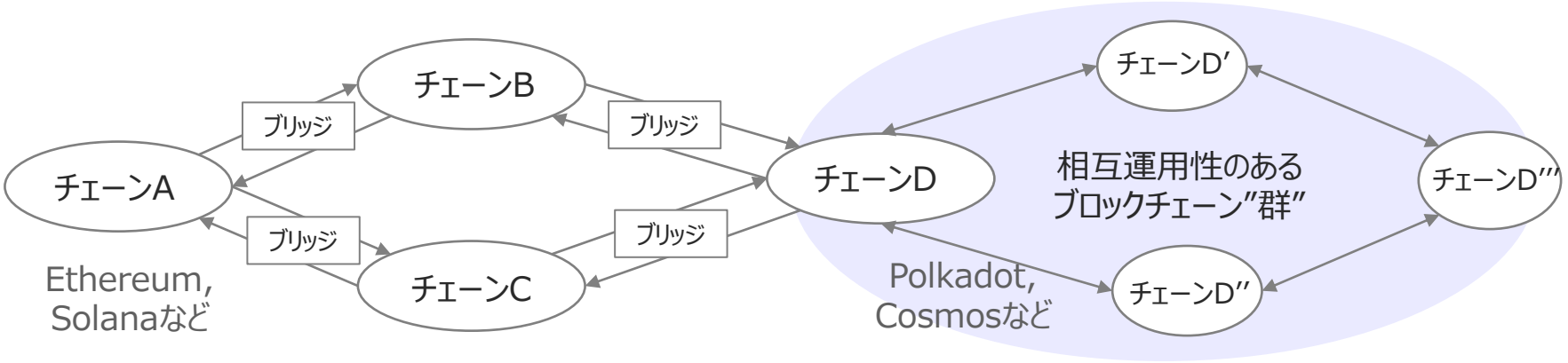
- Rollupとはレイヤー2技術においてレイヤー2とEthereumメインネットの接続方式に関する技術の総称。レイヤー2で処理されたトランザクションのデータをまとめてEthereumのメインネットに巻き上げ（Rollup）するイメージに由来している。
- RollupにはOptimistic RollupとZk-Rollupの二方式ある。複数の実装も存在しており、市場支配を巡ってプラットフォームの開発競争が過熱している。



2.4 ブロックチェーン群による水平スケーリング

- 複数のブロックチェーン同士の相互運用性（インターオペラビリティ）を保ちながら接続する。
- それぞれのブロックチェーンは独自のアプリケーションに特化して運用することができ、並列的に取引を処理し水平的にスケーリングする。

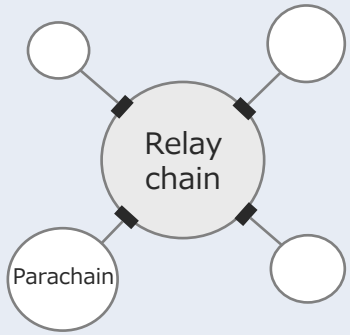
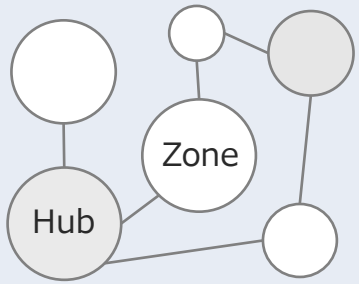
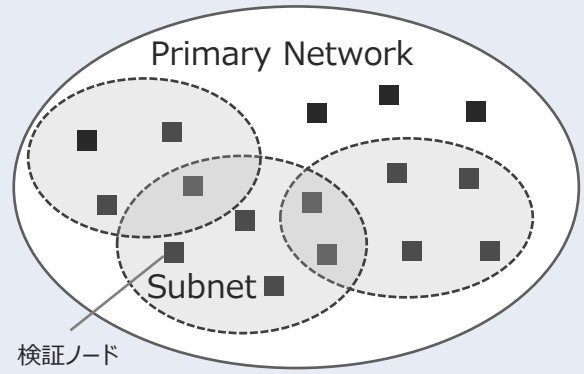
相互運用可能なブロックチェーン群とは



- 通常、ブロックチェーン間におけるトークンや資産の移動（例：Bitcoin-Ethereum間）は、「ブリッジ」と呼ばれるサードパーティの仲介者を必要とする。
- 一方で、より相互運用性のあるプロトコルで接続されたブロックチェーンの"群"では、各ブロックチェーン間でのトークンやデータのやりとりをサードパーティを排して行うことができ、複数のブロックチェーンが接続されるエコシステムを構築される。
- **複数のブロックチェーンにおいて、並列的にトランザクションを処理していくことで系全体としてのスループットが向上する。**

2.4.1 ブロックチェーン群の例 Polkadot, Cosmos, Avalanche

- ブロックチェーン群を展開するプロダクトとしてはPolkadot, Cosmos, Avalancheが知られている。
- スループットという点では、どのプロダクトも水平スケーリングを達成しており、理論上は無制限にスケールが可能。

ブロックチェーン群	Polkadot	Cosmos	Avalanche
ネットワーク構造のイメージ		 Zone: Cosmosにおけるアプリ特化のブロックチェーン Hub: Zone間のルーティングに特化したブロックチェーン	
ネットワークトポロジー	1つの親ブロックチェーン(Relay chain)に接続される多数の子ブロックチェーン（Parachain）という**階層型ネットワーク**。	各ブロックチェーン（ZoneやHub）は親子関係を持たず**並列な関係にあり**、相互に通信可能なネットワーク。	全体ネットワーク（Primary Network）の検証ノード間で小さなグループ（Subnet）を作り**重なり合うように**構成されるブロックチェーンネットワーク
検証ノード数(2023.4時点)	Relay chainの検証ノードは297ノード	各ブロックチェーンにより異なる（主なチェーンとしてCosmosHubに175、Osmosis150, Evmosで150）	Primary Networkの検証ノード数は1243
特徴	• Relay chainによりセキュリティが担保されており、Parachainは独自の検証ノードを必須としない。 • Relay chainの接続可能なParachainの上限が定まっており（100程度）、オークション方式で接続スロットを獲得する必要がある。	• 各ブロックチェーンの独立性が高く、特定の親チェーンを介さずともIBC（Inter-Blockchain Communication）と呼ばれるプロトコルによる相互運用が可能。 • 各ブロックチェーンのセキュリティはチェーン毎に担保する必要がある*。 ＊ 2023年3月にメインチェーンであるCosmosHubのセキュリティを利用できる機能は実装されたが、利用は強制されるものではない。	• Subnetは独自ブロックチェーンやトークンを展開可能である。 • 全体ネットワークには役割の異なる3つのメインチェーンが存在し、スマートコントラクト実行用チェーン「C-chain」はEVM（ethereumのスマートコントラクト実行環境）と互換性がある。 • Subnetの検証ノードは全体ネットワークの検証ノードにも参加する必要がある。

2.4.2 ブロックチェーン群のエンタープライズ利用

- ブロックチェーン群のプロジェクトが提供するSDK等を利用することで、要件に合わせてカスタマイズされたブロックチェーンを構築できる。企業において独自ブロックチェーンを立ち上げる事例が見られる。

SDKを用いたアプリケーション特化型の独自チェーン

	Polkadot	COSMOS	AVALANCHE
プロジェクト（ブロックチェーン群）			
独自チェーン作成用のツール等	Substrate	Cosmos SDK	Subnet-EVM
独自ブロックチェーン数（2023.4時点公表）	42 parachains	56 Zones	42 Subnet blockchains

