Atomically Swapping Coins:
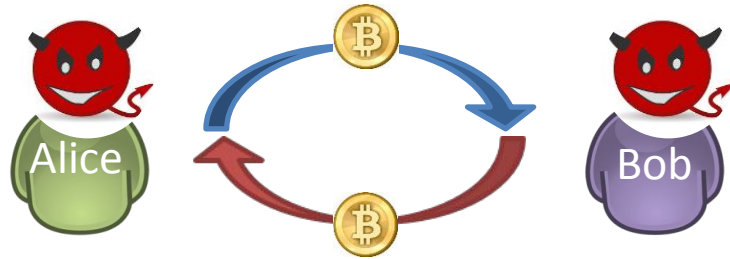## for Privacy or Cross-Blockchain Trades

Ethan Heilman, Nicolas Dorier

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.

Trade happens

OR

Both parties get coins back
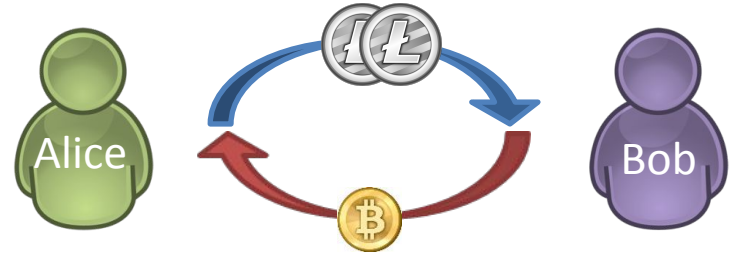
…even if parties are malicious and try to cheat each other!

Uses: Cross-blockchain Trades and Privacy

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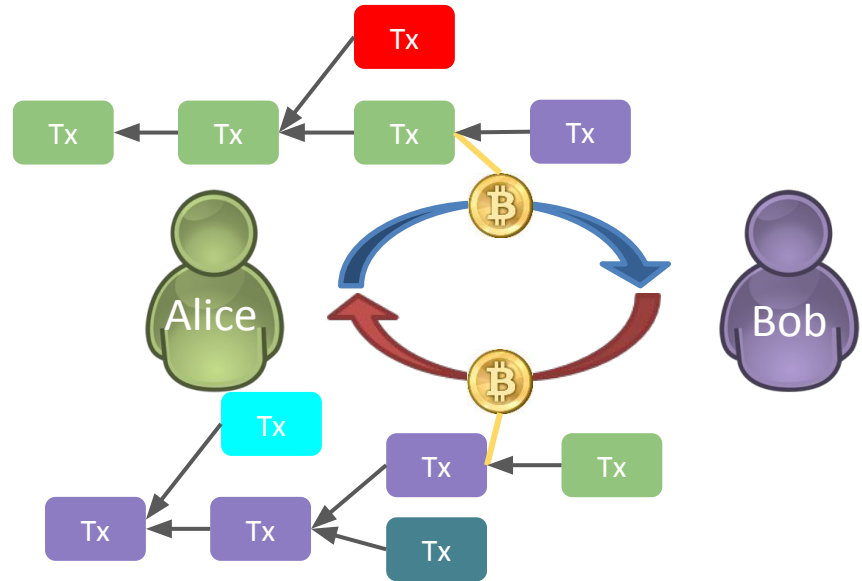Bob has Bitcoin, wants Litecoin
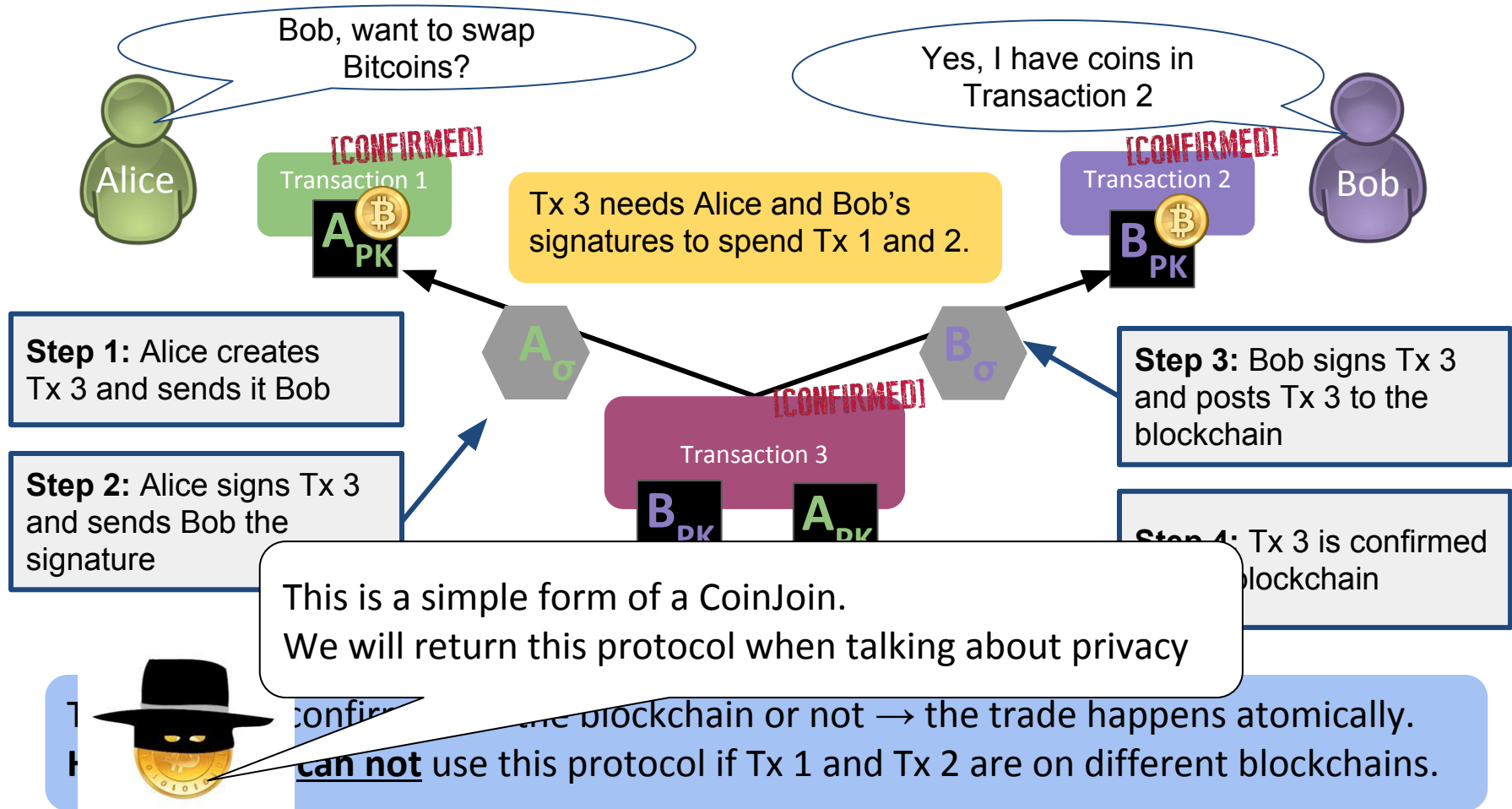**So…** Alice trades Bob 2 LTC for 1 BTC

