BITCOIN LAYER 2 ECOSYSTEM

プロダクト編

MAY - OCTOBER, 2025

Citrea

Citrea

https://citrea.xyz/

- Bridge : Clementine
  - v1: BitVM2 bridge: peg-in額固定(10BTC?)
  - v2: Garbled Circuits and TOOP(under development)
- L2
  - RISC Zeroを使用したzkEVM(type 2.5)
  - zkSNARKもzkSTARKも使っている
- DA
  - Bitcoin L1を使っている
  - Inscription風
- Note:
  - L2上では2秒程度でブロックを作成
  - 1時間ごとにL1に投稿しているらしい



- RISCzero
- revm/reth
- Succinct
- BitVM

Bitlayer

Bitlayer v2

Bitlayer

https://www.bitlayer.org/

- Bridge
  - BitVM2 bridge
- L2
  - 1つの上で複数のVMを扱えるマルチVM構想
    - 現在はEVMのみ
- DA
  - BitVM2での不正証明
- Note:
  - 2025年6月現在はPoSサイドチェーン方式(v1)
  - 2025年Q1/2で Rollup化
  - 2025年Q4でTPSなどの向上



- gethベース

B^2 Network

B² Network

- Bridge
  - 独自のブリッジ(Polygon zkEVM base)
- L2
  - EVM互換(Polygon zkEVM base)
- Note:
  - Bitcoin L1に zk-proof を書き込んで不正申告がなければ受け入れる fraud-proof 方式
  - DA層を別途持っている

B² NETWORK

https://www.bsquared.network/



- Polygon zkEVM

Starknet

Starknet

Starknet は Ethereum mainnet上で運用中。Bitcoin版のロードマップは不明。

STARKNET

https://www.starknet.io/

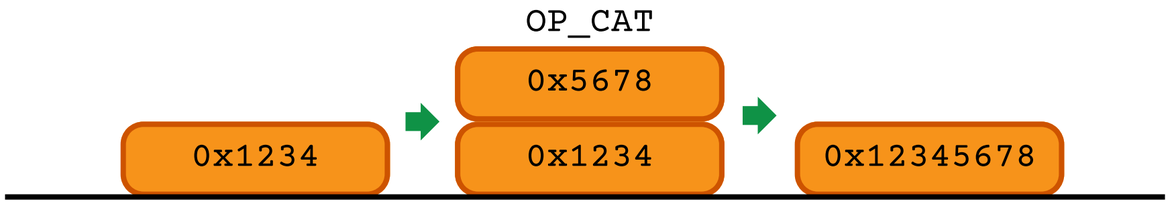
- Bridge
  - OP_CAT推し(mainnetで使えるようになるか不明)
  - それまでのつなぎとして、マルチシグ方式やBitVMでも開発しているそうだ
- L2
  - CairoVM(言語はCairo)
  - EthereumとBitcoinの両方から使えるようにする
  - zkSTARK
- Note:
  - signetでのOP_CAT版PoCあり(2024年11月)



- CairoVM
- STWO

OP_CAT

- concatenate(連結する) の略。ネコではない。
- この命令は、Bitcoinのスタックに載っている 2つのデータを連結する
- 初期のBitcoin Coreには実装されていたが、セキュリティの都合で2010年に廃止になった
- 提案されているBIP-347 では結合後のサイズが 520バイトまででそれを超えるとエラーになる制限を付けた



Word	Opcode	Hex	Input	Output	Description
OP_CAT	126	0x7e	x1 x2	out	Concatenates two strings. *disabled.*
OP_SUBSTR	127	0x7f	in begin size	out	Returns a section of a string. *disabled.*
OP_LEFT	128	0x80	in size	out	Keeps only characters left of the specified point in a string. *disabled.*
OP_RIGHT	129	0x81	in size	out	Keeps only characters right of the specified point in a string. *disabled.*
OP_SIZE	130	0x82	in	in size	Pushes the string length of the top element of the stack (without popping it).



OP_CAT

できなかったことができるようになる

- コベナンツ: 送金先と額に制約を付ける
  - 再帰コベナンツで状態を擬似的に持つなど
- Merkle Treeの構築と検証
- Tree Signaturesという複雑な署名
- 耐量子Lamport署名
- 非ごまかし契約: 二重支払いに対するペナルティ
- STARK検証
- その他いろいろ

OP_CATでのコベナンツ

Bitcoinスクリプトは送金額や送金先アドレスを見ることはできないので、通常であればそれらをスクリプトの条件にすることはできない。

しかしシュノア署名の計算方法を逆手に取り、秘密鍵などに条件を加えることでトランザクションのハッシュ値を算出できる。
直接送金額や送金先アドレスを指定することはできないが、トランザクションハッシュであれば指定できることになる。

そこで送金額と送金先アドレスのハッシュ値をスクリプトに持ち、
それ以外のデータをスタックで与えてもらい、それらを**連結して**トランザクションハッシュの値にして比較することで制約を付ける。

Rootstock

Rootstock



https://rootstock.io/

老舗のサイドチェーン方式。昔は RSK Networkという名前だった。mainnetでの運用もされている。

- L2
  - Rootstock VM(EVM互換)
- Merged Mining
  - Merged Mining という Bitcoinのマイナーがそのまま Rootstockのマイナーになることも出来る方式
    - Auxiliary Proof-of-Work

Liquid Network

Liquid Network

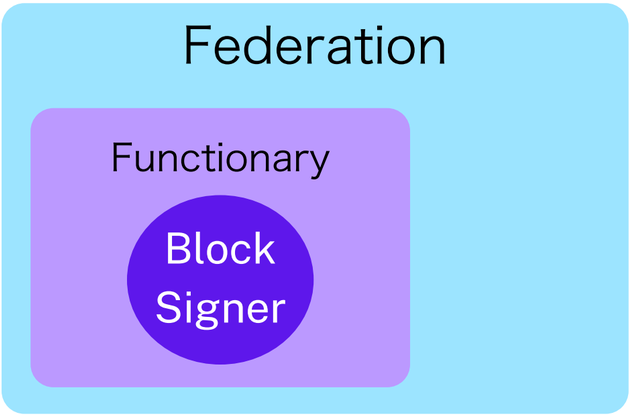


https://liquid.net/

- Blockstream社が開発した Sidechain
- ネイティブトークンは L-BTC
  - Federationの許可を得てトークン発行できる
- ブロック生成は1分間隔
- コンセンサスアルゴリズムは Strong Federation (と呼んでいる)
  - 現在は 11-of-15 のマルチシグ
- Confidential Transaction という金額やアセットを隠蔽したトランザクションの作成が可能
  - 隠蔽はするが検証は可能

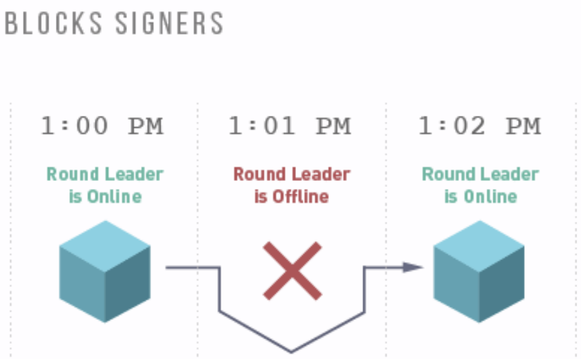
Functionary

- Liquid Federation のメンバーは 81社
  - メンバーはブリッジを運用することができる
- その中でノードを直接運用するメンバーを Functionary と呼ぶ
  - HSM(Hardware Security Module)を搭載した専用サーバー
  - Peg-In/Peg-Out などができる
- Functionary の内の15社が Block Signer
  - ブロック生成の提案や署名を行う
  - 地理的や地政学的多様性を考慮して選定
  - チェーン運用を止めずにメンバー交代可能



Block Signer

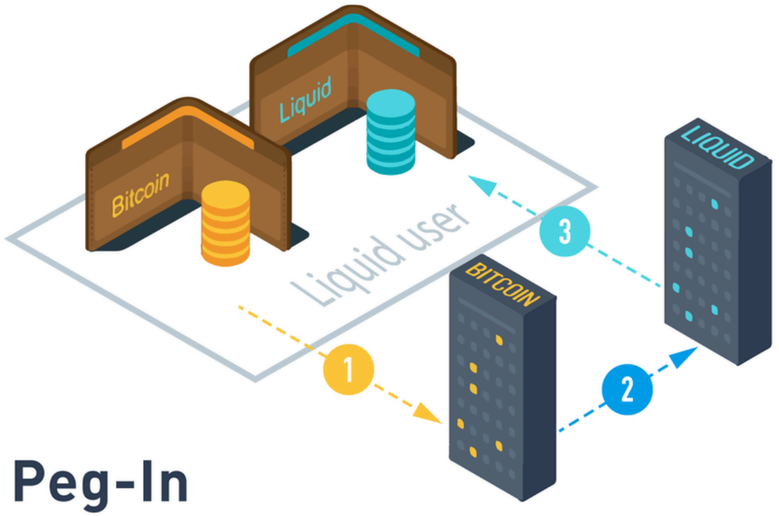
- Block Signer の誰かが担当になってブロックを提案して署名を集約する
  - 署名は15件中11件集まれば良い
    - 署名が集まらない状況での緊急対策は用意されている
  - 署名を集約する担当はラウンドロビンで持ち回り
  - 1分で終わらなかったら、そのラウンドは失敗して次へ進める
- reorg の可能性がわずかにあるのでファイナリティは次ブロックの承認後
  - 通信が不安な場合くらいしか起きない
  - 1ブロック以上の分岐はしない



https://docs.liquid.net/docs/technical-overview

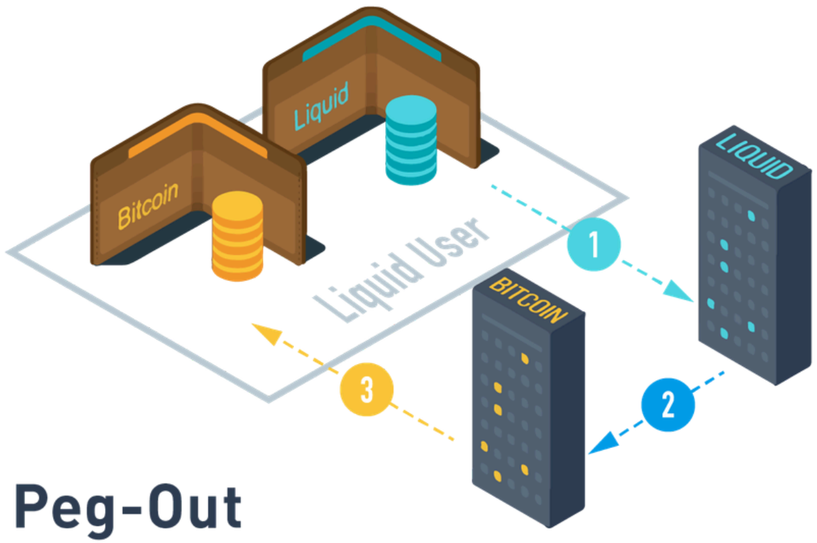
Bridge

- Bitcoin – Liquid のブリッジも Block Singer と同じ鍵を使う



Peg-In

1. Liquid user sends BTC over the Bitcoin Network to peg-in address.
2. Liquid user waits for 102 confirmations. Functionaries in Liquid Network now accept this freezing of BTC and allow access to L-BTC.
3. Liquid user claims L-BTC and it appears in their Liquid wallet.



