B2 Network - Bitcoin L2

#BitcoinL2

B² NETWORK

https://www.bsquared.network/

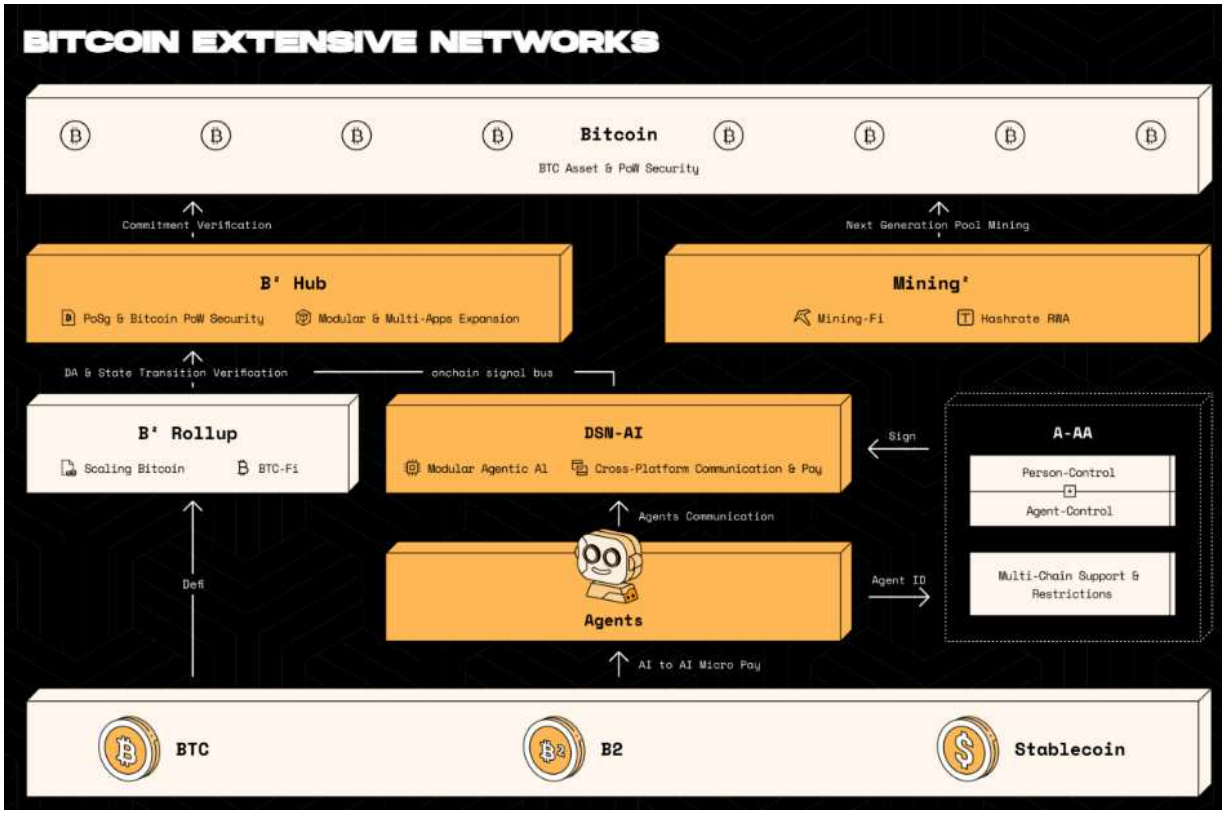
https://blog.bsquared.network/

https://github.com/b2network/b2-zkevm-node

Polygon zkEVMをforkしている

これを書いている時点でforkしたリポジトリは public archive になっていた

ChatGPT



概要

2024年4月30日からmainnet運用

EMV互換

L2もブリッジもBitVM未使用

チャレンジ・レスポンス方式

チャレンジできるのは B2 Node のみ

B2 Nodeを立てるハードウェア要件はけっこう高い

承認されないと参加できなさそう

zkRollup であるが、zkSNARKなのかzkSTARKなのかドキュメントにない

実装がPolygon zkEVMをforkしている。

zkSTARKとzkSNARKのハイブリッド方式で、zkSTARKで証明データを作成した後、その証明データの正しさをzkSNARKで証明する。

ユーザは検証できなさそう

Peg-In

ユーザが Peg-inアドレス(マルチシグ or Taproot)に送金

シーケンサーが L2トランザクションに対するコミットメントを生成

zkRollupバッチの一部として資産を反映

Peg-Out

ユーザがL2上でpeg-outトランザクションを生成

zk-proof と fraud-proof により L2の状態整合性を Bitcoin L1上で確認

チャレンジ期間を経て問題なければ Bitcoinのユーザに返却

オンチェーン確認は Taproot commitmentを参照して行う

DA層はBitcoin L1

Polygon zkEVM を fork してノードを作っているが、Ethereum L1を想定しているのでブリッジもDA層も自分でやったんだろう。

https://docs.bsquared.network/architecture

