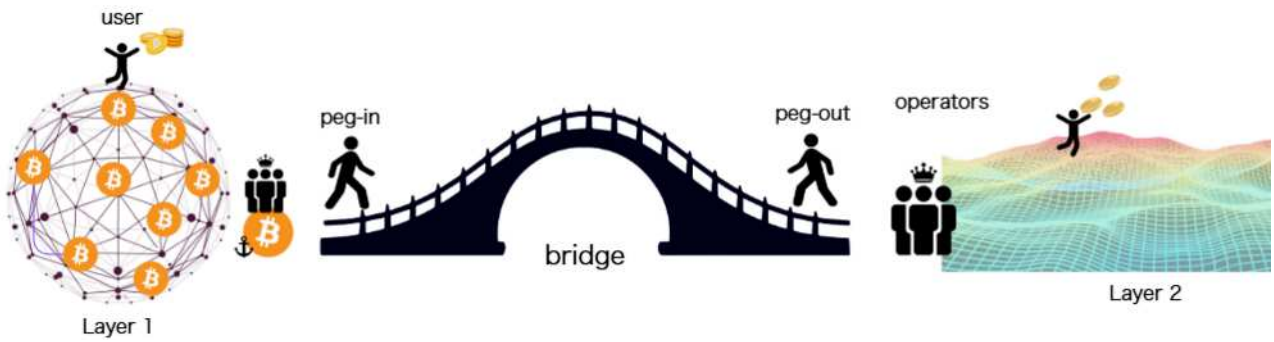
ブリッジ - Bitcoin L2

ChatGPT

今まで Bitcoin L2 の調査をしていてブリッジが出てきたが、一般的なブリッジについて調べておく。



ここは L1/L2 の文脈だったのでこういう図になったが、異なるネットワーク間で資産やデータを移動させるしくみである。
Liquid や Citrea などは L2 の運営側が明確に決まっているので L2 とブリッジをセットで用意するが、Ethereum や Cosmos のようにチェーンが既にあってブリッジだけ実装するというパターンもある。

- 片方向・双方向
  - 片方向のブリッジというのはほとんど存在しない。Bitcoin 売却とトークン購入を行ったと見なされる可能性が高いからだろうし、利便性というのもある。たぶん前者だと思う。
  - 双方向のブリッジは Two-way Peg とも呼ばれる。
    - peg は、テントの四隅などに打つ、あのペグでもあるし、経済用語としては市場操作によってレートを安定させることを意味するペッグでもある。後者だろう。
    - 2015年 BlockchainとSidechain間のtwo way pegについて - Develop with pleasure!
      - Liquid の two-way peg について withdraw 方向の検討をしている
      - サイドチェーン側の SPV を使わないと Bitcoin 側で解けないようなスクリプトを使うので soft fork が必要ではないかという検討をしているが、Liquid では federated peg でスクリプトではなく連合で検証することで SPV は使わないという結論になったようだ。

Lock & Mint方式

基本的にこれ

L1側でスマートコントラクトなどに資金を送金してロックする

L1側でロックされた資金相当の資金をL2側で発行する

L2側の資産を焼却する

L1側でロックしていた資金を解放する

分散型

BitVM2 bridge

zk-proofベース

Covenant + OP_CAT

Peg-Out についてはいろいろ考慮することが多いが、Peg-In は資金をロックできれば良いので複雑なことをしていないようだ。
例えば BitVM2 bridgeは特に Peg-In についての決まりはない(fraud-proof でのチェックはある)。
Bitcoinはスクリプトで ZK-proof ができないので、fraud-proof 方式か参加者承認方式のどちらかになる。

https://arxiv.org/html/2509.10413v1

NotebookLM

Grok

ChatGPT

信頼ベースで即反映

マルチシグ型

Liquid

ウォッチャー型(閾値署名)

tBTC

スクリプト/証明で条件付き反映

HTLC型

Lightning Network

Atomic Swap

SPV型

Rootstock, Drivechain

BitVM bridge (スクリプト＋fraud-proofでの検証あり)

Ark は ユーザとASP の 2-of-2 になるが、あれはロックしたままになって exit するまで運営も使

えなかったはずだ。
他のブリッジはどうしているのか。

ブリッジ運営資金

ChatGPT
実際のところ、Peg-Inで資金をロックするというが運営側のアドレスに送金しているのとほぼ同じだ。それを運営資金にしているなら単なる支払いと同じではないかと思ったが、裏付け資産としての証明のために UTXO のままにしておいた方がよいそうだ。
では運営資金はどのくらい準備したら良いかというと、Peg-In の総額から同時 Peg-Out 率を仮定して決めるそうだ。そこにバッファを設けて安全にする。
BTCとトークンの変換率で調整するというのもあるだろう。

ただトークンの売買をするのであれば運営資金には極力触れずに当事者同士で解決できた方がよい。
HTLC方式のブリッジについて調べていると、交換相手を見つけるのに効率が悪いというような文章が出てくるのはそういうった観点からのようだ。
また、SECの介入を気にするならマルチシグ方式ではカストディ規制の対象になる可能性が高く、HTLC方式だったとしても wrapped token を発行するとそうなるかもしれないとのこと。

