Bitlayer - Bitcoin L2

#BitcoinL2



https://www.bitlayer.org/

https://github.com/bitlayer-org

ロードマップ

Bitlayer - ChatGPT

BitlayerはBitVM2をメインで開発していると言ってもよいレベルである。

2025/12月付近の情報

Bitlayer v2に移行した？ まだ一部だけ？少なくとも運用は開始済みである。

Peg-Inごとにインスタンスを作るタイプだそうだ。そしてそのインスタンスはPeg-Outまで使われるらしい。ユーザ管理的なものではなくUTXO管理と思っておけば良い。
クラウドのVMインスタンスのことではなく何か論理的な単位らしい。
Peg-Outは自分の Peg-Inより大きい額を YBTC で持っていても可能で、その時はオペレーター(brokerというらしい)が burn対象の Peg-Inを使ってPeg-Outするそうだ。Peg-InしたUTXOもちゃんと減らすらしい。
AI回答なので全部を正しいと考えるのは良くないが、そこまで大きくは違っていないように思う。
https://grok.com/share/c2hhcmQtMw_13c7e49c-a904-4ad7-8585-8a2ea62f1ac5

Peg-Out時は先にbrokerがユーザに支払うので多重支払いをどう防ぐか気になったが、Geminiによると
　リクエストを実行するには「予約」が必要というしくみで、それはL2ステートを使っているだそうだ。EthereumのようなL1だとコストがかかるよなあ。
中央データベースの代わりに L2 を使っているからノード間の共有が不要なだけである。

Bridge Protocol

2025/07月付近の情報

Mainnet-V1はサイドチェーンだが Mainnet-V2でRollupに変わる

2025/07/15に v2リリース済み Bitlayer's Biggest Reveals at Summer Launch 2025: BitVM Bridge Mainnet, Bitlayer Network V2 Whitepaper, and V3 Preview - Bitlayer Blog

マルチVM対応の L2プラットフォーム

マルチVMになるのは Mainnet-V2 以降(対応は2025年後半→2025/07/15 に Mainnet-V2リリース)

現時点(2025/06/20)では EVMのみである

プラットフォームではあるが汎用プラットフォームではなく運営主体がある。自由には作ることはできない。

EVM/Cairo/Move/Solanaなどを並列サポート

同じ L2上で扱うことができる

2025年3月にBase, Arbitrum, Starknet, Plume Network, Sonicと戦略提携(記事)

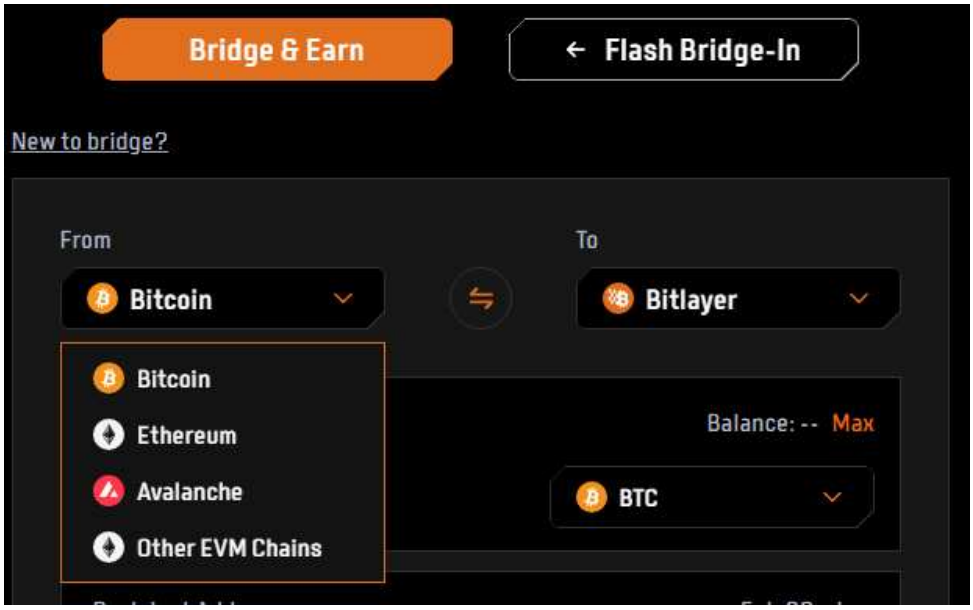
Bitlayer--Bitcoin 間は BitVM bridgeで、Bitlayer–Ethereum や Bitlayer–Sui はまた別のブリッジ(Chainlink CCP や独自ブリッジなど)

