Babylon - Bitcoin L2

#BitcoinL2



https://babylonlabs.io/

https://docs.babylonlabs.io/

https://github.com/babylonlabs-io

ステーキング

ChatGPT

PoSについて - ChatGPT

概要

Bitcoinのセキュリティを生かして、自律的＆信頼不要な方式で Bitcoinをステーキングし、他のPoSチェーンや DeFi プロトコルのセキュリティを強化する。

2025年4月10日に Babylon Genesis がメインネット展開。これが Phase 2 と呼ばれているようで、その前に Phase 1 としてローンチされていたそうだ。

2025/09/03時点で 55483.58 BTCステークされている。

1つの BTCステークで複数のネットワークをセキュアにし、それぞれから報酬を得ることができる

約数日でステーキングの解除が可能(高速 unbonding)

ネットワーク規則違反があった場合、自動的に BTCステークの一部が没収される(スラッシング)

開発フェーズ

Phase 1 : (done) Bitcoin をステーキングできるようにした

Phase 2 : (now!) Babylon Genesis

今(2025年9月)のところ、BSN は Babylon Genesis だけらしい

Phase 3 : BSN(Bitcoin Supercharged Networks)エコシステムの拡張

Cosmosベースのチェーン

OP Stack L2系: Plasma(解散) とか Optimism とか。Base はこれ系らしい。

Arbitrum L2系: Arbitrum One とか Arbitrum Orbit とか

Babylon Genesis

現在の Babylon のチェーン名。Cosmos SDK上に構築されている。

相手側のセキュリティ強化するPoSチェーンがIBCに対応していれば IBCで接続する。対応していなければブリッジを作ったりしないといけない。

ネイティブトークン : BABY

Validator

Babylon Genesisチェーンのトランザクション検証、ブロック生成などを行うノード

申請して参加できる

Finality Provider

一般的に PoSは高速だがファイナリティが PoW のような暗号学的なものではなく経済的なもののため、社会的な要素を含み「弱い」とも言える

Babylong Genesisのブロックに finality を付ける役割

チェックポイントを Bitcoin L1に書き込むこともやる

外部チェーンのセキュリティを強化する以上、元に戻せないチェックポイントを明確にする必要があるのだろう

開発中

Bitcoinの単なるユーザ

Babylon のステーキング用アドレス(スクリプト)に送金する

Taprootの基本ルート2つにはユーザの鍵(`StakerPK`)が必要なのでBabylon運営が勝手に抜き取ることはないし、時間切れの方はユーザの鍵しかないので期限が切れれば自力でウォレットに戻すことができる。

https://docs.babylonlabs.io/guides/overview/babylon_genesis/specifications/bitcoin_staking_scripts/

Timelock Path

```
<StakerPK> OP_CHECKSIGVERIFY  <TimelockBlocks> OP_CHECKSEQUENCEVERIFY
```

Unbonding Path

```
<StakerPk> OP_CHECKSIGVERIFY
<CovenantPk1> OP_CHECKSIG <CovenantPk2> OP_CHECKSIGADD ... <CovenantPkN> OP_CHECKSIGADD
<CovenantThreshold> OP_NUMEQUAL
```

期限までステークしておくと Time-Locked Transaction で戻ってくる

それより前に取り戻すと Unbonding Transaction で戻ってくる

違反行為を行うと Slashing Transaction で減らされるなり没収されるなりする

報酬

Babylon Genesis のネイティブトークン BABY で支払われる

ユーザの Babylon アカウントはステークするスクリプトに埋め込まれている

報酬の量はそのときどきで変わるため、ステーキング時には決まっていない

Babylon Genesis のスマコンで計算される

ユーザはSPV証明によってステークしたことや期間を証明する

最悪、Babylon Genesis チェーンが止まってもステークした BTC は期限が切れれば戻ってくる

他PoSチェーンのセキュリティ強化

他チェーンPoS(Bitcoin Supercharged Network、BSN)は Validator の要件として、自チェーンのネイティブトークンを一定以上ステークする条件に加えて、Babylon にもステークするよう要求する

その Validator が自チェーンで不正をした場合、自チェーンで罰される(スラッシング)だけでなく Babylon の方でも罰される

BSN から Babylon に不正した証拠を通知する

Babylon はそれを暗号学的に検証して、不正があったことが確認できたらスラッシングする

予定

BitVM3

https://docs.babylonlabs.io/guides/research/btc_trustless_vault/#abstract

Babylon、Bitcoinステーキングの仕組みと日本法 - So & Sato