トークンの価値とコベナンツ

Bitcoin Covenants

単にユーザが L2運営のマルチシグアドレスに送金しても、それが L2側で mint に使われるかどうかわからないし、送金額に応じた mint額になるかもわからない。運営を信用するしかない。
運営が不正などすると mint した L2側のトークン価値は下がり、それは BTC と同じ価値にはならない。
同じ価値にしたければ、スクリプト化してチェーンによって自動で動作も検証もするようにしないといけない。



では、そういうスクリプトはどういうものであればよいか。

大ざっぱには、送金に条件を付ける、ということになる。単にマルチシグアドレスに送金するだけだと、そこから先どうするかはマルチシグアドレスが勝手に決めることができる。そうさせないために用途を限定させるのである。
こういうスクリプトをコベナンツと呼んでいる。

ブリッジのセキュリティ

- Bool Network: The Ultimate Solution of Cross Chain Bridges Protected by Dynamic Hidden Committee (DHC)，introducing interoperability to the Bitcoin ecosystem - by DeepSafe - Medium
  - Grok
    ブリッジ構築プラットフォーム事業をやっている会社(Bitlayerのサードパーティーブリッジを提供していた)
    ブリッジはとにかく攻撃を受けやすい
      スマコンのコード脆弱性
      検証ノードの詐欺
    SPV でのローカル検証

ブリッジの研究

Bitcoin Cross-Chain Bridge: A Taxonomy and Its Promise in Artificial Intelligence of Things
2025年9月12日の研究発表。
NotebookLM

AIoT うんぬんは、ここではスルーする。
ブリッジにはいくつかタイプがあるが、どれも一長一短で正解はないというお話。

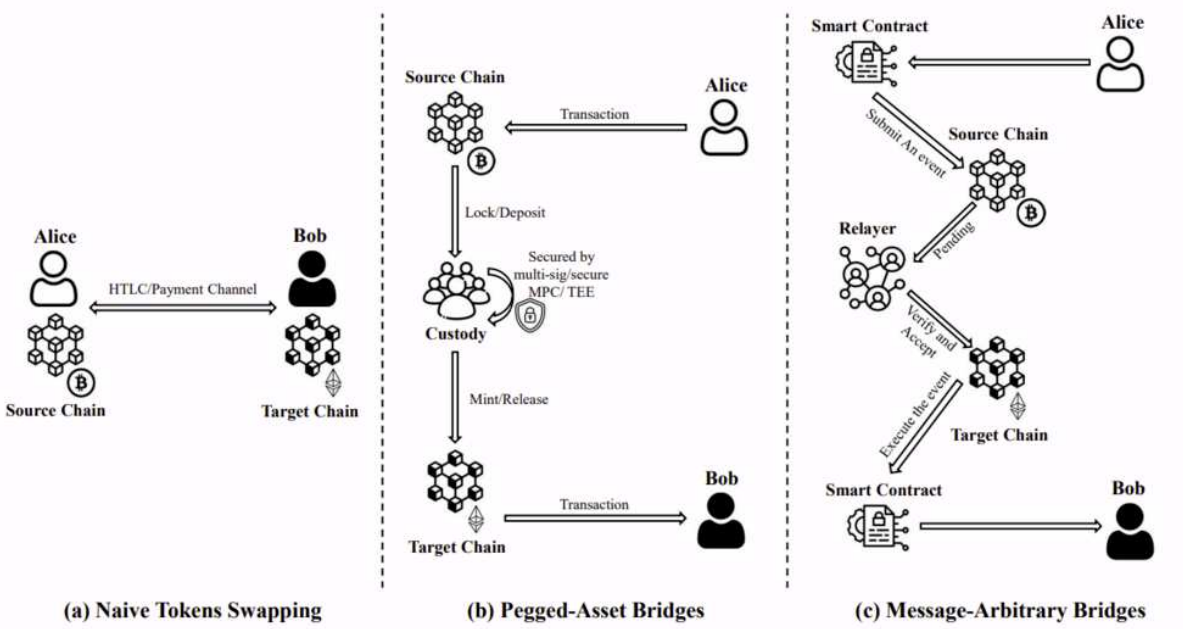


Figure 1. Overview of (a) Naive Tokens Swapping, (b) Pegged-asset Bridges, and (c) the Arbitrary-Message Bridges