運営チームがシーケンサーを運用しているので中央集権的なところがある

ロードマップ

BitVM を本番運用にしようとしているところらしい(2025/06/20)

今は Mainnet-V1 として Bitlayer PoS が動いている。bridge は Centralize している。



Mainnet-V2 で BitVM bridge にする。2025年Q1-Q2 とのこと。だがもう6月なのでQ2終わりかけだ。

2025年Q4 でTPSなどのパフォーマンスなどを向上させる

BitVM2

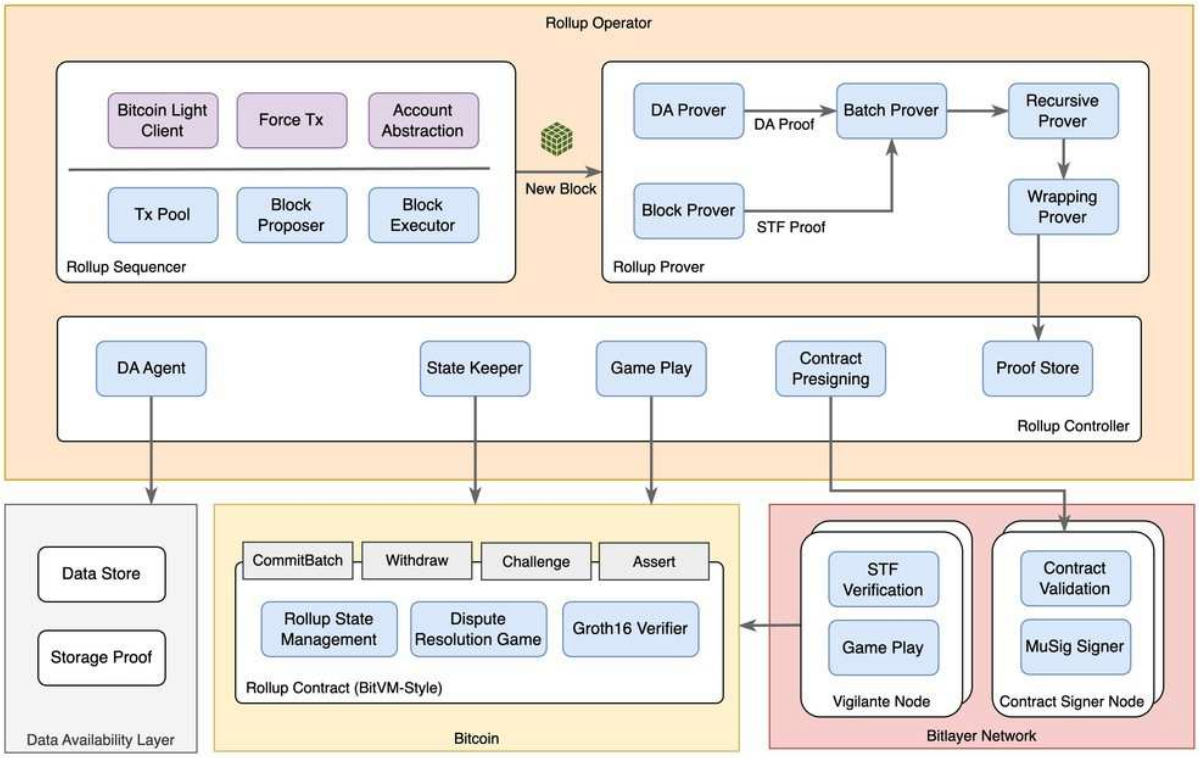
ホームページのトップに「THE FIRST BITVM」と書くくらいに BitVMを推している。

BitVMに対する貢献も多いらしい。

L2 とブリッジのそれぞれに BitVM2 技術を使っている。
いわゆる Bitlayer v2 から BitVMを使うようになった。それまでの Mainnet-V1は PoSだった。