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
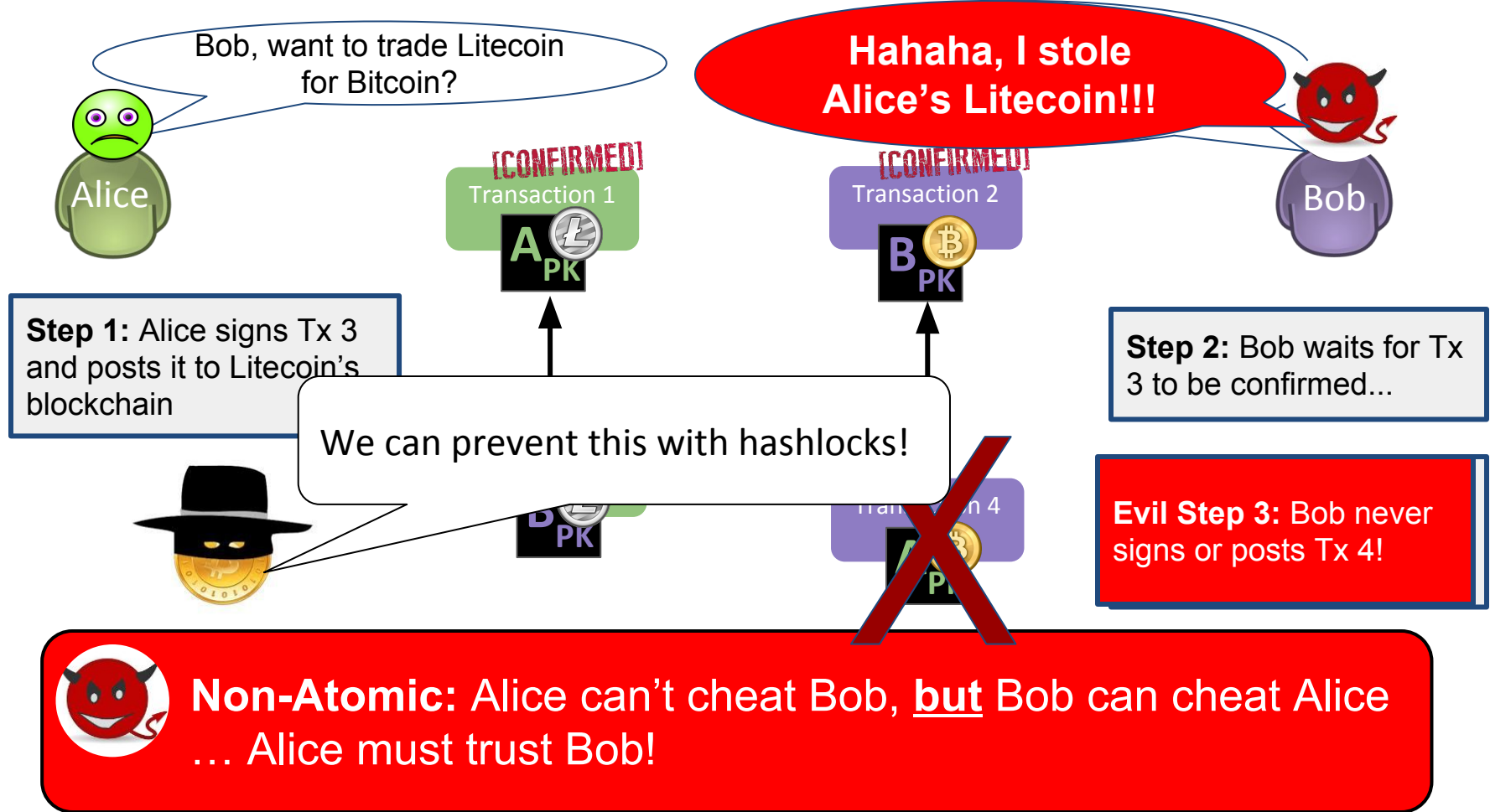
Hashlocking Funds

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

Transaction 1

B_{PK}, Y= H(?)

B_{σ}, X

Transaction 2
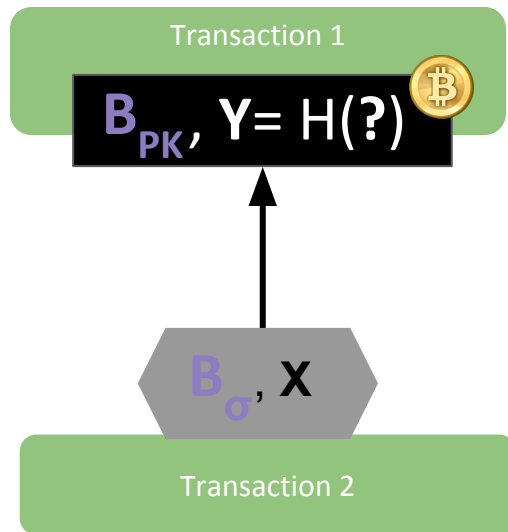
Step 3: Bob learns X and spends Tx 1.

Hashlocks:

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

Atomic Cross-Blockchain Trades

[CONFIRMED]

Transaction 1

$B_{PK}, Y = H(?)$

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

[CONFIRMED]

Transaction 2

$A_{PK}, Y = H(?)$

Step 2: Bob waits for Tx 1 to be confirmed and then posts Tx 2.

B_σ, X

Transaction 4

B_{PK}

A_σ, X

Transaction 3

A_{PK}

Step 3: Alice waits for Tx 2 to be confirmed and then posts Tx 3.