(a) Naive Tokens Swapping

いわゆる HTLC を使った atomic swap 型を指すようだ。

Lightning Network など

スワップ処理期間中、コインがロック状態になるため資金効率が非常に低い

そんなにスワップに時間かかる？ あるいは数時間というのが既に資金的に長い？

(b) Pegged-Asset Bridges

いわゆるマルチシグ型を指すようだ。

サイドチェーンや BitVMがここに入っている

(c) Message-Arbitrary Bridges

直接やりとりするのではなく、リレーを使ってメッセージを仲介してもらう

外部検証者方式

Axelar Network, deBridge, LayerZero

バリデーターの定足数が正直という仮定による

オンチェーンリレー方式

zkBridge, ~~BTCRelay~~, FlyClient, NiPoPow

トラストレスだが証明コストが高いし、スマコンの呼び出しコストも高い

Cosmos の IBC も範囲に含まれるが、元々 IBC が Cosmos 系を扱う想定なのでちょっと違うかも

IBCはMessage-Arbitrary Bridgeか - ChatGPT

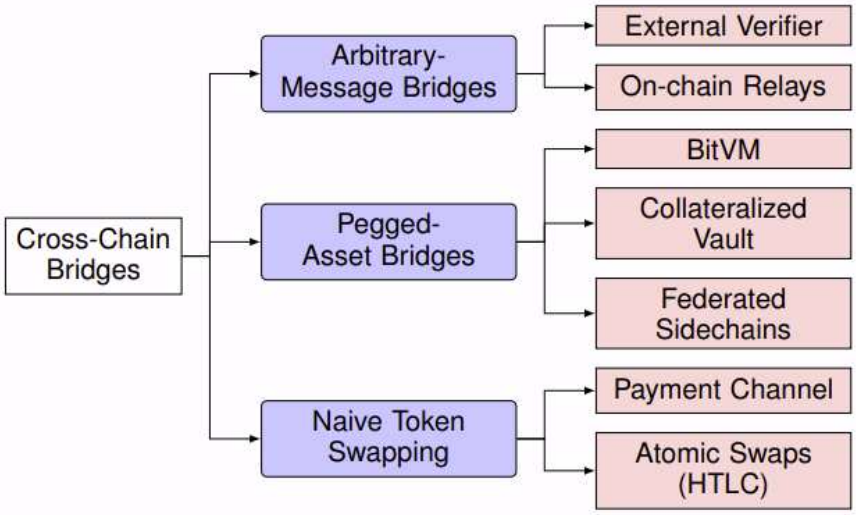


Figure 2. Taxonomy of Cross-Chain Bridges

表I：ビットコインクロスチェーンブリッジ手法の比較

アプローチ方法	信頼モデル	遅延	計算処理消費エネルギー	普遍性	資本効率性	DeFi対応
アトミックスワップ [4, 5]	HTLC（条件付き即時決済）	●	○	○	○	○
決済チャネル [6, 7]	HTLC（条件付き即時決済）	○	○	●	○	○
担保型金庫 [2]	経済的	◐	◐	◐	●	●
オンチェーンリレー [8, 9, 10, 11]	トラストレス	○	●	●	●	●
BitVMブリッジ [12, 13]	信頼最小化型	○	◐	●	●	●
サイドチェーン [17, 19, 20]	過半数が誠実	◐	◐	◐	●	●
外部検証者 [14, 15, 16]	検証者クオラム	◐	○	●	●	●

現在 L2 で採用されている方式(2025年10月前半)

Citrea : Clementine v1

ChatGPT

2025/10/07：まだ mainnet 運用無し

v1 は BitVM2 bridgeベース。

オフチェーンでの ZKP + Bitcoin上での fraud-proof

Peg-in

UTXO は N人の検証者、ブリッジオペレーター、ユーザーで管理

200 ブロック後にはユーザも取り戻せる

十分確認されたら N人検証者とブリッジオペレーターのマルチシグに移動

ユーザは SPV証明を Citrea のスマコンに提出して cBTC を mint してもらう

Peg-out

ユーザは Citrea 上で Bitcoin での受け取り先アドレスを指定して burn

操作が Withdrawal Merdle Tree に登録される

ユーザは Bitcoin側でそのアドレスに送信

Citrea の検証者やオペレーターがそれを検証して BTCの解放を許可

BitVM2 bridge の Peg-out は先に burn を許可したオペレーターがユーザに支払い、その後に fraud-proof の検証をしてオペレーターに払い戻すようにしてユーザに早く払い戻されるようにしていた。Clementine v1はそれについては選択制で検証後にユーザに送信する「直接送信モード」があるそうだ。

Clementine v2は研究中。Garbled Circuits と TOOP。BitVM3の現在の方式とも異なるようだが、研究中なのでどうなるか分からない。

Bitlayer v2 (2025年7月15日にベータリリース済み)

ChatGPT

2025/10/07：v2はまだmainnet運用されていないがブリッジは運用されているそうだ

Bitcoin とのブリッジには BitVM bridgeベース

Peg-in

federationのマルチシグに送金。HTLCになっているなどの詳細は不明。

ロック状態は Bitlayer Rollupに記録され、対応する YBTC が mintされる

Prover が BTCロック状態を Rollup上で証明

Bitlayer は Optimistic Rollup なので Challenger が一定期間監視し、問題があれば差し戻される(はず)

監視期間中もユーザは mint された YBTC を使用できる

不正があったときにどうなるかは記載がないらしい

Peg-out

Bitlayer上でYBTCを burn して Peg-outリクエストを提出

ブリッジのメンバーがマルチシグで BTCを送金(BitVM2 bridgeと異なる)

その後は fraud-proof での検証は行われるが、不正が見つかっても BitVM bridgeの用に担当オペレーターだけが損をするというしくみではないということになる(あえていうなら運営全体で損をする)

