Atomically Swapping Coins: for Privacy or Cross-Blockchain Trades

Feb 2018

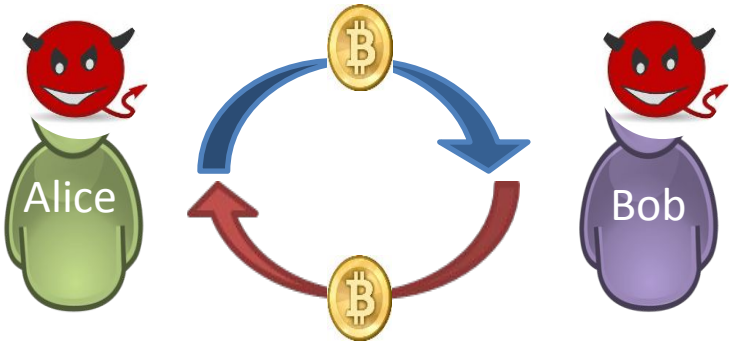
Ethan Heilman

Introduction

Atomic Swaps:

Enables Alice & Bob to trade cryptocurrency, e.g. Bitcoin, such that:

1. **Atomic:** The trade happens or does not happen, neither party can cheat the other by taking coins without sending coins.
2. **Untrusted:** No trusted third party is needed.



OR

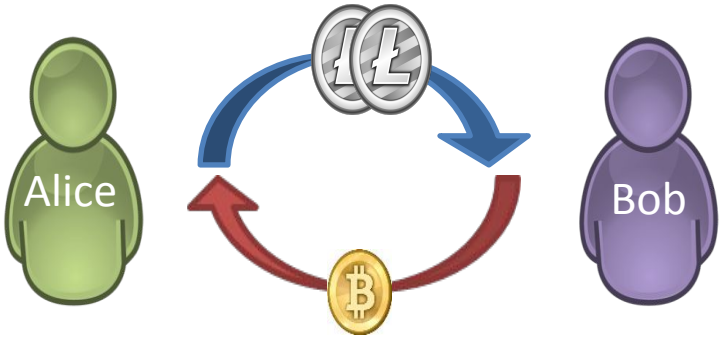
Trade happens

Both parties get coins back

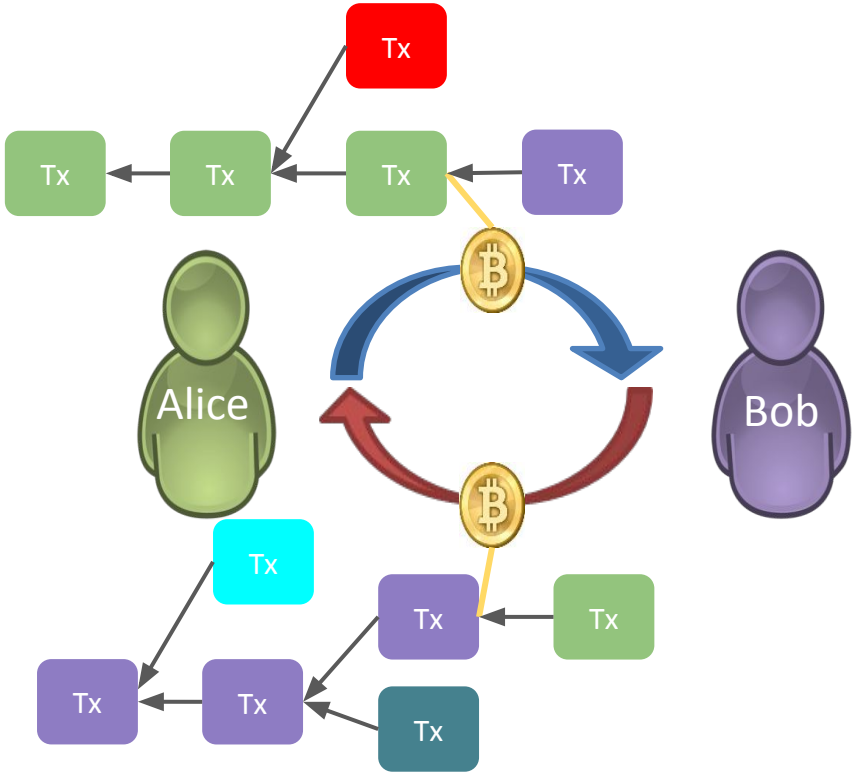
…even if parties are malicious and try to cheat each other!

Uses: Cross-blockchain Trades and Privacy

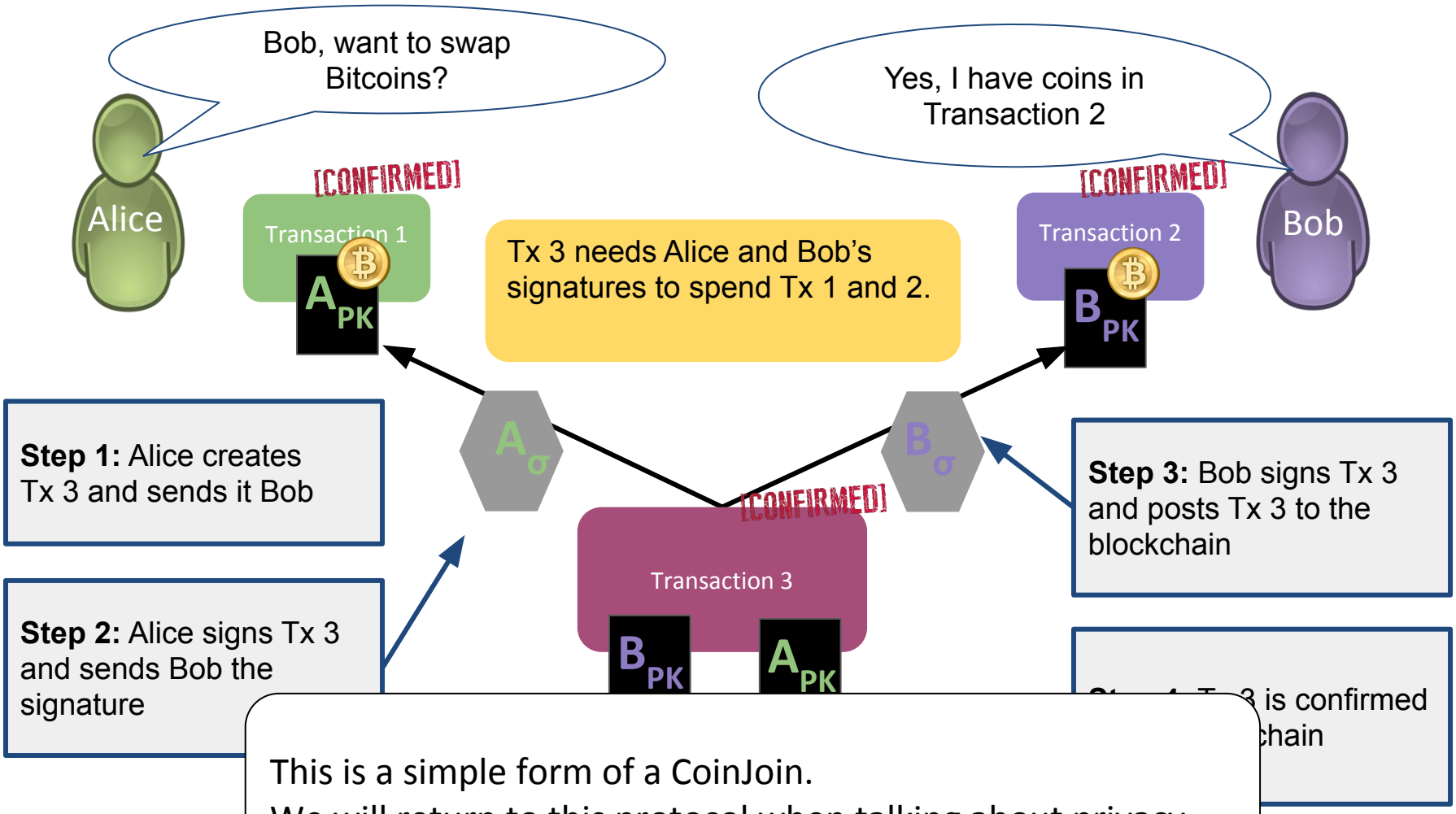
Cross-chain Atomic Swaps:
Alice has Litecoin, wants Bitcoin
Bob has Bitcoin, wants Litecoin
So… Alice trades Bob 2 LTC for 1 BTC