Step 4: Bob learns X from Tx 3 and posts Tx
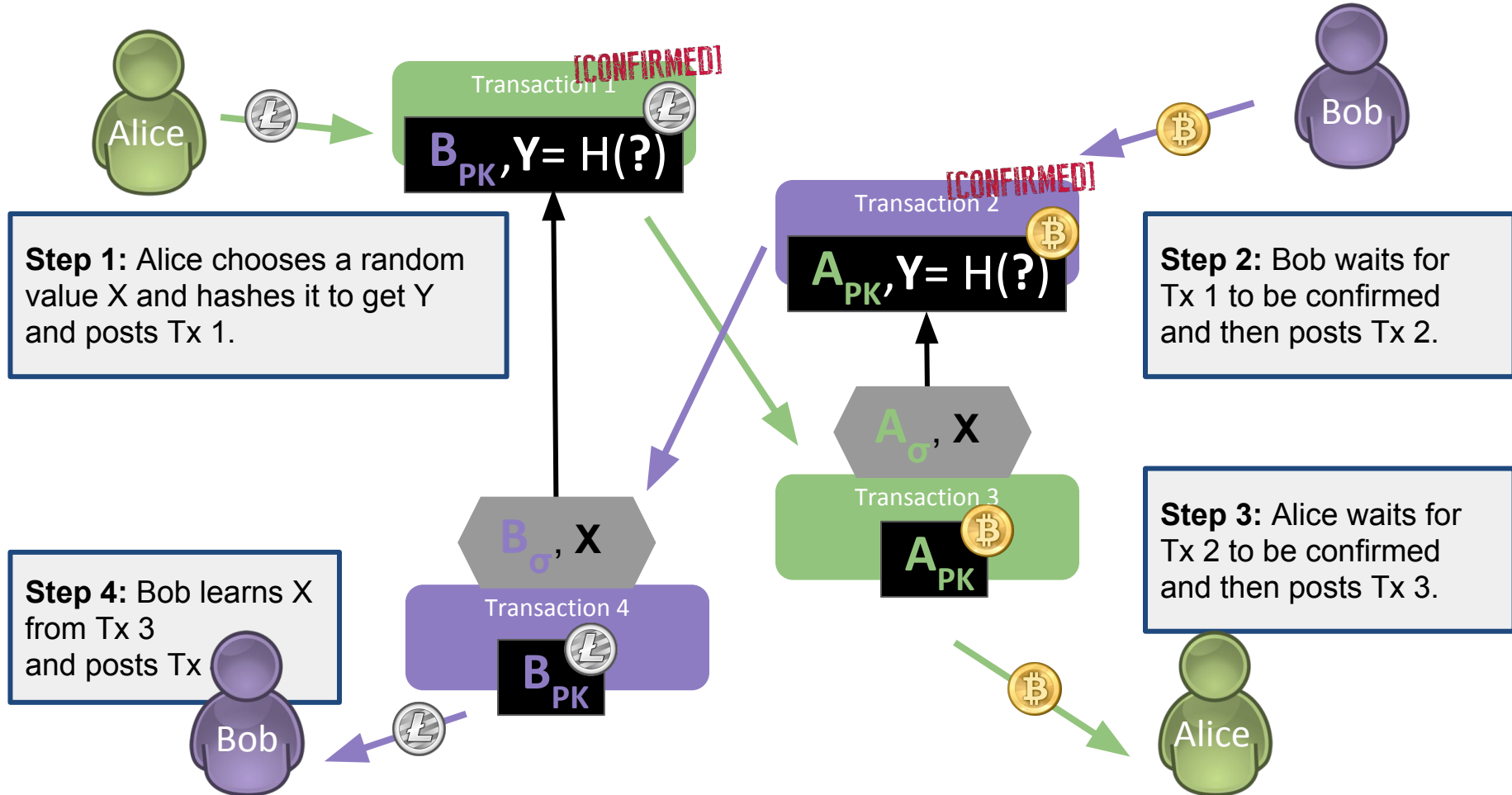
Atomic Cross-Blockchain Trades
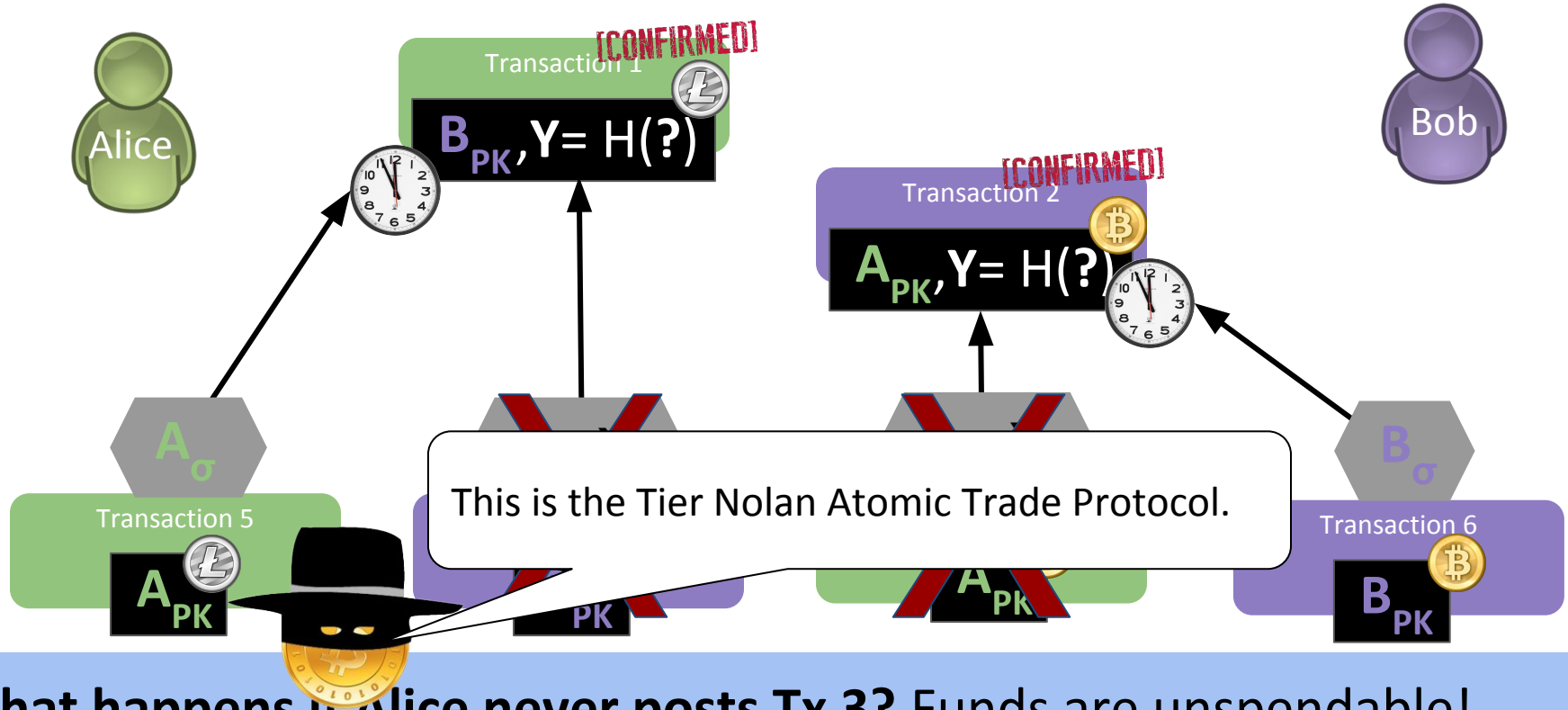
What happens if Alice never posts Tx 3? Funds are unspendable!
We add an additional spend condition, called a timelock, which refunds coins after a time limit has been reached.