Ethereum や Sui とのブリッジは Chainlink CCIP や独自ブリッジになる予定

Arch Network

2025/10/07：まだmainnet運用していない

ArchVM は直接 Bitcoinトランザクションを扱うようになっている

Starknet

2025/10/07：まだmainnet運用していない

まだ研究開発中なので調査しない。

最終的には `OP_CAT` などを使ったネイティブブリッジを作りたいようだが、その前段階としてマルチシグやBitVMを検討しているそうだ。

tBTC v2

2025/10/07：まだmainnet運用していない

Bitcoin – Ethereum 間のブリッジプロトコル

鍵が 3つあり、その 1つが閾値署名(Keep署名者グループ)。

全体のお金は 2-of-3

デポジットでは Keep署名者グループの鍵だけを使っていて、ユーザはそのアドレスに送金する。

Ethereum 側のスマコンを mint 時は運営側が、burn 時はユーザが呼び出したりする

Liquid Network

federation の 11-of-15 マルチシグ

Rootstock

PowPeg federation (5機関)が Peg-In/Out を管理している。

BitVMX bridge というブリッジを開発中。

ブリッジの decentralization について考える

Bitcoin ではアドレスに送金されても、送金が成功するかどうかだけで自動的に何かが行われるということはない。

もし Bitcoinトークンを発行するのであればまだなんとかできるかもしれないが、別のチェーンに何かすることはできない。Ethereum はスマートコントラクトから別のスマートコントラクトを呼び出すことができるし、アカウントベースでスマコンの呼び出し元を知ることができるし、とにかくできることが違う。

Peg-inとPeg-outを分けて考える

機能としてはユーザからのBitcoinをトークンに変換する Peg-in とトークンをユーザにBitcoinで払い戻す Peg-out は対になる動作である。しかしトークンが Bitcoin以外のチェーンになることを前提とすると、必ず Peg-in と Peg-out の間には自動化されていようといまいと運営者の操作が必要となる。

運営者は Bitcoinチェーンが関与できない要素なので trustless ではない。よくて trust-minimize である。



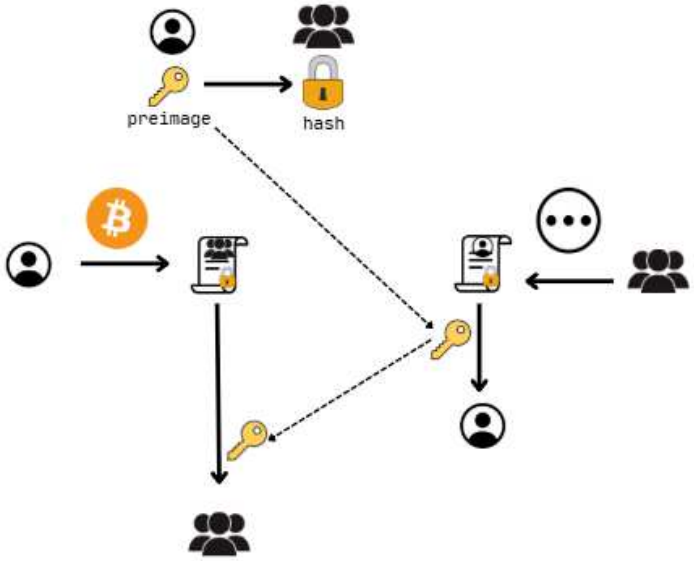
Peg-in と Peg-out が切り離されているのであれば、どちらかの VM で相手側のチェーンについての操作ができればよいのではないか？というのが Arch Network - Bitcoin L2 のやり方だろう。あれはどう判定されるのだろう？ 運営者ではなく VMというかノード自体が鍵を持っているから trustless 寄りの trust-minimize というところか。
まあ、trustless ではない要素が 1つでもあれば decentralize ではないのだ。

ともかく現状では Peg-in と Peg-out は切り離されるので、個別に考えて良いだろう。
ただ、BitVM2ブリッジでは Peg-in 額ごとにインスタンス(スクリプトや検証するセット)を作るようで、詳しくは分からないが Peg-out と関連があるとのこと。

Peg-in
ユーザの Bitcoin を受け取り、それが reorg も含めて確定したと判断したら相手チェーンのトークンを発行する。トークンと書いているが別にネイティブトークンでもよい。例えば Ethereum であれば運営者が所有している ETH から相応する額を相手に払えば良いだけだ。
受け取ったBitcoinの送金元と、発行するトークンの送金先を対応付けする必要がある。

ユーザから受け取った Bitcoinをどうするかは運営次第だが、運用資金の原資をはっきりさせるために別のウォレットに送金せず UTXO のままにしておくという話を聞いた。

ユーザの視点では、指定されたアドレスに送金したがトークンに変換されなかったということはあり得る。なので HTLC にして一定期間を過ぎるとユーザが取り戻せるようにすることはできる。そうすると一定期間内に別のアドレスに送金すれば済むだけなので、相手チェーン側でトークンを発行しないとユーザからの Bitcoinを受け取ることができないようにしなくては意味が無いだろう。ならば相手チェーンでのトークン送金先はユーザのアドレスに直接ではなく hash の preimage を公開しないと受け取ることができないというスクリプトに対してになる。そのスクリプトを運営側で作ると意味が無いので、少なくとも preimage はユーザが作成して hash を渡すだけになる。よくある atomic swap だ。