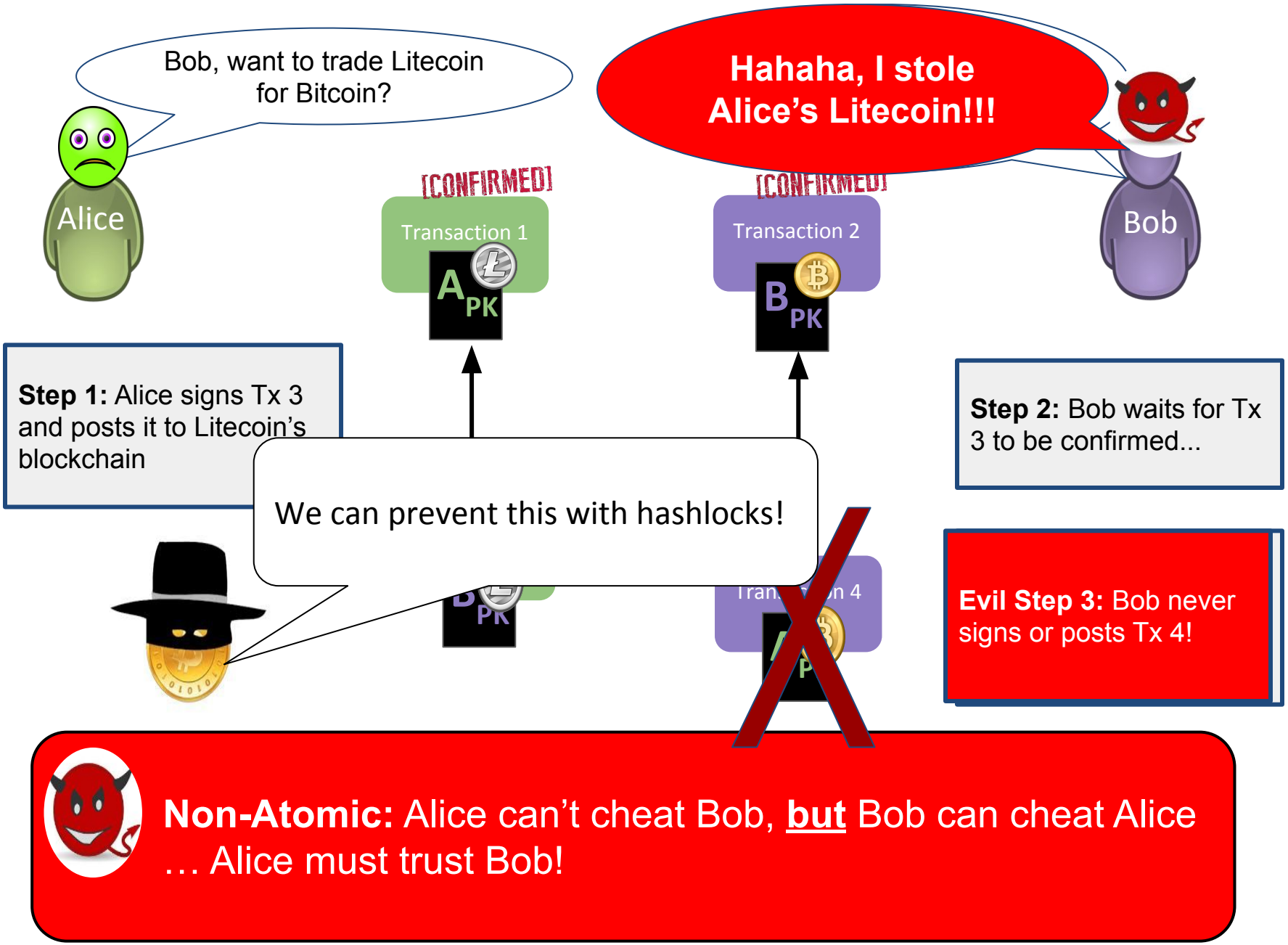
Atomic Swaps for Privacy:
To obfuscate their transaction graph
Alice and Bob trade 1 BTC for 1 BTC
…thus, mixing their coins



Atomic Swaps within the same Blockchain



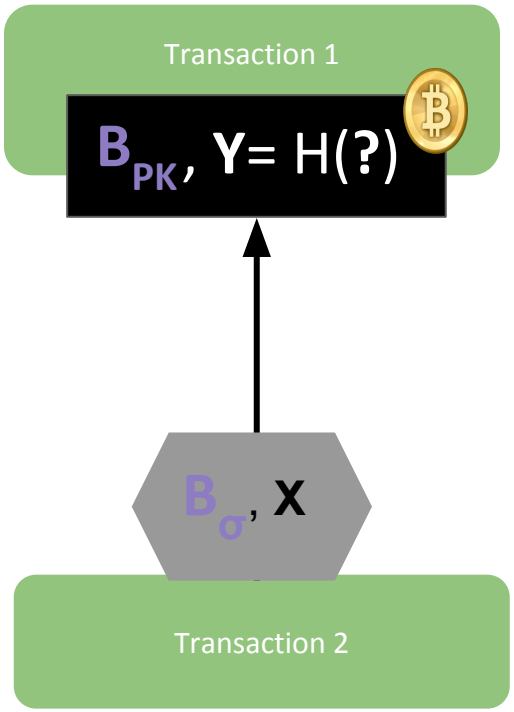
Non-Atomic Cross-Blockchain Trades



Hashlocking Funds

Step 1: Alice chooses a random value X and hashes it to get Y.

Step 2: Alice creates and posts a transaction which can be spent by Bob if Bob learns X

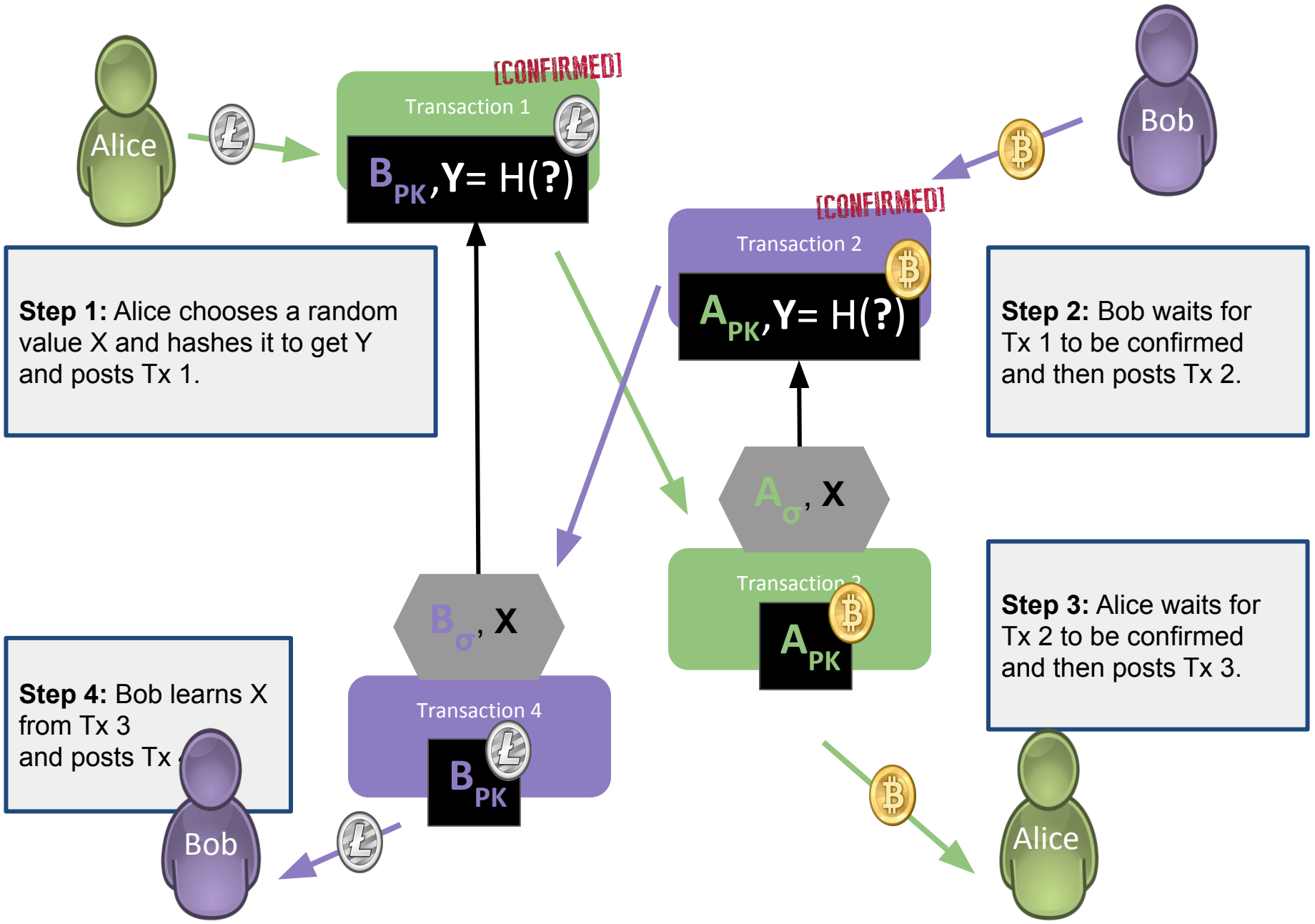


Step 3: Bob learns X and spends Tx 1.