Full Tier-Nolan Atomic Trade Protocol

Alice

Bob

[CONFIRMED]

Transaction 1

$B_{PK}, Y = H(?)$

Transaction 2

$A_{PK}, Y = H(?)$

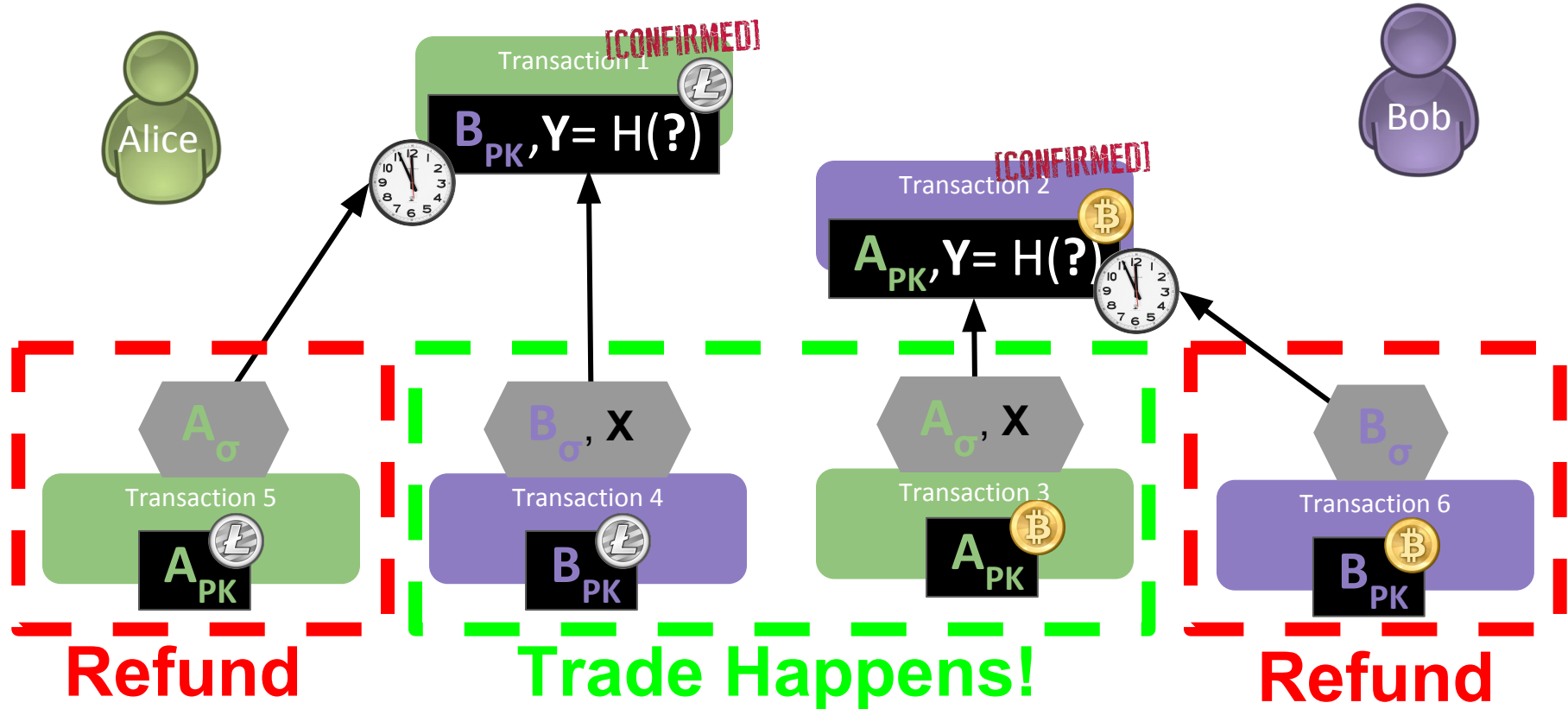**[CONFIRMED]**

A_{σ}

B_{σ}, X

A_{σ}, X

B_{σ}

Transaction 5

A_{PK}

Transaction 4

B_{PK}

Transaction 3

A_{PK}

Transaction 6
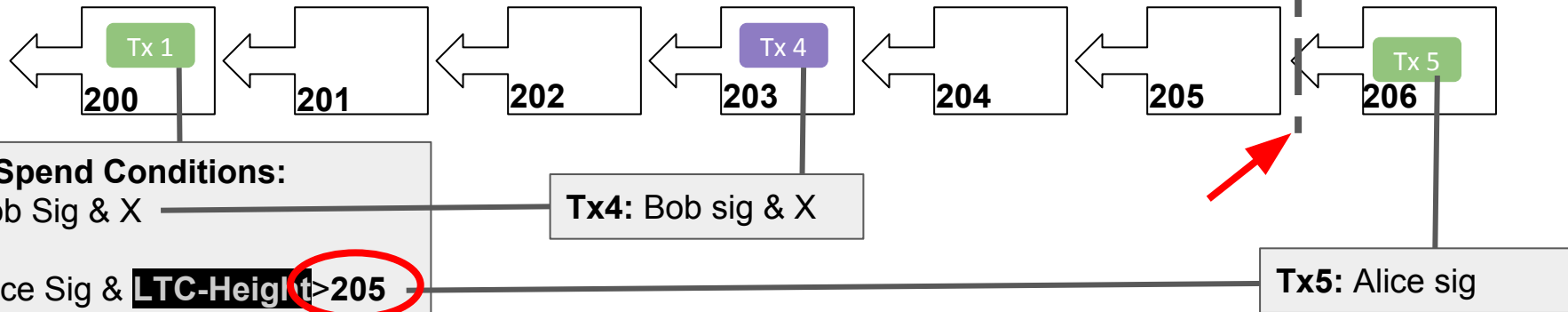
B_{PK}

Refund

Trade Happens!

