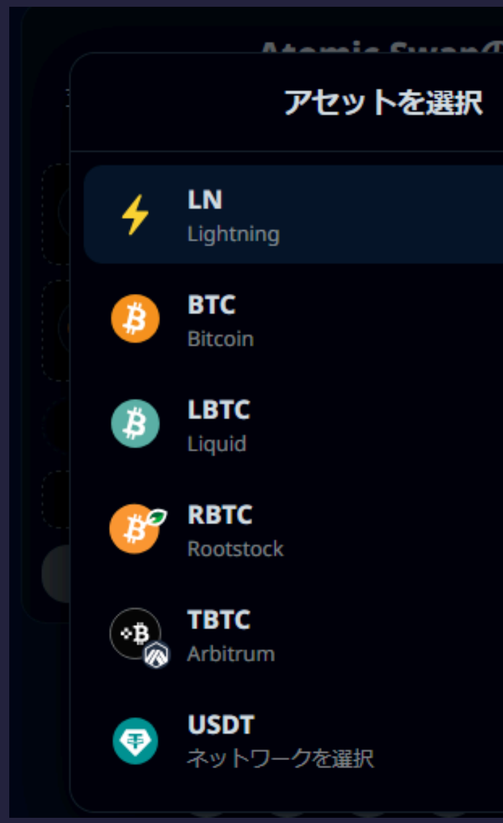
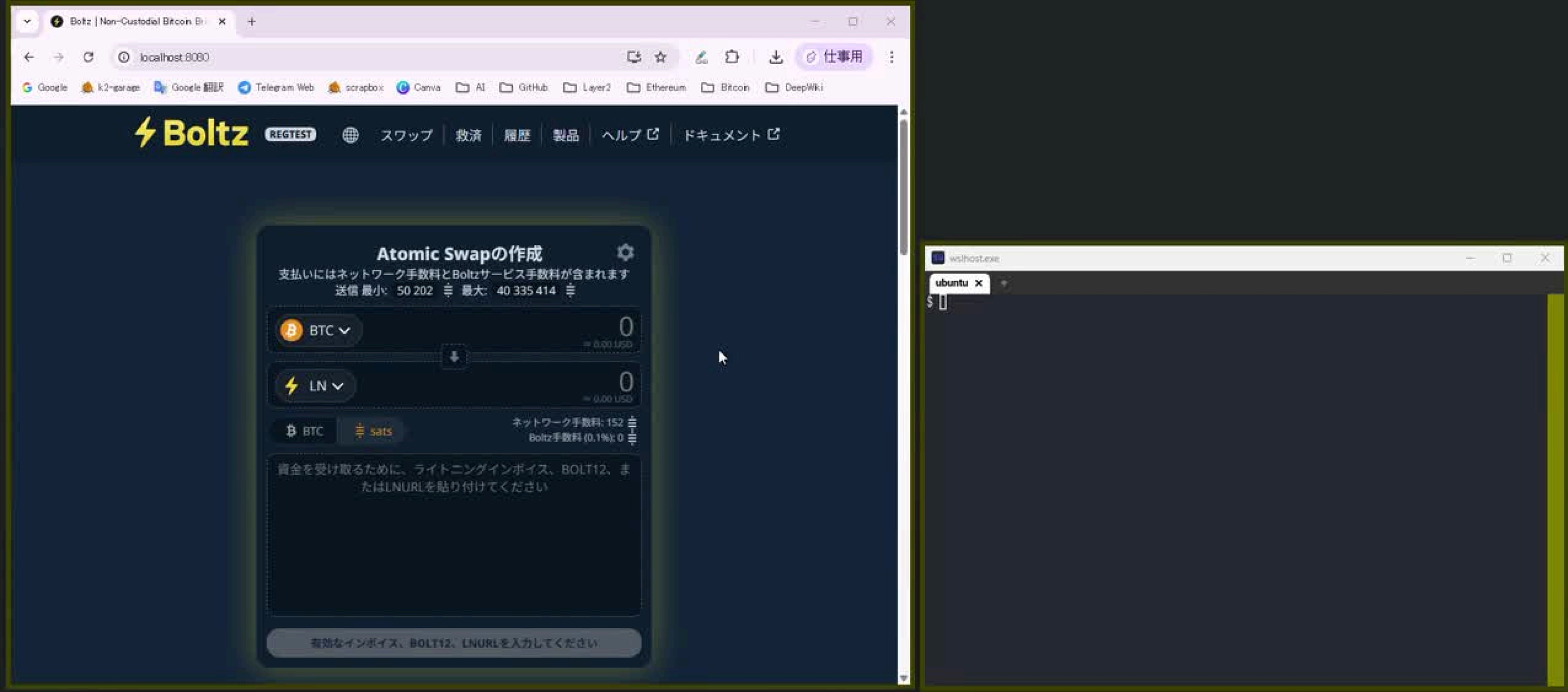
Boltz

