Liquid - Bitcoin L2



#BitcoinL2

- https://liquid.net/
- https://blockstream.com/liquid/
- docs
- elements
  - https://github.com/Blockstream/asset_registry_db
- Grok
- ChatGPT

特徴

- サイドチェーン方式
- 運営主体はBlockstream
- ネイティブトークンは L-BTC
  - Bitcoin と1:1
  - なので Two-way Peg になる
- ブロック生成は1分
  - 時間を単位にしていて、時間が来たらブロック生成を担当する人が切り替わる(決定論的に決められている)
  - ファイナリティはある。トランザクションが承認されたブロックにもう1ブロックつながったときになるそうだ。
    - reorgするリスクがわずかにあるためらしい
- コンセンサス方式は Strong Federation
  - 15人の機能メンバー(functionary)がブロック生成とマルチシグ管理をしている
  - ブロック生成やPeg-In/Out で同じグループが担当している。
- Confidential Transactionで金額やアセットの種類を非公開にできる

Functionary

What are the different types of participants in the Liquid Network?

Liquid ノードの運用は誰でもできる。

Liquid Federation のメンバーが 45社以上存在する(81社らしい)。このすべてがブロック運用に関わるわけではなく、運営やガバナンスなどに参加する。
ブリッジノードの運用もできるが、Peg-In/Out はできない。

Functionary はその中から具体的にネットワーク運用に関わる人たちを指す。どのくらいいるのかは特に把握していないようだ。

- 主な役割
  - Block Signer：ブロックを提案し、署名する
    - Functionary の中から15 社が選ばれている
    - どうやって選んだかは不明(分散性とセキュリティを確保する目的で地理的・地政学的多様性を考慮)
  - Watchmen：Bitcoin L1にロックしている BTCを管理・保全する
    - Peg-In/Out など
    - こちらは Block Signer 以外の Functionary がやるようだが Block Singer の兼任もあるそうだ

秘密鍵は HSM(Hardware Security Module)に格納している。

署名

- How does the Liquid Federation's multisig work?
- Gemini

Blockstream は FROST や ROAST に関するブログを書いているが、Liquid に搭載しているという明確な記述はなさそうだ。

- The Key to FROST: What is Distributed Key Generation?
- ROAST: Robust Asynchronous Schnorr Threshold Signatures

少なくとも peg-in や peg-out、federation のウォレットでは 11-of-15 のマルチシグだそうだ。
3分の2より多いので 4人まで失敗しても大丈夫。
5人以上が鍵を無くすなどするとどうしようもなくなるので、TimeLockを仕込んであり緊急バックアップキー(3キー)でアクセスできるようになっている。

Dynamic Federations(DynaFed)で Block Signer を入替できるようになっている。

- 入替に際してチェーンは止めない

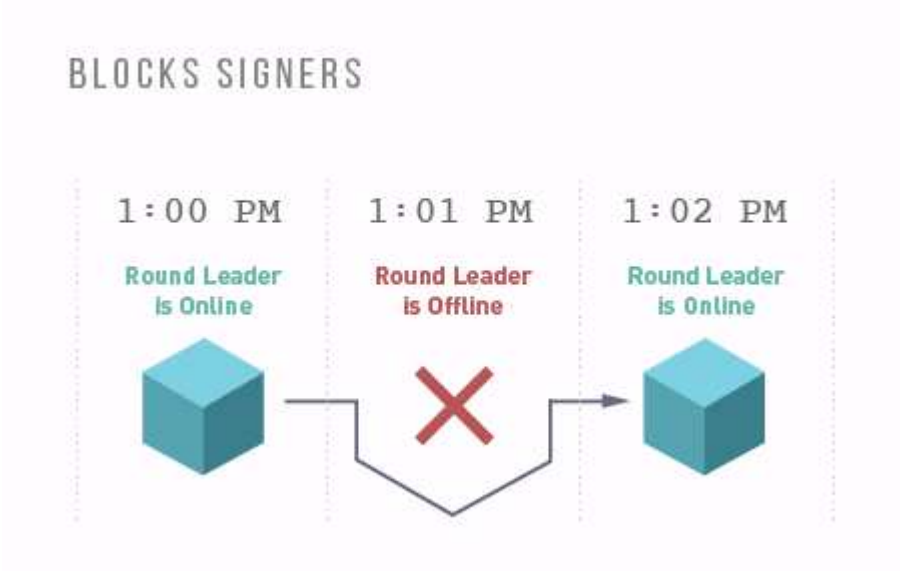
Liquid Federationのメンバーで 15社を決める

Block Signer

そのブロックの署名を担当する署名者がブロックを作り、自分以外の署名者に提案する。それぞれの署名者は提案に問題がなければ署名して担当署名者に返す。これを書いている時点では 11-of-15 マルチシグなので 11人以上の署名が集まれば承認できる。