HTLC方式はユーザにとって安全性が高まるのだが、ユーザが送金した Bitcoin を運営が認めた後にアクションを取らないといけないのが UI を悪くするという話があった。HTLC の期間があるので運営側もそれをユーザごとに気にしなくてはならないし、アプリを作ったらそれを通知するしくみを組み込んだり、アドレスが毎回変わるので監視が面倒になるし、いろいろと大変になる。

また、HTLCを期間内にマルチシグアドレスへ送金することになるため、それが Bitcoin売却によるトークン購入と見なされる可能性がある。つまり Bitcoinの資金をロックしたと見なされない可能性があるということだ。それが下の表(NotebookLM作成)にある「二者間の1回限りの交換」という意味らしい。

マルチシグ方式もペグイン（ロック）とペグアウト（解除）の際に資産をロックしますが、HTLCとは異なる目的と性能を持っています。

特性	HTLC方式 (Atomic Swap) 1 ...	マルチシグ方式 (Federated Sidechain) 3 ...	違いの要点
資本効率 (Capital Efficiency)	**低** (●) 3 。都度ロック、単発利用。	**中** (◐) 3 。一度ロックすれば側鎖内で利用可能。	マルチシグは**継続的な資産の生成と利用**を可能にする。
用途	**二者間の1回限りの交換** 1 4 。	**ペッグされた資産 (Wrapped Asset)** の発行と流通 6 8 。	マルチシグはDeFiとの互換性が高い 8 。
DeFiとの互換性	**低** (○) 3 。交換のみに機能が制限される 1 。	**高** (●) 3 。側鎖内でスマートコントラクトを利用可能 8 。	マルチシグは資産を「流動化」させる。
レイテンシ（遅延）	**低速** (●) 3 。ブロック承認待ちに時間がかかる（例：BTCで6承認） 4 。	**中速** (◐) 3 。ペグイン（ロック）は遅いが、ペグアウト（解除）は速い 7 8 。	HTLCは取引自体の完了が遅い。
資産ロックの性質	**取引ごとに、特定のカウンターパーティ**との間でロック。	**継続的に、フェデレーションが管理するカストディ**アドレスにロック 6 8 。	

Grok に尋ねると、

> 売り買いを同時にさばけないと運営資金を使わなくてはならない。
> HTLC方式の場合は相手も見つけてから実行するので、カウンターパーティが必要

マルチシグ方式の場合は一度 wrapped token などに変換してから扱うので気にしなくてよい。その代わりというか、マルチシグ方式は SECのカストディ規制の対象になる可能性が高い。

なら HTLC方式でも wrapped token に変換すればよさそうだが、HTLC 方式を使うということはノンカストディアル的な運用をして SECなどに目を付けられたくないという思いがあり、wrapped token を発行すると HTLCのアトミック性もなくなるし、カストディアルだと見なされてしまう可能性もあるので向かないとのこと

