A Beginner's Guide to Bitcoin Layers



https://guidetobitcoinlayers.hiro.so/
Bitcoin の Layer2/Sidechain の見方について説明している。
著者はStarksという sidechain系の人らしい。

7章まであるが、全部読まないと思う(2025/05/20)。

L1、L2という書き方をしているところもあるが、"Bitcoin Layer"という書き方をしている場合は L1 ではなく L2 のことを指しているように見える。なので「追加レイヤー」と訳した。

ChatGPTによる補足

1. Evaluating Bitcoin Layers: Benefits vs Risks

https://guidetobitcoinlayers.hiro.so/chapter-one/

- Extending Scale + Functionality
  - スケーラビリティと機能の拡張
    - このレイヤーはBitcoinのスケーリングに役立つか？
      - スループット(ブロックサイズ関連)
        - ネットワークが一度に処理できるトランザクション数(Bitcoinは 7txs/sec)
      - レイテンシー(コンセンサス・決済関連)
        - ネットワークが単一のトランザクションをconfirmできる速度(Bitcoinは約10分)
    - このレイヤーはBitcoinに追加の機能性をもたらすか？
      - スマートコントラクト表現
        - 言語とVMがいる
      - 状態(state)管理

global state：全ノードが共有するstate

local state：特定の相手とだけ共有するstate(LNのチャネルなど)

BitcoinはUTXO管理、Ethereumはアカウント管理

追加特性(プライバシーツールなど)

トラストミニマムとセキュリティの継承

このレイヤーで導入された追加の信頼前提(trust assumption)は何か？

ブリッジデザイン

execution & settlement (ほどよい訳語が思いつかない)

このレイヤーはBitcoinのセキュリティを継承するのか？

Bitcoinファイナリティ/reorg耐性

Bitcoin検閲耐性

Minimizing Trust + Inheriting Security

Minimizing Trust

ブロックチェーンには、何を信頼するのかという前提が必ず付随する。

追加レイヤーではスケールや機能性を追加するときに新たな信頼前提(trust assumption)を最小限に抑えるべきである。

Bitcoinチェーンでのデフォルトの信頼前提は、各ノードがトランザクションとブロックの実行、決済、検証を管理すること。

ノードの51%が正直であれば安全ということになる。

追加レイヤーでの信頼前提の例

ブリッジデザイン

BTCをL1からL2に移したり戻したりする「ブリッジ」が必要になる。

ブリッジの仕方はタイプによって異なる。

集中管理型(カストディアン)

マルチシグ型

スマートコントラクト型

ブリッジは、パーミッションレスなグループだったり、クローズドなフェデレーションで管理したりする。

一般的に.....

集中管理されるブリッジが最も多くの新しい信頼前提が必要

スマートコントラクトのブリッジ(fraud proofとvalidity proofの使用)が最も信頼前提が少ない

実行(execution)

追加レイヤーでトランザクションを展開すること、という意味だと思う

Bitcoinチェーンでトランザクションが実行されると、10分の確認時間(レイテ

ンシー)と固定ブロックサイズ(スループット)の影響を受けるようになる。
トランザクションをBitcoinチェーンで展開せず別の形に置き換えるような拡張を考える。
Rollup とかサイドチェーンでの展開などを指しているのだろう
その拡張を追加レイヤーで行うならば、そのレイヤーのネットワークオペレーターを信頼する必要が出てくる。

Inheriting Security Properties

理想的な追加レイヤーはBitcoinチェーンのセキュリティプロパティを継承する。

ファイナリティ/reorg耐性

追加レイヤー上でconfirmされたトランザクションがBitcoin台帳上でconfirmされたブロックに含まれた瞬間を指す。
そうすることで追加レイヤーのトランザクションはBitcoinトランザクションと同じファイナリティを持つことになる。

検閲耐性

ネットワークへの参加を拒否、または検閲できる範囲を指す。
例えばBitcoinチェーンは51%以上のノードが共謀すると、有効なトランザクションを扱わないようにできてしまう。
追加レイヤーでネットワークオペレーターやシーケンサー(Rollup系かな？)などが検閲できるとBitcoinチェーンレベルの検閲耐性を持たないことになる。

追加レイヤーは同時に2つのことを行う必要がある。
すなわちBitcoinのスケールと機能性を最大化させつつ、信頼前提やリスクを最小化する。

2. Understanding Layer Failure, Risk and Trust

https://guidetobitcoinlayers.hiro.so/chapter-two/

liveness failure や security failure という言葉が出てくるが、分散システムでしばしば使う言葉だそうだ。

ライブネス - Wikipedia

ライブネス特性：「何か良いことが最終的に起こる」。それが起こらないのがliveness failure。
安全性特性：「何か悪いことが起こらない」。それが起きてしまうのがsecurity failure。