概要

- 暗号資産交換サービス
- Webサイトからではわからないが atomic swap を使っている
  - Webサービスの場合は隠しているそうだ
- プロダクト(提供開始順)
  - クライアントサービス
    - コマンドラインから交換したり、Autoswap機能を常駐させたりする
  - BTCPayプラグイン
    - BTCPay ServerにAutoswap機能を組み込み、Lightning Networkのリバランスを自動で行うようにできるらしい
  - Boltz Pro
    - Boltz自身のウォレットやLightningチャネルの流動性をユーザーの力を借りてリバランスする仕組み
    - Boltzへの流動性を助ける対価としてsatsを得られる
- 基本的にはBTC系の交換
  - Rootstockは2024年Q4、USDTは2026年Q1。Arkadeもあるらしい。




Boltz | Non-Custodial Bitcoin Bri
localhost:8080
仕事用
Google
k2-garage
Google 翻訳
Telegram Web
scrapbox
Canva
AI
GitHub
Layer2
Ethereum
Bitcoin
DeepWiki
Boltz
REGTEST
スワップ
救済
履歴
製品
ヘルプ
ドキュメント
Atomic Swapの作成
支払いにはネットワーク手数料とBoltzサービス手数料が含まれます
送信 最小: 50 202 最大: 40 335 414
BTC
0
≈ 0.00 USD
LN
0
≈ 0.00 USD
BTC
sats
ネットワーク手数料: 152
Boltz手数料 (0.1%): 0
資金を受け取るために、ライトニングインボイス、BOLT12、またはLNURLを貼り付けてください
有効なインボイス、BOLT12、LNURLを入力してください
wslhost.exe
ubuntu
$

Atomic Swap (1)

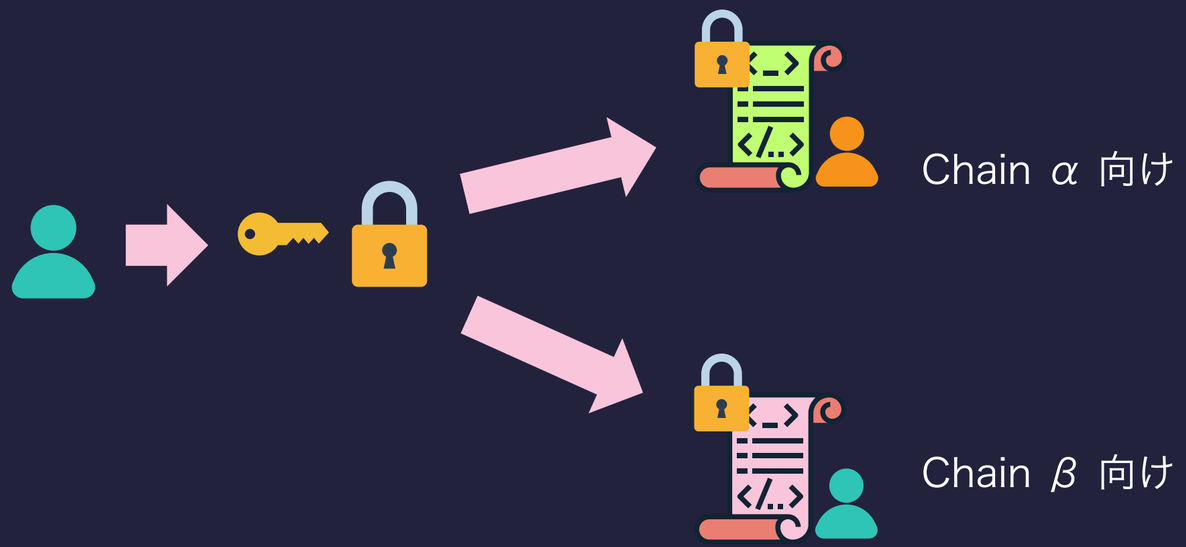
- お互いに信用がないと「お前が送ってくれたら私も送るよ」となってしまうので、ブロックチェーンを使って「交換」ができるようにする

