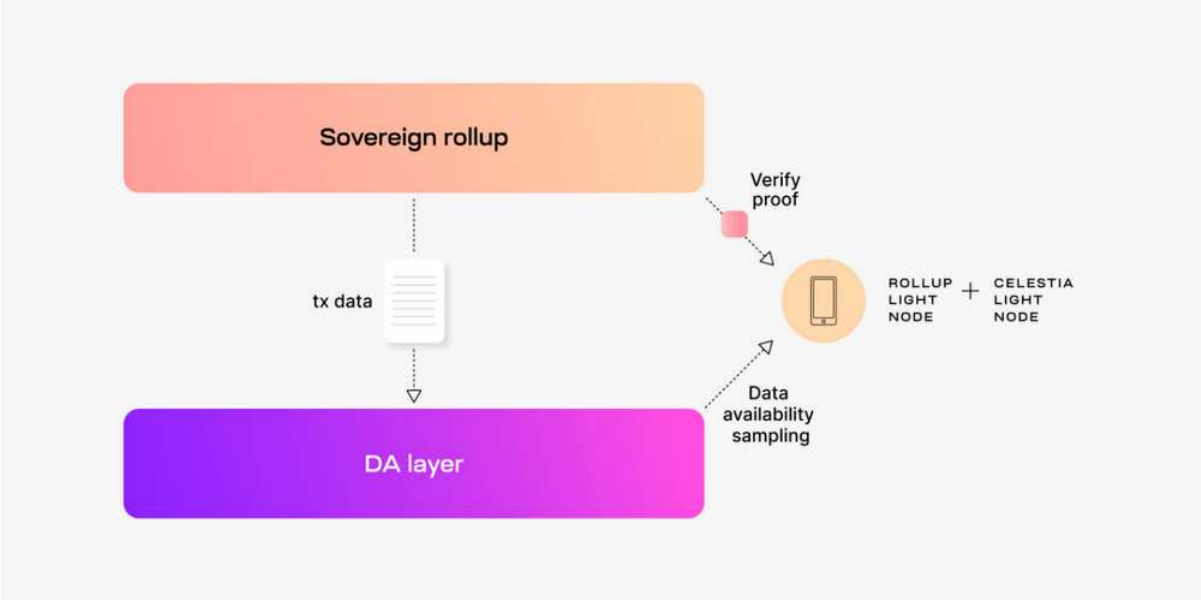
Sovereign Rollup



ChatGPT

Grok

Sovereign Rollup とは、「自分自身（＝Rollup側）で状態の有効性を判断できるLayer2構造」のこと。

L1に依存するのは「データ可用性（Data Availability）」だけ

ステートの解釈（＝有効性検証）はRollupが主権的に行う

スマートコントラクトによる"verification"ではなく、Rollup自体が自律的に状態を検証

Smart Contract Rollup と Sovereign Rollup という分け方のようだ

決済完了は Smart Contract Rollup は L1 のスマコンが実行されて受け入れられたとき、Sovereign Rollup は L2 で完了する。

Sovereign Rollup はそういう意味で自由度が大きいが、L1 にほとんど頼ることができないのでセキュリティなどで弱くなりがち。

rollups

特徴	Ethereum系 zkRollup	Sovereign Rollup
ZK Proof	L1のVerifierコントラクトが検証	L1はProofを検証しない（もしくはできない）
実行環境	L2（EVMなど）	任意（WASM、RISC-Vなど）
状態の有効性	L1が最終判断	Rollupチェーン自身が主権的に判断
L1との関係	スマコンを通じて密結合	データ保存のみの疎結合

L1の例	Ethereum	Bitcoin, Celestia, EigenDA など

Layer1 では検証できないBitcoinでは**どうしてもこの構造にせざるを得ない**。

- Ethereumのようなスマートコントラクトが存在しない
  - zkSNARKの検証をon-chainで行うのが不可能
  - 状態マシンをL1で直接運用するのが難しい

Layer1 に書き込むデータの例

- 状態遷移の履歴（新しいブロックの情報）
  - ブロックのヘッダー情報：Rollupブロックの番号、前ブロックのハッシュ、タイムスタンプ
- ZK証明（該当する場合）
  - ZK証明（オプション）：証明文字列（Proof）や公開入力（Public Inputs）
- ブロックのハッシュやMerkle Root
  - 状態のMerkle root：状態ツリーのルートハッシュ（=状態全体の要約）
  - トランザクションデータのハッシュ：各トランザクションのMerkle rootなど
- （必要に応じて）データへのポインタ（オフチェーンDAの場合）
  - カスタムポインタ：データの全文は外部ストレージ（IPFS等）に保存、そのハッシュだけ投稿する場合もあり
- プロジェクトごとの具体例
  - Citrea：Bitcoin上にOrdinalsのInscriptionsで記録
    - Rollupブロックヘッダー（番号、前ハッシュ）
    - 状態のMerkle root
    - ZK-SNARK証明（Groth16など）
  - Rollkit（Celestia向けだがSovereignモデル）：CelestiaのDAレイヤーにBlobを直接保存
    - 状態のMerkle root
    - トランザクションのMerkle root
    - 任意のBlobデータ（Celestia DA上）
  - Sovereign SDK + Bitcoin：BitcoinのOP_RETURNにハッシュを投稿、実体は外部DAネットワーク or P2Pで配布
    - ブロックごとのMerkle Root
    - 各ブロックのZK証明

Layer1 に書き込むときのトランザクションデータ

- `OP_RETURN` （最大80バイト）
- TaprootのTapscriptやScript pathの利用

Ordinals / Inscriptions（通称「Bitcoin NFT」）

Citrea はこれ

オペレーターが不在になったとき

オペレーターは誰でもなることができる

ブロックを作ることができる

ZK証明の生成が重たい

トランザクションがないときは作らないなどそこそこ自由度がある

状態データとZK証明があれば誰でも再構築できる

運営主体以外のフルノードが多数いないと

検証者(=クライアント)は1つのチェーンしか正当と見なさない

雰囲気としてはマイニングに似ている

複数のブロックが出た場合はだいたい最長のチェーンを選ぶ

オペレーターが不在になって困るのは、peg-in / peg-out ができないこと

BitVM2との相違点

Sovereign Rollup が Rollup 側である Layer2 で検証するのに対し、BitVM はオフチェーンでの検証結果を L1で確認だけ行う。

なので完全な Sovereign Rollup ではない。

Layer1 で Rollup 検証する方式かというと、Challenge されて Assert フェーズで証明を行うので、厳密にはそうでもない。

つまり、その中間くらいの方式である。

心配な点

peg-in / deposit で送金するアドレスが信用できるのか。

~~自分の送受金をシーケンサーに無視されたときに何ができるのか。~~

~~同様に、オペレーターが我々をだましたときに何ができるのか。~~

L1に現状報告のようなデータを載せたとしても、オンチェーンで検証できないのであれば載せる意味はあるのか。

嘘の報告を載せるなら、信頼できないプロジェクトだという証拠になる？

peg-out / withdraw を拒否されたり額が異なったりされることはあるのか。

~~オペレーターが不在になったときに何ができるのか。~~

最低でも現状の額は取り戻したい。

~~Data Availability Layer はオフチェーン上にあるので、それをローカルで持っておくと復元可能？~~