Peg-Out

1. Liquid User creates a peg-out transaction to request release of BTC.
2. Liquid Network releases BTC after 2 Liquid confirmations.
3. Liquid User receives BTC into Bitcoin wallet.

https://docs.liquid.net/docs/technical-overview

Confidential Transaction

- Liquidのトランザクション構成はBitcoinに類似している
- 金額とアセットを秘匿したトランザクション形式も使用可能
  - Confidential Transaction と呼ぶ
  - 送金元や送金先は秘匿できない
- 秘匿しているが検証は可能
  - INPUT の総額と OUTPUT の総額の合計がゼロになること
  - マイナス値だったりオーバーフローしていないこと

スクリプト

オペコード

New
OP_CHECKSIGFROMSTACK
OP_DETERMINISTICRANDOM
OP_INSPECTINPUT
OP_INSPECTOUTPUT
OP_COVENANT
OP_PUSHCURRENTINPUTINDEX
OP_CHECKSIGFROMSTACKVERIFY
OP_CHECKMULTISIGFROMSTACK
OP_CHECKMULTISIGFROMSTACKVERIFY

Enabled
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

SimplicityHL という Rust風の言語で書くことができる。
Bitcoinスクリプトとは別物で
Simplicity が直接動く。



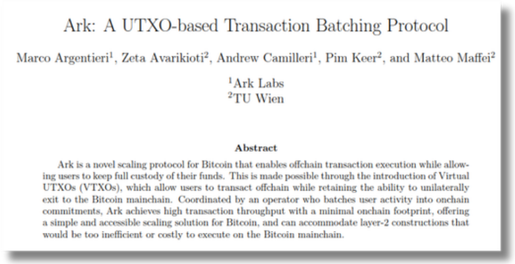
ARK

Arkプロトコル

https://ark-protocol.org/

Arkプロトコルは、最初はLightning Networkのオンボーディングのために考えられていたが、設計変更して独立した L2になった。

今のところ、実装しているのはArk Labs社とSecond社がよく知られている。



Ark: A UTXO-based Transaction Batching Protocol

Marco Argentieri[1], Zeta Avarikioti[2], Andrew Camilleri[1], Pim Keer[2], and Matteo Maffei[2]

[1]Ark Labs
[2]TU Wien

Abstract

Ark is a novel scaling protocol for Bitcoin that enables offchain transaction execution while allowing users to keep full custody of their funds. This is made possible through the introduction of Virtual UTXOs (VTXOs), which allow users to transact offchain while retaining the ability to unilaterally exit to the Bitcoin mainchain. Coordinated by an operator who batches user activity into onchain commitments, Ark achieves high transaction throughput with a minimal onchain footprint, offering a simple and accessible scaling solution for Bitcoin, and can accommodate layer-2 constructions that would be too inefficient or costly to execute on the Bitcoin mainchain.

ARK LABS

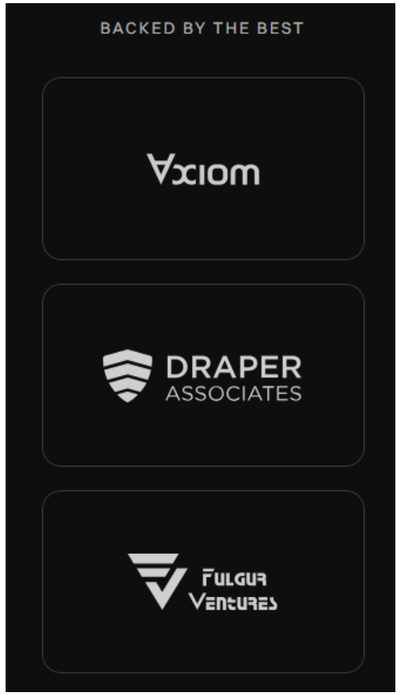
second

Ark Labs

https://arklabs.xyz/
https://arkadeos.com/

Ark Labs社の Arkadeは、Ark実装の arkd やウォレットを展開している。
2023年にArk protoclを公開し、2024年半ばにArk Labsを立ち上げたそうである。

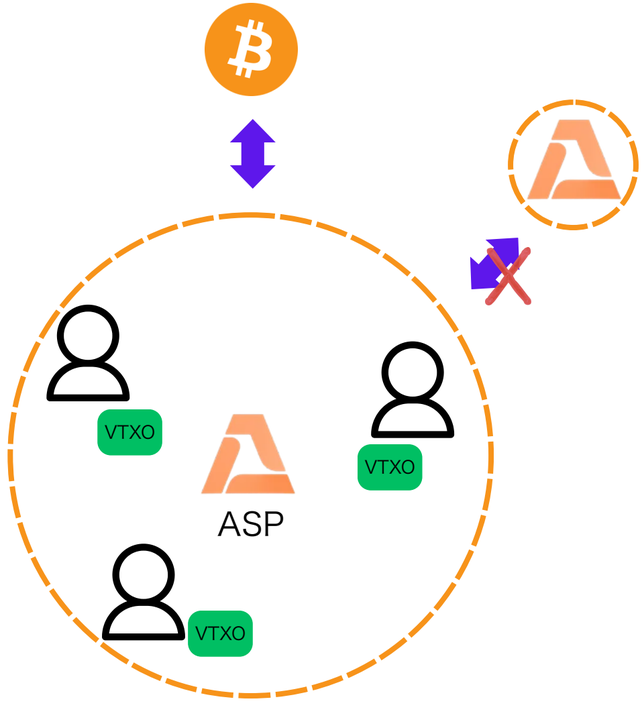
Arkプロトコルの主な実装をやってきていて、製品として Arkade ブランドを立ち上げたというところだろう。
特徴は、ライブラリの実装が進んでいることと、スマートコントラクトの実装があることだろう。またTEE(セキュアなハードウェア実行環境)も含んでいるようだ。

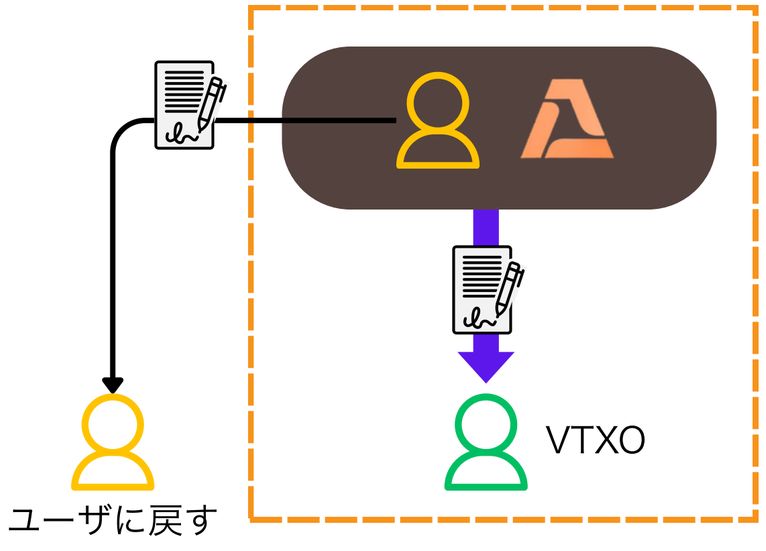


Ark

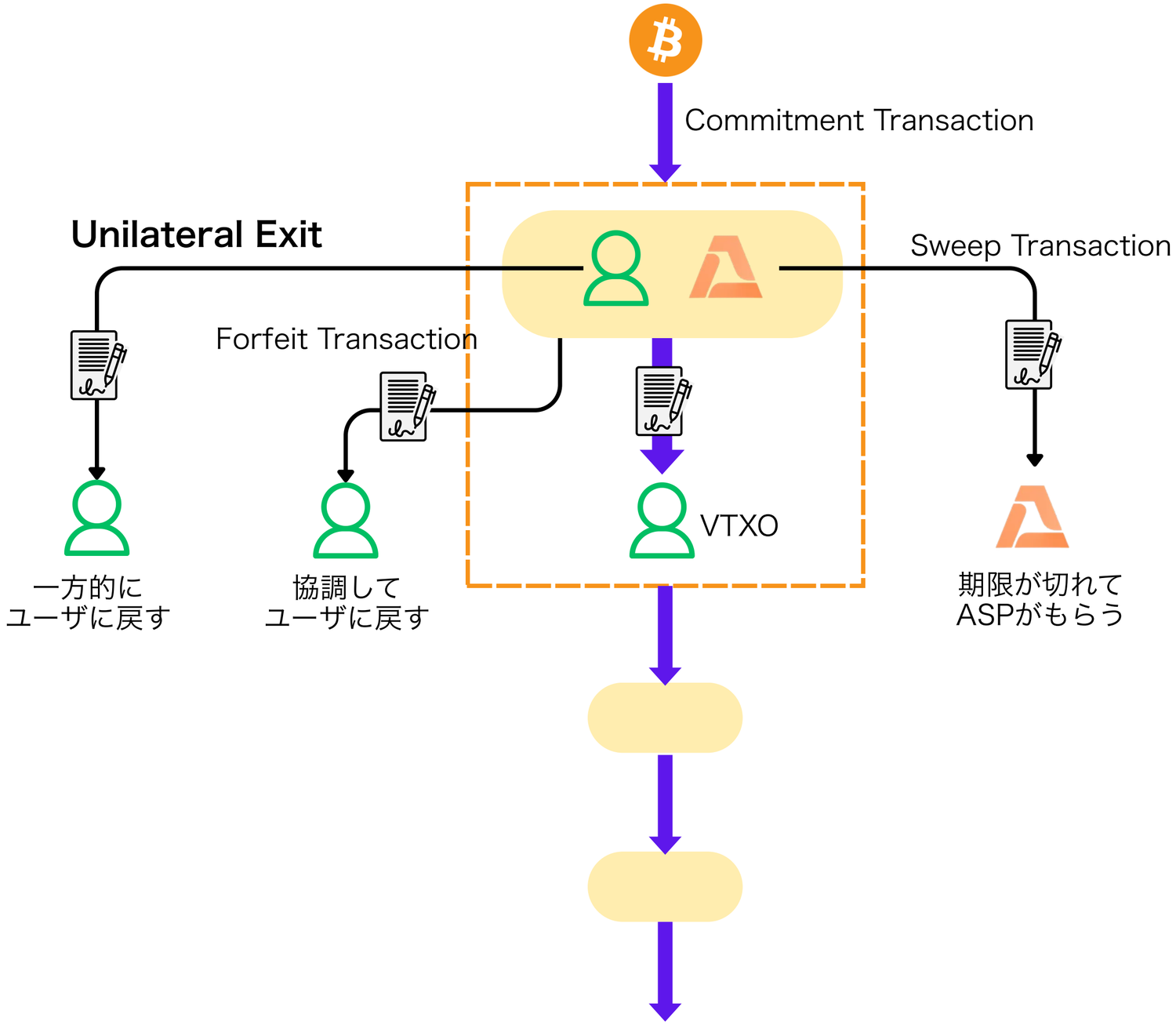
ASP(Ark Service Provider)にクライアントがぶら下がる形で運用される。
ASP間は通信しないので、別ASPへの送金はできない(少なくとも Arkade の方は)。