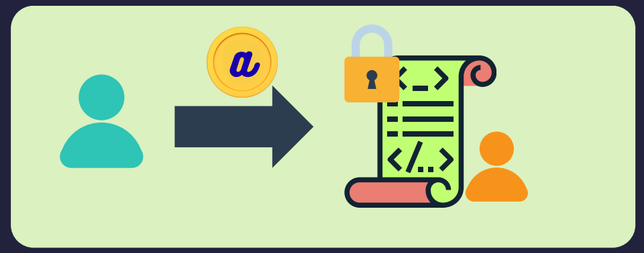
- Aさんがαチェーンでトークンを送り、Bさんがβチェーンでトークンを送るという形で交換したいとする
- 当然、どちらもだまされたくないと思っている。



Atomic Swap (2)

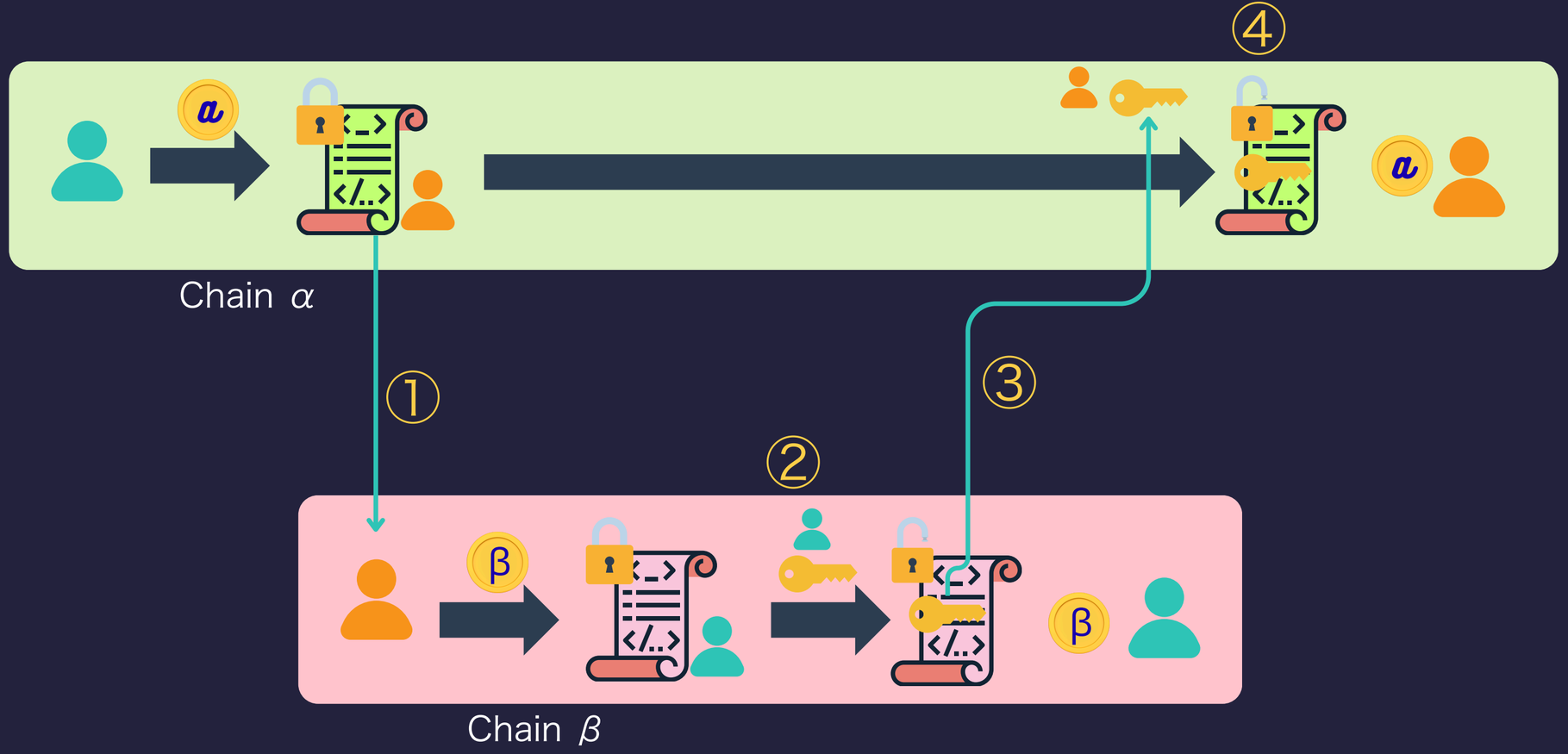
- Aさんは鍵データを作り、その鍵を公開しないと受け取ることができないスクリプトをチェーンαとβ向けにそれぞれ作る(そのスクリプトには鍵そのものは含まれない)
- AさんはトークンTaをスクリプトに向けて送金する