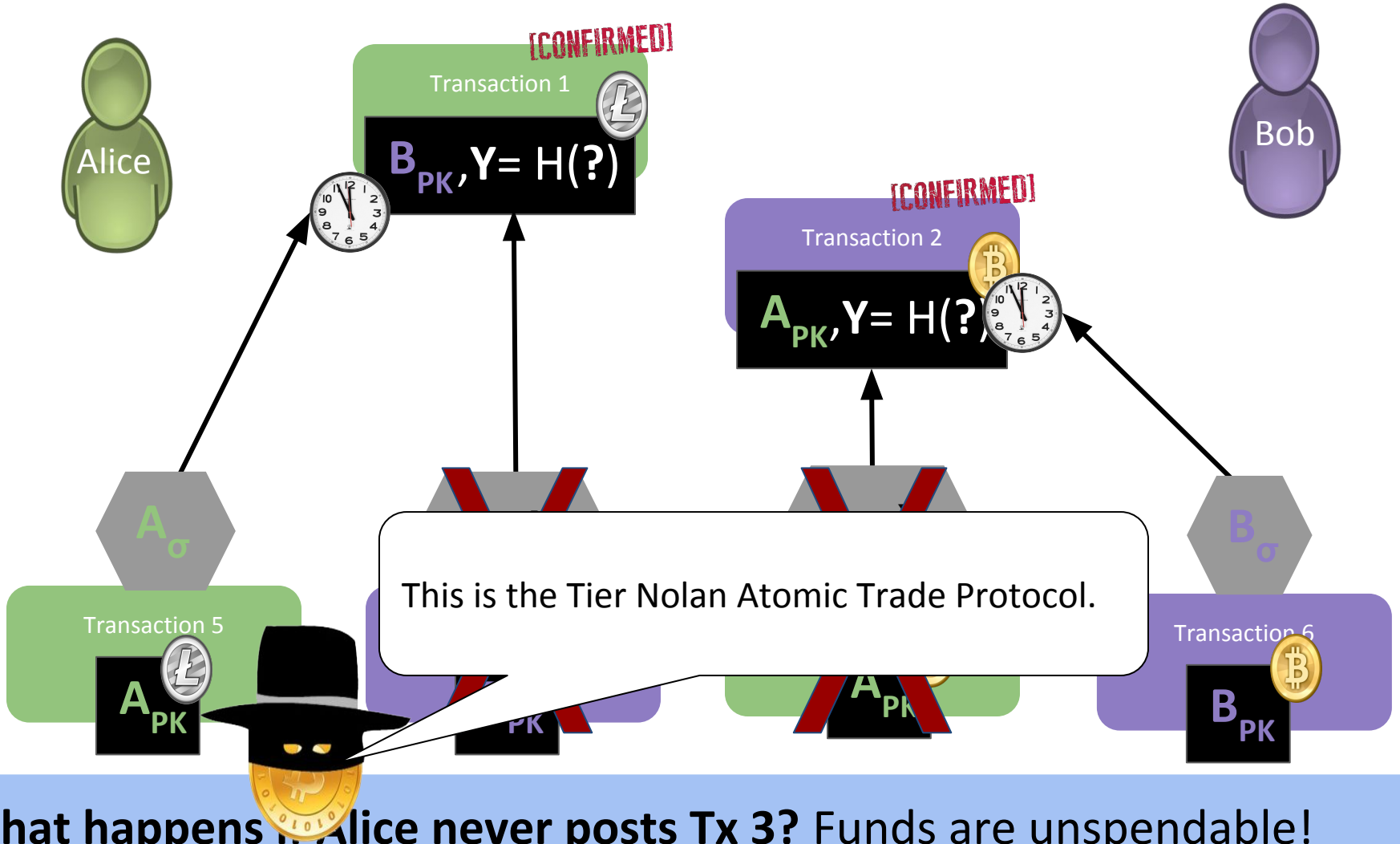
Hashlocks:

To spend a Tx output the input you must provide a value **X**, such that H(**X**) = **Y**

