

# Atomic Swap Network

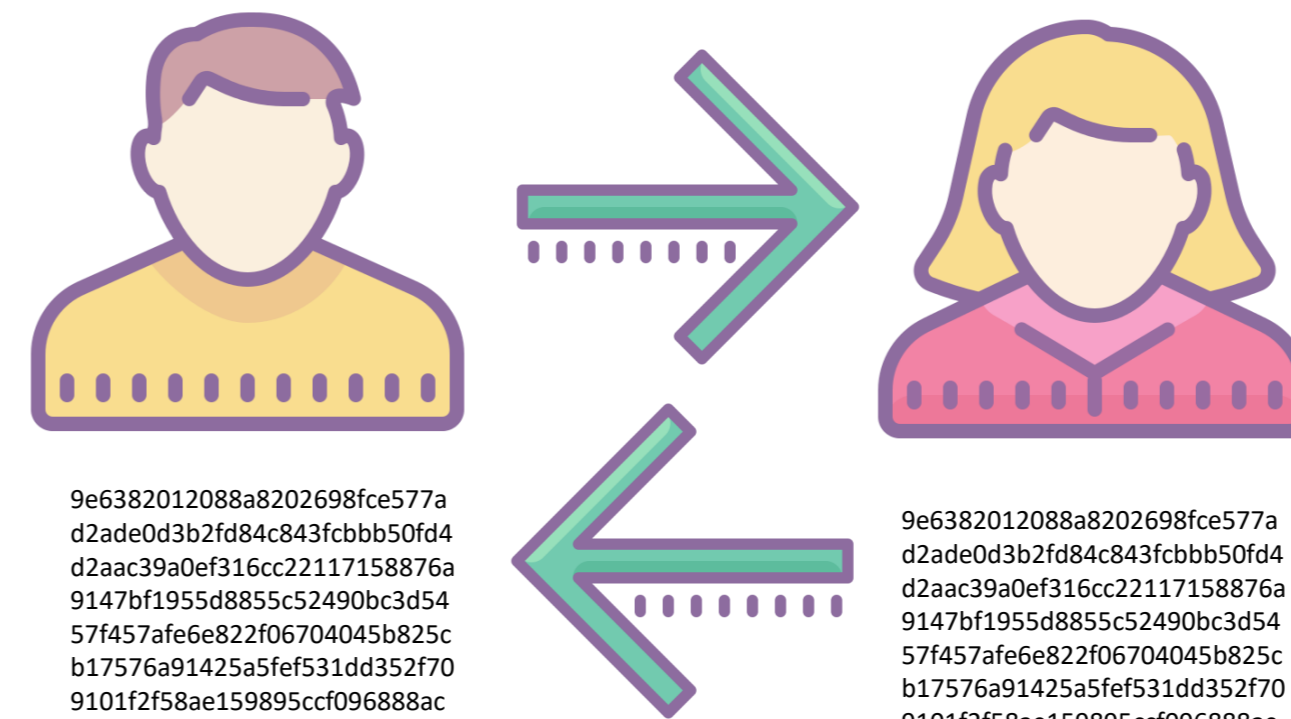
～暗号通貨の二者間取引を支援するシステム～

開発駆動コース 仲山ゼミ 芦田 裕飛

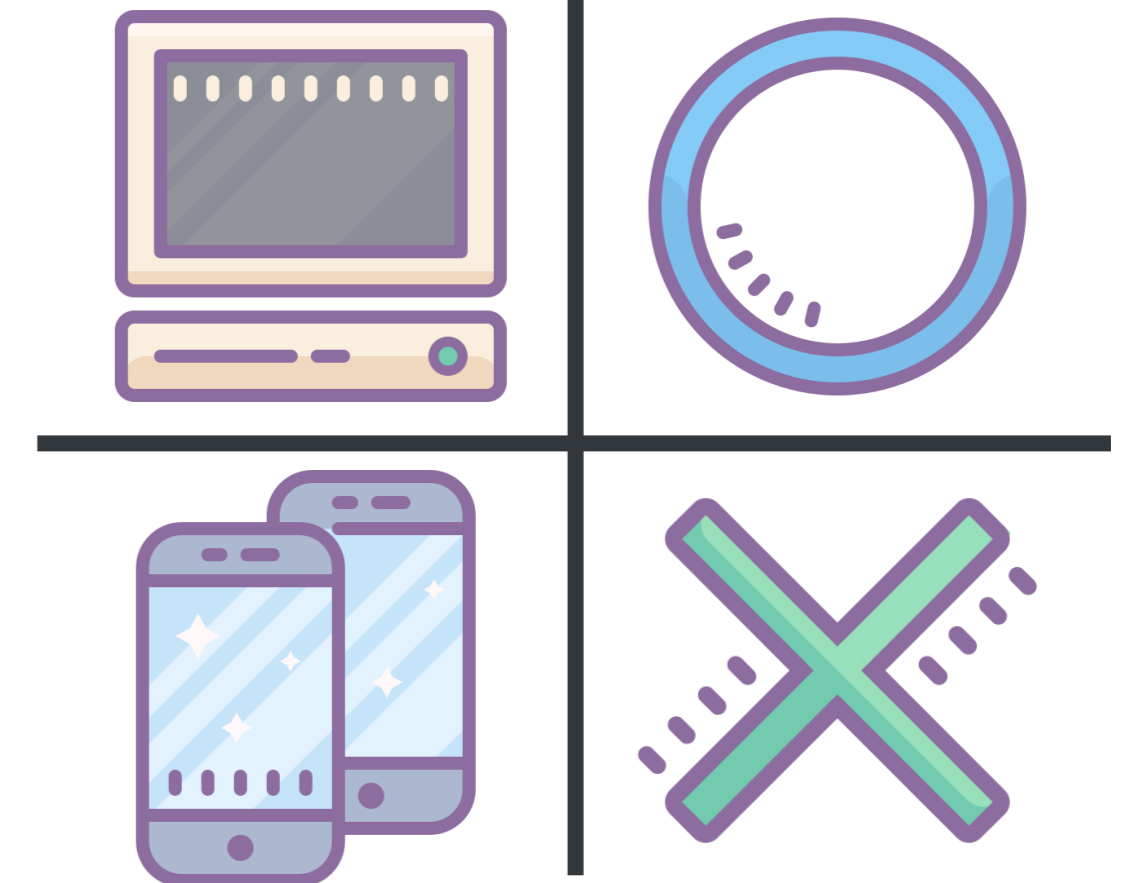
## 1. Atomic Swapについて

- 暗号通貨を取引所などの第三者を介さずに取引(交換)できる技術
- 先述の通り第三者を介する必要がなく、相手すらも信頼する必要がない
- 唯一、ブロックチェーンさえ信用すれば取引が可能なプロトコル
- 使いにくさゆえにあまり普及はしていない