ならば Bitcoin L2 はどうなのかというと、Citrea の peg-in もマルチシグ方式だしゴニョゴニョ。。。

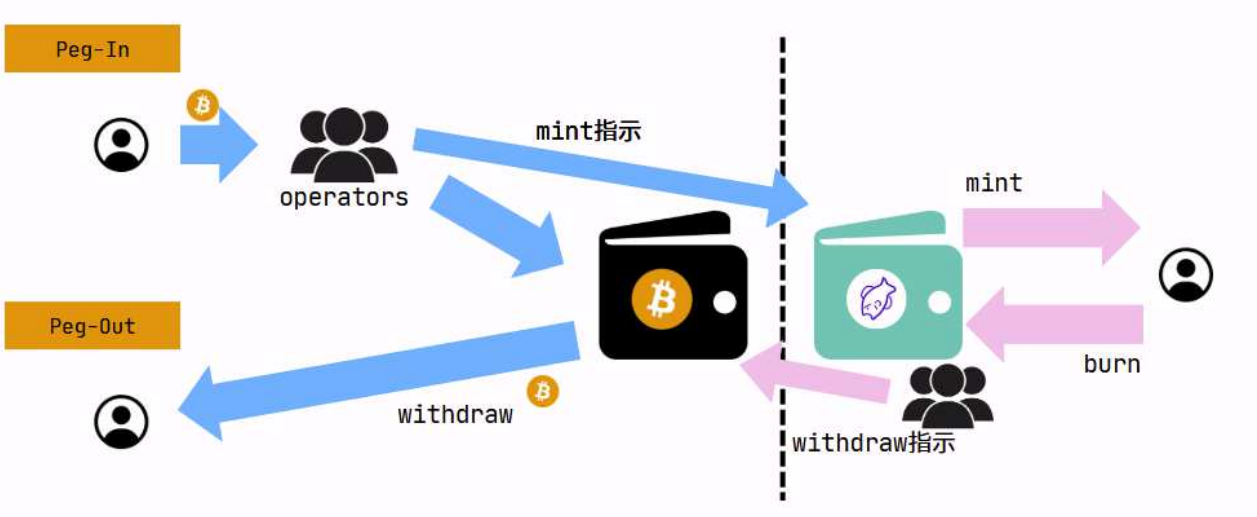
Peg-out

現実的なブリッジ実装案

マルチシグ

よくあるのは、運営者だけ鍵で作ったマルチシグアドレスを用意して送金してもらう方法である。

peg-in はそれでよいが、peg-out は peg-in したトランザクションを使わず、別途運営が管理しているウォレットから送金することがほとんどだろう。



単純なマルチシグではなく FROST のような閾値署名を使ったマルチシグも考えられる。

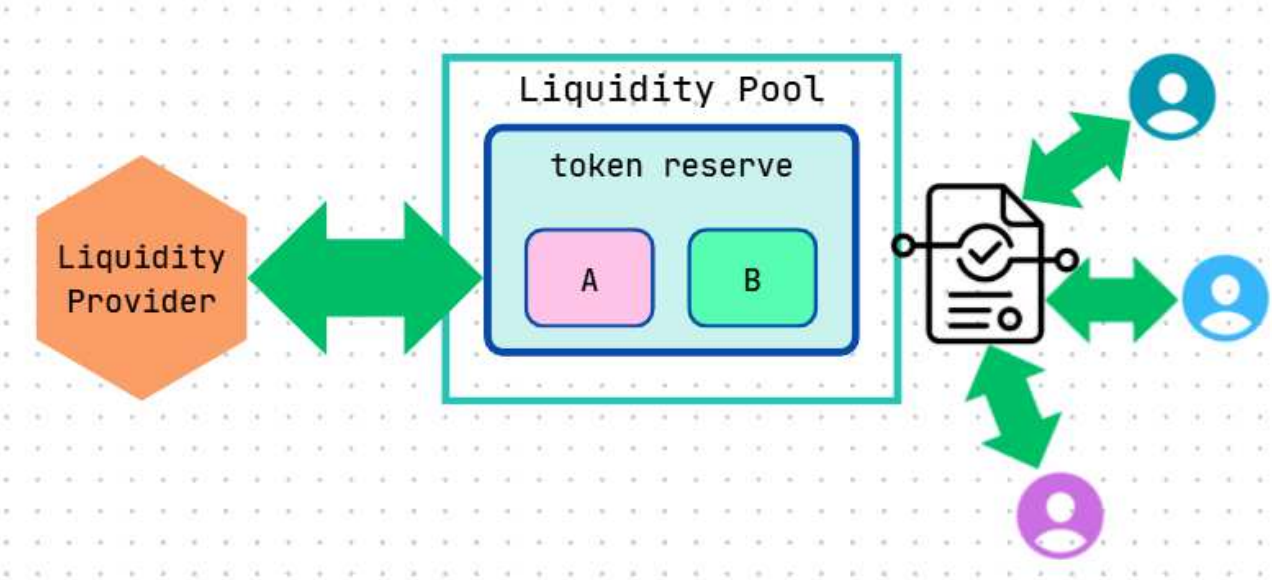
Lightspark の UTXO 管理では FROST を組み合わせたマルチシグにしたり、所有権の移動なども考慮していたりする。

Spark - Bitcoin L2#1adc16

マルチシグ方式は運用者が mint や burn 後の withdraw を処理するので decentralized にならない。
Bitcoin 側の BTC とブリッジ先の価値に運用者の操作が関わる点が、運営国において法律的に許可を得るなどの必要性に影響を及ぼす可能性がある。

DEX AMM型

DEX AMM型のようにすべてスマートコントラクトで実現できるなら、まだ自由にできる可能性はある。



しかしこれは同じスマートコントラクトが動くチェーンだからできることであり、Bitcoinとその他、となるとできない。Bitcoin系のトークンとであればできるかもしれないが、Bitcoinスクリプトの自由度ではなんとなくできないような気がする。
やりたいなら Bitcoin を一度 EVM などでトークン化しておくことになるが、その作業がそもそもブリッジである。

BitVM2 bridge

BitVMを参照。
fraud-proof で

BitVM3s

NotebookLM
BitVM2 bridgeよりも運用コストが下がる。なんと 1,000倍！！
最初のセットアップで 280 GB の容量が必要になるが、それ以降は大きいトランザクションでも 100kB いかない(66 kBくらい)。

こちらも fraud-proof なので正直な評価者がいて間違いを指摘しない限りは「正しい」ということになってしまう。

設計として評価者になることは誰にでもできるので、心配なら自分で評価しなさい、というくらいしかない。

BitVMX bridge

BitVMX Bridge - Rootstock (RSK)