Atomic Cross-Blockchain Trades

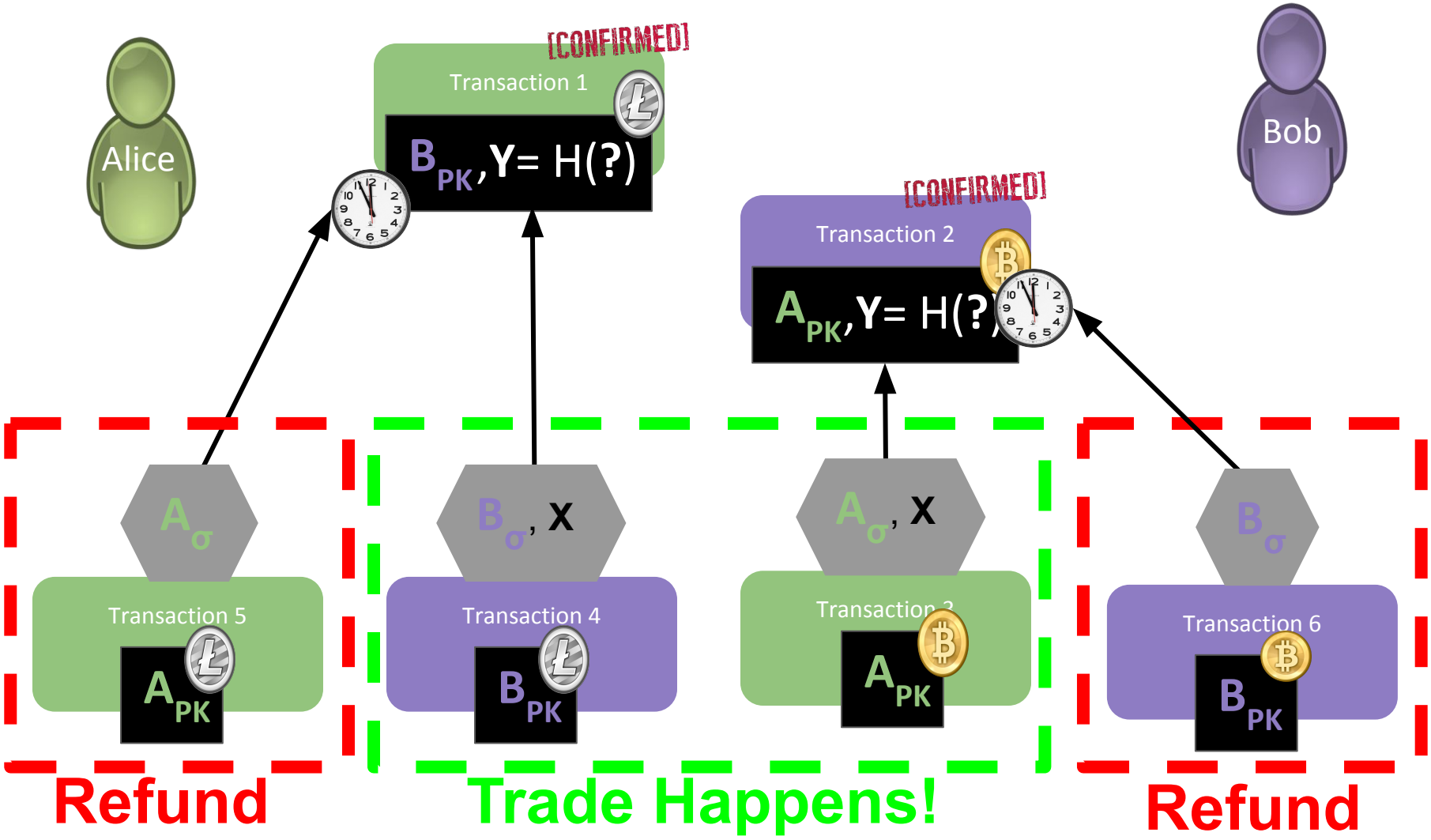


Atomic Cross-Blockchain Trades



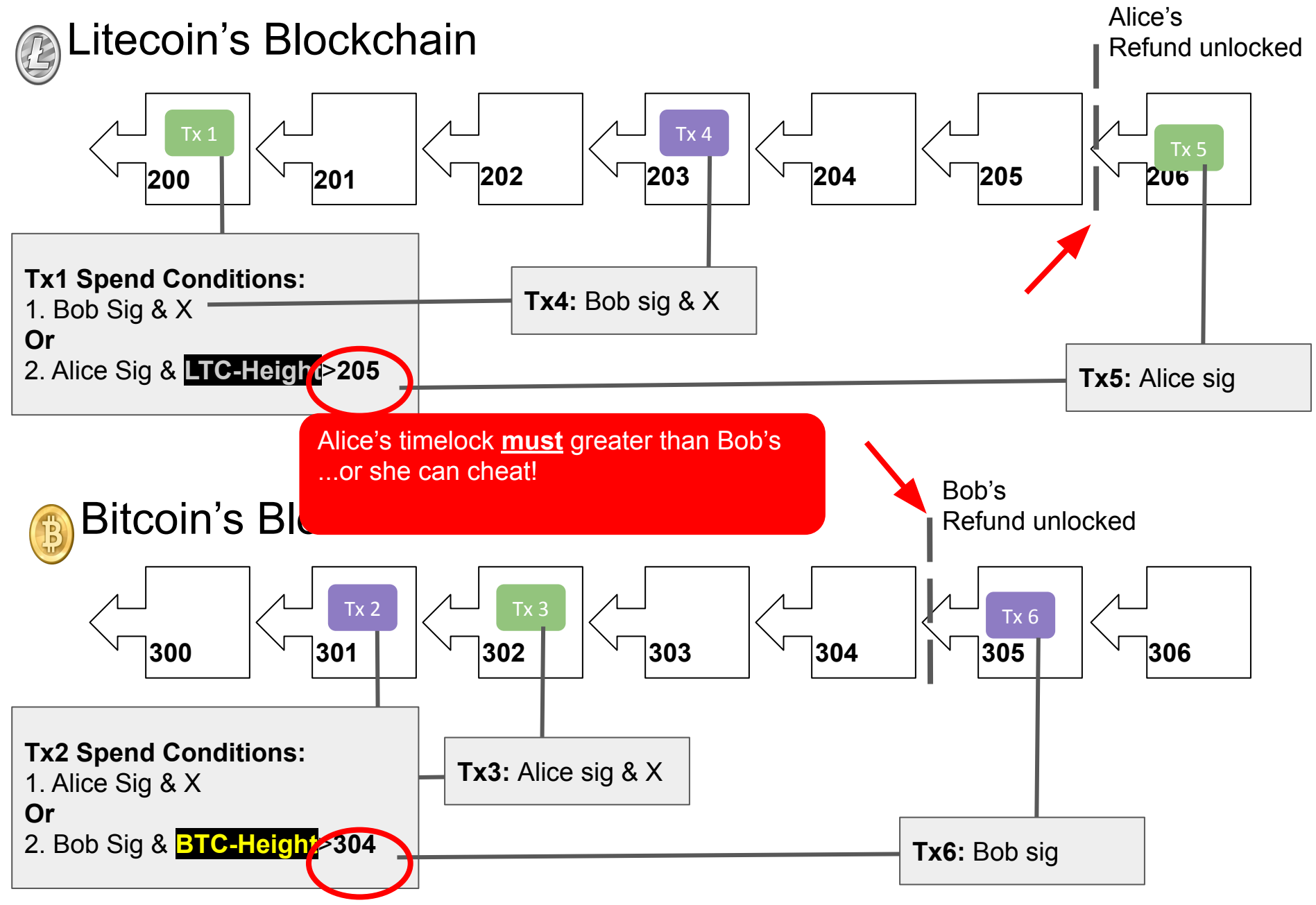
What happens if Alice never posts Tx 3? Funds are unspendable! We add an additional spend condition, called a timelock, which refunds coins after a time limit has been reached.

Full Tier-Nolan Atomic Trade Protocol

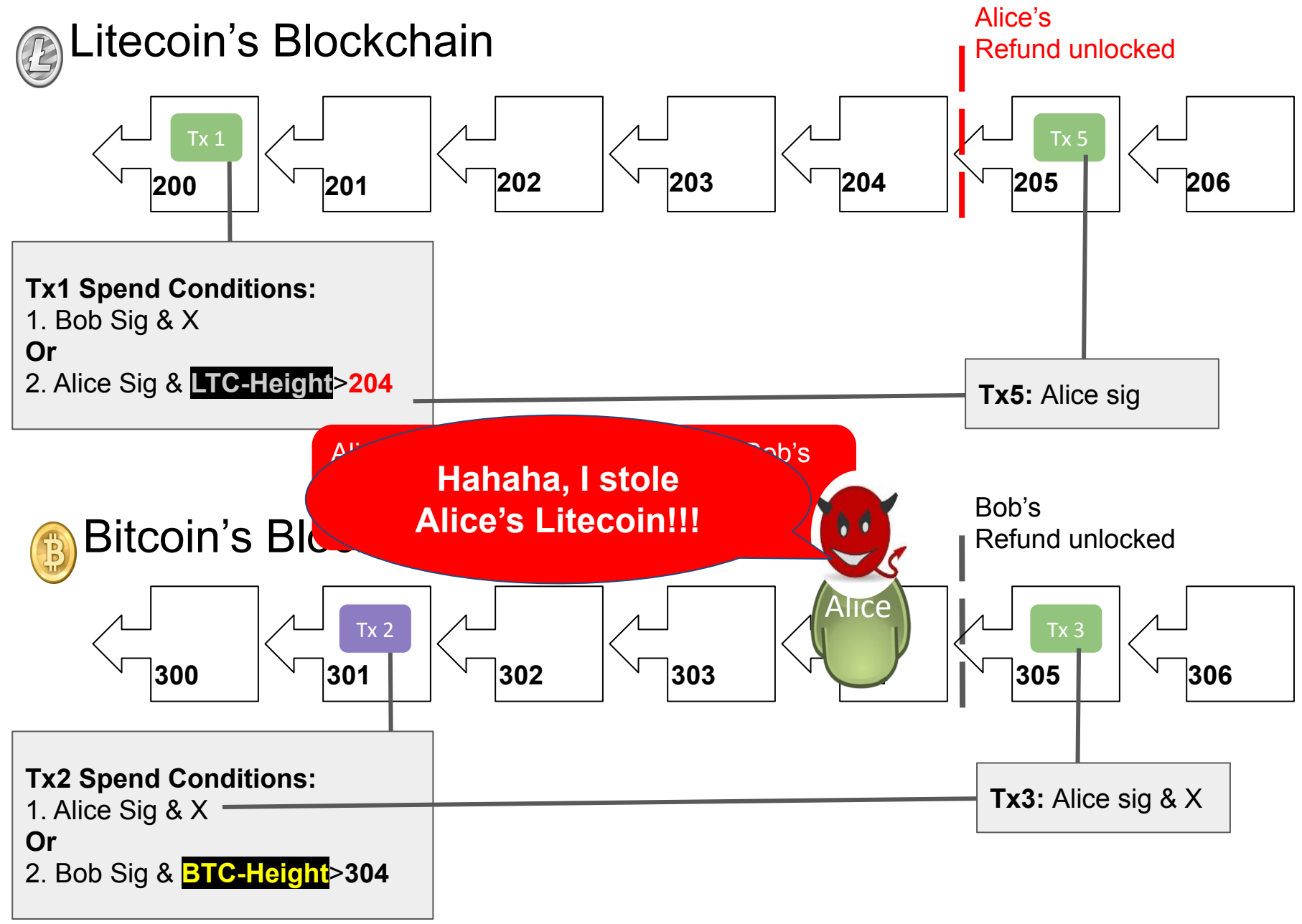


Bitcoin has two timelock functions: absolute **CLTV (BIP-65)** and relative **CSV (BIP-112)**
We will be using **CLTV** here.

Full Tier-Nolan Atomic Trade Protocol: Timing



Full Tier-Nolan Atomic Trade Protocol: Timing



Full Tier-Nolan Atomic Scripts

Offer:

```
OP_DEPTH OP_2 OP_EQUAL
OP_IF
        OP_HASH160 <AliceSecretHash> OP_EQUALVERIFY <Bob>
OP_ELSE
        <Timeout> OP_CLTV OP_DROP <Alice>
OP_ENDIF
OP_CHECKSIG
```

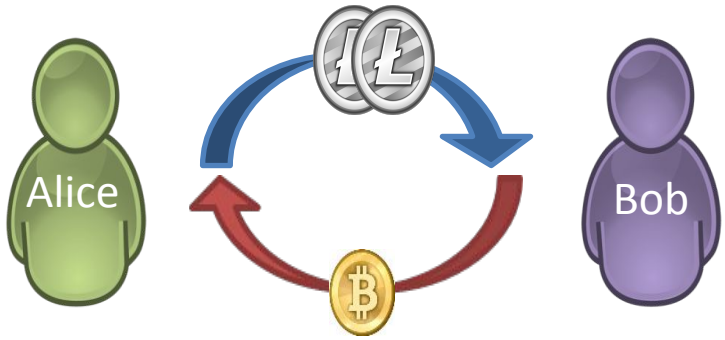
Counter Offer:

```
OP_DEPTH OP_2 OP_EQUAL
OP_IF
        OP_HASH160 <AliceSecretHash> OP_EQUALVERIFY <Bob>
OP_ELSE
        <Timeout> OP_CLTV OP_DROP <Alice>
OP_ENDIF
OP_CHECKSIG
```

http://n.bitcoin.ninja/checkscript?savedScript=04efb6e0-8676-4283-a201-6b5d8d6426dd

Summary: Cross-Chain Atomic Swaps

Cross-chain Atomic Swaps:
Alice has Litecoin, wants Bitcoin
Bob has Bitcoin, wants Litecoin
So… Alice trades Bob 2 LTC for 1 BTC

