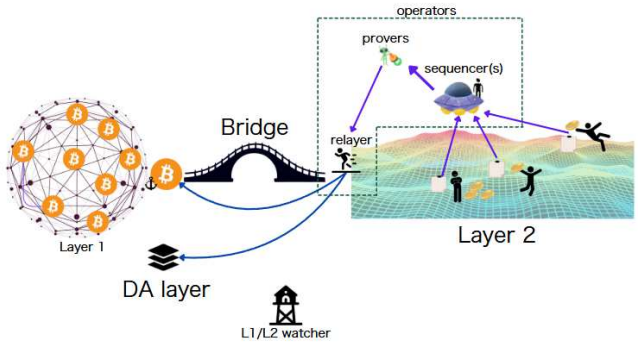
Rollup型 - Bitcoin L2

Bitcoinのトランザクションをオフチェーンでまとめる(Rollup)タイプ。
Rollup は Ethereum で考えられたものなので Bitcoin にそのまま当てはめられない機能もある。



L1からBitcoinをデポジットしてL2で使えるコインを発行してもらう。
L2ではそのコインを使って送受金する。
L2でのコインをwithdrawする場合、ユーザはオペレータ(operator)が指示する方法でコインをburnさせ、オペレータはそれを確認したらL1でBitcoinにしてユーザに支払う。

L1とL2を橋渡しする機能をブリッジ(bridge)と呼ぶ。
オペレーターは役割として「シーケンサー(sequencer)」「プローバー(prover)」「リレイヤー(relayer)」に分かれる。

L2でのアカウントの残高のようなステート変化を記録するストレージのようなものを「DAレイヤー(Data Availability Layer)」と呼ぶ。DAは情報用語で「データ可用性」と訳される。ブロックチェーンでは、そのチェーンを検証することができるデータそのものや、それを保存していること、検証方法などをひっくるめて使うことが多い。Ethereum の場合は L2 のステート変化を L1 に保存することが多い。スマートコントラクトで検証するので同じ場所にある方が都合がよいのかもしれない。
Bitcoin の場合はブロックサイズに制限があるので L1 を DAレイヤーとする L2 はないと思われる。本来であればすべてのステートを再現できるようにフルノードデータのような全部を保存するのかもしれないが、ゼロ知識証明によって正しいことを証明したデータだけにせざるを得ないようである。Bitcoinスクリプトで検証する計算ができないのも理由に挙げられるだろう。

Optimistic Rollup

不正の申告期間を持ち、その期間に誰も不正申告チャレンジがなければ正当と見なされる。チャレンジがあればオペレーターが正当であることを証明する。
BitVMは正直な人のChallengeで成り立つので Optimistic な感じだが、そもそも BitVM2 は Rollup 技術ではない。
ただ、Bitcoinで「zkRollup」と言った場合でも BitVM2を使っていたのであれば純粋な zkRollup ではないことになる。

zkRollup

zkSNARKやzkSTARKなどのゼロ知識証明を使うプロジェクトがほとんどだが、現在のBitcoinスクリプトでZKPの検証はできない(BitVMを使うことでできるようになるかも？くらいな感じ)。
BitcoinのZKPプロジェクト - ChatGPT

EthereumのL2はスマートコントラクトでZKP検証まで行えるが、Bitcoin内でZKPの検証を行わない/行えないので Sovereign Rollup などと呼んだりする
- From Sovereign Rollup to zk-Rollup - Untold Story of Bitcoin Layer 2
  - Citrea - Bitcoin L2 は zkRollup と主張しているが、ブリッジはマルチシグのままだし、L1 に Inscription としてZK証明を書き込んではいるが Bitcoin上では検証してないし、 Sovereign Rollup のままだよと言いたいのかな。
    - Clementine v2 では BitVM ブリッジを脱却しようとしているが、それでも l1 で ZK検証できないなら同じだろう。

zkRollupと検証

ZKデータをL1に置いて検証するときはDA層のデータがなくても検証だけできるらしい。ただ、検証したデータが検証しようとしたL2のデータかどうかはわからない。ただ外部DA層を持つのは費用もかかるしプロジェクトとしては多くないのではないか。