メリット	• ビジネス要件や法規制に合わせてカスタマイズが可能（手数料やバリデータ等の調整が可能、プライベート型とすることができる、など）。 • 他ブロックチェーンのセキュリティを利用することもできる（Polkadot、Cosmos） • ブロックチェーン群に属する他のブロックチェーンと相互運用性がある。（「ブリッジ」を介さずに資産転送が可能）
デメリット	• スマートコントラクトのみの活用と比べて、初期の開発や運用保守でのコスト負担が大きい。

ブロックチェーン群が提供するプラットフォームのSDK/技術を活用して、企業が独自チェーンを立ち上げる事例

	ブロックチェーン	立ち上げ企業	利用ツール	特徴
国外	BNB Beacon Chain（旧Binance Chain）	Binance	Cosmos SDK	最大手の取引所Binance主導で立ち上げられた独自チェーン。暗号資産は「BNB」。元々は取引所の手数料等のユーティリティトークンとして活用されていた。現在はBNB Chainエコシステムのステーキングとガバナンス投票を担う。
国内	LINE Blockchain	LINE	Cosmos SDK	LINEが独自開発・運営するブロックチェーン。暗号資産は「LINK」。Cosmos SDKの技術を利用しており、独自のトークンエコノミーをLINEブロックチェーン上で導入可能。LINEユーザ基盤との連携にも強み。
国内	Astar Network	Stake Technologies	Substrate	Polkadotの子チェーン（Parachain）として、日本発のパブリックブロックチェーンを立ち上げ。暗号資産は「ASTR」。Polkadot上でのコントラクト・ハブとなることを目指している。NTTドコモ等の国内大手企業と提携が進む。

2.5 コンセンサス・アルゴリズムの改良

- コンセンサス・アルゴリズムとはブロックチェーンによる分散台帳が一つの状態について合意するための方法。
- Bitcoinの実装で提案されたNakamoto Consensusは、パラメータを調整したりアルゴリズムの一部を他の手法に置き換えるなど、改良が試みられてきた。

2008年頃	**Bitcoinの登場（Nakamoto Consensus）**	Nakamoto Consensusは「計算競争によるバリデータの選出」「確率的なファイナライズ」「インセンティブ設計」を組合わせ、従来の分散コンピューティングで用いられてきた合意形成とは異なる確率的なアプローチを提案。	Bitcoin、Litecoinなど
2012年頃	**Proof-of-Stakeによる代替**	暗号資産の保有量によってブロック生成者を選出するProof-of-Stakeアルゴリズムが提案されるなど、Nakamoto Consensusの一部を改良した暗号資産が誕生した。	Peercoin、NXTなど
2016年頃	**古典的な分散合意アルゴリズムとの組み合わせなど模索が続く**	従来の分散コンピューティング分野で発展してきたアルゴリズム（PBFT等）をブロックチェーンのシナリオに導入し性能向上を探る局面が続く。DAG（有効巡回グラフ）などNakamoto Consensusに囚われない手法の提案も見られた。	Tendermint、IOTAなど
2019年頃～	**コンセンサスの洗練化**	ブロックを提案できる「バリデータ」の選出と、バリデータ群による「ファイナライズ」において、実績ある方式を組み合わせたコンセンサスが主流に。（例：Avalancheはバリデータの選出にDPoS*、ファイナライズにDAGベースを組合わせている）理論上1000のオーダーのTPSの処理が可能となる。	Avalanche、Solanaなど

* DPoS（Delegated Proof of Stake)とはProof of Stakeの後継にあたるアルゴリズムで、暗号資産の保有者に対して保有量に応じた投票権を与え、取引の承認作業を他のノードに委託（Delegated）することができるアルゴリズム。

2.5.1 コンセンサスの改良例　Solana

- コンセンサスアルゴリズムのプロセス各所を効率化し、高スループットを実現するブロックチェーン基盤。
- Ethereumの手数料（Gas fee）が高騰する中で、低い手数料と高い性能を武器に急成長。

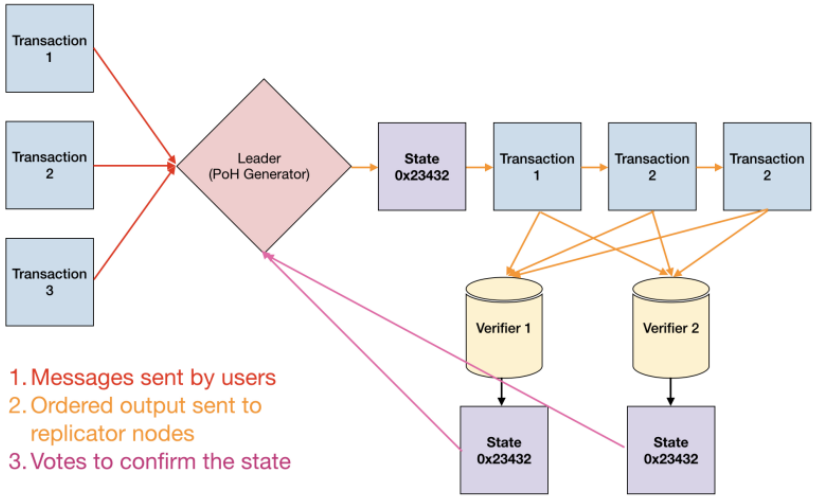


Figure 1: Transaction flow throughout the network.

Solanaホワイトペーパー記載ののトランザクション処理フロー。
図出所：https://solana.com/solana-whitepaper.pdf
（閲覧：2023.5.19）

ユーザが送信したトランザクションを検証ノードのリーダー（交代制）が集める。
1. リーダーはトランザクションの順番付けを行い、ブロックを作成しブロードキャストする。
2. 各検証ノードで投票を行いブロックをファイナライズ（最終合意）する。

* Anatoly Yakovenko（Solanaの共同創業者）「Proof of History: A Clock for Blockchain」https://medium.com/solana-labs/proof-of-history-a-clock-for-blockchain-cf47a61a9274

毎秒5万トランザクションでの処理を可能に

- Solanaのテストネット環境において200ノードで毎秒5万トランザクションの実行を確認*。
- コンセンサスは、ノード間における相互通信や同期をできる限り排するよう工夫がなされており、 Proof-of-HistoryやTower BFTと呼ばれるアルゴリズムを組み合わせている。
- ブロックの最終合意は、ブロックへの投票がベースであり、検証ノードの過半数の投票によりファイナライズする。
- リーダーノード（リーダーは交代制）が提案したブロックを、各バリデータが「非同期的に」承認していくことで高スループットを実現。

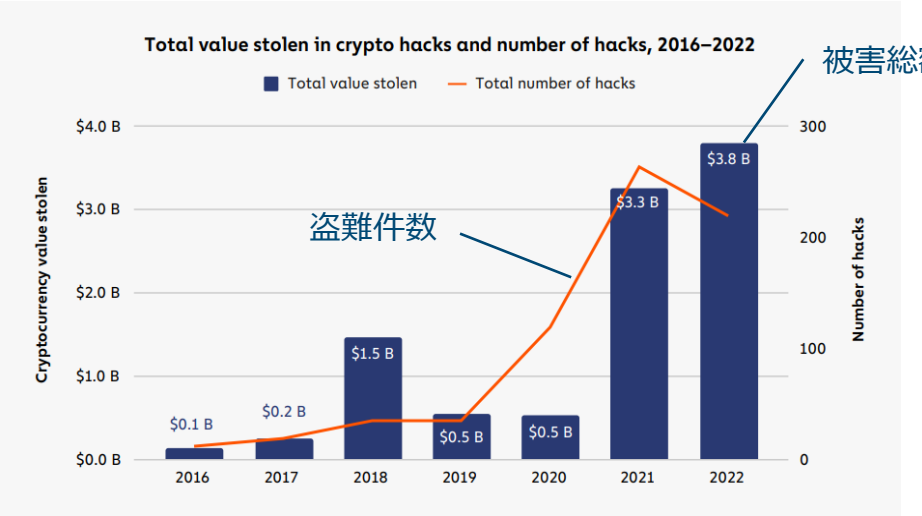
観点	特徴
スループット	テストネットで5万TPSを実現。（レイヤー１の垂直スケーリングの公表値としては最高性能。）
分散性	検証ノード数は1700程度（2023年4月現在）。検証ノード選出はDPoS方式による。なお検証ノードとなるために高性能なハードウェアや通信帯域が要求される。
セキュリティ	ネットワークを乗っ取るためにはDPoS方式でステークされている33%を支配する必要がある。（2023年4月時点で30ノードに相当）