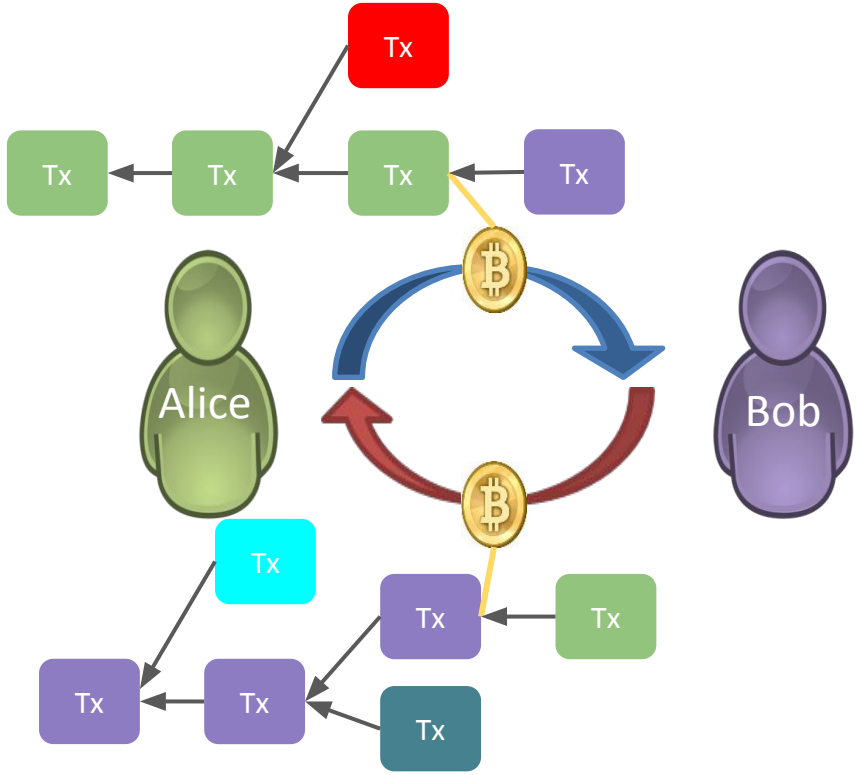


Tier-Nolan Atomic Trades:

- Enables two parties to trade cryptocurrencies
- Neither party can cheat each other
- Timelocks must be carefully selected to ensure Alice can't cheat
- Works between any cryptocurrencies that support hashlocks and timelocks
  - Fancier math can remove hashlock requirement
- Requires four on-blockchain transactions
  - If Alice trusts Bob this can be reduced to two transactions

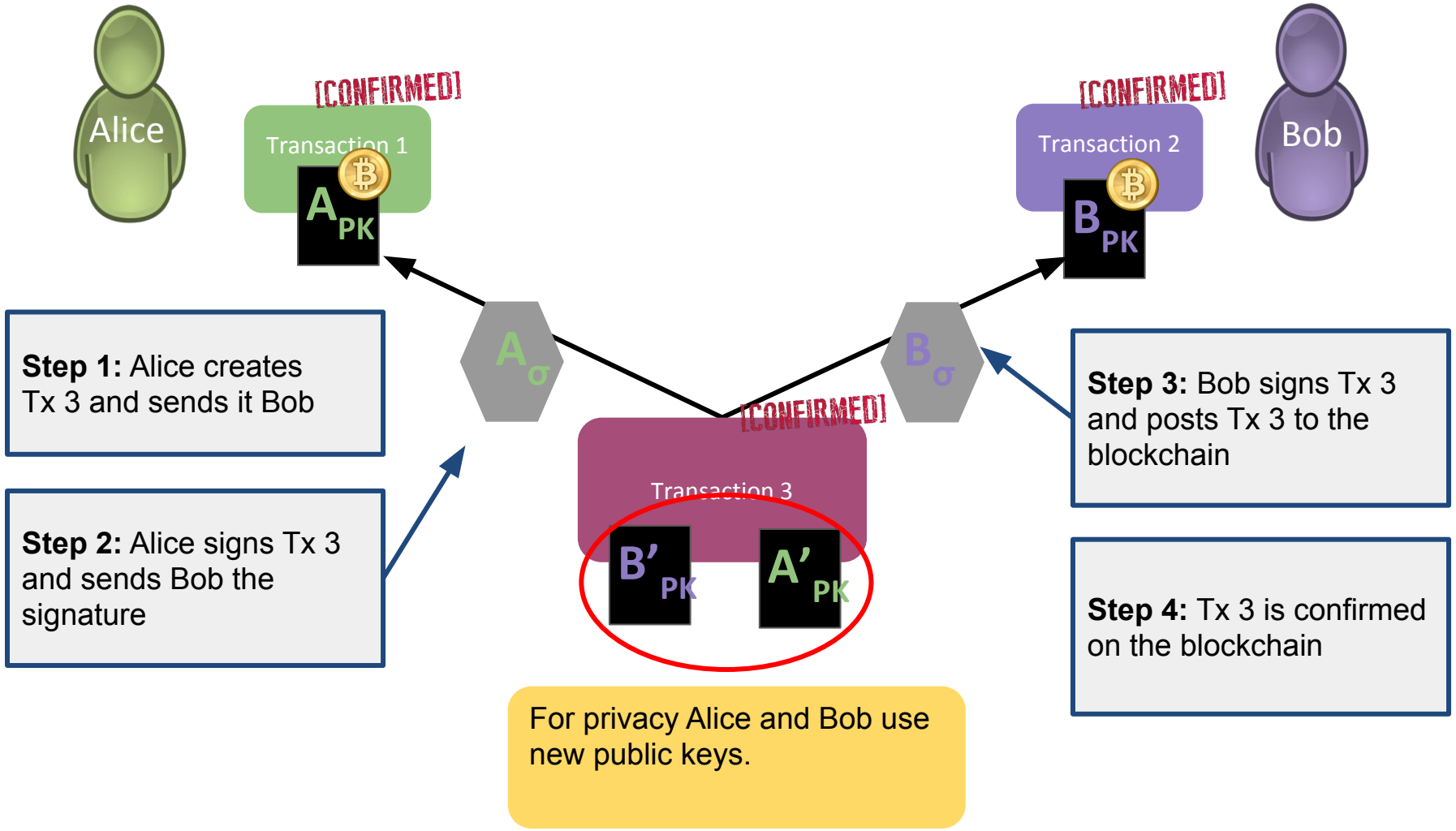
Privacy

Atomic Swaps for Privacy:
To obfuscate their transaction graph
Alice and Bob trade 1 BTC for 1 BTC
...thus, mixing their coins



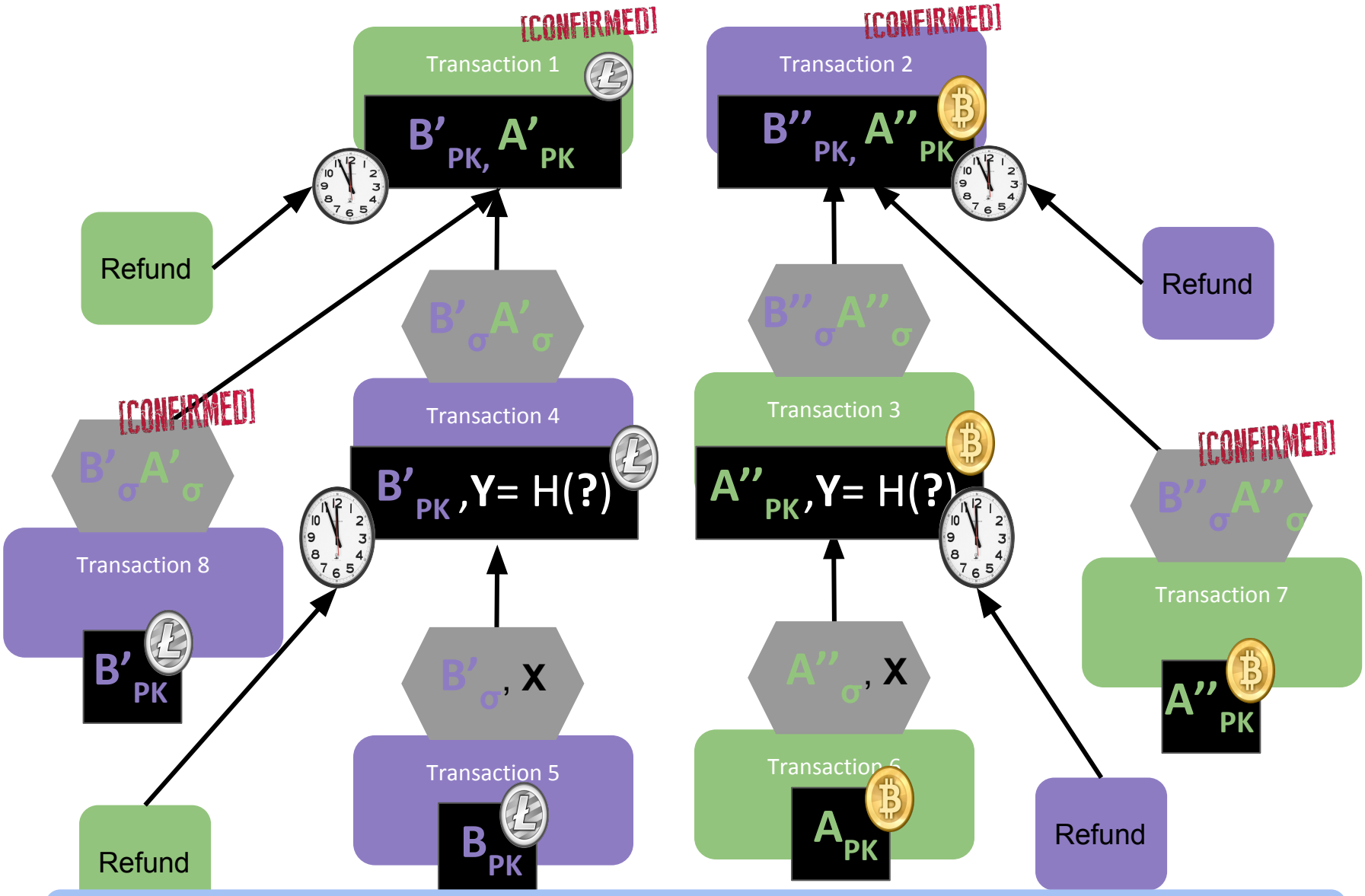
- The idea is to break linkages in the transaction graph
- We will briefly discuss two protocols:
  - Single-transaction CoinJoin
  - and CoinSwap (Private Atomic Swaps)

