EthereumのL2

BitcoinのLightning Networkは2者間で MultiSig を作ってデポジットし、その後は LN上でやりとり、最後はチャネルをクローズする、という流れだった。
EthereumのL2はどうなっているのか？ いろいろパターンがあるかもしれないので、今調べているStarknet - Bitcoin L2がRollupなので、それについて調べる。

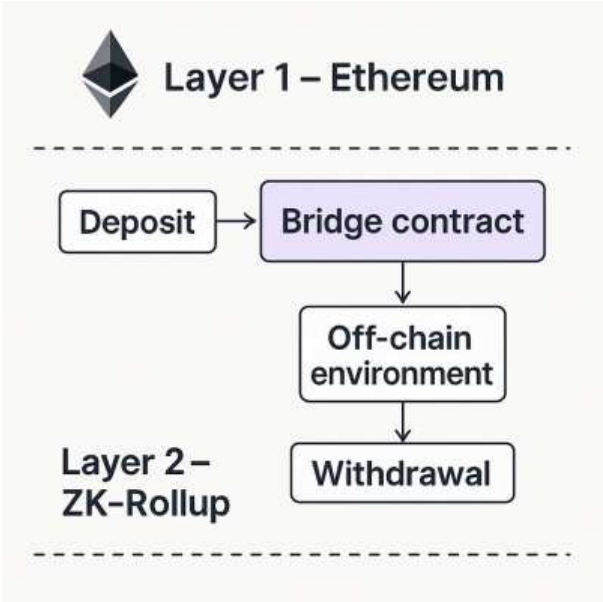
ChatGPT

zkRollup - ChatGPT
zkRollup（ZKロールアップ）を使う場合、最初に**Layer1（Ethereumメインチェーン）からLayer2（zkRollup側）へデポジット**する必要があります。

正確には、あなたの資産（ETHやERC-20トークン）をLayer2用のスマートコントラクトにロック（預け入れ）します。
このロック情報をもとに、Layer2側で取引や送金ができるようになります。
つまり流れはこうです：

1. Layer1上の**ロールアップのブリッジコントラクト**に対して資産を送る（＝デポジットする）
2. その証拠を元に、Layer2のオフチェーン環境であなたのアカウントに反映される
3. あとはLayer2内で安く・高速に取引できる

最終的にLayer1に資産を戻したいときは「Withdrawal（出金）」という形で、またブリッジコントラクト経由で引き出します。
要するに、「預ける→Layer2で動かす→必要なら引き出す」というのが基本的な運用です。



用語: データ可用性(Data Availability)

L2の状態を再構成するために必要なデータが、誰でもアクセス可能な状態であること。

感想

Ethereumはアカウントモデルなのでスマートコントラクトのアドレスは同じでも複数の人がそれぞれ支払っても別々の処理することができる(コントラクトののコード中で見分けられる)。

BitcoinはUTXOモデルなので同じスクリプトアドレスに支払うことは可能。ただEthereumのように支払ったら自動でスクリプトが実行される訳ではない。スクリプトに支払ったら、その支払いを使うときにスクリプトを解いて別のアドレスに送金する。スクリプトでは誰から送金されたとか誰に送金するだとかは見ることができない。

このようにコントラクトが動作するタイミングやコントラクトの中で見えるデータがずいぶんと異なる。

L2での不正を検出するしくみ

ChatGPT

主な不正

- 自分のL2入金がL1に投稿されているのに、L2のステートに反映されていない（Sequencerが無視している）
- 他人の送金がL2上で不正に改ざんされている（署名なし転送など）

基本

DA層(Ethererum L1)にトランザクション情報が公開されているので、それを確認する。

zkRollupの場合はステート遷移を zkSNARKなどで証明するので不正はしづらいが、Sequencerがスルーするとそもそもステート遷移が発生しないので暗号的証明に影響しないことになる。送受金したふりというのは難しいので、Gas代不足などで認めないようにしたり、順序を入れ替えてトランザクションを意図的に後回しにするなどはできる。「悪意による検閲か」「偶発的な遅延か」の区別は難しいという感じ。

例

CoinbaseのBase - ChatGPT

乱立してない？

ChatGPT

立ち上げることに対しては静観。

StarkWare や Optimism が Rollup を標準化しようとしている。

Rollup以外のL2

- State Channels
  - LN っぽくチャネル間でやりとりして結果だけ L1に書き込む
  - Raiden Network など
- Plasma
  - 子チェーンを作って定期的に親チェーンにまとめて確定(Rollupと違うの？)
    - L1 に書き込むのは Validator が使えないようなハッシュ値で Sovereign Rollup みたいな感じ。
  - OmiseGO Plasma など
- Sidechains
  - いわゆるサイドチェーン
  - Polygon PoS など
- Validium / zkPorter
  - オフチェーン型ZKでデータをチェーン外に持つ
  - StarkEx(Validiumモード)、zkPorter(StarkWare提案)など