ASPがいわゆるオペレーターですべてを管理する。
ただ、ユーザーからL2への入金はユーザーとASPで管理するスクリプトに対して行われる。
スクリプトの条件はユーザーに対して有利になっていて、ASPはユーザーの署名がないと送信できないようになっているが、ユーザーは自分の署名があれば送信できるようになっている。





Ark

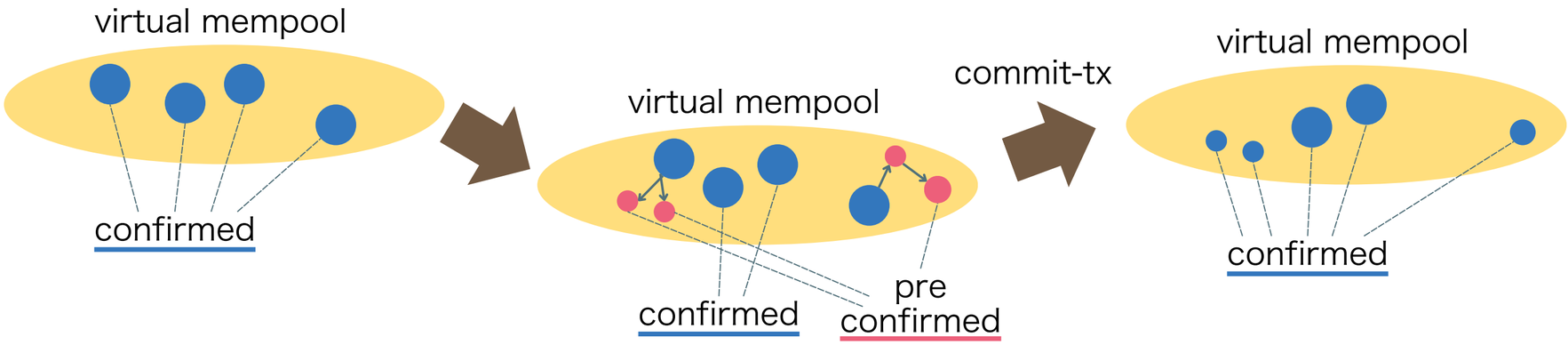


- Commitment Transaction
- Boarding Transaction
- Sweep Transaction
- Forfeit Transaction

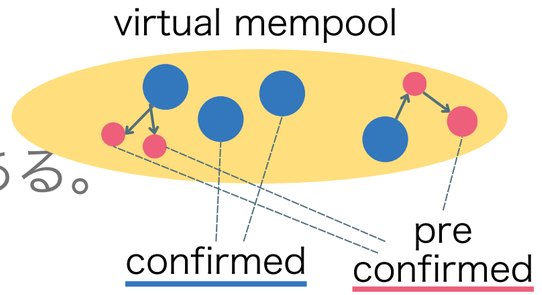
Ark

運営者のサーバー(ASP)で運用されている仮想的なmempoolがある。
仮想mempool空間の中に各ユーザーの仮想的なUTXOがある。
ユーザーは仮想UTXOを送受信する。
その間の仮想UTXOは “pre-confirm” な状態と呼ばれる。

運営者は定期的に仮想mempoolの内容をオンチェーンに書き込む。そうすると仮想UTXOは “confirmed” な状態になる。



Ark



“confirmed”なVTXOはオンチェーンに紐付いているので「安全」である。

“pre-confirmed”なVTXOは送金者とASP管理者の両者が
署名しているだけの状態。
悪い送金者と悪いASP管理者が共謀すると、一度使用したVTXOを
別の人に署名すると「二重支払い」ができてしまう。

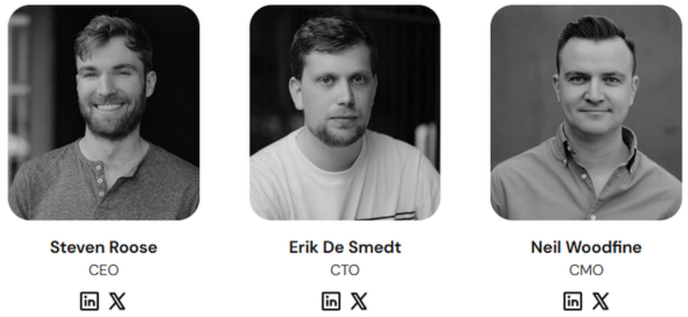
二重支払いしないインセンティブとして以下の説明がある。

- そのASPの信頼がなくなる
- 不正はL1に戻すときにバレる

Arkade はハードウェアで保護した実行環境を提供し、そこで動いているバイナリが改造されていないなどを暗号的に確認できるようにしている。

Second

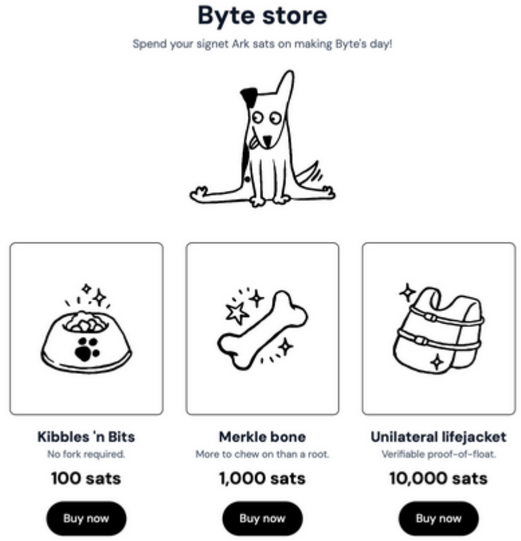
https://second.tech/



Second社は元Blockstreamの人たちで構成されている。
こちらも2024年に作られた会社である。

特徴は、Arkの支払いによって Lightning Network 請求書の支払いをできることである。それ以外にeCash や他のArkサーバーに支払うこともできる。

Arkade社とは異なるArkプロトコル実装で、互換性はないと思われる。



RGB

RGB

LNP/BP Association という非営利団体のワーキンググループの1つが RGB-WG である。Maxim Orlovsky(Dr. Orlovsky) が中心。

LNP/BP Association https://www.lnp-bp.org/

RGB Consortium https://consortium.rgb.tech/

Pandora Prime

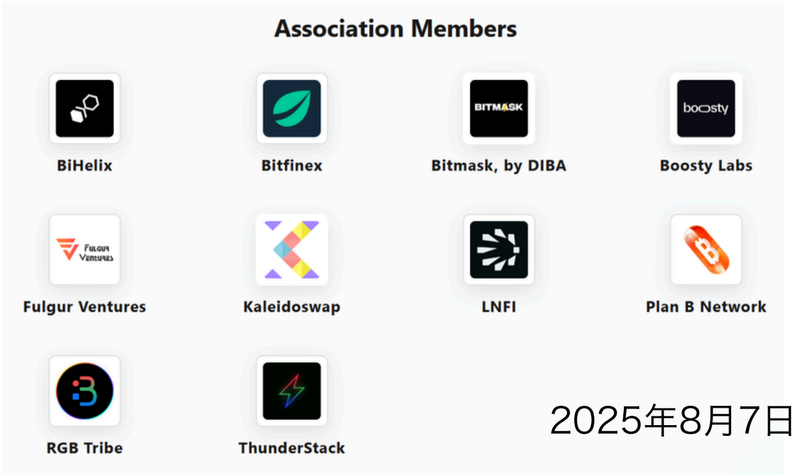


Dr. Maxim Orlovsky
dr-orlovsky · Their Majesty

2025年7月14日に RGB Protocol Association という団体が発表された。

RGB Protocol Association https://rgbprotocol.org/

https://rgb.info/



2025年8月7日現在

最近の動向

2025年7月に大きな動きがあった。

- RGB v0.12 のコンセンサス公開(アプリは RC版)
  - コントラクトは将来のバージョンとの互換性が確保された
  - zk-AluVMの導入
  - その他、結構v0.11から変更されている
- RGB Protocol Associationの設立
  - 有料の会員制らしい
  - RGB v0.11.1 版の公開
- USDT on RGB の正式展開

