Starting to define layers, a year later - bitcoinlayers.org



https://www.bitcoinlayers.org/

「Bitcoin Layers」というサイトだがA Beginner's Guide to Bitcoin Layersとは関係なさそう。

Bitcoin native protocols

> レイヤー2は、オフチェーンシステムのオペレーターがオフラインになった場合にユーザーがシステムから離脱できるようにするプロトコルであり、同時にシステムのオペレーターが不正行為を行えないことを保証する。これらの前提はいずれも、オンチェーン上で証明可能かつ強制可能である必要がある。

これは一番厳しい Bitcoin L2 の定義となるだろう。

- ユーザが L2 にロックした UTXO を請求することができるし、相手がいなくても取り戻すことができる
- オフチェーンの状態遷移の正当性をオンチェーンで証明できる

LN は直接の相手と Commitment Transaction を常に交換することで、そのままオンチェーンで展開すれば UTXO を自分だけで取り戻すことができる(自分がデータを失ってSCBを使った場合は多少怪しいが、それは失う方が悪い)。相手が最新ではない Commitment Transaction で取り戻そうとしたらオンチェーンに展開されるので検知できるし、奪い返すことができる。オンチェーンを監視し続けるなどモバイルでは厳しい条件はあるが、プロトコルとしては可能になっているという点は大きいだろう。

今のところこの条件を満たしているプロトコルは3つだといっている。

- Lightning Network
- Statechains
- Ark

Sidesystems

サイドチェーンは Bitcoin建て(bitcoin-denominated)の独立したモノリシックブロックチェーン。

Rootstockなどがそう。

Client-Side Validation のようなシステムはサイドチェーンではない。理由としては、ユーザがコンセンサスとファイナリティのために独立したブロックチェーンに依存しないため。しかしBitcoinの「ブリッジ」が必要なので BTCサイドシステムというカテゴリーになる。Rollup系も同様にBTCサイドシステムで、サイドチェーンよりもBTCと密接している。

Stacksのようなシステムはサイドチェーンではない(といいつつStacksのページには"sidechain"と書いてる)。理由としては、Stacks が機能のために別のトークンに基づいたバリデータセットに依存しているため。BitcoinにL2を固定(anchor)することでチェーンの reorgを保護するシステムである。

Arch Network のような次世代システム(upcoming systems)は、L2の実行環境が L1スクリプトやPSBTと対話できる(互換性があるとかそういう意味？)別のブロックチェーンである。これらはL1でもL2でも実行できるということでハイブリッドチェーンと呼んでいる。

Bitcoinをステーキングする PoS システムはステークチェーンと呼ぶ。リモートでのステーキングが可能で、独自のコンセンサスメカニズムには代替トークンを使用するシステムもハイブリッドチェーンと呼んでいる。それは、ユーザがL1スクリプトでやりとりもできるし、コンセンサス、トランザクションの確定、スラッシングの調整、ステークの割り当てには独自のトークンを持つ代替チェーンが使用されるためである。

https://www.lxresearch.co/starting-to-define-layers-a-year-later/

2025/07/23時点

	name	type
Bitcoin native protocols	Lightning Network	State Channels
	Mercury Layer	Statechain
	Spark	Statechain
Sidesystems	Stacks	Anchor
	Botanix	Federation
	Liquid	Federation
	Mezo	Federation
	Internet Computer	Hybrid
	Rootstock	Merged-mined
	Nomic	PoS Network
	Side Protocol	PoS Network