システム側

https://docs.bitlayer.org/docs/Learn/Bitlayer%20Rollup/system-design



ブリッジ側 (このときはまだv1だった)

https://docs.bitlayer.org/docs/Learn/Bitlayer%20Rollup/bridge

BitVM2 bridge は使わず、OP-DLC(**OP**timistic **D**iscrete **L**og **C**ontract)

実装

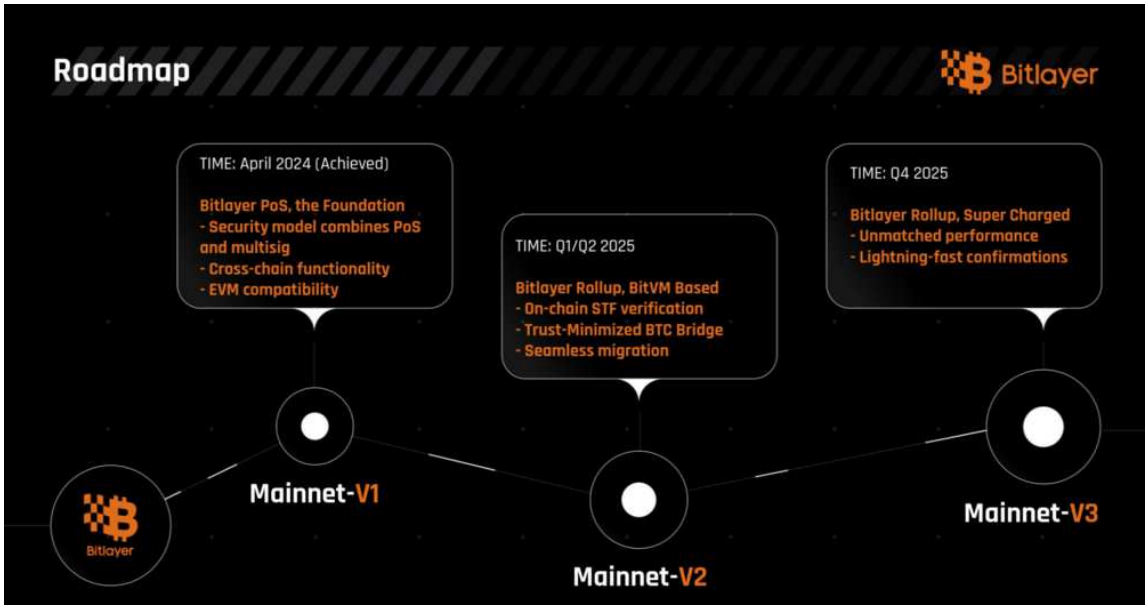
L2 の bitlayer-l2 は gethベース(v1.13.9の1commit前)から自分で改造している。