3.1 セキュリティに関する現状

- 違法行為に関連する暗号資産取引（マネーロンダリングや投資詐欺）の被害額のうち、約20%が「暗号資産の盗難」であり、技術的なセキュリティの問題に起因する。
- 暗号資産を持つパブロックブロックチェーンの活用は、セキュリティ面に十分配慮する必要がある。

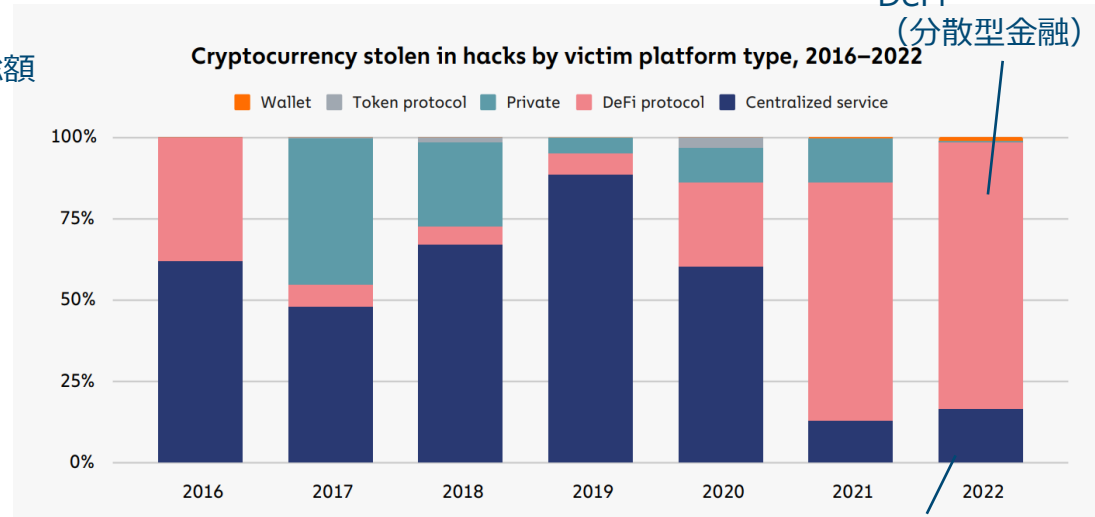
暗号資産の盗難事件の傾向

盗難された暗号資産の総額と総件数



出所：Chainalysis「The Chainalysis 2023 Crypto Crime Report」

被害を受けたプラットフォームの種別



- 2021年から暗号資産の盗難は急増しており、2022年は38億ドル相当がハッキング等により流出。
- 要因として、ハッキングの攻撃対象が、近年セキュリティが強固となった中央集権的な取引所から、DeFi（分散型金融）関連のサービスへ移行したことが挙げられる。特に、2022年は80%以上がDeFiからの流出となった。
- 攻撃方法として「コントラクトの脆弱性利用」「オラクル価格操作」「秘密鍵の漏洩」等があげられる（次頁詳細）。

3.2 攻撃方法・対策の概要

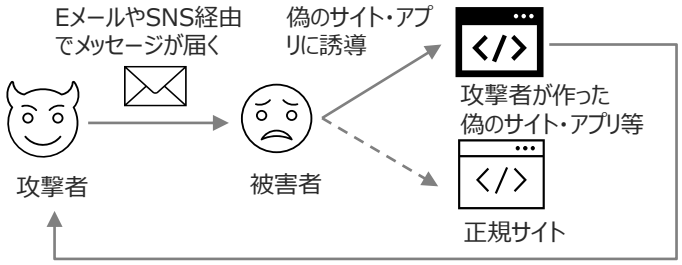
・秘密鍵の漏洩は、現在も暗号資産の盗難において一般的。暗号資産ウォレットでの対策が有効。
・コントラクトの脆弱性の利用も多く、対策としてはセキュリティ監査が一般的。
・オラクルの価格操作は、近年増加する攻撃。コードの悪用なくとも市場操作により成立する。

攻撃方法	概要	対策	事例
秘密鍵の漏洩	フィッシング攻撃を利用するなど、暗号資産の保有権を証明する秘密鍵が漏洩し、攻撃者が不正に資産にアクセスしたり送金する。	• **ハードウェアウォレットやコールドウォレット**を使用し、秘密鍵のオンライン上のリスクを減らす。 • **多要素認証**を導入しアカウントへのアクセスを制限する。 • 秘密鍵の定期的な変更やパスワードマネージャを使用して秘密鍵を安全に管理する。	暗号資産取引所BXHにて管理者の秘密鍵が漏洩（2021）
コントラクトの脆弱性利用	スマートコントラクトに存在するセキュリティ上の脆弱性を悪用して、不正に資金にアクセスしたり、資金を盗む。	• **セキュリティ監査**を行い、コントラクトの脆弱性を特定・修正する。 • コントラクト開発者による**厳密なテストとレビュー**を実施する。 • **バグバウンティプログラム**を設立して、外部の専門家による脆弱性の検証を促す。	DeFiプラットフォームのPoly Networkのコントラクトをハッキング（2021）
オラクルの価格操作	オラクルとはブロックチェーン外のデータをブロックチェーン上のスマートコントラクトに提供するサービス。悪意のある攻撃者がオラクルの価格情報を操作し、スマートコントラクト上で不正な取引や資産移動を行う。	• **複数のオラクルデータソース**を利用し、データの信頼性と整合性を確保する。 • **分散型オラクル**の導入により、単一のデータソースに依存しない仕組みを作る。 • オラクルデータに関する**異常値検出**を行い、異常値を検出した場合はアラートを出す。	分散取引所Mango Marketsでオラクル価格が不正操作（2022）

3.3 秘密鍵の漏洩

- 「Not your keys, not your coins （鍵を持たぬ者は、コインを持たず）」は暗号資産取引の世界で用いられる表現であり、秘密鍵を自身で管理することは重要視されている。
- 一方で、一般的なユーザにとっては秘密鍵の管理やセキュリティの確保が難しく、ブロックチェーン技術の大衆化に向けて技術課題となっている。

フィッシング攻撃による秘密鍵の漏洩



- 暗号資産のインシデントにおいて、フィッシング攻撃は、ユーザの秘密鍵を奪取する常套手段。
- 電子メールやSNSのメッセージ経由で偽のサイトや悪意のあるアプリケーションに誘導され、**秘密鍵の入力を促される**。
- ユーザ側の対策としては「二要素認証の利用」「ブラウザURLの確認」「不審なメッセージに応じない」などが挙げられるが、DNSハイジャック*1やアイス・フィッシング*2など手法が巧妙化してきており、被害は後を絶たない。