Refund

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

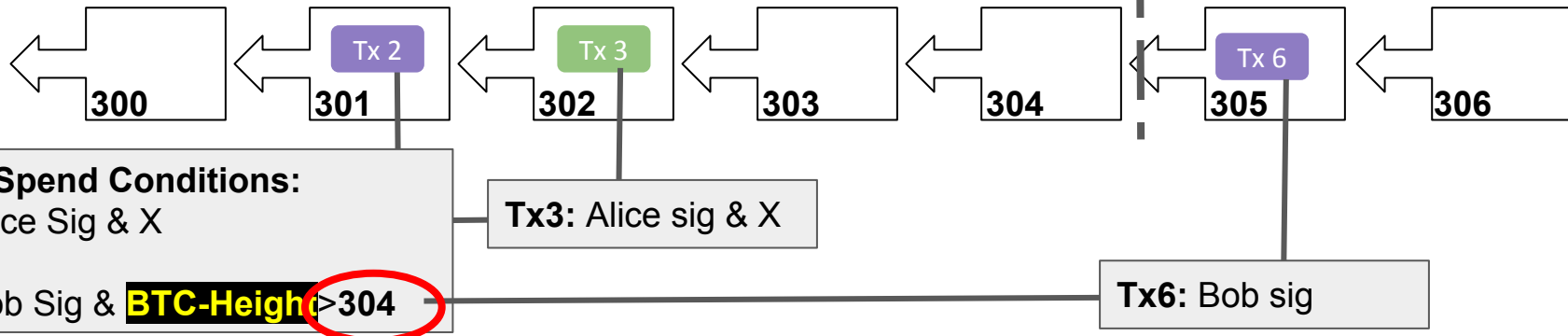# Full Tier-Nolan Atomic Trade Protocol: Timing

Litecoin's Blockchain

Alice's Refund unlocked

Tx 1			Tx 4			Tx 5
200	201	202	203	204	205	206

Tx1 Spend Conditions:
1. Bob Sig & X
Or
2. Alice Sig & LTC-Height>205

Tx4: Bob sig & X

Tx5: Alice sig

Alice's timelock **must** greater than Bob's ...or she can cheat!

Bitcoin's Blockchain

Bob's Refund unlocked

	Tx 2	Tx 3			Tx 6	
300	301	302	303	304	305	306

Tx2 Spend Conditions:
1. Alice Sig & X
Or
2. Bob Sig & BTC-Height>304

Tx3: Alice sig & X

Tx6: Bob sig
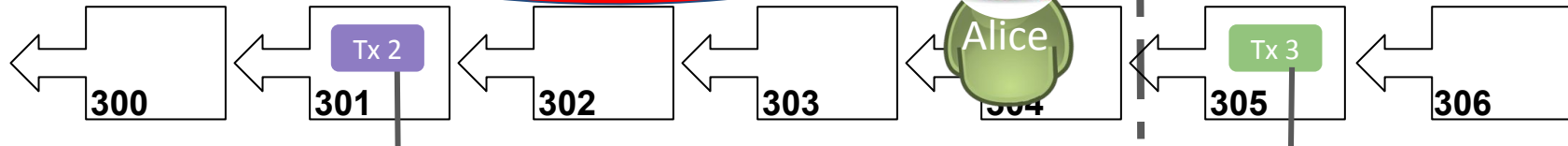
Full Tier-Nolan Atomic Trade Protocol: Timing

Let's perform
A cross-chain atomic swap

Full Tier-Nolan Atomic Trade Protocol

Alice

Bob

Here is my public key

1 BTCA vs 2 BTCB ?

Ok!

Broadcast Offer
Offer on BTCA:

Bob + AliceSecret => 1 BTCA
Alice + Timeout   => 1 BTCA

Broadcast Counter Offer
Counter Offer on BTCB:

Alice + AliceSecret => 2 BTCB
Bob + Timeout   => 2 BTCB

Wait confirmation

Take Counter Offer on BTCB

−AliceSecret is now known by Bob
−Alice received 2 BTCB

Take offer on BTCA:

