Arch Network - Bitcoin L2



https://www.arch.network/

ドキュメント

- https://docs.arch.network/ 2024年11月くらい
- https://book.arch.network/ 更新頻度高め？
- https://arch-network.gitbook.io/arch-documentation 2024年8月くらい
  - ロードマップ coming soon

https://www.blog.arch.network/

https://github.com/arch-network

ChatGPT

Grok

概要

- Bitcoin で直接スマートコントラクト相当の機能を実現したい
- 2025/10/07時点ではまだ mainnet で稼働していない
- ネイティブトークンは `$ARCH`
- 運営ではなくArchVMが分散して鍵を持っている
  - スマコンの実行は ArchVMが行う
  - ブリッジは作らずArch VMがやる
- ブロック生成はdPoSでリーダーが選ばれて作って FROST+ROAST で承認を得た後にBitcoin L1に書き込む

詳細

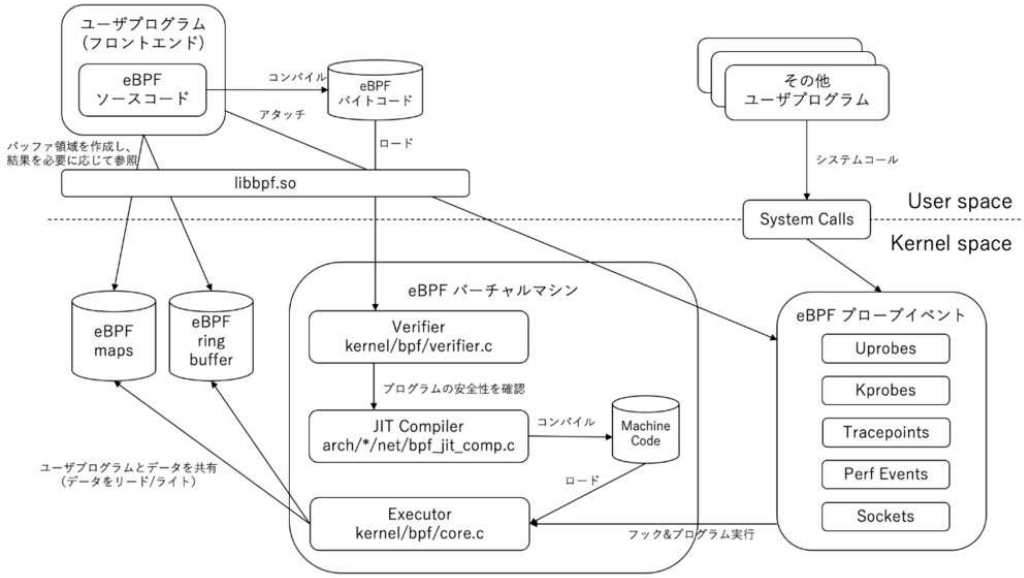
- ブリッジ不要.....
  - もちろんデポジットはいる。
  - ユーザーが資産を外部チェーンやセカンダリウォレットに転送しないでスマートコントラクトとやりとりできる、ということを言っている
  - 他チェーンとブリッジを作らないということに重点を置いている感じか。Bitcoinのセキュリティを活用しつつ高パフォーマンスな環境で動作させたい。

ArchVM

eBPFをベースにし、Bitcoin のトランザクションを直接扱うような改造が行われている

extended Berkeley Packet Filter、という名前なのだが Virtual Machine らしい。パケット関係で使われることが多いのでそういう名前になったのか。

Linux カーネルが提供するような一般的なVM。シンプルで軽量らしい。Solana もeBPFをベースにしているそうだ。



ArchVM 上にスマコンを発行すると、syscall でBitcoinアドレスを取得できる。そのアドレスに Bitcoinを送金すると Bitcoin側からスマコンを実行できる。

正確には、ユーザが Bitcoinを送金して RPCインターフェースを呼び出すと実行される。

RPCを呼び出す必要があることはまだよいとして、RPCがきちんと作動するかどうかはわからん。

ArchVM がアドレスを発行する＝ArchVMが鍵を持っている(運営ではなく)、になる。

複数のArchVMノードが分散して閾値署名

FROST threshold signature と ROAST を使っている。

Arch Networkでは...

署名するバリデーターたち(バリデーターセット)は dPoSコンセンサスで選出される

バリデーターセットの中から署名を集めるリーダーと、安全のためのバックアップリーダーが指定される

ブロックはリーダーが作成し、FROST+ROASTで承認され、Bitcoin L1にコミットメントとしてハッシュを書き込む

Runes、BRC-20、Ordinals などがよく出てくる

ウォレットの対応も、Xverse や Unimat のようなブラウザ拡張で取引所とやりとりできるものが紹介されているので、共通なプロトコルがある？

ChatGPTを見ると独自っぽいが、各社で仕様は公開しているようだ。

オフチェーン処理

State Transitions Anchored on Bitcoin - Arch Documentation

オフチェーンの結果はトランザクションを介してBitcoinにアンカーされる

基本的に毎回オンチェーンに載せるらしいが、バッチでまとめるという話もあった

つまり、Sovereign Rollup ということか

Saturn DEXによるBitcoinでのトラストレスAMM

https://www.blog.arch.network/first-trustless-amm-on-bitcoin/ 2024年11月

Saturn は Bitcoin L1 に構築された DEX

https://docs.saturnbtc.io/

https://www.saturnbtc.io/app/swap/TESTNETRUNEBUSD-sat

テストネット？

Base 上で Arch を使って Bitcoin と USDCをクロスチェーンスワップできるそうだ

https://funkybit.fun と書いてあるが開けない。GitHubも2025年3月くらいが最後だ。

#BitcoinL2