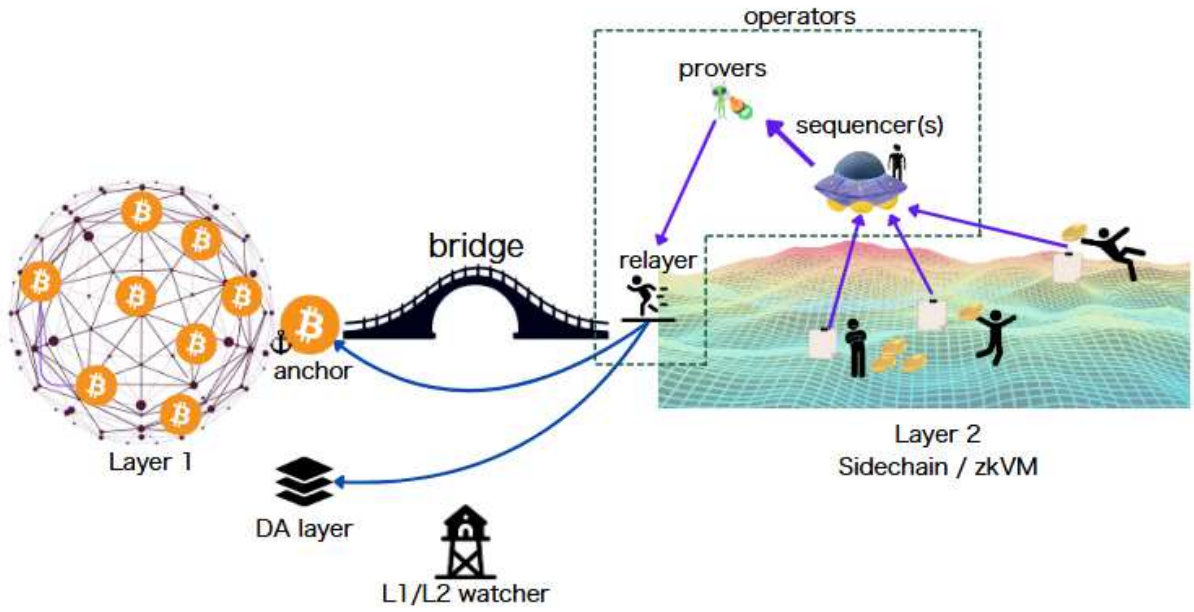
Bitcoin L2調査



おおよその構成(ChatGPT)

L2 がzkVM の場合、ほぼアカウントモデルになると考えて良いだろう。つまり Ethereum のようなチェーンがあると思えば良い。各アカウントのamountなどの状態(ステート)が送受金で変化するのでそのステートの変化を DA層に記録する。

ステートの変化をまるまる記録するのか、Merkle ルートのようにしてまとめたデータ(ステートルート)だけを記録するのかは L2プロジェクトによって異なる。だいたいの場合 L2 上のブロック生成は L1 よりも短い間隔で行われ、ステートの変化もその分発生する。

- Layer 1 : Bitcoinネットワーク
- Layer 2 : サイドチェーンやEthereum互換のVMなどによるネットワーク
- bridge : L1 と L2 を行き来するためのしくみ。
  - peg-in : L1 --> L2
  - peg-out : L2 –> L1
- deposit : ユーザは L1 で deposit して peg-in することで L2 に参入することもできるが、直接 L2 の運営になんらかの支払いをして L2 上で直接受け取ることもできるだろう。
- L1/L2 watcher
  - peg-in / peg-out のために L1 を監視したり L2 を監視したりする。
- L2管理者
  - Sequencer
    - 役割

        - ユーザからのトランザクション受け取って整合性チェック
        - トランザクションの順序を決め、L2ブロックを作成
        - L2ブロックを生成したのでステート変更を反映
            - ステートというのは、
        - L1に対してステートルート / zk証明を展開する準備
    - 複数 Sequencer のプロジェクトはほぼない。類似系なのが Rootstock、Botanix、Spiderchains など。
- Operator
    - 役割
        - L2 ブロックの状態を L1 に反映
        - zk証明や fraud proof などの L1に展開するデータを生成、管理