RGB

RGB自体の目標は、Bitcoin上でスマートコントラクトを実装するためのインフラを提供すること。

現状でBitcoin L1とLightning Networkで動かすことができている。

最近、トークンの発行だけでなくスマートコントラクトも動かせるようになったらしい

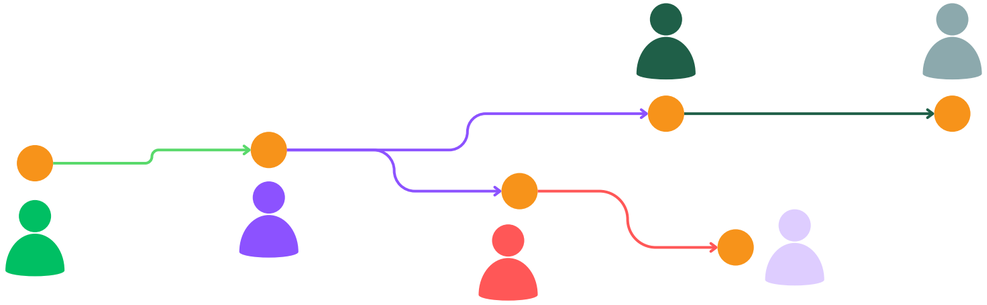


ステート管理

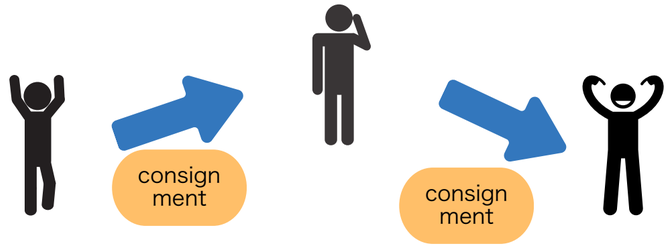
サイドチェーンやRollupはステート全体を管理する方式である。
ステートがちゃんとしているかどうかを検証する方式を考えたり実現したりするのはかなり大変である。コストもかかる。全員が参照できてしまう。



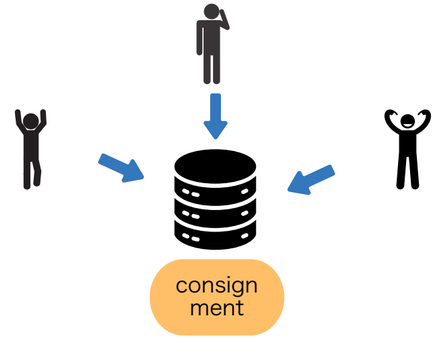
異なるアプローチとして、全体のステートを持たずにステートに関係ある人たちが、自分のステートに関するところだけ管理する方法がある。
RGB が採用しているのもこの方式である。



Client Side Validation



ステートを共有せずに済ませるために、何らかの方法で
関連するステートのデータを相手に伝える。
(そのデータは consignment と呼ばれる)

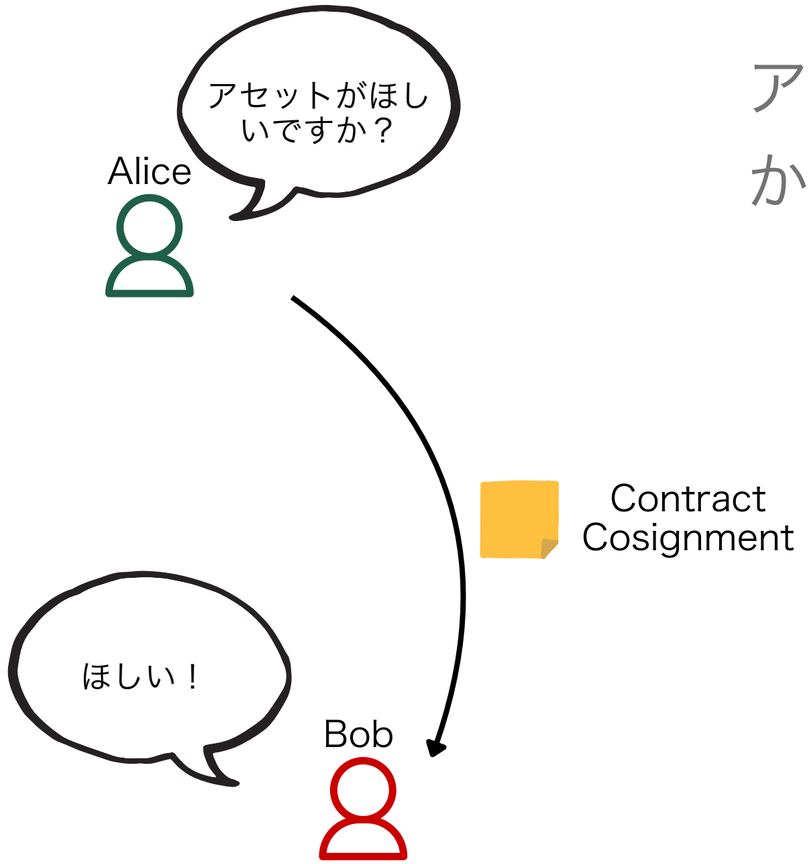


それよりも考慮すべきことは、そのステートの正しさである。
それぞれが自分のステートしか持っていないので、自分で正しさを検証できるようにしないといけない。

Client Side Validation(CSV)と呼ばれ、
RGBはその中でも TxO2 という方式を採用している。

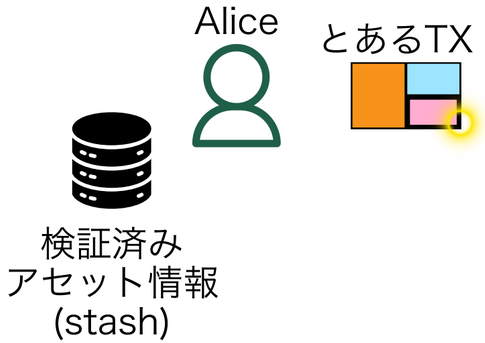
Method	Seal Definition	Seal Closing	Additional Requirements
PkO	Public key value	Transaction output	P2(W)PKH
TxO2	Transaction output	Transaction output	Requires Deterministic Bitcoin Commitments
PkI	Public key value	Transaction input	Taproot-only - Not working with legacy wallets
TxOI	Transaction output	Transaction input	Taproot-only - Not working with legacy wallets

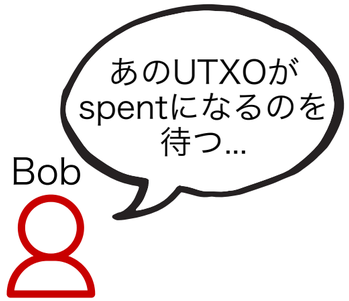
RGB動作概要



アセット/トークンは、定義を持っている相手にしか渡すことができない。

RGB動作概要

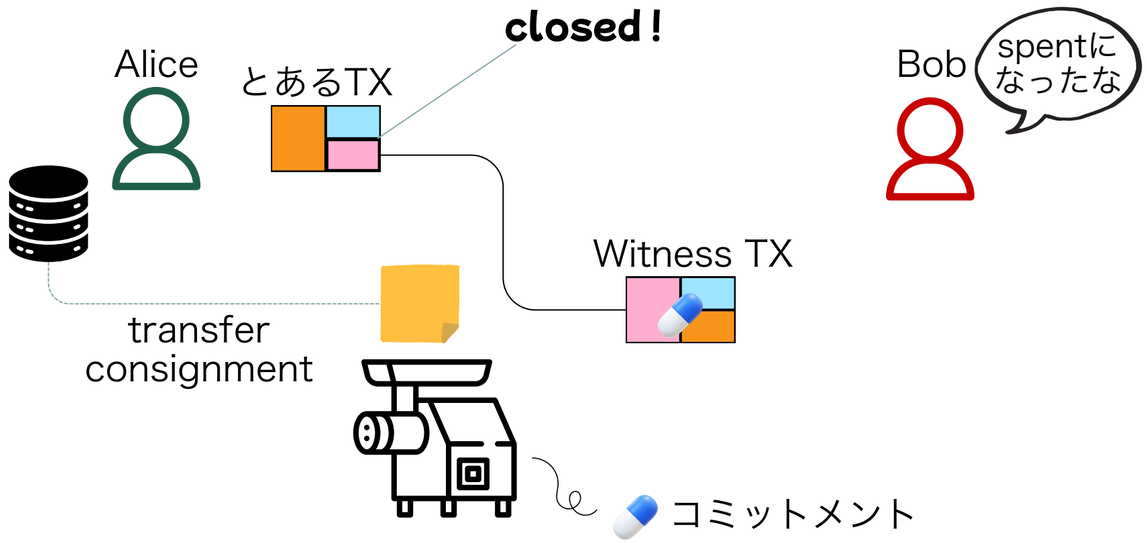




AliceはUTXOであるoutPoint を「検証済みデータを参照している」と決める。
これを「シールの定義」と呼ぶ。

そうすると、この outPoint が spent になると「何かイベントが起きた」という意味を持つ。
今回は「Bobにアセットが移動された」という意味を持たせる。
AliceはそのことをBobには伝えておく。

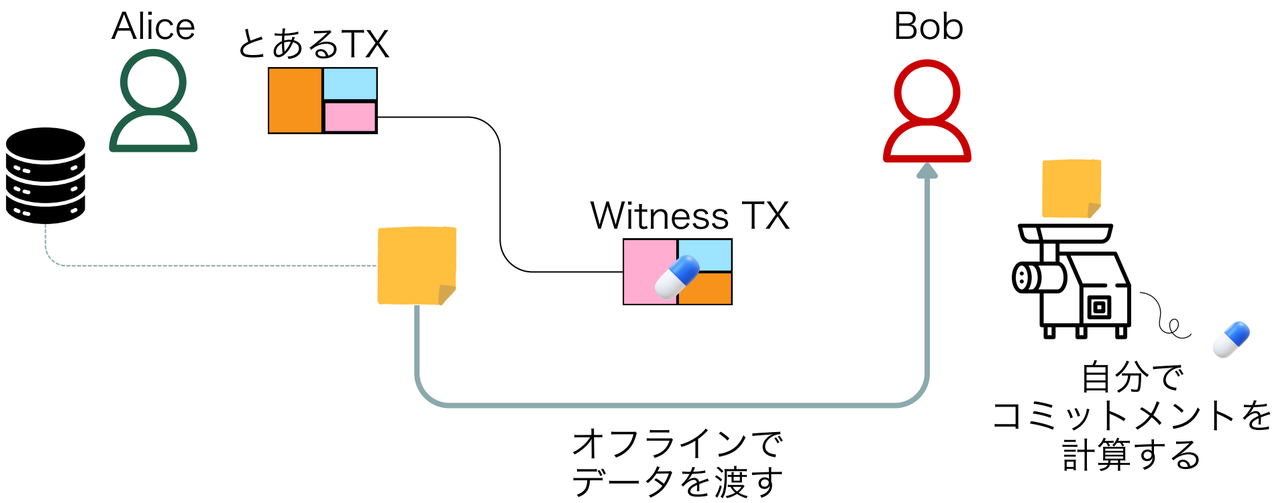
RGB動作概要



Alice がシール定義された outPoint を spent になることをRGBでは「シールが閉じられた」と表現する。
他のトランザクションを指すことができないので二重支払いもできない。
閉じたら閉じっぱなしになるので Single-use Seal と呼んでいる。