−Alice received 2 BTCB
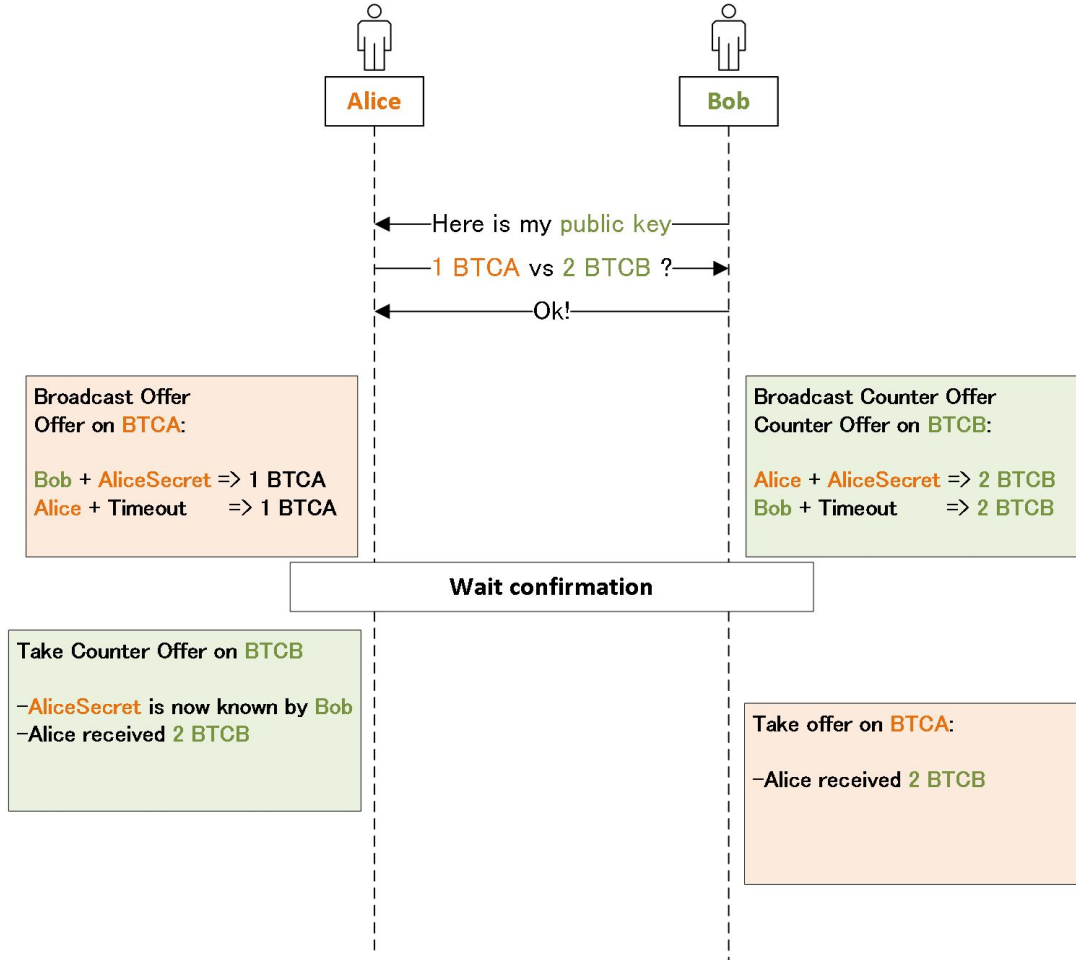
Full Tier-Nolan Atomic Scripts

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

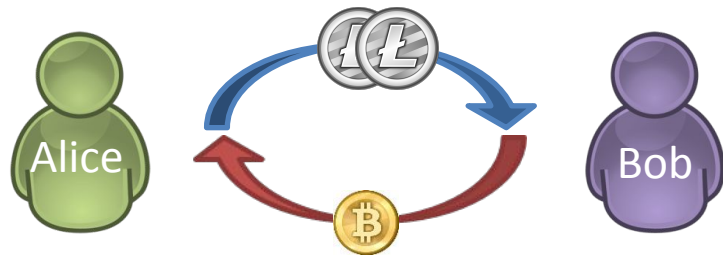http://n.bitcoin.ninja/checkscript?savedScript=04efb6e0-8676-4283-a201-6b5d8d6426dd

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
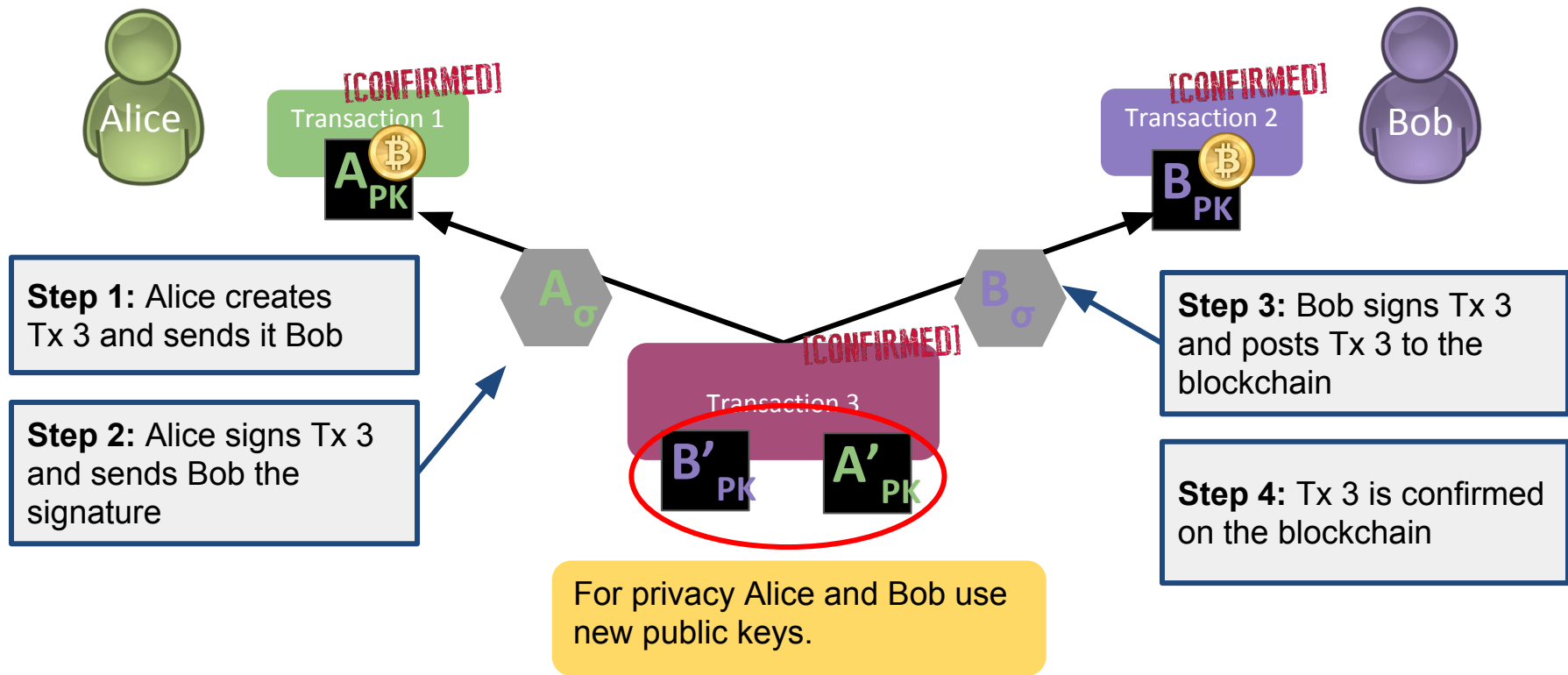 - If Alice trusts Bob this can be reduced to two transactions