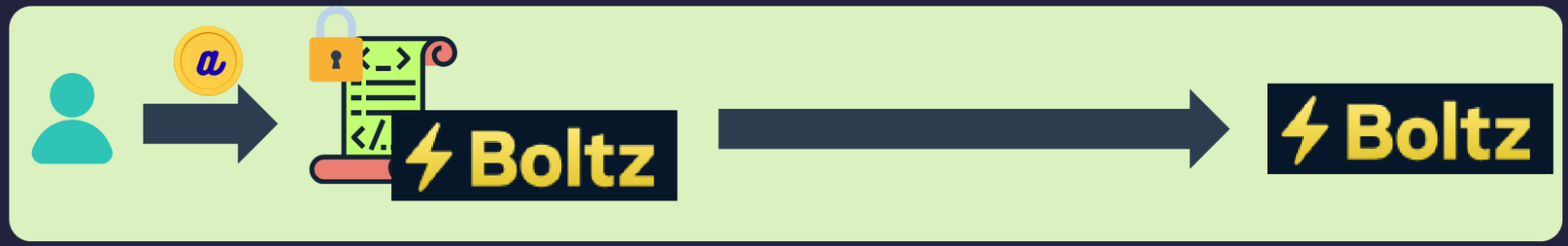
Atomic Swap (3)

- ①Bさんはそれを確認してトークンTbをスクリプトに向けて送金する
- ②Aさんはトークンを Tb をもらうためにスクリプトを解く。そのときに鍵データをチェーン β 上に展開する
- ③Bさんはチェーン β を確認して鍵データを取得
- ④チェーン α にその鍵を作ったスクリプトを展開してトークンTaをもらう



Atomic Swap (4)

- 実際は、ブロックの生成間隔の違いなどを考慮して相手だけが取り逃げしたりできないようにしたり、交換するトークン量を偽らないように事前にトランザクションの形を決めたりなどする。
- 鍵と錠で表したものは、Lightning Networkの preimage と payment-hash のようにお互いのチェーンがスクリプトで計算できるハッシュ演算を使うことが多い。SHA-256など。
- Boltzサービスはアカウントがないので、送り手と受け手が同じ人かどうかは区別できない