Rootstock 開発中のブリッジ。以前は単体で BitVMX の開発(Rootstockとは関係ない)という感じだったのだが、

trust minimized で verifiable bridge だそうだ。

ロードマップでは 2026年Q1 にメインネットリリース予定。

元の BitVMX は 2025年Q2リリースだったのが結局これになったということか。

同じく fraud-proof方式らしいが詳細は不明。

シンプルなブリッジを考える

2-of-2マルチシグ

2-of-2 マルチシグのブリッジを考える。

実際に使うなら TimeLock して期限を過ぎても mint されないならユーザが回収するようにすべきだろう。

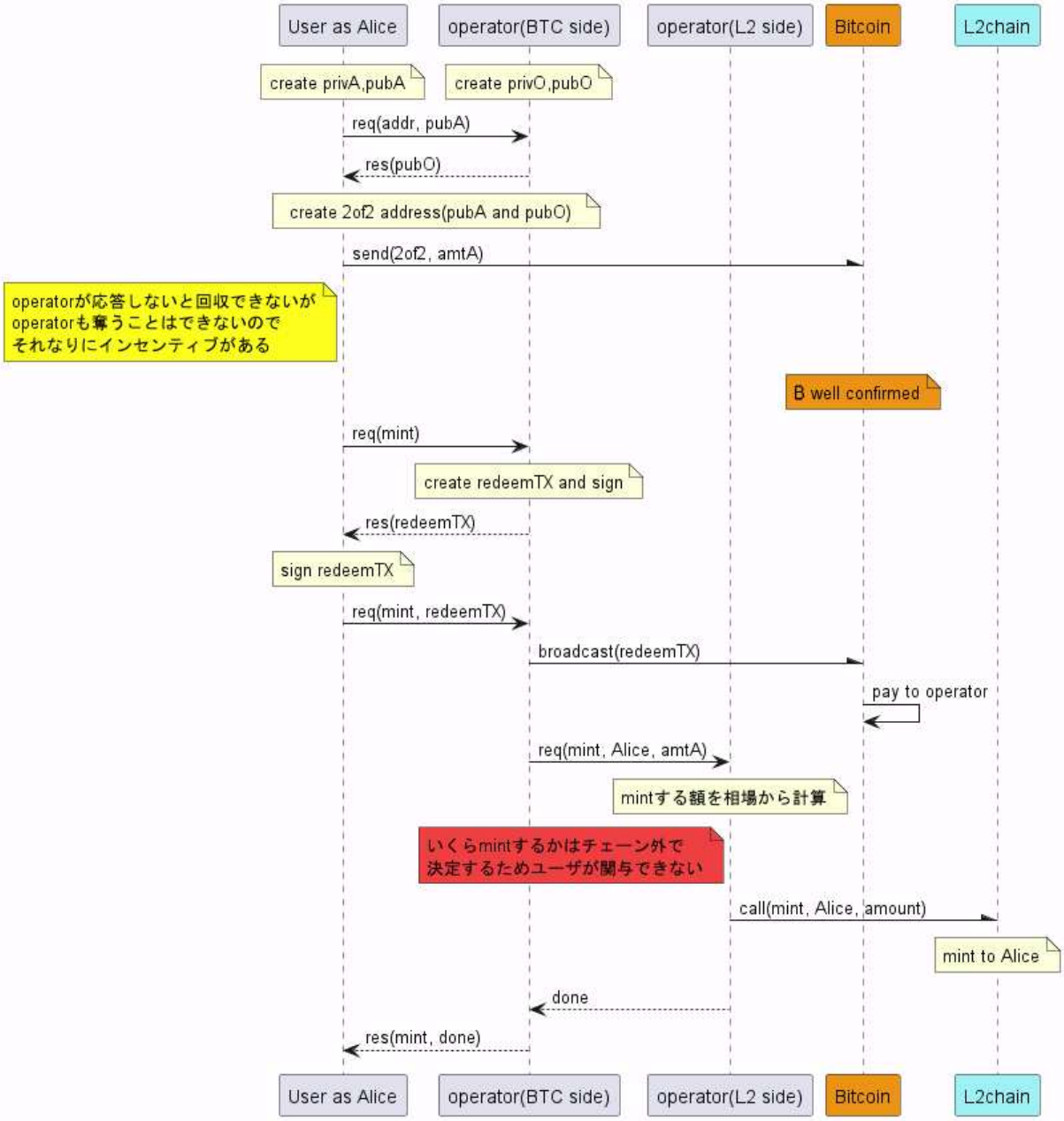
特にL2が何かを考慮せず、L2自体の管理者ではなくトークン発行者、あるいはトークン保持者。

ユーザとのマルチシグなので、ユーザが署名に応じない限り運営者は利益を得ることができない、というインセンティブがある。

しかし mint する額をスクリプトなどで縛ることができないので、mint されなかったり期待よりも少ない額だったりする可能性はある。

運営者が mint したあとにユーザが署名する方式にすると、今度はユーザが逃げる可能性がある。

それを避けるには HTLC というか atomic swap がよいのだが、L2チェーン側にユーザの何かが必要になる。しかし L2側のユーザに何かあるくらいなら直接そちらからトークンをmintしてもらえばよい。そうしないのは Bitcoinしか持っていないユーザのためのシステムだからだ。



HLTC

ChatGPT

ユーザの BTC支払先を hash lock したスクリプトにして、L2チェーン側でユーザが運用側に mint したトークンで preimage を送るまで mintしたトークンはロックする