Simple Two Party CoinJoin Protocol



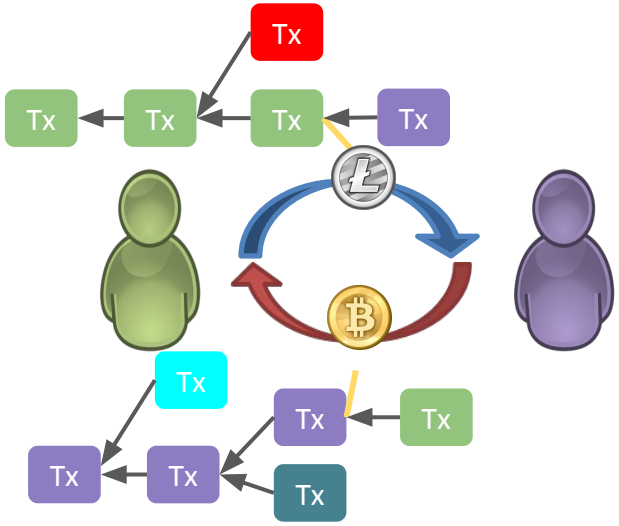
Privacy Offered: ½ chance of guessing which Tx 3 pubkey is Alice

Private Atomic Swaps



Privacy Offered: Only Tx 1, Tx 2, Tx7, Tx8 show up on Blockchain, no linkage.

Privacy Summary



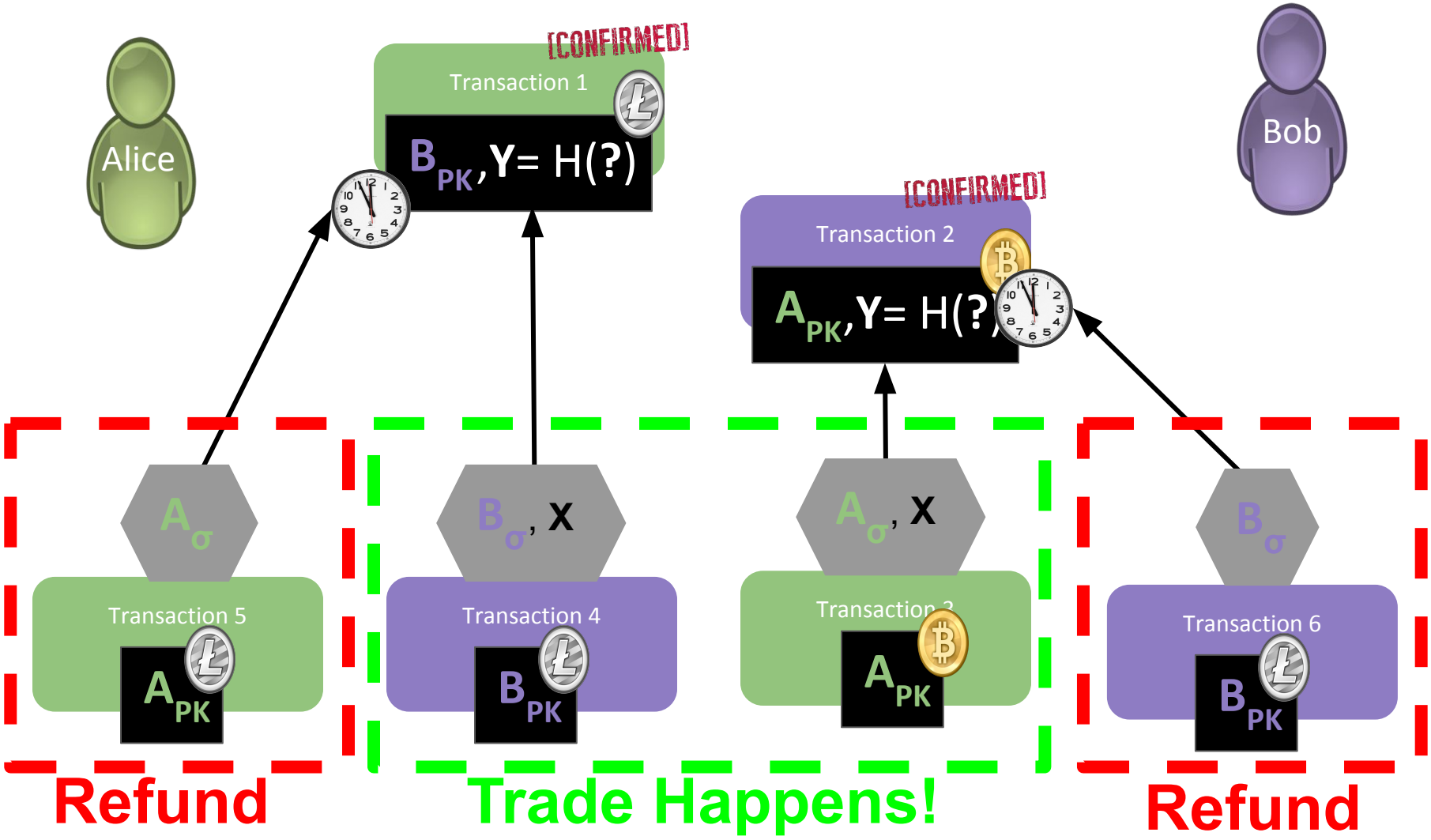
- Maxwell's CoinSwaps make Cross-Chain Atomic Swaps indistinguishable ….from four multisig transactions on different blockchains.
  - However they can be correlated by price, timing, network information,...
- There are several other Atomic Swap based privacy protocols
  - Barber's Fair Exchange/XIM
  - TumbleBit
  - ...

Questions?