Alice が展開したトランザクションにはアセット情報をハッシュ計算などして隠した形で Tapscript か OP_RETURN に載せている。

RGB動作概要



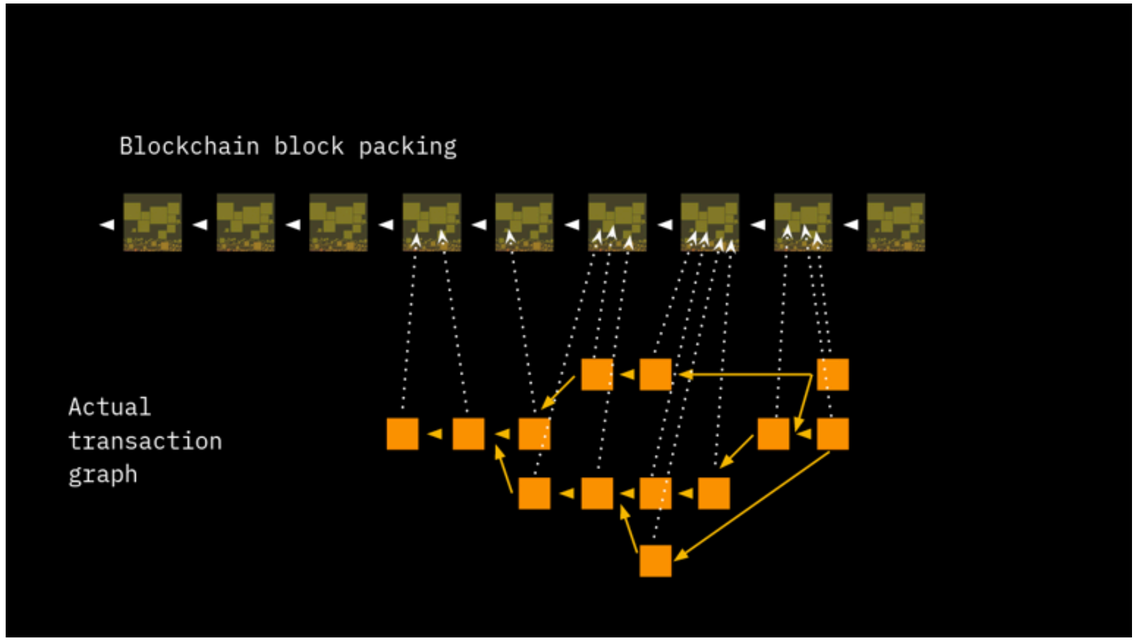
Alice から Bob に転送するアセット情報のデータを渡す。
データは“Transfer Cosignment”と呼ばれる。

Bob は受け取った consignment から自分で計算して同じデータがWitness Transactionに埋め込まれていることを確認できる。

RGB動作概要

Alice から Bob への転送について検証した。

Consignment にはアセット発行からここに至るまでのすべての履歴が載っていて、各クライアントは根っこから現在まで確認できるようになっている。



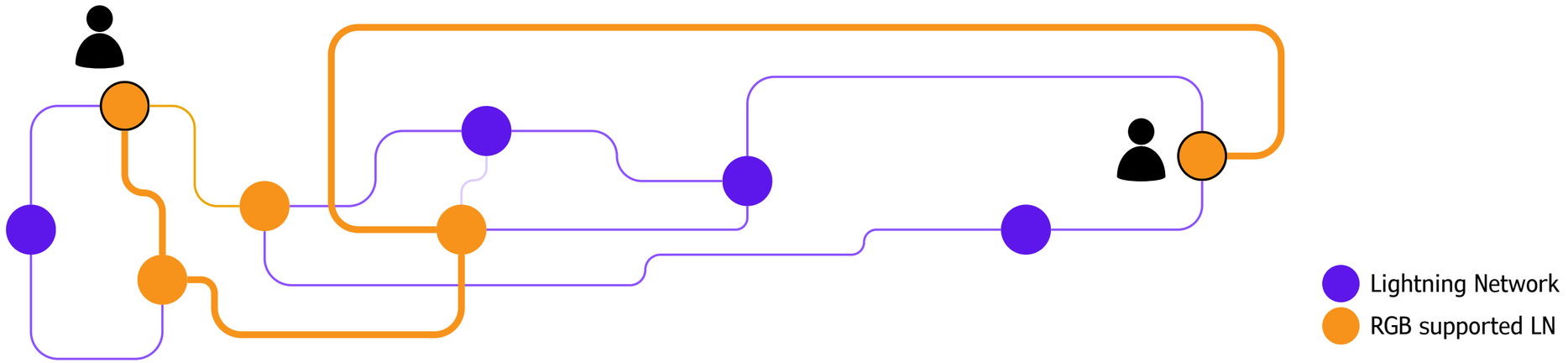
https://docs.rgb.info/distributed-computing-concepts/client-side-validation

このようにクライアント側で検証でき、またそれ以外に検証ができないので Client Side Validation と呼ぶ。

Lightning Network対応

- Commitment Transactionを改造する
- なのでチャネルの相手もRGB対応したノードが必要
- ルーティングもできるが、その経路もすべて同じ条件が必要

この辺は Lightning Labs の Taproot Asset も同じだそうだ。



Arch Network

Arch Network

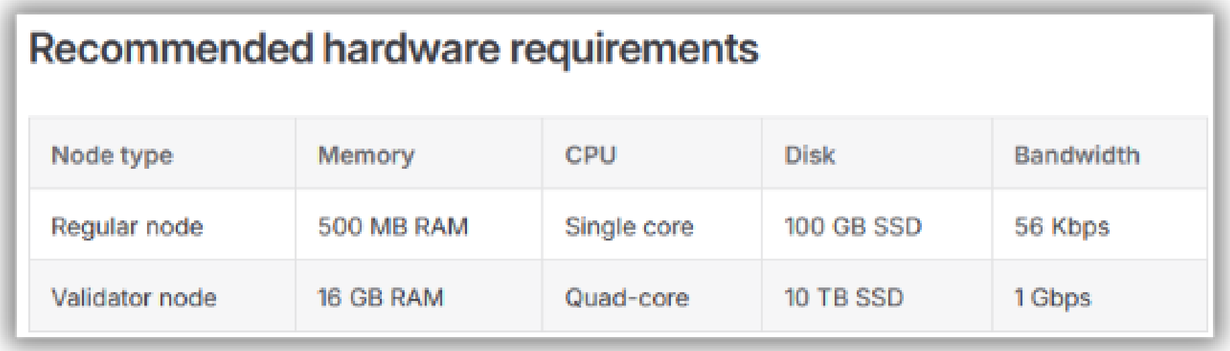


https://www.arch.network/

- ブリッジを作らない
  - デポジットはする
- ArchVMは eBPFという Linux や Solana で使われているVMをベースにして、直接Bitcoinネットワークにアクセスしたりトランザクションを作ったり展開する拡張を行っている
- ArchVMからBitcoinトランザクションを展開するには51%以上の署名を集めないといけない(FROST)

スマートコントラクト

- ステート管理はUTXOモデルを基盤としている
  - どうやらL1でトランザクションに結果を書き込むようだ
  - mempoolの間でも処理は進められるのでスループットは下がらないという言い方をしている



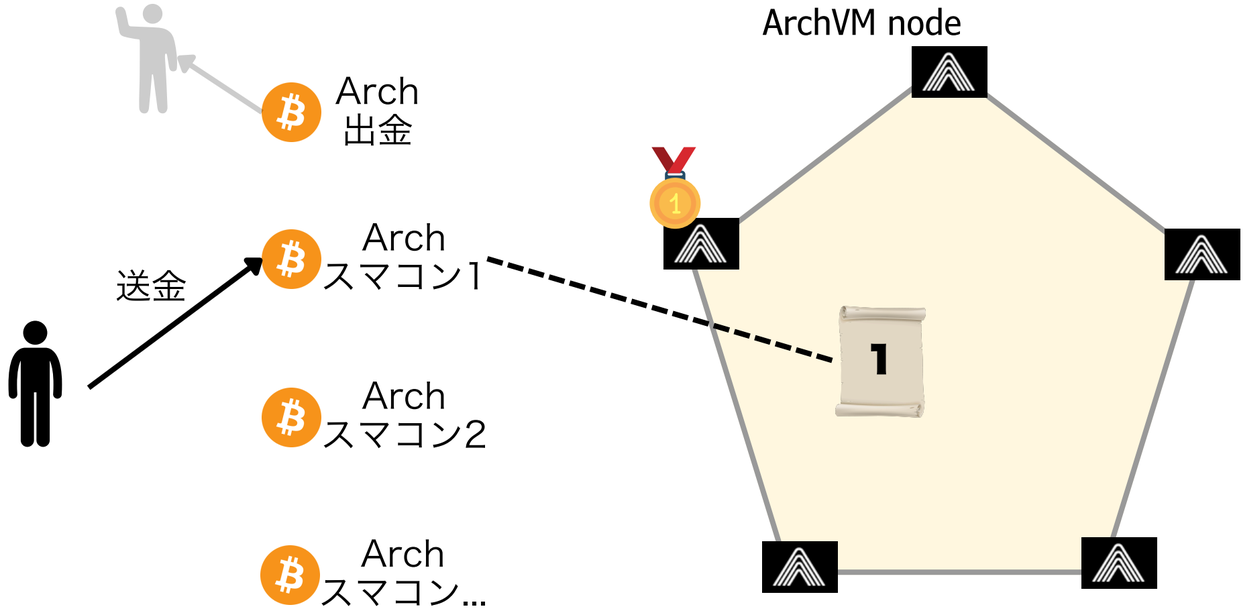
Recommended hardware requirements

Node type	Memory	CPU	Disk	Bandwidth
Regular node	500 MB RAM	Single core	100 GB SSD	56 Kbps
Validator node	16 GB RAM	Quad-core	10 TB SSD	1 Gbps