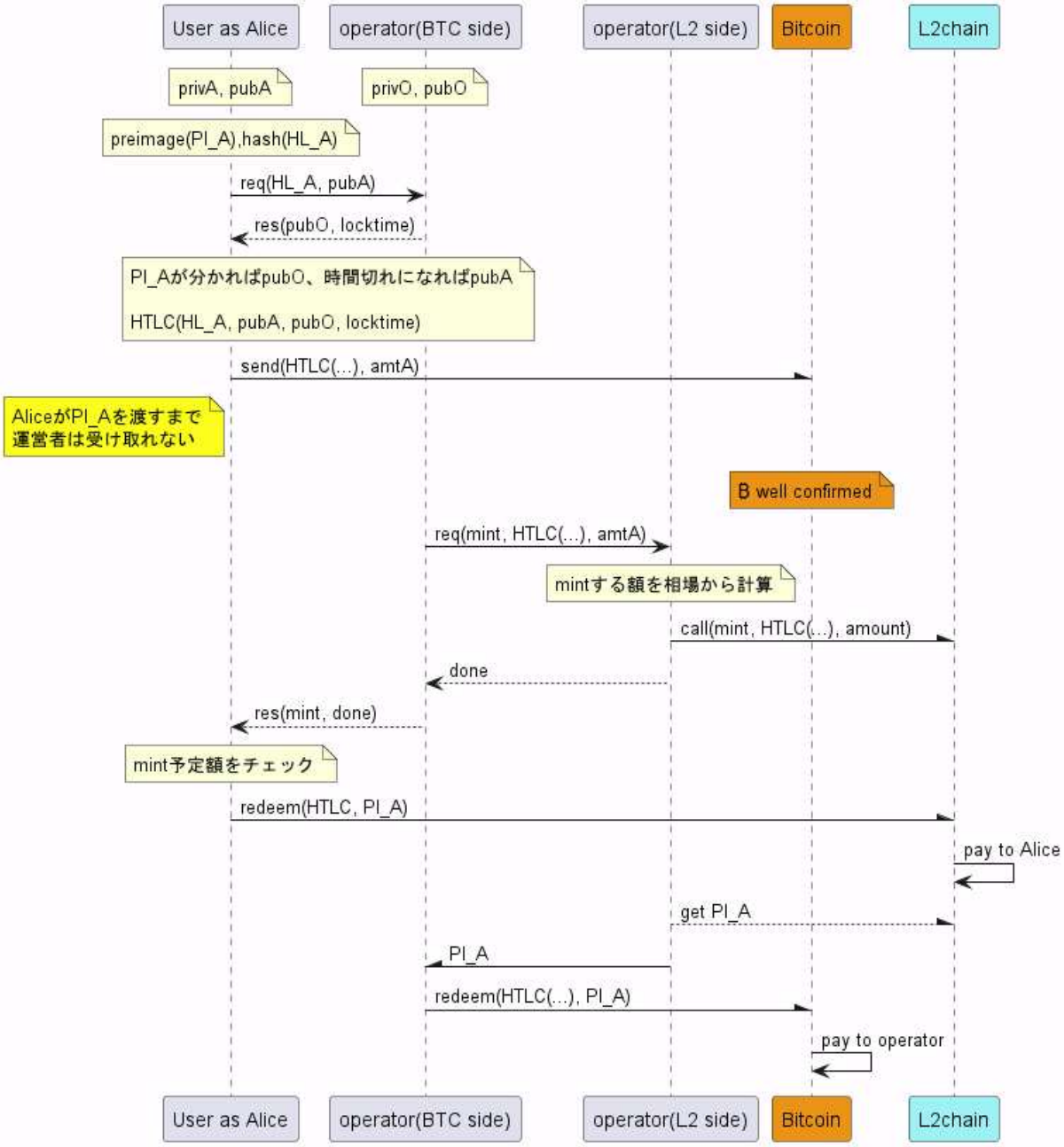
それだけでは運営者が mint ロックを解除しない心配があるので、mint 側も同じ preimage で hash lock しておく。

考慮漏れを ChatGPT に確認した。採用されにくい理由。

双方がオンラインでないといけないので利便性が悪い

タイムロックなどの管理が面倒。運用の手間が大きい。

トランザクションが増える。


User as Alice
operator(BTC side)
operator(L2 side)
Bitcoin
L2chain
privA, pubA
privO, pubO
preimage(PI_A),hash(HL_A)
req(HL_A, pubA)
res(pubO, locktime)
PI_Aが分かればpubO、時間切れになればpubA
HTLC(HL_A, pubA, pubO, locktime)
send(HTLC(...), amtA)
AliceがPI_Aを渡すまで
運営者は受け取れない
B well confirmed
req(mint, HTLC(...), amtA)
mintする額を相場から計算
call(mint, HTLC(...), amount)
done
res(mint, done)
mint予定額をチェック
redeem(HTLC, PI_A)
pay to Alice
get PI_A
PI_A
redeem(HTLC(...), PI_A)
pay to operator
User as Alice
operator(BTC side)
operator(L2 side)
Bitcoin
L2chain