*1 ドメイン名の管理権限を持たない第三者が不正にドメイン名を支配下に置くこと。ユーザは正規のアドレスと同じURLの偽サイトに誘導されてしまう。
*2 資産を管理させる権限を攻撃者に対して付与するよう誘導するフィッシング攻撃。秘密鍵を入力させる従来手法とは異なり、ユーザは不正なトランザクションに承認するだけで成立する。

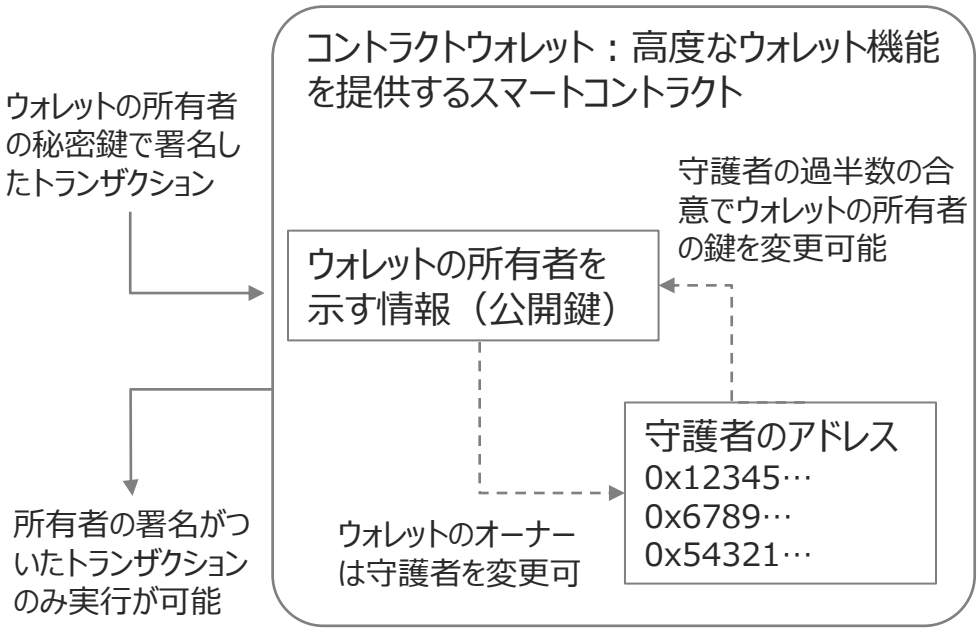
暗号資産ウォレットサービスによるインシデント

- 2022年は暗号資産ウォレットサービスによるインシデントによる秘密鍵の漏洩も相次いだ。
- 秘密鍵を預ける中央集権的な取引所だけでなく、非カストディアルなウォレット（個人で秘密鍵を管理するウォレット）も狙われており、ウォレットの脆弱性や配布サイトのハッキングが攻撃の手口として用いられる。

事例	特徴
Slope Wallet	Slopeのログサーバーに秘密鍵の情報（ニーモニック）が暗号化されずに転送されていた。約8000の秘密鍵が影響を受け、推定10億円の資産が盗まれたとされる。
Bitkeep Wallet	AndroidのアプリのAPKダウンロードが攻撃者によってハイジャックされ、アップデート時にウォレット内にマルウェアが侵入し、ウォレット内の資産が盗まれるインシデント。約10億円相当の資産が被害に。
Profanity	ウォレットアドレスを生成するツール。秘密鍵の生成プロセスに不備があり、安全でないシード値から秘密鍵が生成されるため、攻撃者によってアドレスから秘密鍵が不正に復元された。

3.3.1 秘密鍵の管理に関する技術開発　Social Recovery

- 秘密鍵のソーシャルリカバリーとは、秘密鍵の紛失や盗難に備えるソリューションの一つ。
- 複数の個人や組織を鍵の「守護者」に指定し、守護者が合意した場合に鍵を変更することができる。



ソーシャルリカバリーの概念図。Ethereum共同創始者Vitalik氏の投稿記事(https://vitalik.ca/general/2021/01/11/recovery.html)を元に作成。

マルチシグからソーシャルリカバリーへ

- 従来より複数人で鍵を管理する手法としてはマルチシグ（multi-signature）が知られている。マルチシグでは、資産を動かすためには複数の秘密鍵による署名が必要*1。
- 一方で、複数鍵の管理が煩雑になったり、全ての取引で複数の鍵による署名が必要のため、使いやすさの点に課題があった。
- ソーシャルリカバリーでは、ユーザは単一の鍵のみを管理すればよく、取引への承認も一つの署名のみ付ければよい。
- 鍵を紛失したり盗難された時の緊急時には、守護者*2（Guardians）と呼ばれる複数の管理者が合意することによって鍵を変更することができる。
- スマートコントラクトを利用する新しいタイプのウォレットに採用が進む（ArgentやLoopring Walletなど）。

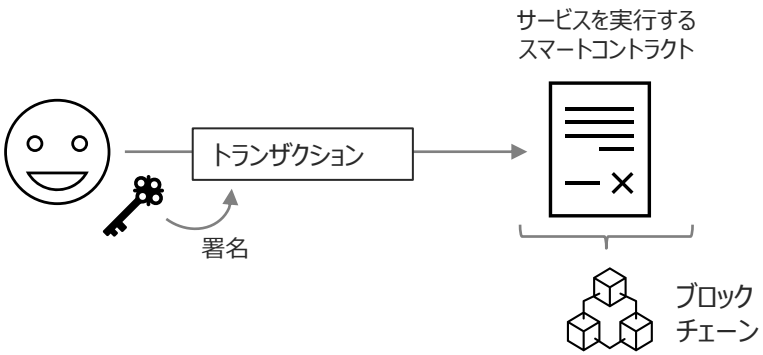
*1 例えば、「事前に作られた3つの鍵のうち、2つの鍵を使って署名」しなければ資産を動かせない。一つのデバイスに保管していた鍵を紛失したとしても、別のデバイスの鍵が安全であれば、資産の盗難は防がれる。
*2 守護者として誰を選ぶかは、例えば次のような選択肢がある。
①友人や家族 ②本人確認等の手段がある機関 ③自身のその他のデバイス

3.3.2 秘密鍵の管理に関する技術開発　Account Abstraction

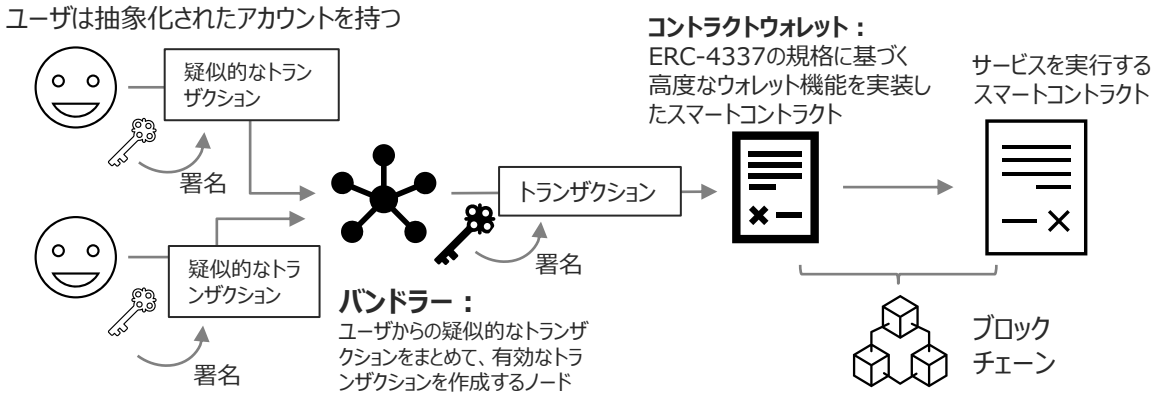
- Ethereumコミュニティにおいては、ウォレットが抱える諸問題に対処するためAccount Abstraction（アカウント抽象化）と呼ばれるソリューションについて、研究開発が進められてきた。
- アカウント抽象化によって、マルチシグ認証やアカウントのリカバリーなど、より柔軟なセキュリティロジックを実装することができる。