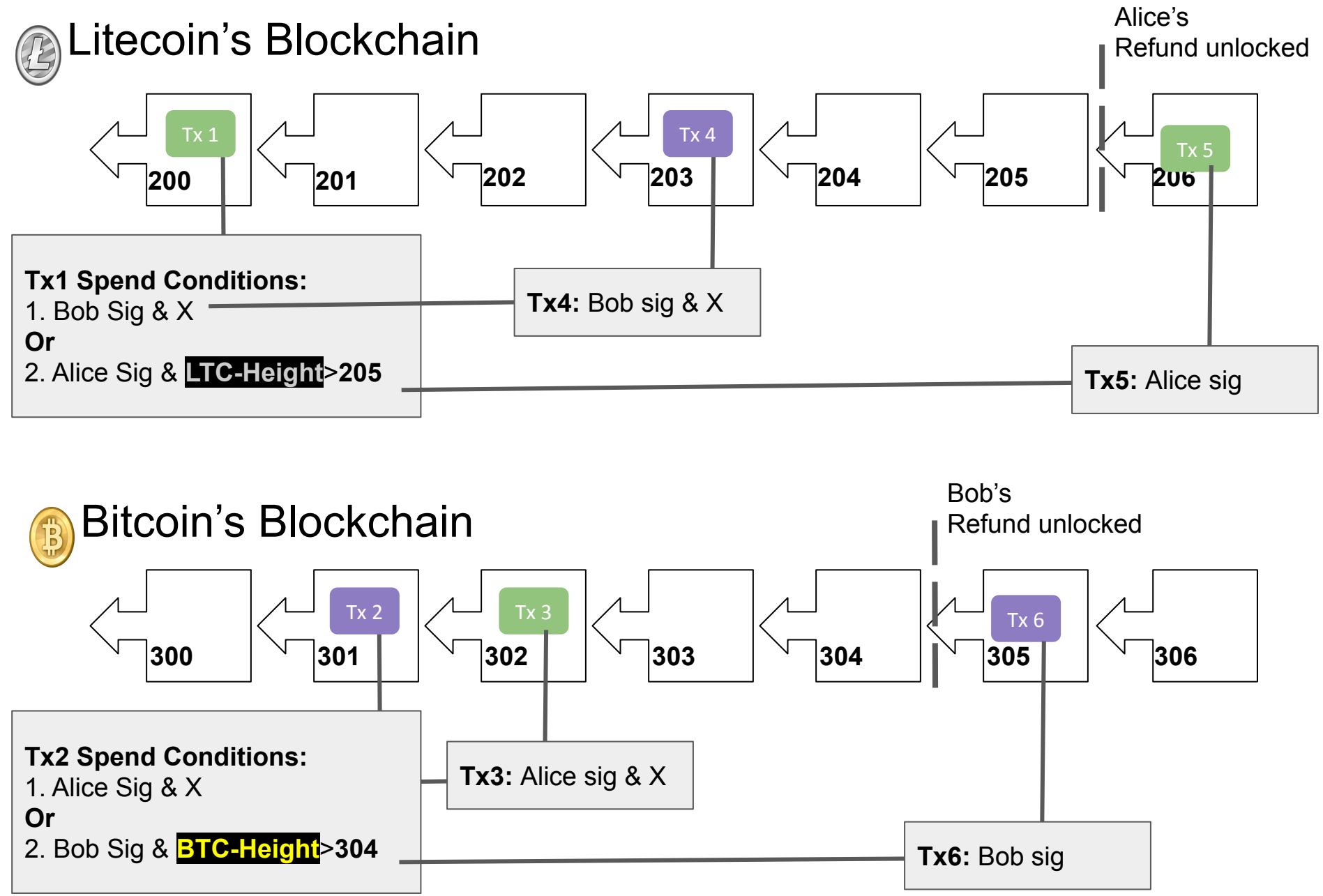
Topics Discussed:

- Simple trading protocols
  - Trades that trust one party
  - Atomic Trades that work across one blockchain
- Cross-Chain Atomic Swaps
  - Hashlocks/Timelocks
  - Tier Nolan Atomic Trade Protocol
- Privacy
  - Two-party CoinJoin
  - Making Atomic Trades Private