署名者はラウンドロビンで1分ごとに交代する

しかし、通信不安定や署名者の不足などでブロックの承認ができない場合、そのラウンドはスキップされて次の 1分まで延期される。



reorgする可能性について

ネットワークが不安定で、新しく作ったブロックが展開されたのを受け取る前にラウンドロビンで担当者が交代するタイミングになり、前のラウンドは失敗したと考えて

Block Signerは1ブロックを超えるreorgを引き起こす署名を拒否するしくみがある

ブロックの承認に 11社は必要で、Block Signer に選ぶのは地理的などを含めて分散させているのでまとめて障害が起きる可能性が低くなっているそうだ。

ブロックを作る担当Signerはラウンドロビンで交代する。決定論的に決まっている。

担当Singerがオフラインの場合にスキップする、とは明記されていないので、その場合はラウンドが失敗するのだろう。

「ラウンド」という概念が曖昧だが、Block Signer が決定論的に決まっているので、決められた Block Signer がブロック生成を担当する 1分間、という考え方になるだろう。

つまり、ネットワーク障害などで「ブロック生成の遅延」はあるが「ラウンドの遅延」は発生しないことになる。

ありうるならこんな感じか？

担当Aがブロックを提案して署名を集める

Aのところに11以上集まったが、Aが承認データを展開したところでネットワークが不安定になり、受け取ったのは10ノード

ラウンドロビンして Bが担当になった。

B が Aの承認データを受け取っていた場合

A に続くブロックを作って提案する

署名できる他の Block Signer 10社以上が Aの承認データを受け取っていたら Bの提案も承認して本線になる。受け取ったのが 9社以下であれば拒否されて次ラウンドに持ち越される。

B が Aの承認データを受け取っていない場合

A が失敗したと判断して Aが作ろうとしていたのと同じブロック高のデータを提案する

署名できる他の Block Signer 10社以上が Aの承認データを受け取っていたら Bの提案は拒否される。受け取っていないのが 10社以上であれば承認されてそのグループでは Bの方が本線になる。

こういう感じで、reorg するというよりは新しい提案で 11以上署名を集めてネットワークにも展開できればそれが正になるということらしい。

ブリッジ

Federated Peg。

マルチシグ方式で Block Signerと同じ。

Peg-in(BTC → LBTC)

ユーザはBitcoinをfunctionaryのマルチシグアドレスに送金

十分confirmしたらfunctionaryがLiquid上でL-BTCを発行

102 conf

Peg-out(LBTC → BTC)

ユーザがPeg-out申請すると functionaryがBTCをL-BTCに対応して払い戻す

この申請が取引所になっていると、取引所がL-BTCに対応していないと払い戻してもらえない。日本など。

特徴

trust minimizedではなく連合に依存

Confidential Transaction

金額や資産タイプを暗号化したトランザクション。

Pedersen Commitment などの暗号技術を用いて、暗号化しつつも検証できるようにしている。

金額の隠蔽

トランザクションの IN と OUT の金額を暗号化して第三者には見えないようにしている。検証では 全IN + 全OUT == 0 であることを確認できるようになっている。

マイナス値やオーバーフローしないことは Range Proof(Blletproofs)というもので証明している

IN については元々トランザクションに金額情報はなく UTXO データを参照している

資産タイプの隠蔽

送金元や送金先は隠蔽できない

スクリプト言語

Bitcoinスクリプトを拡張したものと Simplicity というスクリプト言語を搭載している。

Bitcoin script

通常の Bitcoinスクリプトに加えて OPコードが有効になっていたり追加されたりしている。

追加

- OP_CHECKSIGFROMSTACK
- OP_DETERMINISTICRANDOM
- OP_INSPECTINPUT
- OP_INSPECTOUTPUT
- OP_COVENANT
- OP_PUSHCURRENTINPUTINDEX
- OP_CHECKSIGFROMSTACKVERIFY
- OP_CHECKMULTISIGFROMSTACK
- OP_CHECKMULTISIGFROMSTACKVERIFY

有効化

- OP_CAT
- OP_SUBSTR
- OP_LEFT
- OP_RIGHT
- OP_INVERT
- OP_AND
- OP_OR
- OP_XOR
- OP_MUL
- OP_DIV
- OP_MOD

OP_LSHIFT

OP_RSHIFT

Simplicity

Simplicity は2025年7月31日に mainnet展開された。

Simplicity Launches on Liquid Mainnet

Simplicity: Next-Generation Smart Contracts for Bitcoin

docs

Simplicity というスクリプト言語で、Bitcoinスクリプトに変換するというわけではない。

Simplicity として動く。

形式検証が可能で、検証ツールなどで数学的にプログラムが仕様を満たすことを保証できる。

高級言語として SimplicityHL という Rust風の言語が用意されている。