ERC-4337によるアカウント抽象化

現状



ERC-4337方式のアカウント抽象化



- ERC-4337はアカウント抽象化を実現する標準化提案の一つで、最も検討が進んでいる。
- 既存のEthereumプロトコルと互換性があり基盤のアップデートが不要。
- ユーザは疑似的なトランザクションを作成する。バンドラーと呼ばれるノードがこれを一つのトランザクションにまとめて実行する。
- 疑似的なトランザクションには秘密鍵による署名が必要だが、秘密鍵の種類（署名方式）は複数の異なる方式から選択可能であり、より柔軟なセキュリティロジックを組むことができる。

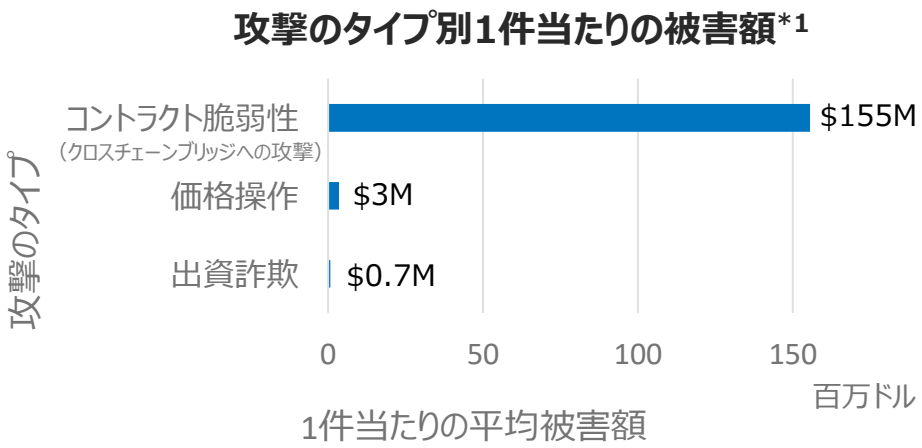
コントラクトウォレットに組み込むことができるセキュリティロジックの例

例	概要
マルチシグ認証	複数の信頼できるユーザまたはデバイスが署名することで取引が有効になる。
アカウントの復元	秘密鍵を紛失した場合に備えて、バックアップ用のアカウントを指定する。バックアップ用のアカウントの承認を経て、アカウントへのアクセスを復旧させる。
ホワイトリストの作成	安全であることが分かっている特定のアドレスへのトランザクションのみ許可する。

3.4 コントラクトの脆弱性利用

- スマートコントラクトはパブリックブロックチェーンに公開されており、脆弱性があると攻撃の対象となる。
- 2022年は特にクロスチェーン・ブリッジへの攻撃が増加。開発者のセキュリティ意識の低さも要因の一つ

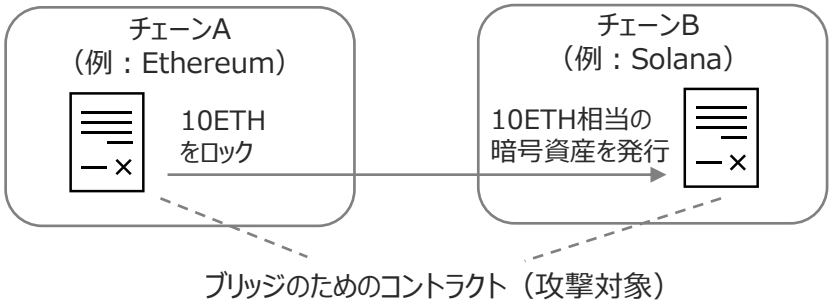
狙われるDeFiアプリケーション



- 技術的な難易度が高く総件数は少ないが、1件当たりの被害額は甚大。
- 透明性を維持するためDeFiで用いられるスマートコントラクトの多くはデフォルトで公開されている。コミュニティによる監査が受けられる反面、スクリプトを解析して悪用できるため、攻撃者から狙われやすい。

*1 CERTIK社レポート(https://indd.adobe.com/view/4bee0f7a-0a74-4223-81b4-af5b56a7b6bb)を元に日本総研作成

クロスチェーン・ブリッジへの攻撃が増加



- クロスチェーン・ブリッジとはユーザが暗号通貨をあるブロックチェーンから別のブロックチェーンに転送するためのプロトコルで、通常元のチェーン上のスマートコントラクトに暗号資産をロックし、2 番目のチェーンで同等の暗号資産を発行する。
- コントラクト自体がブリッジされた資産を支える巨大な”金庫”となるため、攻撃を受けると被害が甚大となる。

根本的な要因の一つとして「DeFiの開発者が何よりも成長を優先し、ユーザを引き付けるためセキュリティ対策に充てられる資金を報酬に回してしまう」と指摘されている*2。

*2 Chainalysis「The Chainalysis 2023 Crypto Crime Report」

3.4.1 コントラクトの脆弱性利用　対策

- これまでのインシデントや脆弱性の解析の蓄積により、スマートコントラクトのセキュリティを高めるためのベストプラクティスは地道に追及されてきた。
- Ethereumコミュニティは安全なコントラクトを開発するためのガイドライン*を公表している。

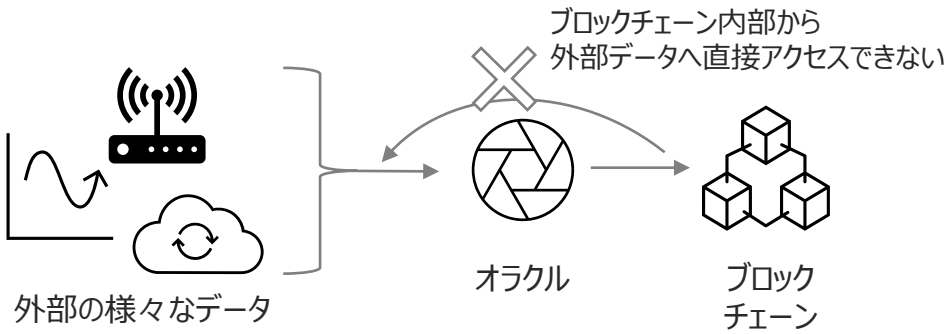
項目例	概要	具体例
適切なアクセス制御設計	コントラクト機能へのアクセスを制限し不正利用を防ぐ	Ownableパターンの採用、ロールベースのアクセス制御、マルチシグウォレットの利用
コントラクト操作を保護するステートメントを使用する	コントラクトに対して問題のある操作が行われた際にコード内部に例外処理などの防御策を講じる	require()、assert()、revert()ステートメントでエラーや例外を検知させ、コントラクトの実行を中止する。
スマートコントラクトのテストとコード正確性の検証	コントラクトは不変性が高いため高品質なテストが必要。単体テストのみらず、いくつかの解析や検証手法を組み合わせて安全性を高める。	静的解析（制御フローグラフ、抽象構文木）、動的解析（ファジング）、形式検証
第三者コードレビューの依頼	監査サービスの利用やバグ報酬金プログラムの利用	監査サービス提供：ConsenSys、OpenZeppelin バグ報酬金プラットフォーム：Immunefi, HackerOne
堅牢な災害復旧計画の実装	悪意のある攻撃や失敗に備えて適切な復旧計画が必要	コントラクトのアップグレードの仕組みを用意（「プロキシパターン」の採用）、緊急停止用の関数を実装、イベントのログ監視
安全なガバナンスシステムの設計	フラッシュローン攻撃等により悪意のある投票でコントラクトのガバナンスが乗っ取られることを防ぐ必要がある。	タイムロックを使用し、特定の時間が経過するまでアクションが実行できないようにする。トークンがロックされている期間に応じた投票の重みづけなど。