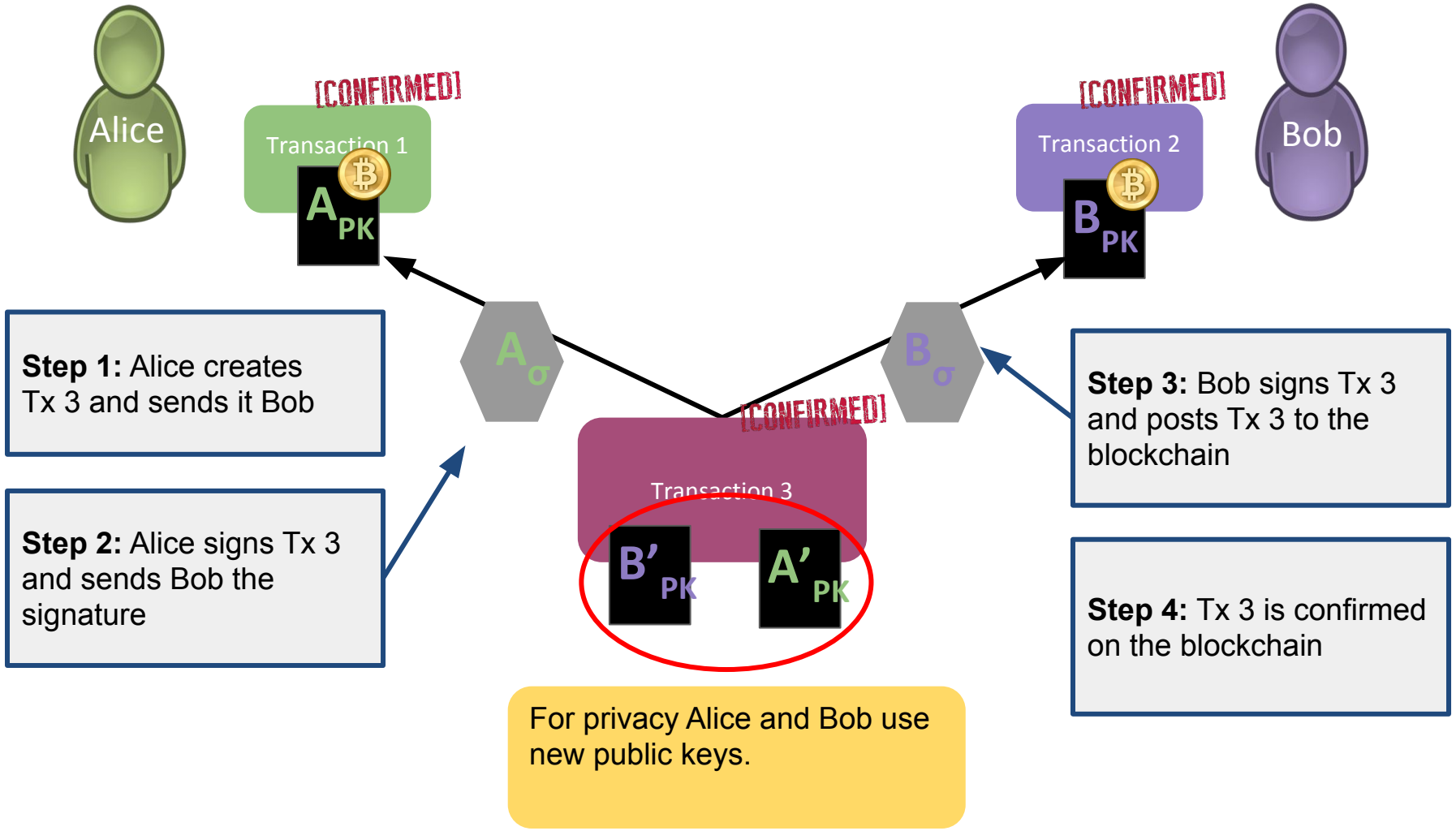
Full Tier-Nolan Atomic Trade Protocol



Full Tier-Nolan Atomic Trade Protocol



Simple Two Party CoinJoin Protocol



Privacy Offered: ½ chance of guessing which Tx 3 pubkey is Alice

Barber et al's Fair-Exchange Protocol

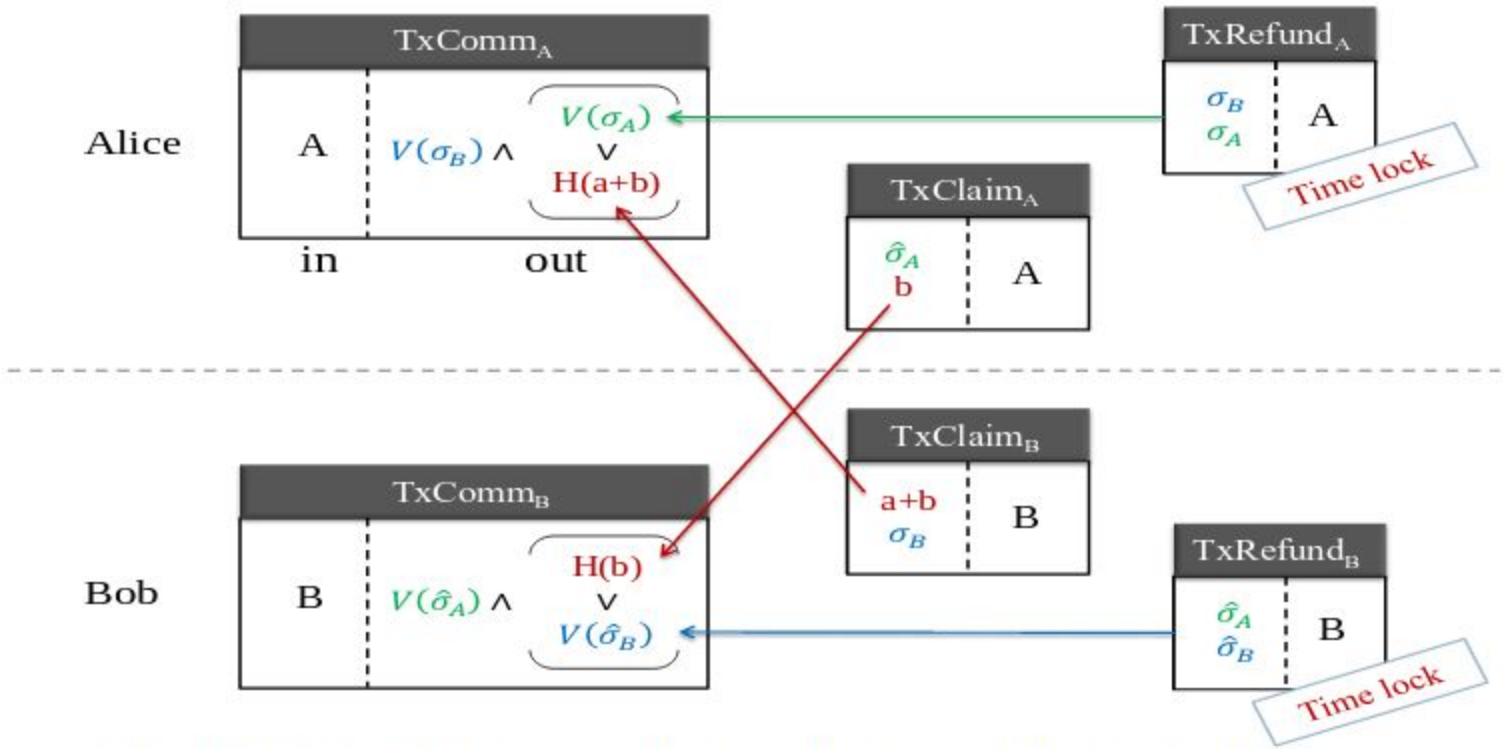
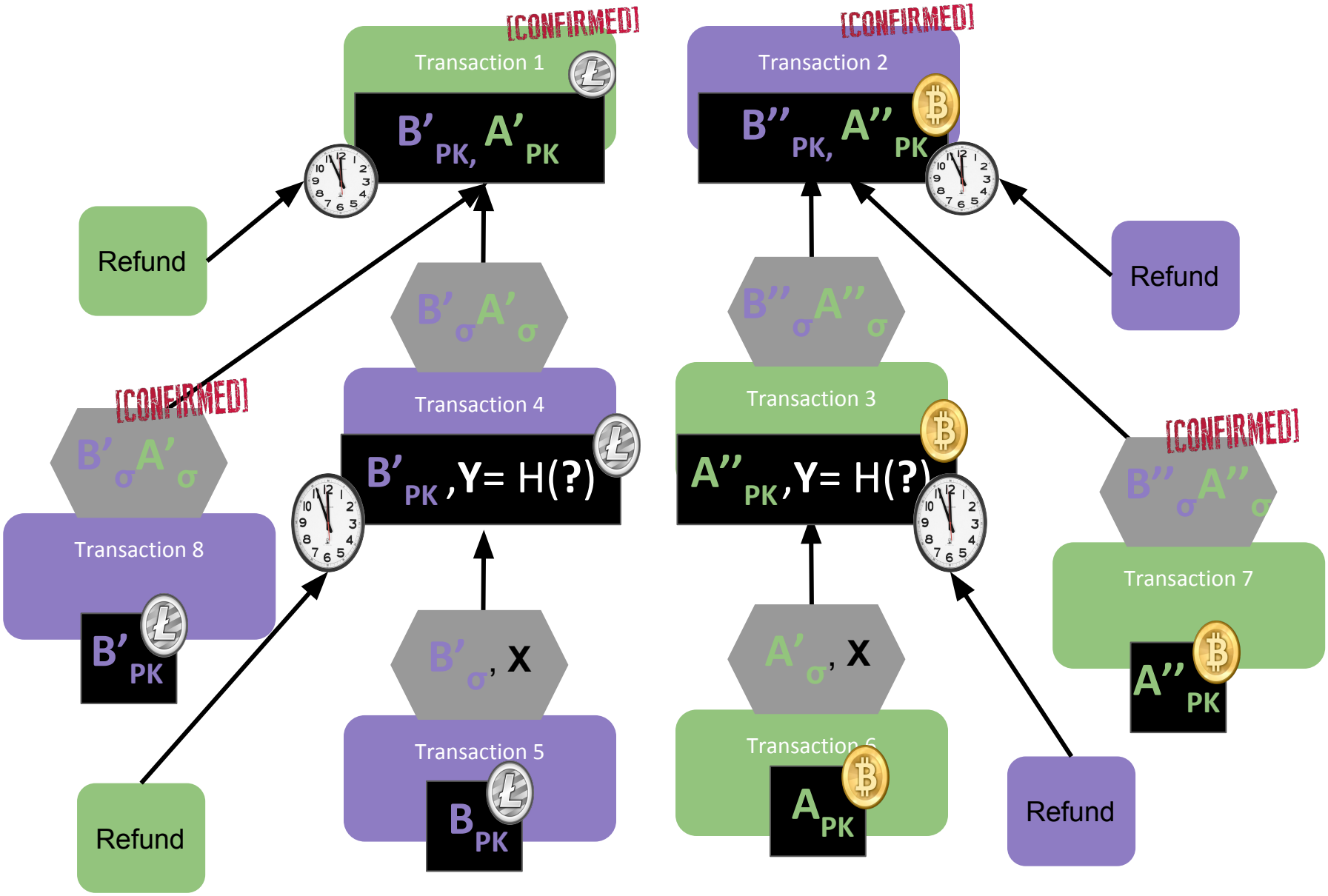


Fig. 1: A fair exchange protocol: mixing Bitcoins with an untrusted mixer.

[0] "Bitter to Better —How to Make Bitcoin a Better Currency", Barber et al.

Barber Protocol



Barber et al's Fair-Exchange Protocol

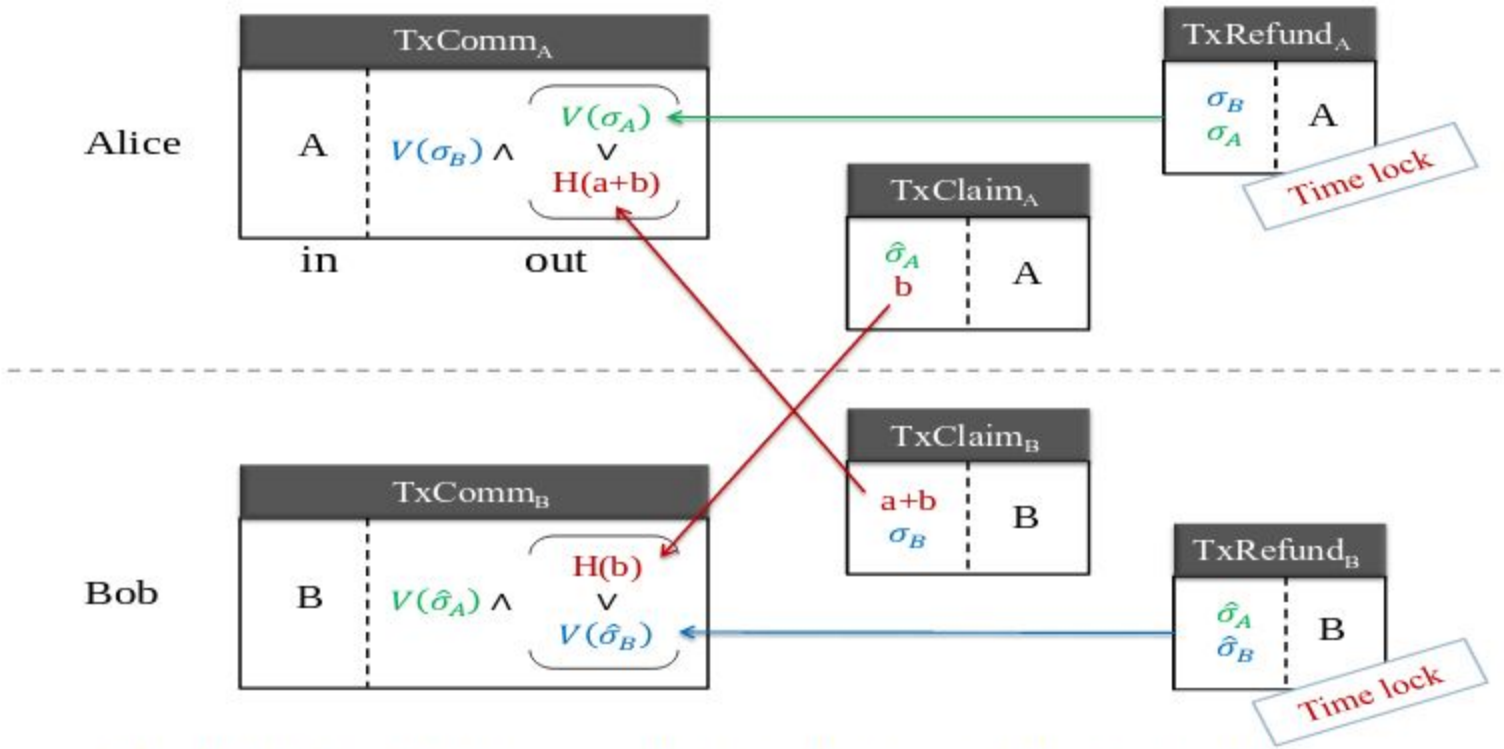


Fig. 1: A fair exchange protocol: mixing Bitcoins with an untrusted mixer.

[0] "Bitter to Better —How to Make Bitcoin a Better Currency", Barber et al.