- 検証で使う3要素(ここにDAデータは含まれない)
  - 公開入力(Public Input)
    - 以前の状態と今回の状態(State Rootというハッシュ値だけだそうだ)
  - ZK証明(Proof)
    - proverが生成した証明データ
  - 検証鍵(Verification Key)
    - L2のルールが書き込まれた数式

- 検証
  - 確認できること

以前の状態から今回の状態に変化するまでにルール違反はなかった
計算の根拠となるDAデータをproverが持っていた

確認できないこと

誰が誰に送金したのかなどの具体的な中身
自分の今の残高
L1へ資産を戻すための証明

個別調査

Starknet - Bitcoin L2

Citrea - Bitcoin L2、Citrea (2) - Bitcoin L2

Bitlayer - Bitcoin L2

2024年はサイドチェーン(PoS)だが BitVMを採用した Rollupを開発中

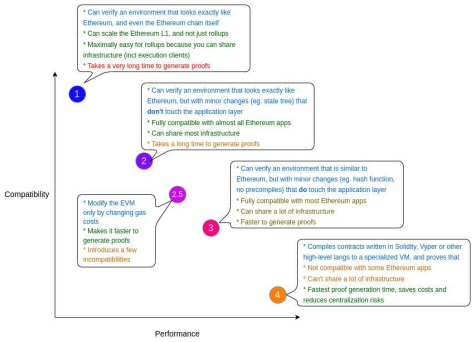
B2 Network - Bitcoin L2

---

zkVM

zkVM - ChatGPT

Layer2 のためのチェーンというかコンピュータがいる。
ZKP の Virtual Machine なので zkVM。EVM互換であれば zkEVM という。
なお zkEVM は Vitalik によるタイプ分類 がある。



zkevm type

タイプ	内容	プロジェクト例
Type 1	完全にEthereumとバイナリ互換（難易度高）	無し（理論上のみ）
Type 2	高度なEVM互換（実装最適化なし）	Scroll（近い）
Type 2.5	一部最適化・ガスコスト削減	Linea, Scroll
Type 3	ソースコードレベル互換だが内部構造は非互換あり	Polygon zkEVM
Type 4	Solidity互換コンパイラを使用しEVMバイトコードには非互換	zkSync Era（custom Yulコンパイラ）

EVM互換のチェーンを使うことが多いが、そうではない有名なプロジェクトもある。EVM互換の利点は MetaMask のような EVMの資産を使うことができるところである。

zkVM とかなんとか

zkVM技術の比較とユースケース(途中までしか読めない)｜zkEVM、zkWasm、RISC Zero - HashHub Research

著名な zkVMプロジェクト - Googleスプレッド

zkevm

```
zkRollup
├── zkEVM（EVM互換あり）
│   ├── Polygon zkEVM
│   ├── Scroll
│   ├── zkSync Era
│   ├── Taiko
│   └── Linea など
└── zkVM系（EVM非互換）
    ├── StarkNet（Cairo）
    └── zkSync（custom VM）
```

その他ライブラリ

RISC ZERO

RISC-VアーキテクチャをベースにしたzkVMらしい

zkSTARK系 prover

zkSTARK-to-zkSNARK wrapperが2023年11月に実装済み？

使用プロジェクト

Citrea - Bitcoin L2

Sovereign SDK - ChatGPT

Sovereign Labsという会社がやっている Rollup SDK

オープンソースで開発中(2025年6月現在)

VM は持っておらず、RISC ZERO や Reth などを選択できる

DA層も持っていないので、Celestia - Bitcoin L2 や EigenDA などを利用する

汎用インターフェースにしているので対応がしやすくなっている

Citrea - Bitcoin L2 の Chainway社が DA層アダプタをオープンソースにしたという記事がある

立ち位置としては、Rollkit や FuelVM になるそうだ

Cosmos SDK の設計に似ているそうだ

使用プロジェクト

?