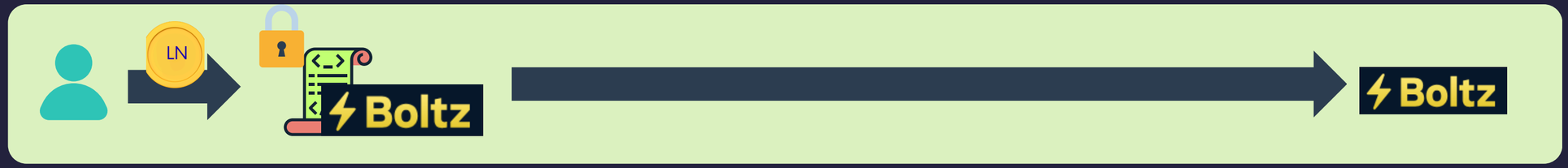


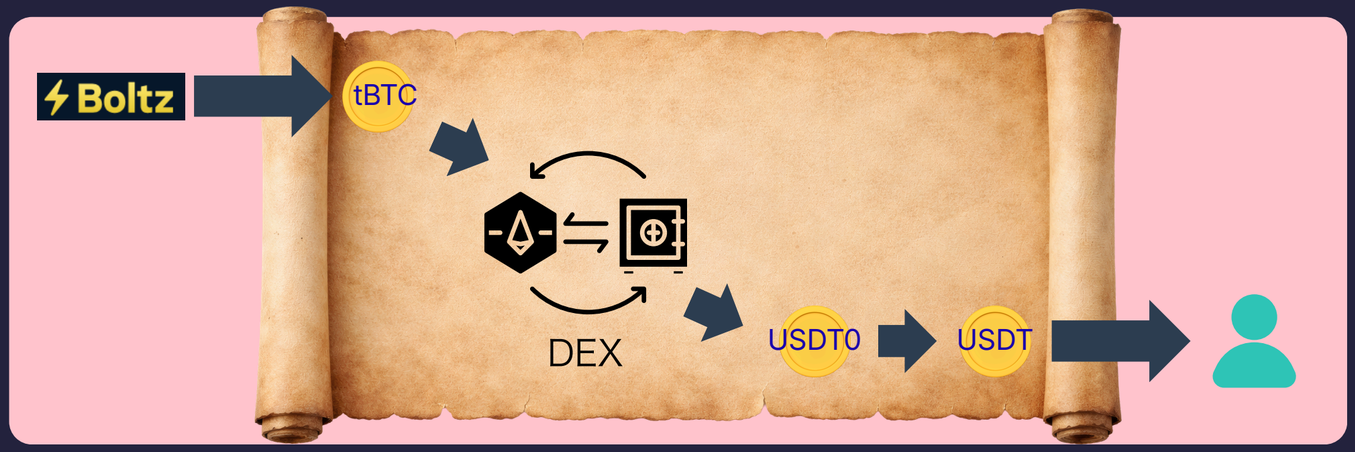


USDT

Boltzは直接USDTを持っているのではなく、tBTCを間に挟んでいる。

1. LNでsatsをBoltzに送る
2. Boltzはそれを変換先チェーンの tBTC に変換する
3. チェーン上のコントラクトでtBTCをUniswapなどのDEXを通じて USDT0 と交換
4. さらに USDT0 を USDT と交換するところも同じコントラクトで一括して行う





個人の感想

- Atomic swapを使っているのをブラウザ版だと隠せるというのがよくわかってない
- 最大で 0.2BTC と低めなのは犯罪防止のためか
  - ノンカストディアルなのでマネーロンダリングには使われやすいだろう
- ブリッジではなく交換なので、atomic swapなので持ち逃げされないとしてもそれぞれのトークンをBoltzが持っていないといけないのは資金的に大変そうだ。
  - 枯渇しにくいように Boltz Pro で流動性を得やすくしたのだろうか

Spark

概要

*Spark

lightspark

- lightspark社のプロダクト
- Bitcoin L2
- 管理者であるSO(Spark Operator)とユーザ間のマルチシグアドレスにデポジット
  - 正しくは簡易FROSTによる2-of-2の集約鍵
  - SOはクローズドで、今はSpark社とFlashnet社の2つしかいない
- Sparkユーザ間のやりとりはオフチェーンで行われ、即時かつ手数料無料
  - ここで statechain という技術が使われている
- Sparkから抜けるときは、協調してExitするパターンと一方的にExitするパターンがある
  - LNの mutual close と force close と思っておけばよいだろう
- スマートコントラクトやVirtual Machineは持たない。決済専用。
- Lightning Networkの機能もあるが、Spark標準の機能ではないというかなんというか
  - SOではなくSSP(Spark Service Provider)が担当する
  - SSPはユーザの使い勝手向上という役割でSparkに必須ではない
  - その代わり、誰でも参加できる
- オープンソースになっている