* https://ethereum.org/ja/developers/docs/smart-contracts/security/#smart-contract-security-guidelines

3.5 オラクル価格操作

- オラクルは外部データをブロックチェーン内に提供する仕組み*1。クロスチェーン・ブリッジやオラクルなどブロックチェーン外部と接点となるサービスや仕組みは、攻撃を受けやすい。

オラクルとは



- オラクルとは、ブロックチェーンの外部のデータ（株価やセンサー情報、他のブロックチェーン情報など）をブロックチェーン上のスマートコントラクトに提供する仕組み。
- スマートコントラクト単体では外部データ取得のためのアクセス手段（HTTPリクエスト等）を持たない。外部データに基づいたロジックを実行するために、オラクルが代理で外部データを取得し、スマートコントラクトへデータ提供を行う。
- オラクルサービスとしては分散型のChainlinkや中央集権型のProvableなどが知られている。

オラクルの価格操作

スマートコントラクトはオラクルから提供されるデータを信頼する必要があるため、**誤った情報が提供されたりオラクル自体がハッキングを受けるというリスク**がある。また、以下のフラッシュローン攻撃のように、コントラクトに脆弱性がない場合にも**市場操作**によって損害をうける可能性がある。

フラッシュローン攻撃

- フラッシュローンとは、無担保*2で一時的に暗号資産を借りることができるDeFiの特徴的な機能。
- 攻撃者はフラッシュローンで借り入れた暗号資産を元手に、オラクルが管理する価格を人工的に変動させて、不当に安く暗号資産を購入するなどして利益を上げる。（事例：bZxプラットフォーム）

*1　本ページにおける"オラクル"はブロックチェーン周辺技術の用語であり、米オラクル社の提供するOracle Database等の製品との関連はない。オラクル（Oracle）という単語はもともと「神託」や「預言」と言った意味を指す。

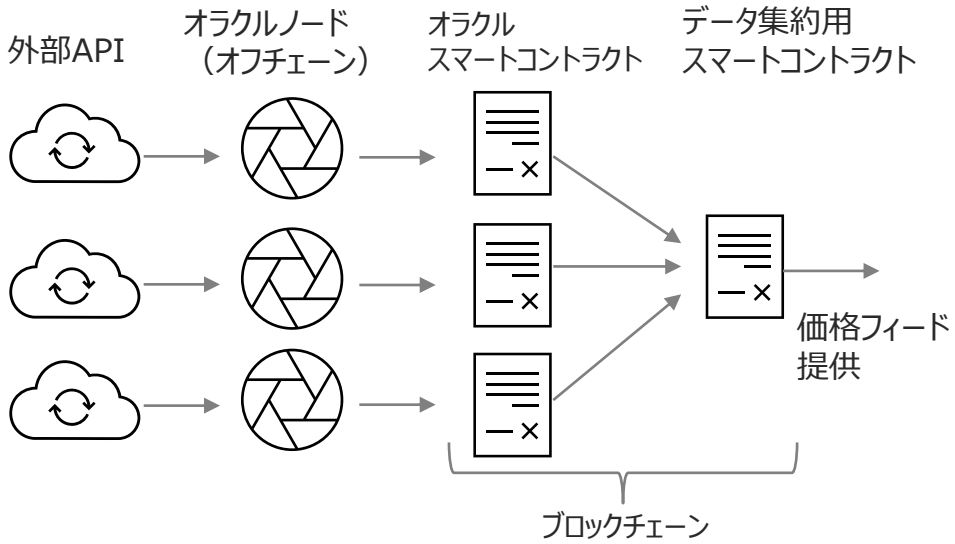
*2 技術的に1回のトランザクションで瞬間的（フラッシュ）に暗号資産の借り入れと返却を実現している。貸し手にはリスク少なく、無担保での借り入れが可能になる。

3.5.1 オラクル価格操作への対策　Chainlink

- Chainlinkは分散型のオラクルサービス。集中化されたデータプロバイダーに依存せず、複数の独立したノードからデータを取得するため、信頼性やセキュリティ高くオラクルを利用できる。

複数のオラクルデータを集約したデータフィードを提供

図出所：https://data.chain.link/ethereum/mainnet/commodities/xau-usd
（閲覧：2023.3.27）



- オラクルへの不正を防ぐ方法として、複数のオラクルからのデータを集約して取得することが推奨される。
- Chainlinkは分散型のオラクルサービスを運営しており、独立した複数のオラクルデータの中央値を算出しデータフィードのAPIを提供している。（各オラクル運営者は「LINK」トークンをインセンティブとして受取る）
- 一方で、Chainlinkが集約しているデータフィードは暗号資産のカテゴリーに偏っており、提供外のデータソースを利用するためには、開発者自身でオラクルの仕組みを構築する必要がある。

4.1 プライバシー・機密性の必要性

- エンタープライズ用途では、機密情報を扱うユースケースにおいてデータプライバシーは必須の要件。
- 従来プライベート型のブロックチェーンでのアプローチが多く行われてきたが、パブリック型でのプライバシー保護技術の開発が進んでいる。

エンタープライズ活用で求められる機密性

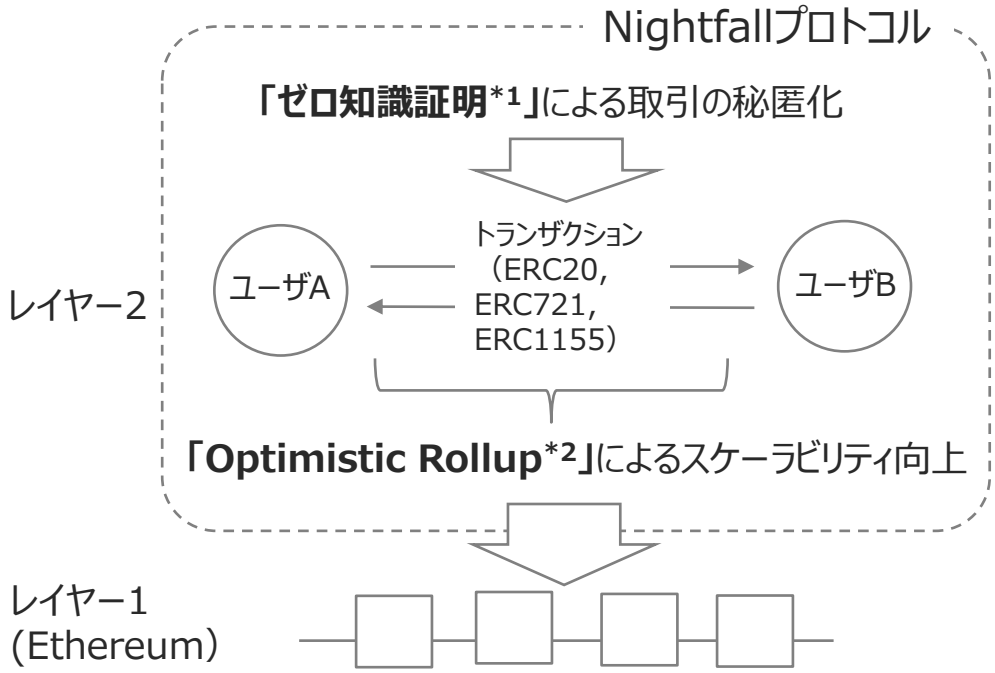
- パブリックなブロックチェーンのPF（レイヤー2含む）において取引（トランザクション）の内容を公開することで、第三者による検証が可能になる。
- 一方で、以下のようなエンタープライズ用途においては機密性の高い情報を扱うこともあり、パブリック利用の障壁となっている。
  - **金融取引において、機関投資家が市場に大きな影響を与えずプライベートに取引を行う。**
  - **サプライチェーンのトレーサビリティにおいて、競合他社へ情報を開示せず発注や在庫情報を共有する。**
  - **ヘルスケア分野において、ユーザの健康状態などセンシティブな情報は限られたエンティティにのみ共有する。**