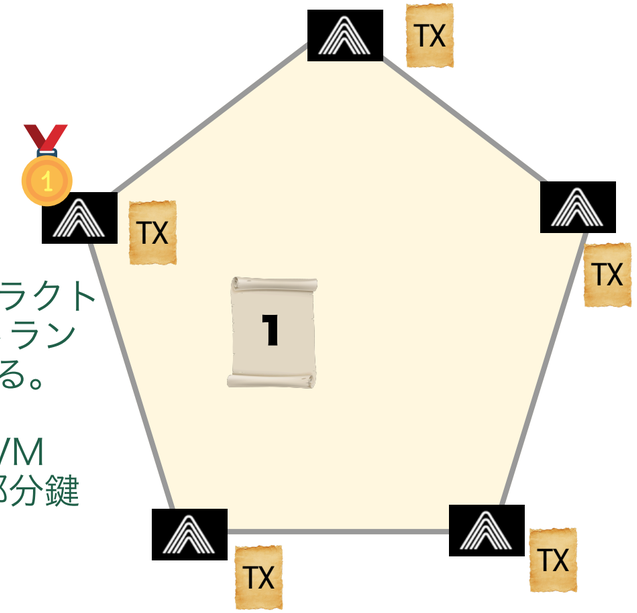
https://book.arch.network/docs/quick-start/requirements

ArchVM

- ArchVMはFROST+ROASTでバリデータたちの署名を受け取って集約する。集約し終わるとトランザクションをBitcoinネットワークに展開する。
- ArchVMがトランザクションを展開するのは、スマートコントラクトで拡張システムコールを呼び出したときや、なにがしかステートに関する処理など
- 最終的な責任はトランザクションを展開するリーダーが負う
- スマートコントラクトはユーザーが自由に置いて、自由にBitcoinに出金するシステムコールを呼ぶことができるそうだ。
    - スマートコントラクトはBitcoinアドレスを持ち、ユーザーはそのアドレスに資金を転送することで「実行」できる。

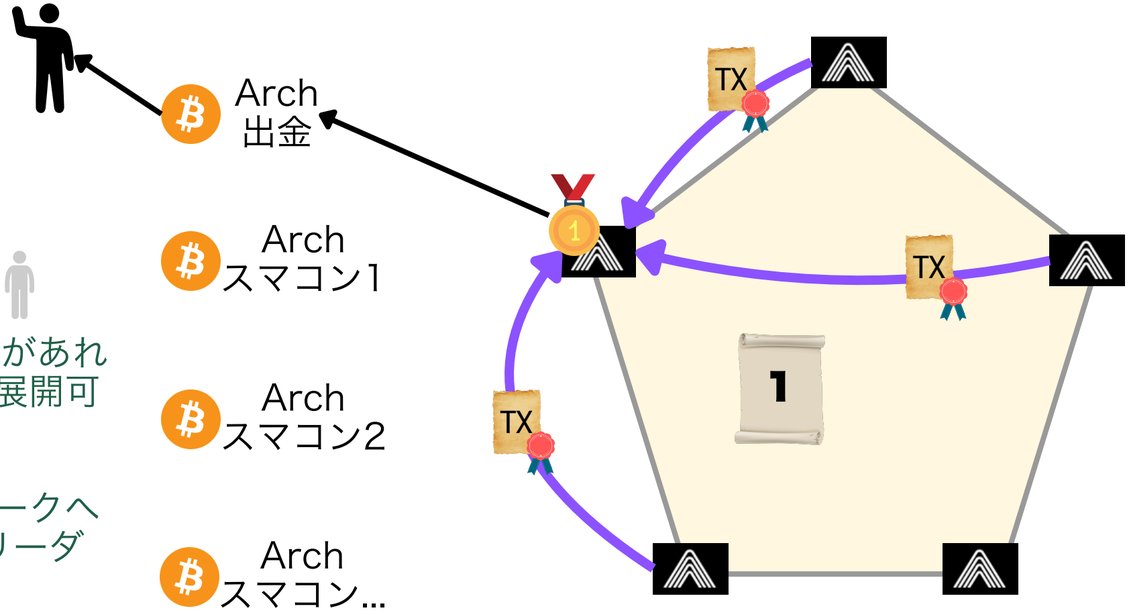


ユーザはスマートコントラクトを実行するために該当するBitcoinアドレスへ送金する。



ArchVMはスマートコントラクトを実行して自分でBitcoinトランザクション作ることができる。

ValidatorたちもまたArchVMで、それぞれがFROSTの部分鍵を持っていて署名できる。



Validatorの51%以上の署名があればBitcoinトランザクション展開可能。

署名集約とBitcoinネットワークへのトランザクション展開はリーダーのArchVMが行う。

FROST

Flexible **R**ound-**O**ptimized **S**chnorr **T**hreshold Signatures

- シュノアベースの閾値署名スキームでBitcoinマルチシグを効率的にするために考えられた
- m-of-n ができる
  - MuSig は n-of-n
- 集約することで単独鍵のシュノア署名になる
  - スクリプト長を気にする必要なし
- 署名を2ラウンドで行う
  - 悪意ある署名者によるプロセス妨害が可能
    - ROASTプロトコルによって信頼性を強化する

ROAST

Robust **A**synchronous **S**chnorr **T**hreshold Signatures



- FROSTのような閾値署名スキームの wrapper になって非同期ネットワークでの信頼性を強化する手順。
  - 署名計算ではなくプロトコル
- 署名する人のプールを作っておき、署名を送ってこない人がいたらその人を除外した組み合わせを作ってプロセスを進める。
- 署名を集める人をどう決めるかは ROAST の範囲外
  - ArchではdPoSコンセンサスでバリデーターたちを決める
  - バリデーターの中から署名を集めるリーダーとサブリーダーを選ぶ
- リーダーは署名してほしいトランザクションをネットワークに投げ、バリデーターたちは署名して展開する。
- リーダーは署名されたトランザクションを集約してブロードキャストする。

Babylon

Babylon



babylon

https://babylonlabs.io/

- ユーザーはBitcoin を Babylonスクリプトのアドレスに送金することでステークしたことになる。
  - Staking TX : 期限までステークした
  - Unbonding TX : 期限前に引き戻した
  - Slashing TX : 悪いことをして没収

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

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

- 1つの BTCステークで複数のチェーンをセキュアにし、それぞれのチェーンから報酬を受け取ることができる
- ステーキングの解除(unbonding)の期間は短い(数日程度)
- ユーザーが違反した場合は自動的にステークした一部が没収される

報酬はBTCではなく Babylon のネイティブトークン BABY で支払われる。
最悪でも、ユーザーが送金したBTC だけは期限が切れると戻ってくる。

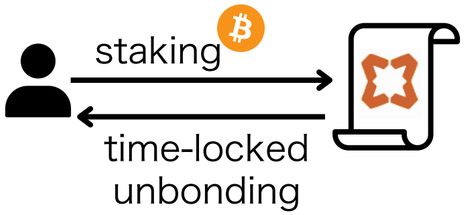
PoSチェーンの問題点

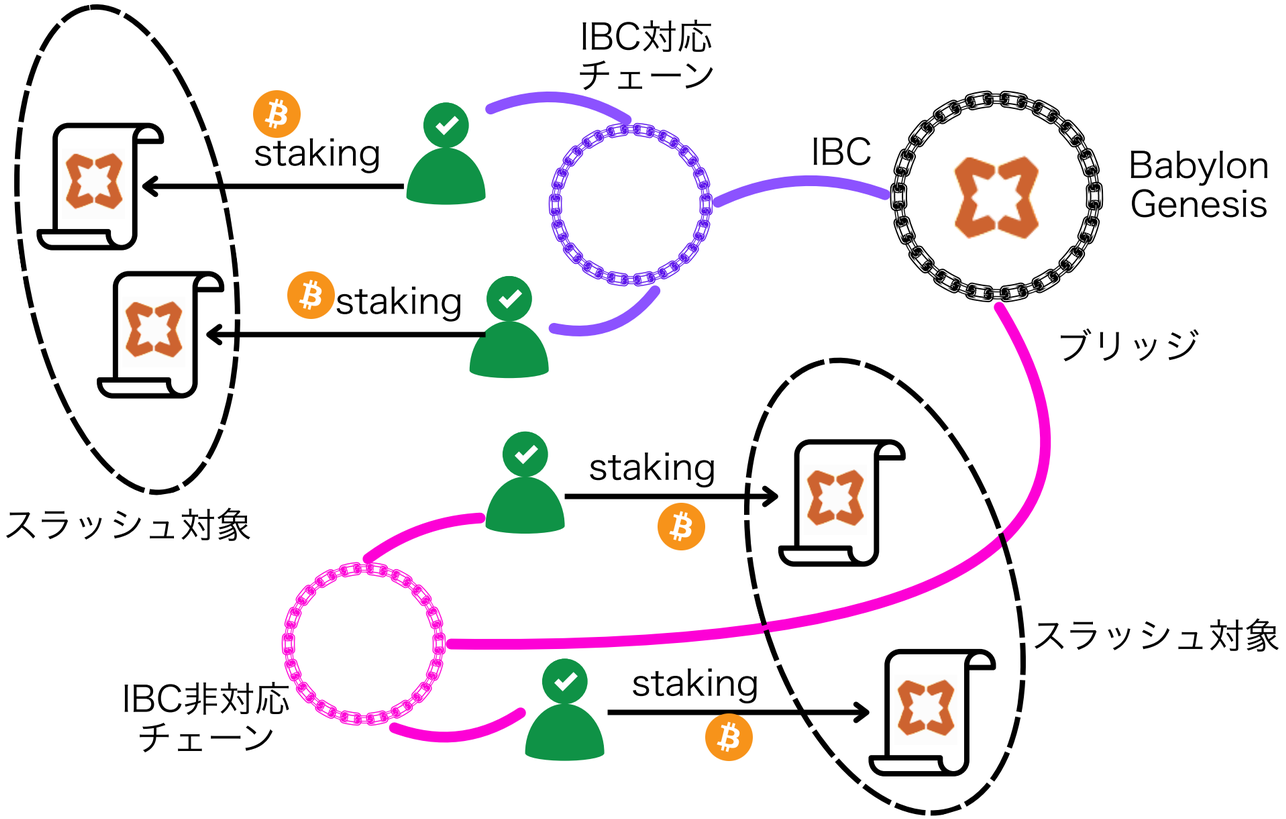
Babylon は PoSチェーンのセキュリティを強化するというサービス

- PoSチェーンは立ち上げたばかりや発行量が少ないなどで市場価値が低い場合はいろいろとセキュリティ的に弱い
  - Validator が少なくて検証が弱い
  - Validator になるためのコストが低く、悪意がある人もなりやすい
  - 攻撃的が発覚しても、攻撃者として失うものが少ない