Reth - ChatGPT

Paradigm

Ethereum のフルノード実装。 `geth` の代わりになることも出来るくらい。

各コンポーネントが疎結合なので、他のプロジェクトが一部だけ使うということができる。

いろいろ使われていそうだが、表立って「使っている」と書かないくらい Rust のプロジェクトでは使われているもののようだ。

Succinct

Proofer / Prover

使用プロジェクト

Citrea - Bitcoin L2

Polygon zkEVM

Polygonシリーズの1つ。Ethereumで稼働中。

ブリッジはあるがEthereum L1向け。

DA層はEthereum L1を使う。

今はcdk-erigonリポジトリか？

使用プロジェクト

B2 Network - Bitcoin L2

ZKsync Era

ZKsyncシリーズの1つ。Ethereumで稼働中。

ColliderVM

StarknetのXを見てたら出てきた

BitVM2がオフチェーンで処理して fraud-proof で処理するところを、Bitcoinスクリプトにして zkRollup 風にできる

オンチェーンサイズが大きいが正直なオペレータが不要

まだ研究段階か？

不正

不正をした - ChatGPT

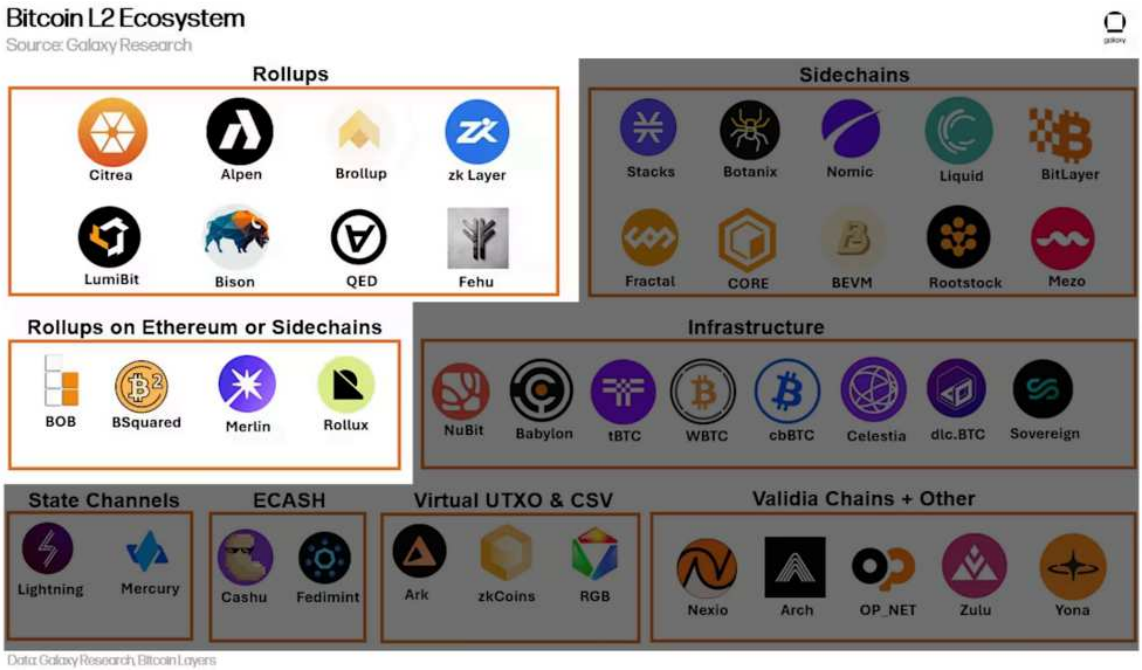
(参考)Ethereumでの不正検出

L2 はオペレーターの管理下でユーザはほぼいいなりになる。オペレーターによって不正が起きると、どうなるのかは気になるところである。

自力の調査ではないが、読んだ限りでは L2 の不正対策は難しいし現状では未対策なところが多い。

ステートが遷移すればそれを検証することで不正を訴えることはできるだろう。しかしシーケンサーによる不正というか検閲というかは証拠が残りにくい。

2024年11月20日 Galaxyレポート Bitcoin L2s



「Rollups on Ethereum or Sidechains」は Rollup に分類して良いだろう。