従来のプライベート型でのアプローチ

- 機密性の高い情報を扱うためプライベート・コンソーシアム型を用いたブロックチェーン活用がなされてきた。
  - **Cordaは取引の当事者のみデータ共有が可能な設計を採用することでデータプライバシーを確保している。**
  - **Hyperledger Fabricはプライベートデータコレクションの機能によりデータの一部を秘匿化できる。**
- 一方で、プライベート型ではネットワークのサイロ化や維持コストの問題がある。
- トランザクションを秘匿化することにより、パブリックブロックチェーンにおいてデータプライバシーを実現するアプローチが模索されている（次頁）。

4.2 プライバシー保護のレイヤー2プロトコル Nightfall

- Nightfallは、エンタープライズ向けにプライバシー保護とスケーリングのソリューションを提供するレイヤー2プロトコル。ユースケースは機密性の高い金融取引やサプライチェーン管理などビジネス用途をターゲットとしている。
- Ernst & Young（EY）社とPolygonが協働で開発し、EY社のブロックチェーンソリューションEY OpsChain等での利用が始まっている。



*1 機密の情報を明かさずに、ある特定の条件を満たすことを証明する技術の総称。ユーザ認証など様々な応用があるが、Nightfallのゼロ知識証明では、取引の内容を明かさずに、トークンや暗号資産が動いたことを証明する技術に用いられている。
*2 レイヤー2のRollup技術の一種。レイヤー2の取引を圧縮して、出金などある時点でレイヤー1に登録する。

ゼロ知識証明とOptimistic Rollupを活用

- Nightfallはトランザクションの秘匿化にゼロ知識証明*1を、スケーラビリティの向上にOptimistic Rollup*2を組合わせたプロトコル。
- Ethereumのメインチェーン上にプライベートトランザクションを記録することが可能。
- 匿名性の高い暗号資産（ZcashやMonero等）に対して、現在マネーロンダリング規制が強まっている。Nightfallにおいては、エンタープライズクラスの「X.509証明書」を必須とすることで**匿名での利用を防ぎつつ、市場や競合に影響を与えないよう取引を秘匿化できる。**

4.3 匿名性とマネーロンダリング規制

- 米国財務省は2022年8月に暗号資産で匿名性を提供する分散型の大手ミキシングサービス「Tornado Cash」を制裁対象（使用禁止および関連する暗号資産の凍結）に指定。北朝鮮のハッカー集団（Lazarus）がTornado Cashをマネーロンダリングに使用していた。
- プライバシー保護を掲げる暗号資産サービスへ規制の圧力は強まっている。

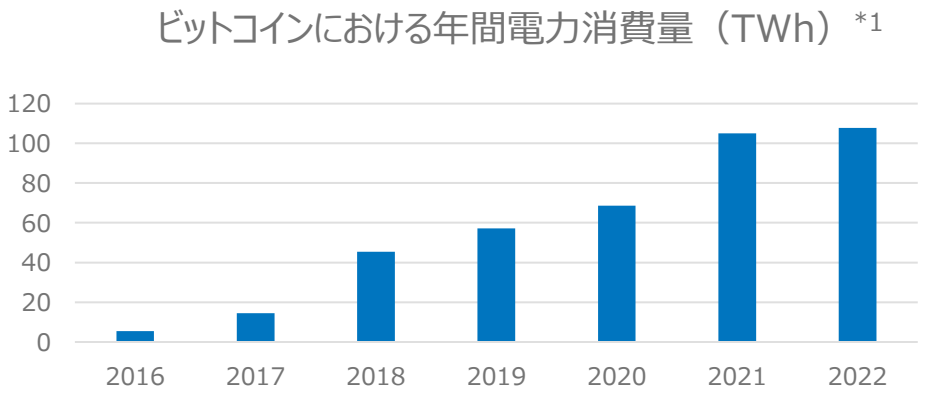
分類	サービス例	仕組み	影響
匿名暗号資産（プライバシーコイン）	Zcash	ゼロ知識証明を使用しトランザクションの詳細を隠ぺい。	• 現在日本の取引所では取り扱いなし。（JVCEA*1の自主規制により禁止） • 2022年9月、大手暗号資産取引所Huobiは各国の規制強化を理由に匿名暗号資産の上場廃止 • 2023年2月UAEドバイが匿名暗号資産を禁止
	Monero	リング署名やワンタイムアドレスを利用してトランザクションの詳細を隠ぺい。	
ミキシングサービス	Blender.io	集中型のミキシングサービス。複数ユーザからの送金された資金を運営チームのプールで混ぜ合わせて新しいアドレスに資金を送金。	• 2022年5月に米国財務省が初めて制裁対象に加えたミキシングサービス。 • 北朝鮮のハッカー集団によるマネーロンダリングの温床となっていた。
	Tornado Cash	分散型のミキシングサービス。ゼロ知識証明を利用して入金と出金の紐づけを曖昧にする。スマートコントラクト上で提供されていた。	• 米国財務省により2022年8月に制裁。不特定多数が分散型で利用するスマートコントラクトへの初の制裁となり、開発者のGithubアカウントや関連するステーブルコインのアドレスも凍結されるなど広範囲に影響した。 • オランダではTornado Cashのエンジニアをマネーロンダリングほう助により逮捕されている。暗号資産業界からは政府の強硬策への批判の声も上がる。
プライバシー特化レイヤー２	Aztec Protocol	プライバシーを重視したレイヤー２プロトコル。レイヤー2上でゼロ知識証明を用いてプライバシーが保護されたトランザクションを実現する。アカウントの匿名性も提供。	• 2022年3月Aztec Protocolを利用したzk.moneyおよびAztec Connectの閉鎖を発表。 • 一部のユーザから規制の圧力による閉鎖ではないかとの疑われていたが、Aztec側は商業的な側面が理由と反論している*2。

*1 一般社団法人　日本暗号資産取引業協会
*2 https://www.coindesk.com/consensus-magazine/2023/03/24/founders-deny-regulatory-pressure-forced-aztec-connect-zkmoney-shutdown/

5.1 電力消費問題

- ビットコインのコンセンサスアルゴリズムであるProof-of-Workは取引の検証（マイニング）に大量の電力を消費し、環境への影響が懸念されている。
- 一部の国や地域では、電力消費の影響を抑制するためマイニングに関する規制を受ける流れ。

Proof-of-Workによる電力消費



- BitcoinのコンセンサスProof-of-Work(PoW)は大量の電力を必要とし、地球環境への悪影響が懸念されている。
- 2022年におけるBitcoinの年間電力消費量は107.65 TWhと推計される*1
- Bitcoinの年間電力消費量は全世界の約0.4%を占めており、1件当たりの取引における電力消費量は国際決済ネットワーク VISAの97万倍である*2