Privacy

Atomic Swaps for Privacy:
To obfuscate their transaction graph Alice and Bob trade 1 BTC for 1 BTC
...thus, mixing their coins
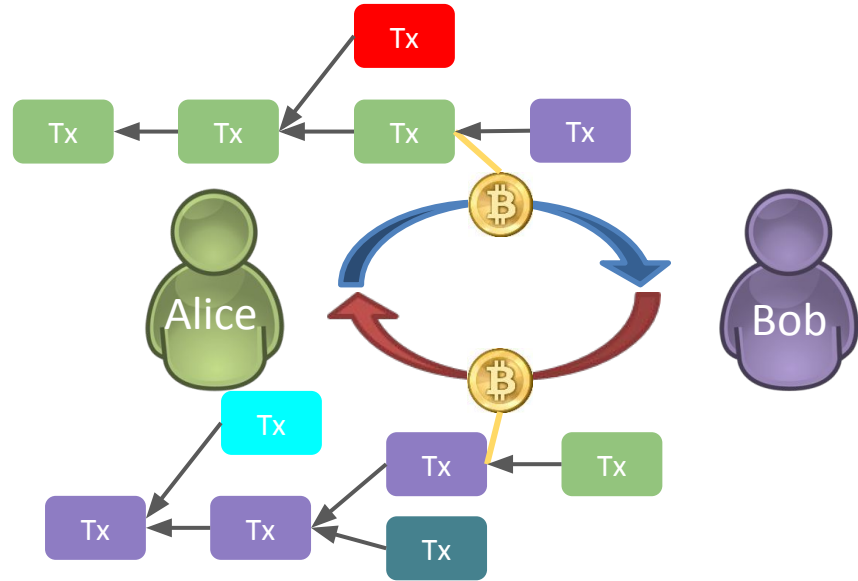
- The idea is to break linkages in the transaction graph
- We will briefly discuss two protocols:
  - Single-transaction CoinJoin
  - and Maxwell's CoinSwap (Private Atomic Swaps)

Simple Two Party CoinJoin Protocol

Alice

[CONFIRMED]
Transaction 1

A PK

Bob

[CONFIRMED]
Transaction 2

B PK

A σ

B σ

[CONFIRMED]
Transaction 3

B' PK   A' PK

Step 1: Alice creates Tx 3 and sends it Bob

Step 2: Alice signs Tx 3 and sends Bob the signature

Step 3: Bob signs Tx 3 and posts Tx 3 to the blockchain

Step 4: Tx 3 is confirmed on the blockchain

For privacy Alice and Bob use new public keys.

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

Private Atomic Swaps (Maxwell's CoinSwap)

Transaction 1 [CONFIRMED]

$B'_{PK,}\ A'_{PK}$

Transaction 2 [CONFIRMED]

$B''_{PK,}\ A''_{PK}$

Refund

Refund

$B'_{\sigma}\ A'_{\sigma}$

$B''_{\sigma}\ A''_{\sigma}$

[CONFIRMED] $B'_{\sigma}\ A'_{\sigma}$

Transaction 4

$B'_{PK},Y = H(?)$

Transaction 3

$A''_{PK},Y = H(?)$

[CONFIRMED] $B''_{\sigma}\ A''_{\sigma}$

Transaction 8

B'_{PK}

Transaction 7

A''_{PK}

$B'_{\sigma},\ X$

$A''_{\sigma},\ X$

Refund

Transaction 5

B_{PK}

Transaction 6

A_{PK}

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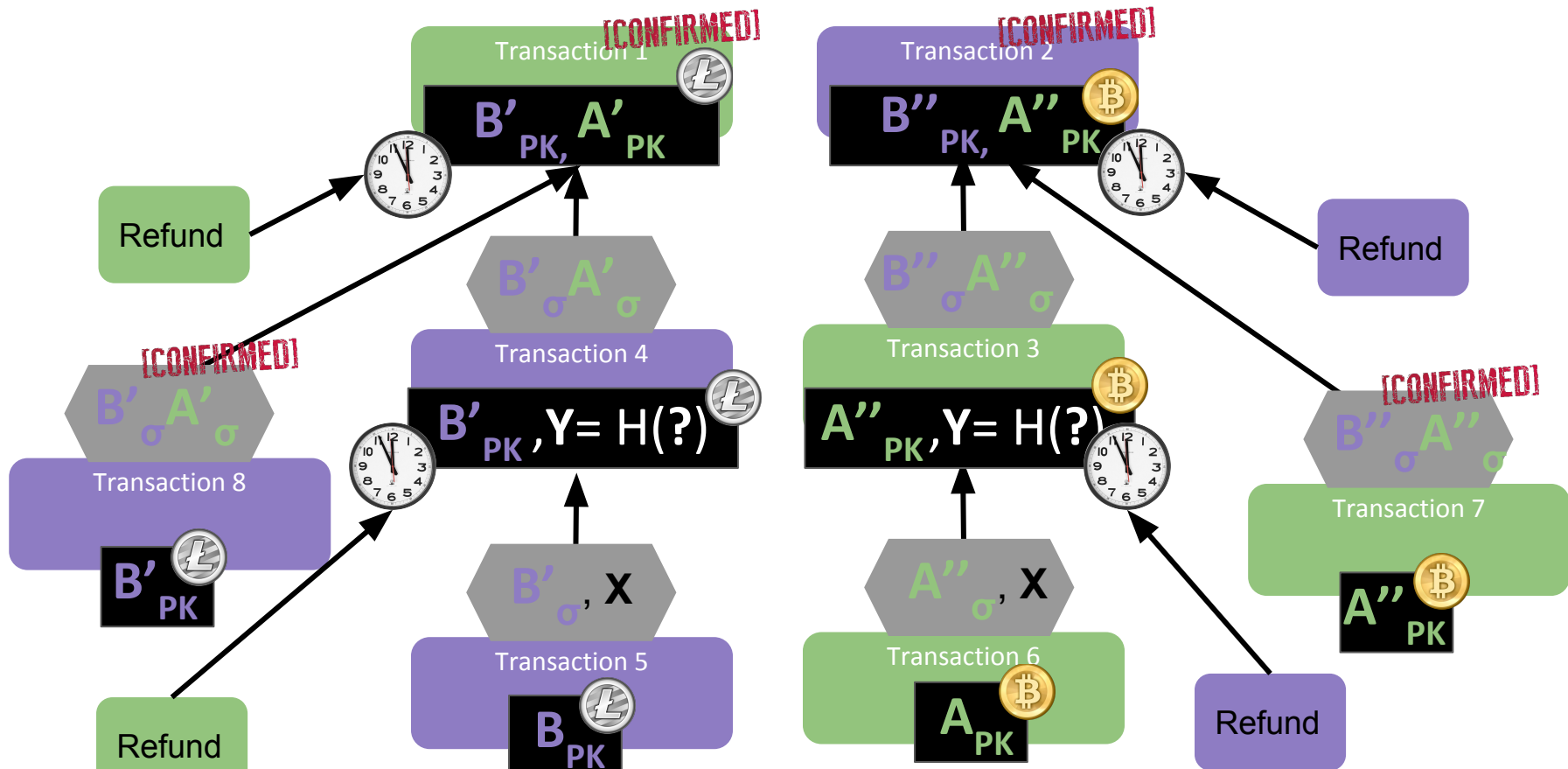
Privacy Offered: Only Tx 1, Tx 2, Tx7, Tx8 show up on Blockchain, no linkage.