決済の完了

L2 上で送受金を行った決済の完了をいつと見なすのかは立場による。

- L2 上のブロックにトランザクションが取り込まれた
    - 一番早いが、Sequencer が偽って後から取り込まないブロックを作ってしまう余地はある

L2の個別調査

- 比較表
- Rollup型 - Bitcoin L2
- サイドチェーン型 - Bitcoin L2
- BitcoinL2 それぞれの Bitcoin L2を個別に調査したページ

DA層

- Celestia - Bitcoin L2

BitVM2の立ち位置について

この分野では BitVM の話が良く出てくるので最初に書いておく。

BitVM自体は Bitcoin スクリプトが現在の仕様の範囲にありながらチューリング完全なプログラムを動かそうとしているプロジェクトである。Layer2 用のプロジェクトでもないし ZKP のプロジェクトでもない。
紛らわしいことに、BitVM2 の応用例としてブリッジのデモが実装されてリポジトリに入ってい

る。また、サンプルとして ZKP検証するコードも入っているらしい(未確認)。また、BitVM2 はオンチェーンのサイズが大きく、そこまでして動かしたい複雑なスクリプトとなると ZKP 関係くらいしかないのだろう。
そういう事情があって BitVM と Layer2 が近しい感じに思われるようになったのだろう。

BitVM2ブリッジは L1 も使って正当性を確認することが出来るので L2 だけで行うタイプよりは信頼性は高いかもしれない。しかし、Challenge されない限りはそのままだし(Optimistic)、デポジット額が固定になるという制約がある(他にも制約はいろいろある)。

分類

- State Channel系
  - Lightning Network
    - RGB - Bitcoin L2
- サイドチェーン型 - Bitcoin L2
  - Liquid
  - Rootstock
  - Bitlayer(2024年版)
- Rollup型 - Bitcoin L2
  - Optimistic Rollup系
    - BitVM がこの系統で、誰か1人でも正直な管理者がいて嘘つきがいたら不正報告をChallengeする
      - BitVM2 bridge は BitVM2 技術を使ったブリッジであって L2ではない。
    - Bitlocker(2025年版)は BitVM2 bridgeを使うようなので Optimistic Rollup系になるのかな？
    - Citreaのブリッジは Clementine というが、v1 では BitVM2 を使っているのでこちらになる？
      - Citrea 自身は「初の zkRollup」と自称しているので、違うやんって思われている節がある
  - zkRollup系
    - ほとんどがこちら。
    - Ethereumと違ってBitcoinスクリプトではZK証明の実行が出来ないので、オフチェーンで証明計算した結果だけをオンチェーンに載せる方式を採る。
      - オフチェーンだけで検証する方式をSovereign Rollupと呼ぶ
      - BitVM2 でZK検証する L2だったとしても、BitVM2 は L1も使うので、Sovereign Rollup というわけではない。が L1 で完結するわけでもないから Ethereum のような Validity Rollup でもない。Optimistic な側面もある。

- Ark - Bitcoin L2
- Stacks - Bitcoin L2

基礎

- A Beginner's Guide to Bitcoin Layers
- Bitcoin Layers
- Sovereign Rollup
- ゼロ知識証明
- zkSNARK
- zkSTARK
- ステーキング
- BitVM
- 胡散臭いL2プロジェクトの特徴

AI

- Bitcoin L2 - ChatGPT(随時更新)
- Bitcoin Layer2プロジェクトの調査 - 2025/05/29(Gemini Research)
- Bitcoin L2プロジェクト - NotebookLM

L2方式はいろいろあるがやりたいことは主にこれら。

- スケーラビリティ
  - L1 が約 7 txs/sec と言われている
  - VISAの決済システムが 1700 TPS と言われているので、同等以上(数千から数百万)にしたい
- 手数料の削減
  - 取引をオフチェーンで行い、複数の取引を何らかの形でバッチ化してL1に記録を残すようにすることで削減
- 機能性の強化
  - L2 でスマートコントラクトを扱えるようにするなど