*1 University of Cambridge「Cambridge Bitcoin Electricity Consumption Index」https://ccaf.io/cbnsi/cbeci
*2 Yusuke Kaneko「Electricity Consumption and Environmental Impact Reduction Measures in Public Blockchain」In IEEE ISTAS 2022

法規制と産業界の動き

事例	内容
ニューヨーク州	2022年6月米ニューヨーク州での化石燃料を動力源としたマイニング事業について新たな許可や更新が2年間禁止される法案が可決。
EU委員会	暗号資産市場規制法案（MiCA）において、暗号資産業界に環境や機構への影響に関する情報を開示するよう義務付ける流れ。
カザフスタン	中国での暗号資産の規制に伴い2021年からマイニング業者が流入、同年のブロック生成比率で世界二位を占めた（現在は第三位）。2021年以降、マイニング課税の強化やマイニングの電力源の制限などの規制が強まっている。

- 2021年に中国政府においてマイニングが禁止されると、米国によるマイニングのシェアは上昇。
- 米国ではMarathon Digital社、Riot Blockchain社等のマイニング企業が上場している。
- 環境負荷軽減を推進させるため、暗号資産業界を中心に協議会を発足させる動きも進む
  例：Crypto Climate Accord、Bitcoin Mining Council

5.2 再生可能エネルギーの採用と代替コンセンサスへの移行

- 電力問題の対応策として、マイニングに対する再生可能エネルギーの採用やProof of Workに代わるコンセンサスへの移行が進んでいる

再生可能エネルギーの採用

- 米テスラ社・ブロック社らが太陽光発電でのビットコインマイニングを協業する*1など、マイニングに水力、太陽光、地熱等の再生可能エネルギーを採用していく動きが見られる。
- 一方で、供給源を示す統計値については、機関・研究者によって異なる数字が公表されることもあり、実態の把握が難しい。
  - ケンブリッジ大学の統計値によると、2020年に45.2%であった脱炭素エネルギーの比率は**2022年には37.6%に低下している*2。**これは、水力発電が主であった中国のマイニング事業が2021年に禁止されたためと考えられる。
  - マイニング業界団体BMCは、**2021年4月以降の同比率は50%後半で推移している**と公表*3。

Proof-of-Stakeにより99%以上削減

- Ethereumは2022年9月コンセンサスの方式をProof-of-WorkからProof-of-Stake（暗号資産の保有量によりブロック生成者が決定するアルゴリズム）へ変更し、**年間78TWhのエネルギー消費を0.0026TWhまで縮小***4
- 2023年4月時点で、時価総額Top100の暗号資産のうち、PoWの採用は9%であり、ビットコインの時価総額はそのうちの94%を占めている*5。
- PoW以外のコンセンサスの移行が進むも以下のような懸念もある。
  - PoSやDelegated PoSはトークンの寡占化により分散性やセキュリティ面でPoWに劣る。
  - 米SECのゲンスラー委員長はProof of Stakeを用いた暗号資産は証券規制の対象となる可能性を示唆している*6。

*1 CNBC「Tesla, Block and Blockstream team up to mine bitcoin off solar power in Texas」https://www.cnbc.com/2022/04/08/tesla-block-blockstream-to-mine-bitcoin-off-solar-power-in-texas.html
*2 University of Cambridge「Cambridge Bitcoin Electricity Consumption Index」https://ccaf.io/cbnsi/cbeci/ghg
*3 BMC「GLOBAL BITCOIN MINING DATA REVIEW」https://bitcoinminingcouncil.com/wp-content/uploads/2023/01/BMC-Q4-2022-Presentation.pdf
*4 Ethereum.org「Ethereum's energy expenditure」https://ethereum.org/en/energy-consumption/
*5 CoinMarketCap「Top PoW Tokens by Market Capitalization」https://coinmarketcap.com/view/pow/
*6 CoinDesk「SEC Chairman Gensler Suggests Again That Proof-of-Stake Tokens Are Securities: Report」https://www.coindesk.com/policy/2023/03/15/sec-chairman-gensler-suggests-again-that-proof-of-stake-tokens-are-securities-report/

6.1 技術課題の概況と考察・展望

- 本レポートで述べた技術課題の現況を整理し、下記に考察・展望をまとめる。

課題	概況	考察・展望
スケーラビリティ	初期パブリックブロックチェーン（Bitcoin, Ethereum等）において指摘されていたスケーラビリティに係る問題は、近年発表された新興のブロックチェーン（Solana, Avalanche等）やレイヤー２技術（Optimism Rollup等）において解消が進む。	• スケーラビリティを優先させることによる、他の特性（分散性やセキュリティ）へのトレードオフについては学術的・理論的な研究は追い付いていない側面もある。 • 今後も新興ブロックチェーンやレイヤー2プラットフォームが安定して稼働し続けるかの判断には、更なる検証や実績が必要。
セキュリティ	• 企業運営の中央集権型への取引所からDeFi（分散型金融）のプロジェクトへと攻撃対象が変化している。 • サービス提供側にとっては、成長を優先し、セキュリティへの投資を怠ることが根本的な原因。 • ユーザ側にとっては、秘密鍵の管理が引き続き課題であり、抜本的な技術や解決手段は登場していない。	• サービス提供側においては、コントラクトの監査や品質の向上の取り組みによって、攻撃の被害を減らすことは可能と考えられる。 • ユーザ側においては、ウォレットの安全性を高める技術の開発や普及が望まれる。また、ユーザ自身のリテラシー向上（フィッシングサイトでないか確認する等）も必要と思われる。
プライバシー・機密性	全世界的にマネーロンダリング規制の強化が進んでおり、匿名性を高める暗号資産やミキシングサービスへの風当たりが強まっている。	DeFiなど個人向けのサービスについてはプライバシー保護技術の開発は停滞すると思われる。エンタープライズ向けには、規制と足並みを揃えての技術開発が求められてくる。
電力消費	再生可能エネルギーやProof-of-Stakeなど解決手段は存在している。	技術的な課題は解消していると思われる。マイニング企業での再生可能エネルギーの推進など、社会や法律の要請に応じて進展すると思われる。

6.2 まとめ

- 本レポートにおいて、パブリックブロックチェーンの企業活用に向けての技術課題の現況について「スケーラビリティ」「セキュリティ」「プライバシー・機密性」「電力消費」の観点で調査を行った。
- 技術の進展に伴って、各観点において技術課題は部分的には解消されつつある。特に、電力消費問題については、Ethereumがコンセンサスアルゴリズムへの移行によって、消費量の99.9%以上削減するなど大きな進捗も見受けられる。
- 一方で、技術課題に対するアプローチは複数存在しており、プラットフォーム間（レイヤー2やブロックチェーン群など）の競争は依然として激しい。ただし、マネーロンダリング対策などの規制強化や暗号資産セクターへの投資が落ち着きを見せるなど外部環境も変化しており、今後、数年間で淘汰は進むと考えられる。

パブリックブロックチェーンを活用する際の技術的な留意点

- 活用するブロックチェーン・プラットフォームにおいて、展開するアプリ（主に、スマートコントラクト）の移植性やデータの移植方法について十分に検討することを推奨する。例えば、いくつかのプラットフォームでは、スマートコントラクトの実行環境としてEVM（Ethereum Virtual Machine）を採用しており、プラットフォーム間で互換性あるスマートコントラクトが実現できる。
- セキュアなスマートコントラクトの設計・実装についてはEthereumコミュニティよりガイドライン（P.25参照）が発出されており、事前に対策を施すことで攻撃のリスクを軽減できる。昨今、パブリックブロックチェーンへの攻撃は増加しており入念に備えることを推奨する。