Liveness Failureとは「正しくても処理されず、いつまでも進まない」状態(ChatGPT)

「トランザクションが正しく処理される」が『何か良いこと』なのだろう。
例：処理が進まない、資産が動かせない、ブロックが生成されない

Security Failureは「一貫性や安全性が壊れること」。

例：二重支払い、データ改ざん、資金喪失

Finality Delayは、取引の確定に時間がかかること(ChatGPTが説明していたので載せておく)

failure とは限らない

だいたいこういうことを期待している。

BTCは、ビットコインブロックチェーンがライブで安全である限り、盗難や凍結から安全です。

取引は検閲されません。

信頼できる第三者に頼らずに、レイヤーを自由に終了することができます。

追加レイヤーは、意図したとおりに機能します。

リスク最小化のために

BTCの盗難や凍結対策

ノンカストディアルなブリッジ

理想的には、橋はオープンで許可されたメンバーシップによって運用され、カウンターパーティのリスクを減らします。

一方的な(追加レイヤーからの)脱出

L1トランザクションからブリッジを出て、ブリッジの liveness failure と security failure に対する保護を提供することができます。

トランザクションの検閲対策

強制包含(forced inclusion)またはセルフシーケンス

追加レイヤーのオペレーターにトランザクションを含めるように強制することができます

(通常、Bitcoinチェーンを介して追加レイヤーのトランザクションを送信するオプションを設定できるようにする)

追加レイヤーオペレーターの分散化

追加レイヤーがオープンでパーミッションレスな会員によって操作される場合、個々のシーケンサーまたはオペレーターが特定のトランザクションを検閲することがより困難になります。

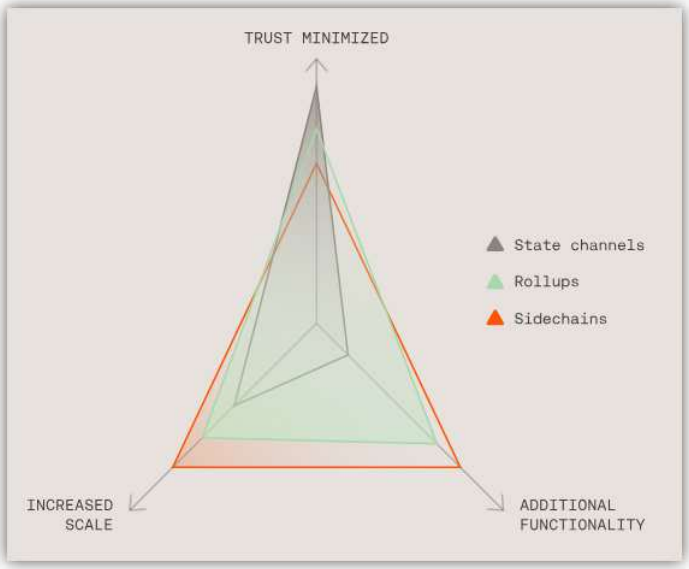
reorgによるトランザクション(取引)の巻き戻し対策

Bitcoinファイナリティ

追加レイヤーで確認されたトランザクションが、Bitcoinブロックチェーンのconfirmされたブロックに含まれている瞬間を指します。これにより、確認されたトランザクションは、ビットコイントランザクションと同じ最終性を与えます。

3. Types of Bitcoin Layers

https://guidetobitcoinlayers.hiro.so/chapter-three/



Sidechain型は、チェーンが別になっているのでいろいろ自由にできるが、新たなチェーンに関しての信頼前提が追加になる。

State Channel型(Lightning Networkなど)は信頼前提の少なさやスケーリング効果はよいが、スマートコントラクトを動かすような機能性はない。

Rollupはまだ発展途上なので何とも言えない。

BitcoinスクリプトではRollupの検証ができないので、その問題をどう回避するかというのが課題になる。

理想的な追加レイヤー

機能性とスケーリング

完全なVMサポートと、表現力豊かな高水準言語によるプログラミング能力。

トランザクションとブロックの時間が速い（ビットコインのブロックを10～30分待つ必要がない）。

L2アプリに導入され、L2取引手数料の支払いに使用される主要資産としてのBTC。

追加になるリスクや信頼を最小限にする

オープンソースで分散型の開発プロセス。

L1 と L2 の間で BTC を移動させる信頼最小化方法。

カウンターパーティーリスクがなく、L2から一方的にBTCを引き出すことができる。

ビットコインの最終性（再整理耐性）と検閲耐性を継承。