ロードマップ

2025/10/06

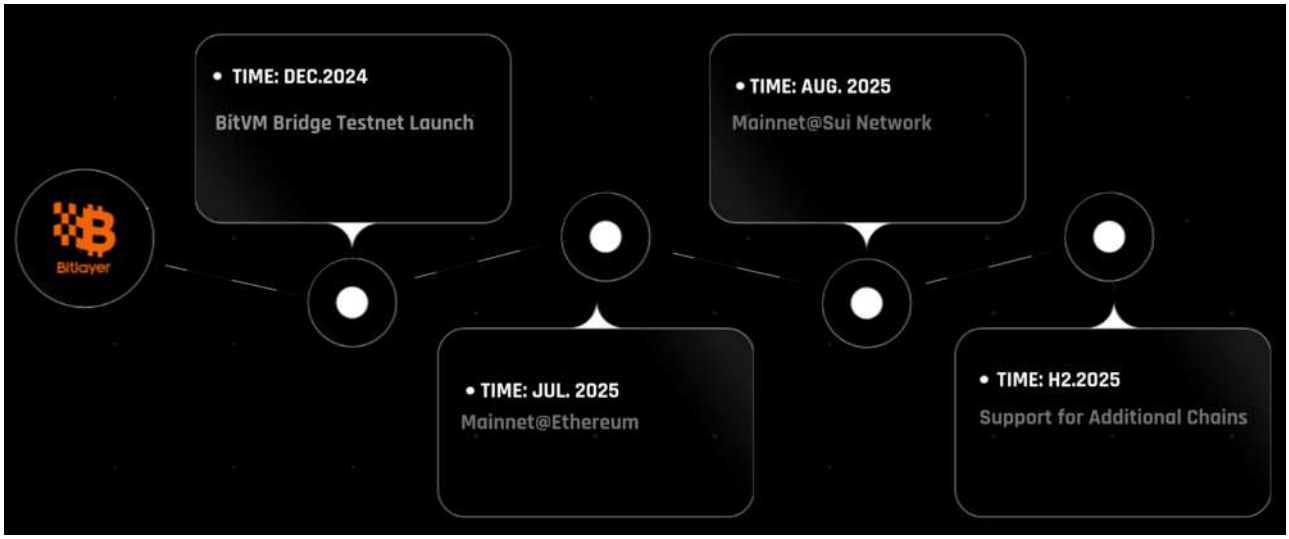
Bitlayer全体のロードマップ

https://docs.bitlayer.org/docs/Learn/Introduction/Roadmap/



BitVM Bridge専用ロードマップ

https://docs.bitlayer.org/docs/BitVMBridge/Concepts/roadmap/

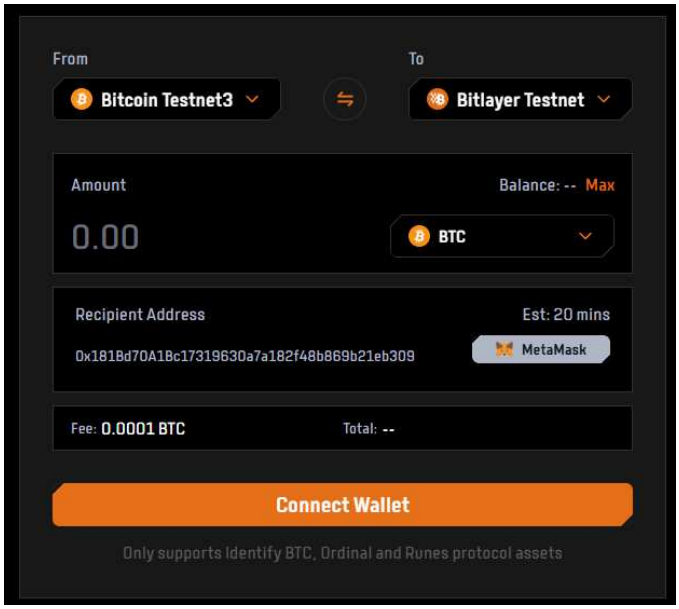


Testnetブリッジ

https://www.bitlayer.org/bridge/testnet

Bitcoin は UniSat Wallet を、Bitlayer Testnet は MetaMask などを使うことができた。

mainnet 版だと Bitcoin 側もいくつか選択できる。



Peg-in の送金をしている様子はこちら→MP4

`OP_RETURN` に送金先の EVMアカウントが ASCII文字列で表現されている。

https://mempool.space/ja/testnet/tx/fbf49c8bb2f6c9ee96f7022beb8a81f170f80a1f485498ac0f33fc8aff851245#vout=1

```
peg-in
   02000000
   0001

   <VIN>
   01

   <VIN#0>
   0379d9b0c2dbe76ac9fe5e19132082c6970afd52939b1007c92e7fa91fc46aa501000000
   00