PoSチェーンのセキュリティ強化

- Validator に Babylon へのステーキングを必須にする
- もし Validator が外部PoSチェーンで不正をすると、Babylon 側でも罰される
  - 外部PoSチェーンからの不正報告をBabylonが暗号学的に検証して、攻撃者にスラッシュを行う。





BRC-20 v2.0

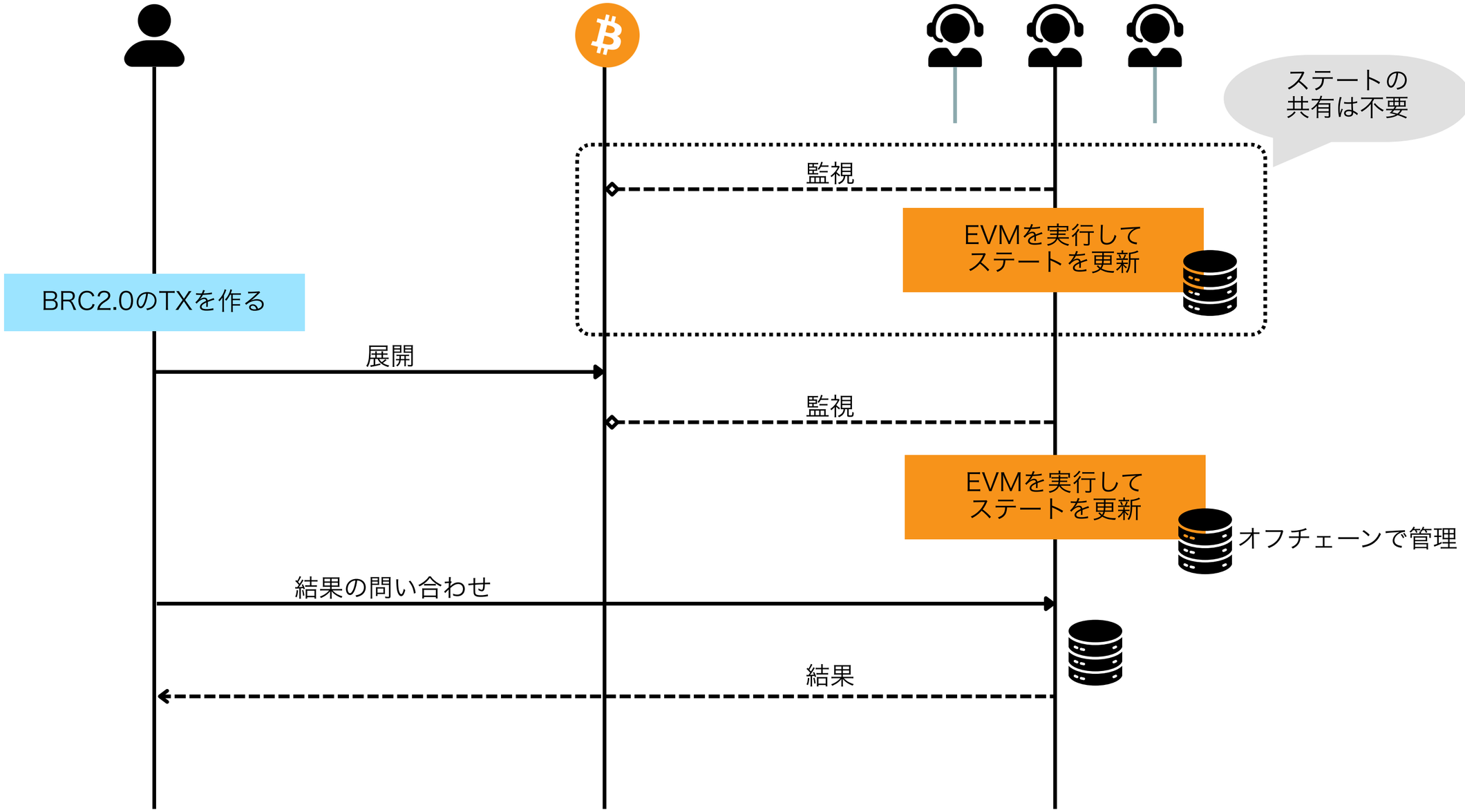
BRC 2.0



[Best in Slot]

BRC-20 という、Ordinals の Inscription を使ったトークンがある。v2.0 が 2025年9月1日に mainnet に公開された。

- EVM は動かすが L2 ではない
- TPS向上を目指したものではない
- Ordinals Inscription のデータに EVMで動く何かが書かれて、それをサーバが Bitcoin L1 から読み取って、オフチェーンのステートを更新する


ステートの
共有は不要
監視
EVMを実行して
ステートを更新
BRC2.0のTXを作る
展開
監視
EVMを実行して
ステートを更新
オフチェーンで管理
結果の問い合わせ
結果

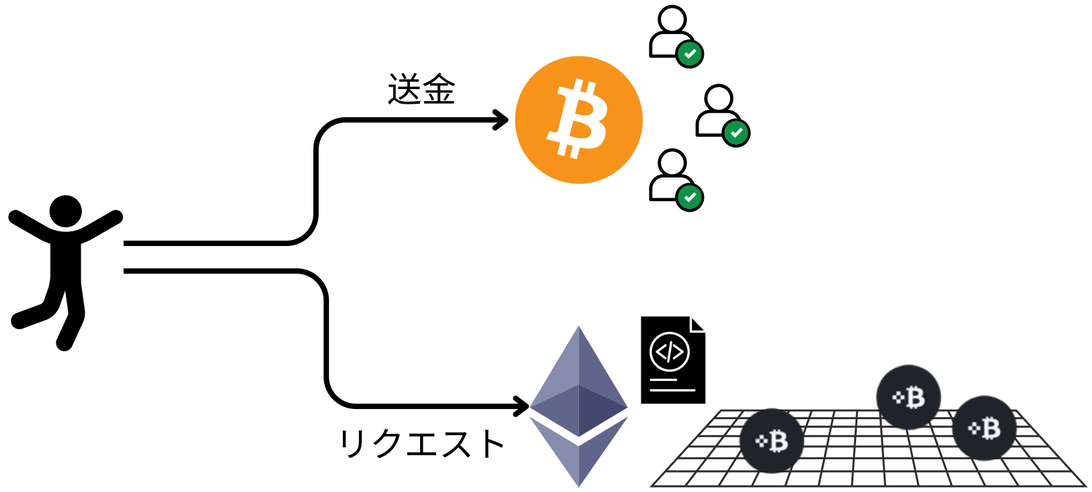
tBTC v2

tBTC

THRESHOLD

https://www.threshold.network/

- Threshold Network という DAO
  - Keep Network と NuCypher というプロジェクトが合併
  - DAO の基盤トークンは T token (Threshold token)
- tBTC は Bitcoin---EVM系のブリッジプロトコル
  - ERC-20 の wrapped token
    - 1 tBTC = 1 BTC
- ユーザはブリッジのアドレスに BTC を送金しつつスマートコントラクトを呼び出す



Layer2ではないので
Bitcoin L1で検証したりしない

Signer

- 現在は鍵の生成に参加したノードだけ署名できる
  - GG18というアルゴリズム(ECDSA)
  - T tokenを一定以上ステーキングしているメンバーで鍵を生成する
  - 鍵生成は定期的や必要に応じて行われる
- FROSTやBitVMなどが成熟したら乗り換える予定

Spark

Spark

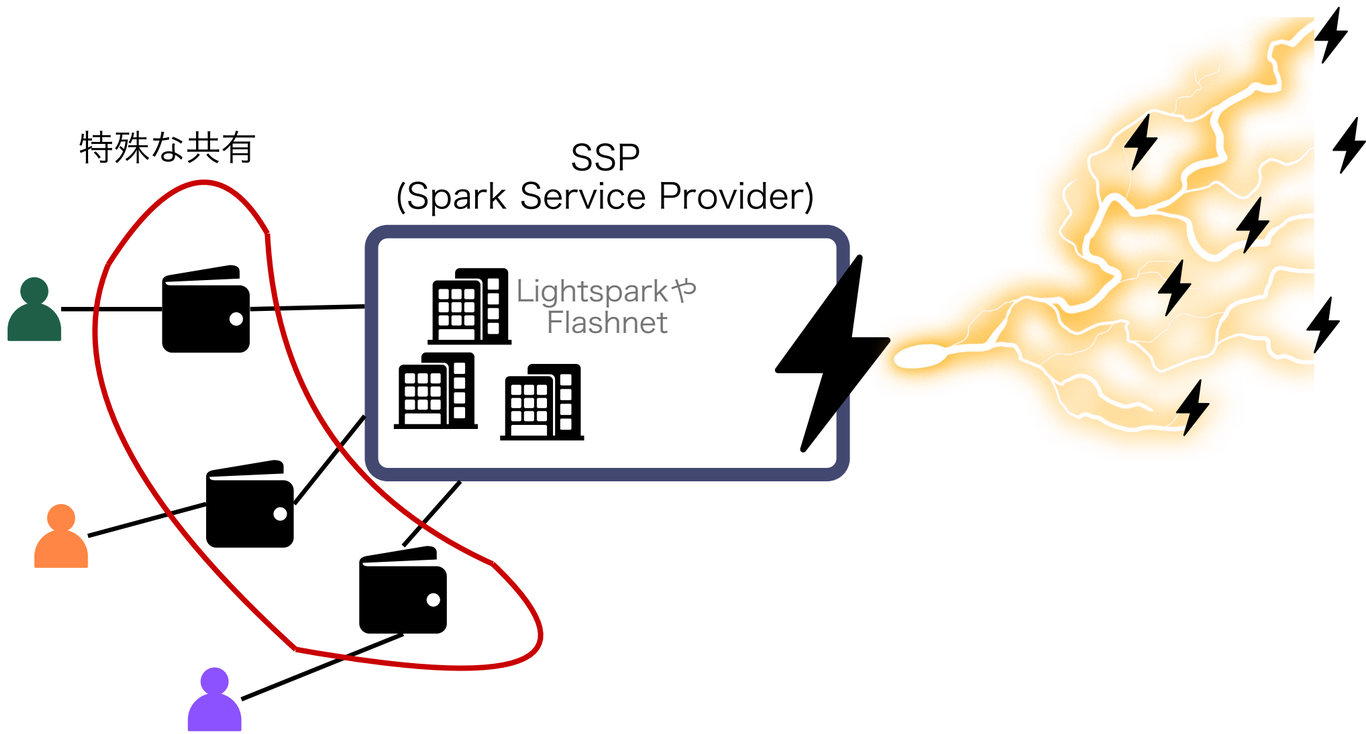


https://www.lightspark.com/

- mainnetで運用している(2025年10月)
- VMは持たないし、Rollupなどでもない。決済に特化。
- トークンの発行は可能。
    - Taproot Assets、RGB、LRC-20 などにも対応
- L2内の手数料は無料、LN-Spark間は0.25%や0.15%。