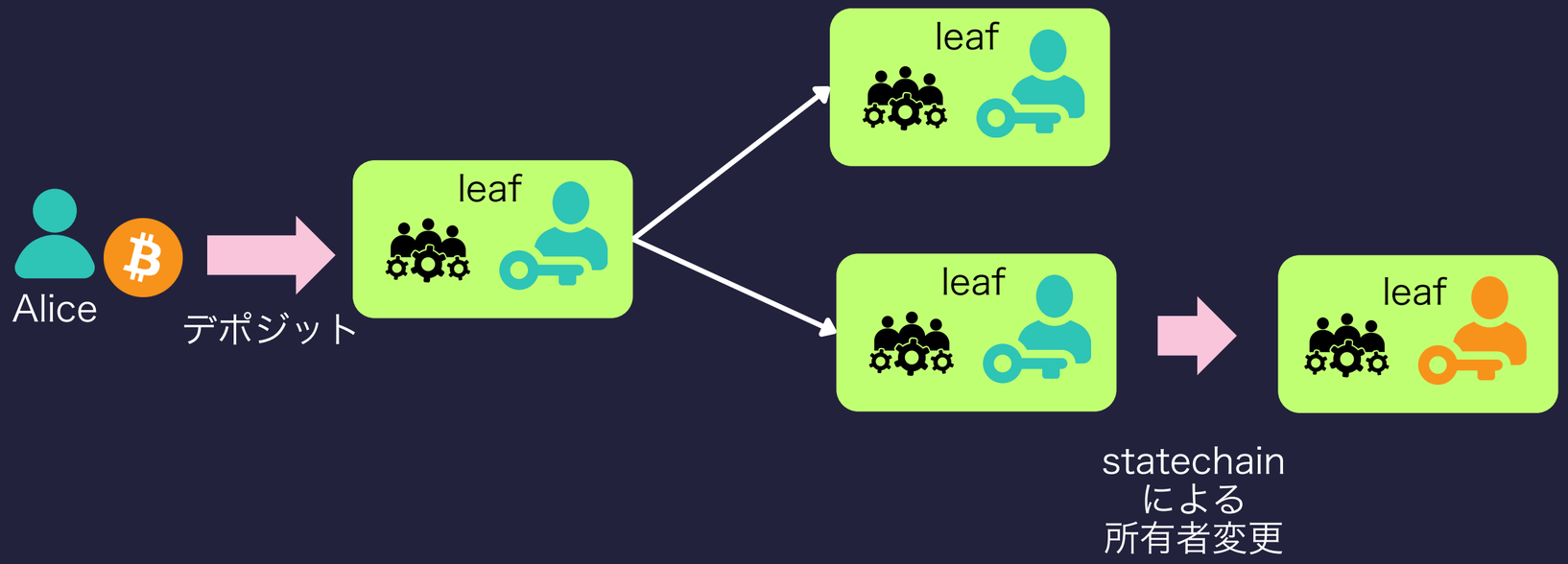
Is Spark open source?

Yes, Spark is open source. You can read the code or contribute directly **here**.

statechain

*Spark

- ユーザとSOの共有アドレスにデポジットすると、そのUTXOがユーザのL2での通貨になる
  - L2での通貨はそのままBTCと同じ価値を持つ
  - それ以外にステーブルトークンなどもサポートしているらしい
- UTXOは “leaf” という単位で扱われる
  - 他ユーザに送金するときは leaf を分割して所有権を委譲する
  - 所有権の委譲はオフチェーンで行われ、statechain という技術を使っている
- Lightning Networkと同じような弱点がある



個人の感想

*Spark

lightspark

- 方式が異なるArkみたいな
  - L2でもUTXOベースで管理している
  - L2内では即時送金
  - L2外に送金するときは別のプロトコルを使う
- オープンソースになっているが、自分でデプロイできるようになっているかはわからない
  - regtestでの動作手順でlightsparkのサイトを使っているので、改造しないとlightspark社用にしかならないんじゃなかろうか
- SSP(Spark Service Provider)になってLN機能を提供するということはできそう。