## 2. 普及しない理由

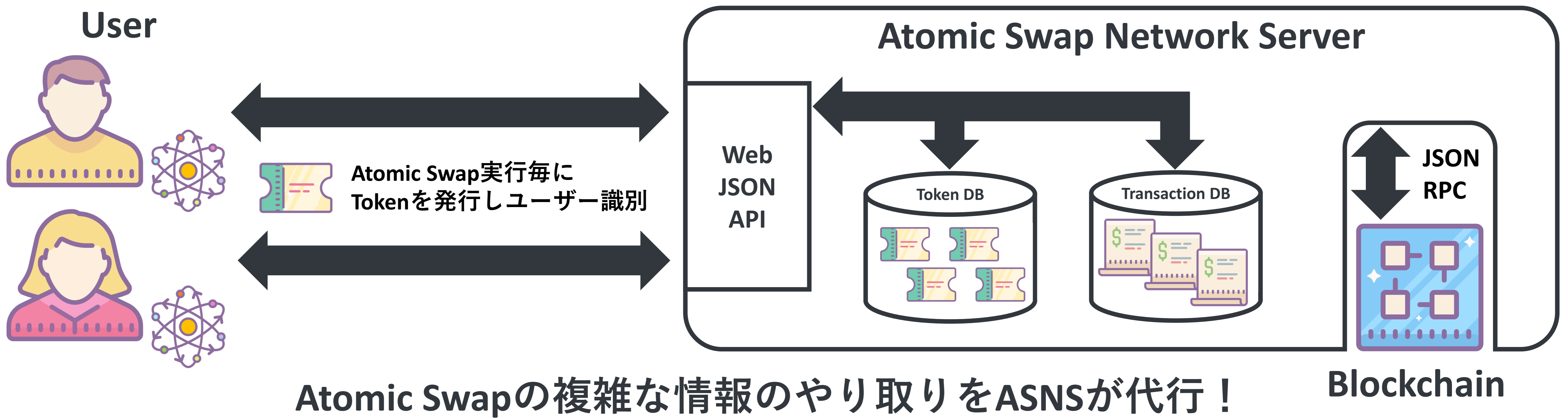


セキュアゆえに複雑な情報のやり取りが必要

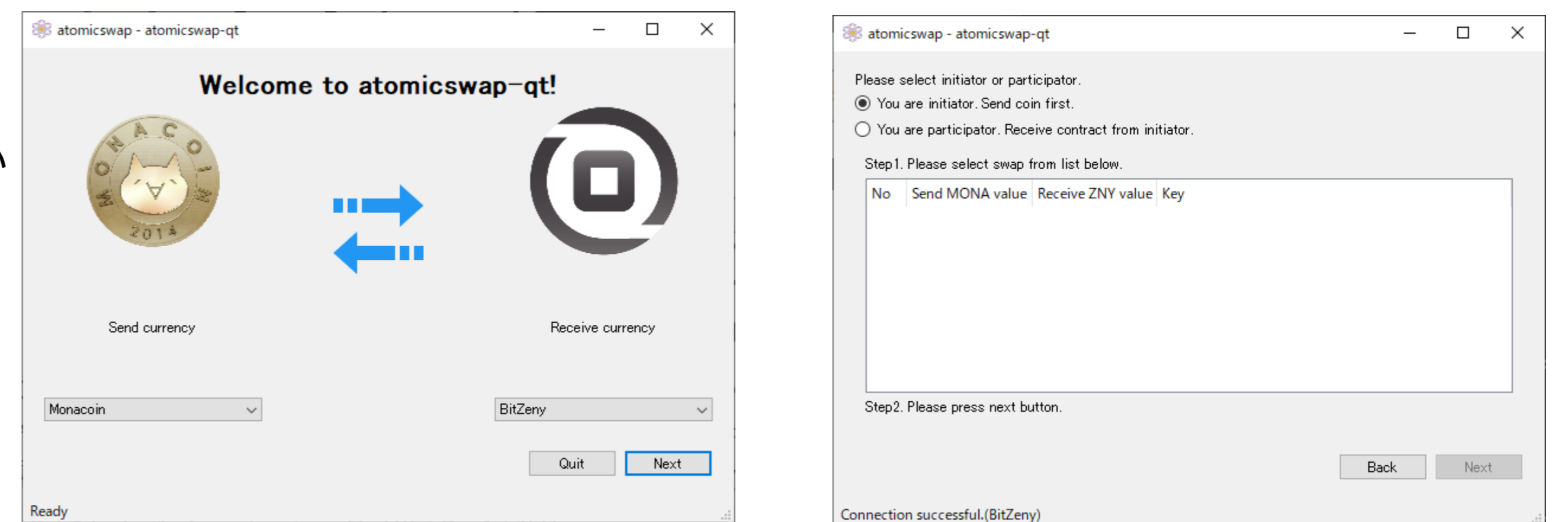


モバイル端末では利用しにくい特性

## 3. Atomic Swap Networkの全体像



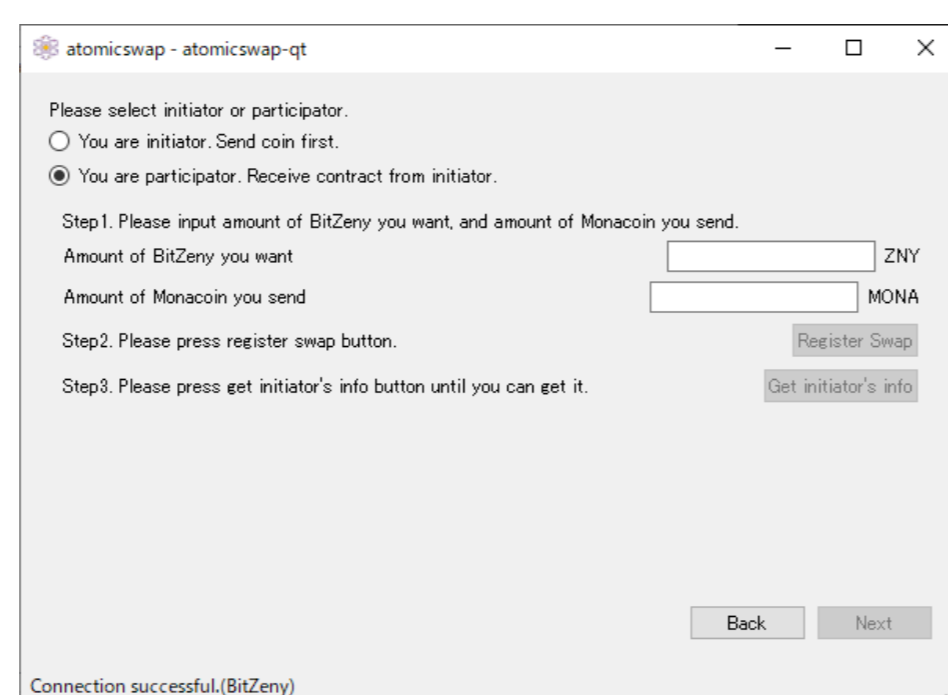
- SecHack365では単一サーバで稼働するデモを作成
  - 特定の第三者が介するとAtomic Swapの利点を潰しかねない
  - P2Pネットワークという監視された、特定ではない第三者を頼ることで回避することが理想
- ユーザーが操作しなければならないものや回数を極力減らす
  - **UXの向上を図る**



API操作の補助を担うデモアプリ「atomicswap-qt」

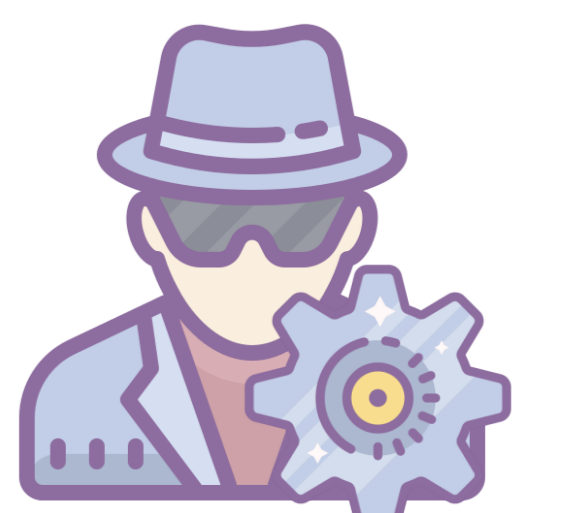
## 4. ASNSを用いた結果

- 従来の手法では平均して**3分程度**かかった
  - 操作数(コピペの回数・ボタンを押す回数)が合計**約40回**
- ASNS & atomicswap-qt の組み合わせでは平均**1分程度**
  - 操作数は合計**約20回**
  - 操作のほとんどが**ボタン操作となり、面倒なコピペが不要に！**



## 5. 今後の展望

- UXの向上は叶ったが、現在の設計ではサーバ運用者が不正出来てしまうなどの問題が山積み
  - 悪いServer Adminが出現すると取引が成立しなくなる
- 不正を起こしにくくする実装
  - P2Pネットワークの構築
  - Atomic Swapプロトコルの改善
- ブロックチェーンを拡張する2nd Layer Networkとなれるようにしたい
- atomicswap-qtのモバイル版作成



悪いServer Admin