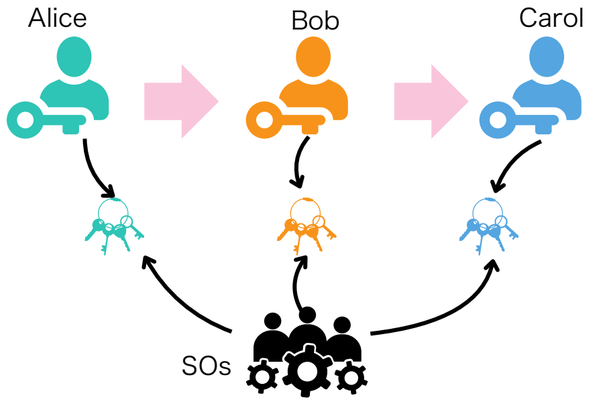
Spark

- Federated Statechain方式の L2。
- 一方的に抜ける(unilateral exit)はできるそうだ。
    - これができるから「セルフカストディ」といってるのだろう



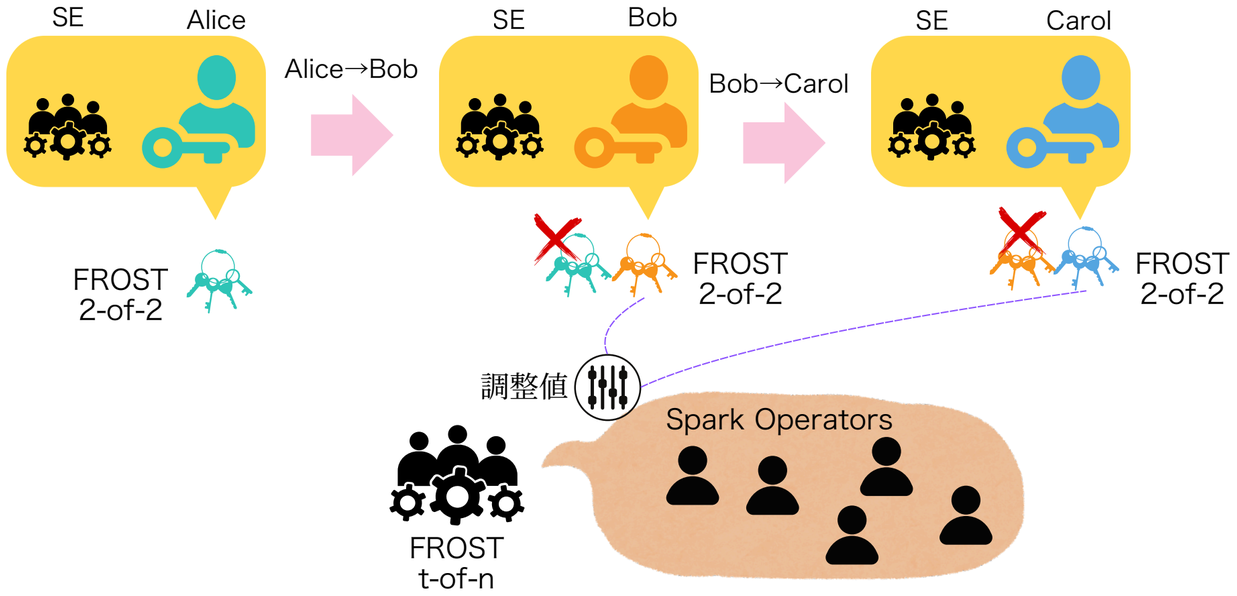
SparkのUTXO委譲

- Federation型のStatechain方式
  - UTXO の所有者をオフチェーンで委譲、再委譲するしくみ
  - FROST閾値署名スキームを利用してトランザクションに共同署名を行う。
  - Federationのメンバーは Lightspark と Flashnet の2社
- L2 上で UTXO の所有者を委譲することで送金と同じ効果を得る
  - FROSTとマルチシグを組み合わせることで、ユーザの署名を必要としつつオペレータの組み合わせを柔軟にしている



SparkのUTXO委譲

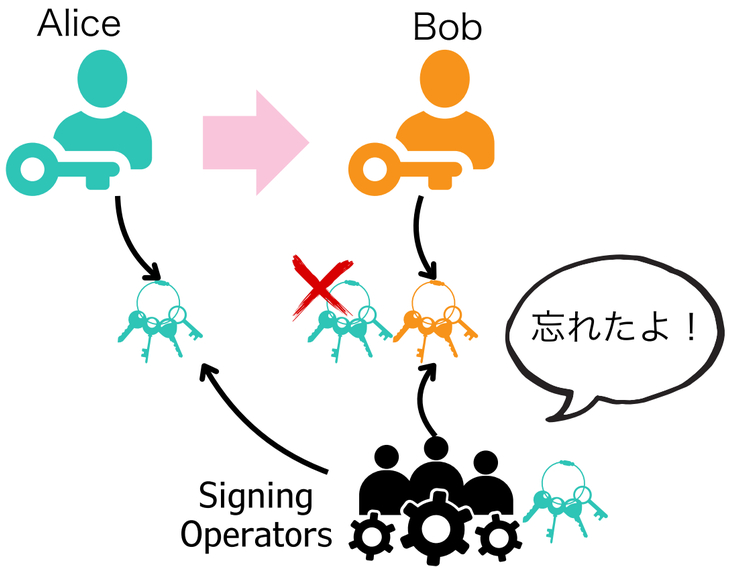
- オペレータたちは FROST で t-of-n の閾値署名鍵を作る
- ユーザとオペレータ(Statechain Entity)も FROST で 2-of-2 の閾値署名鍵を作る
- 署名の時にそれぞれの鍵を持ち寄って、閾値以上集まれば署名できる
- UTXO の所有者が変わっても、オペレータの FROST鍵を調整すると新しい所有者の署名で UTXO から spent することができる



Trust Model

https://docs.spark.money/learn/trust-model

- オペレータは前のUTXO所有者のときの鍵セットを破棄しないといけないが、つまりそれは共謀できるポイントにもなってしまう。
- 破棄した証明書を作ったりはするが、そういうのも偽造しようとすればできてしまうので、最終的には「Unilateral Exit」で抜けられるという割り切り方になっているようだ。



Drivechain

LayerTwo Labs

https://www.drivechain.info/



Paul Sztorc ✓
@Truthcoin

- Drivechain を提案した Paul Sztorc氏(CEO)の会社
- 事業
  - Drivechainの開発と普及
  - サイドチェーン設計
  - 予測市場やNamecoinの復活など
- 2022年12月に 300万ドルの資金調達
- Bitcoin の状況なんとかしたいという考えがあるようだ
  - ビットコインを将来にわたり存続させ、あらゆるイノベーションを取り込み、ユーザーの多様なニーズを尊重する、究極のスケーリングソリューション
    - 同じコンセンサスではなくユーザが選択できる
    - Permissionless Innovation
      - 誰でも新しい機能やルールセットを試すことができる

Drivechain

- Bitcoin L1 を大きく変えずに、機能拡張をサイドチェーンで実現しようとする提案
- BIP-300(2017年) / 301(2019年) として提案されている
  - soft forkが発生する提案で、どちらも Draft 段階
- 議論自体は行われている模様

BIP-300 : Hashrate Escrows

- ブリッジの部分と思っておけばよい
- peg-in
  - フォーマットが決まったスクリプトを準備する。
  - ユーザはそのアドレスに資金を送金するとサイドチェーン側でトークン発行
  - ロックされるだけで運用者は手に入れられない
- peg-out
  - サイドチェーン側で資金をburnすると peg-outリクエストが発行
  - リクエストに対してBitcoinマイナーがcoinbaseトランザクションにデータを埋め込むことで投票を行う
  - 投票期間は3ヶ月程度で、51%以上の投票があってようやく承認
  - 承認後、ロックされた資金の範囲内でユーザーに戻される

BIP-300 : QA

https://drivechain.info/faq/index.html

- peg-in は資金をロックするだけで運営者は使うことができない
- peg-out は peg-in した額の中でしかできない
- peg-outに時間がかかりすぎでは
  - 取引所が間に入って、ユーザは取引所と HTLC などで期間を短くしたら良い(FAQ)

BIP-301 : Blind Merged Mining

- merged mining はサイドチェーン側のブロックをマイナーに承認してもらうしくみ
  - Rootstock も merged mining だが方式が異なる
- サイドチェーンのブロックハッシュをマイナーのcoinbaseトランザクションに埋め込んでもらう。そのブロックが承認されたらサイドチェーンのブロックも承認されたことになる。
- サイドチェーンのマイナーはサイドチェーン側で報酬をもらい、Bitcoinのマイナーはサイドチェーンのマイナーから報酬をもらう



BIP-301 : Blind Merged Mining

1. サイドチェーンの承認者はサイドチェーンのブロックを作り、Bitcoin側には「この値をcoinbaseトランザクションに含めて承認したマイナーに報酬を渡す」というトランザクションを展開
2. Bitcoinマイナーの中でBIP-301がわかるマイナーはそのトランザクションを見てcoinbaseトランザクションを作りマイニングを行う
3. そのマイナーのブロックがBitcoinで承認されたら、サイドチェーンも該当するブロックが承認されたと見なす
4. サイドチェーンのマイナーはその Bitcoinマイナーに報酬を払う

Drivechain

- permissionless innovation
  - 許可なく新機能を実装可能
  - そうすることで他のチェーンに移行する理由がなくなる
  - ユーザは opt-in で選択できる
  - 問題発生時は soft fork で無効化可能
- 価値がBitcoin と 1:1

THANK YOU