   fdffffff

   <VOUT>
   03

   <VOUT#0>
   b0ad010000000000
   1976a914d831566c9d4f5589d64397a3efbdb03fb428e65688ac

   <VOUT#1>
```

```
e2f1050000000000
225120f480dbfe748a1db001e296aacba0d914490cf6553414903e3693a4eab75e0322

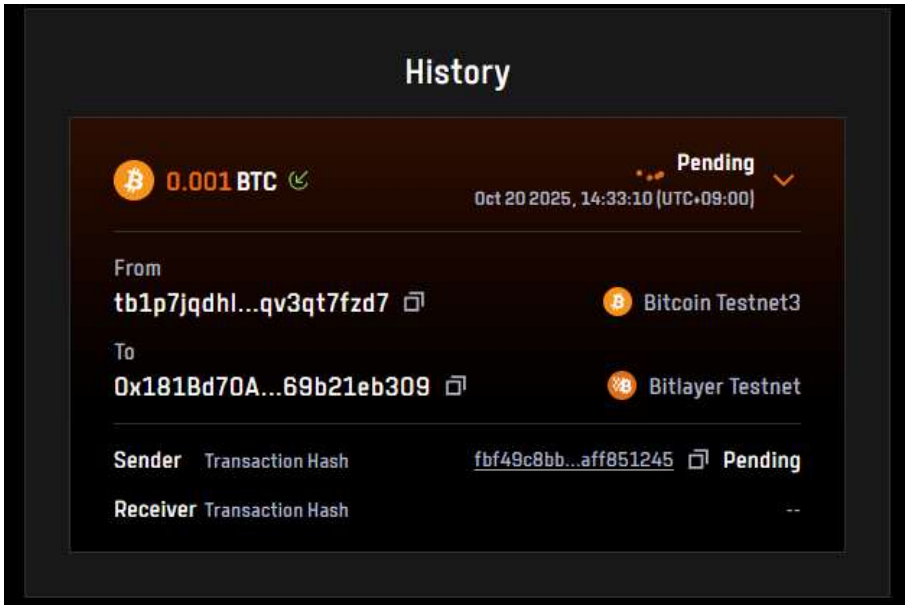
<VOUT#2>
0000000000000000
2c6a2a3078313831426437304131426331373331393633306137613138326634386238363962323165
6
2333039

<WITNESS>
01

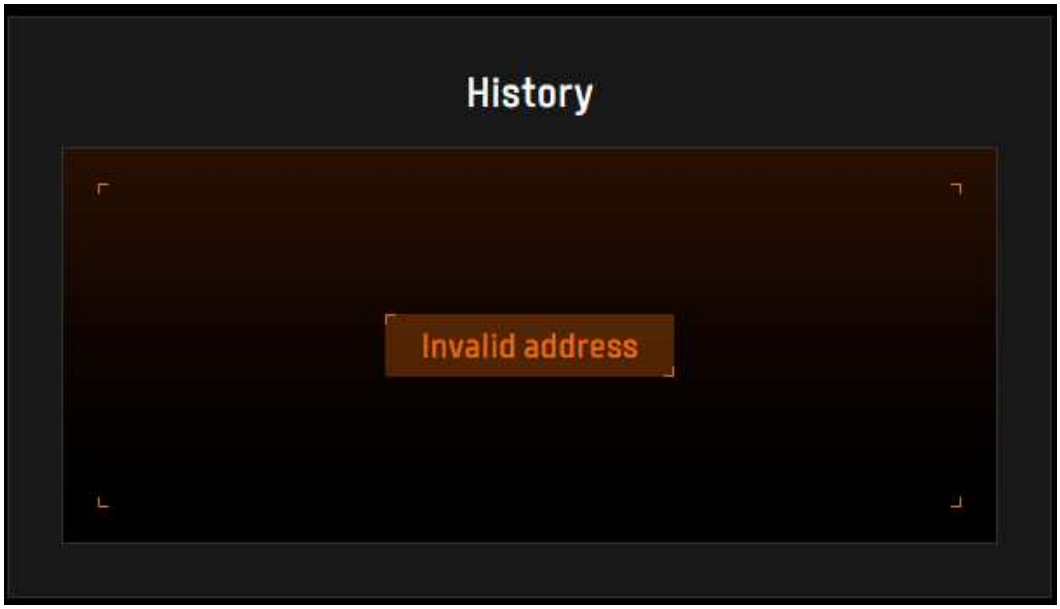
<WITNESS#0>
4016e0ba17eacd532fe705c30cddc2fc93d7323cf87260800a2faec45a28dcba3f4ea963dcad5dddf5d
0187996dc1aaf880a6a0b130b2e38dfdc35f10539f093eb

<LOCKTIME>
00000000
```

confirm されるまでは Peniding がぐるぐる回っている。
6 conf 程度ではこのままみたい。



UniSat walletがロックされると Invalid address になった。
ロック解除すると監視が再開された。


History
Invalid address