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
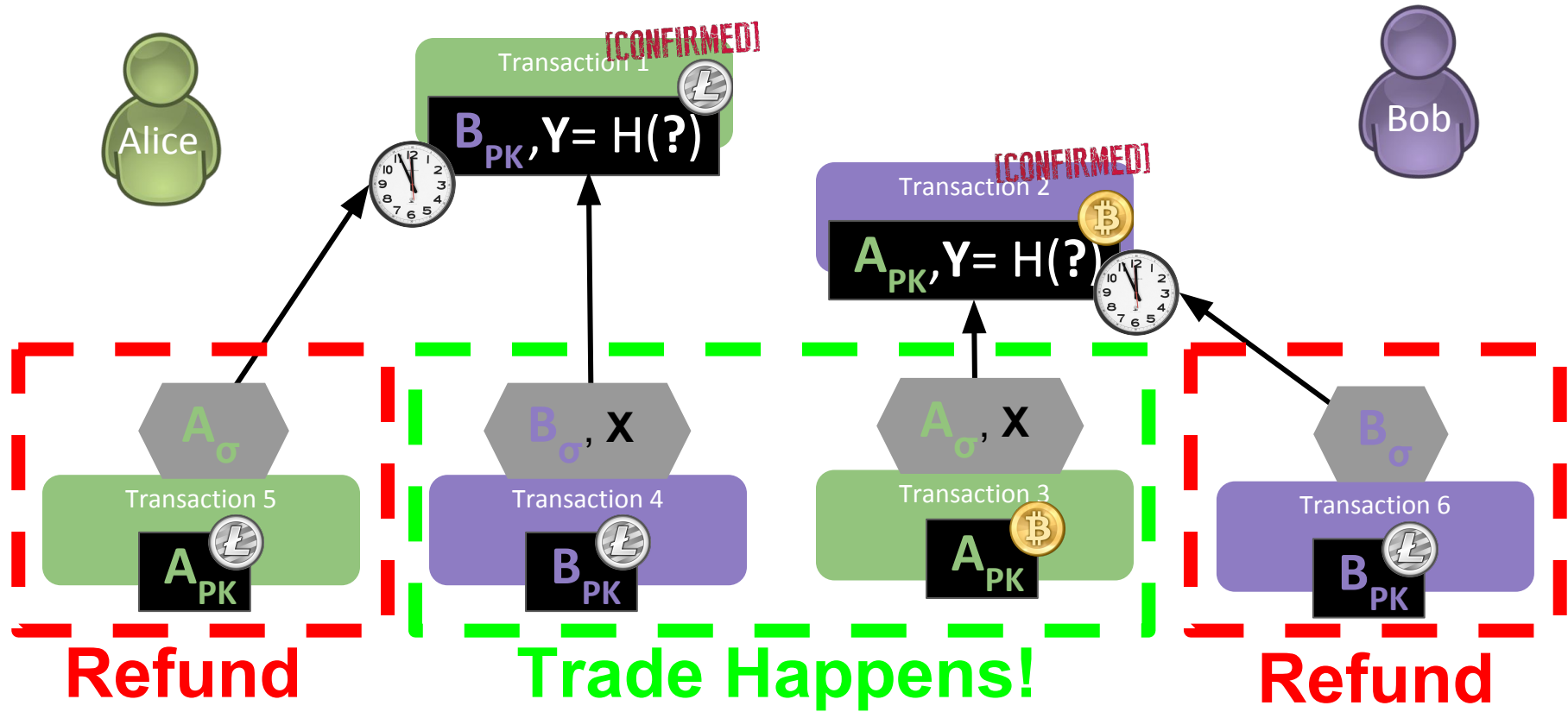 - Barber's Fair Exchange/XIM
  - TumbleBit
  - ...

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

Backup slides

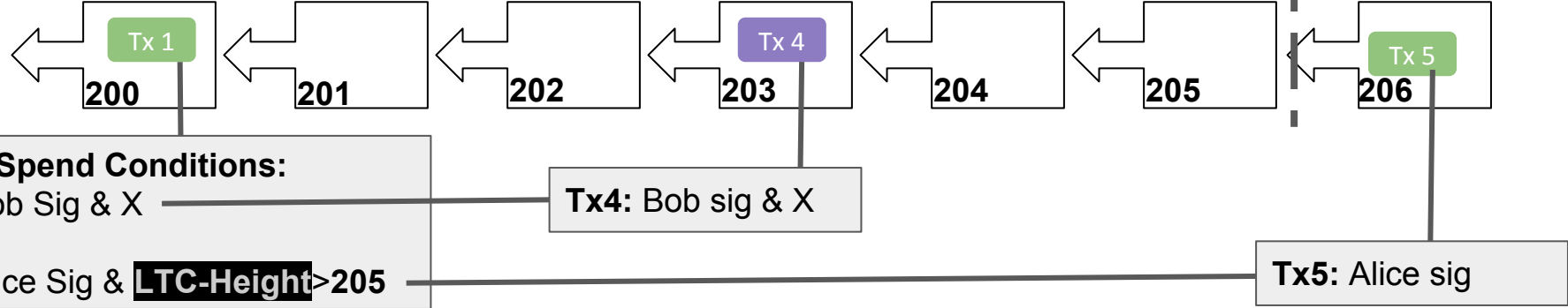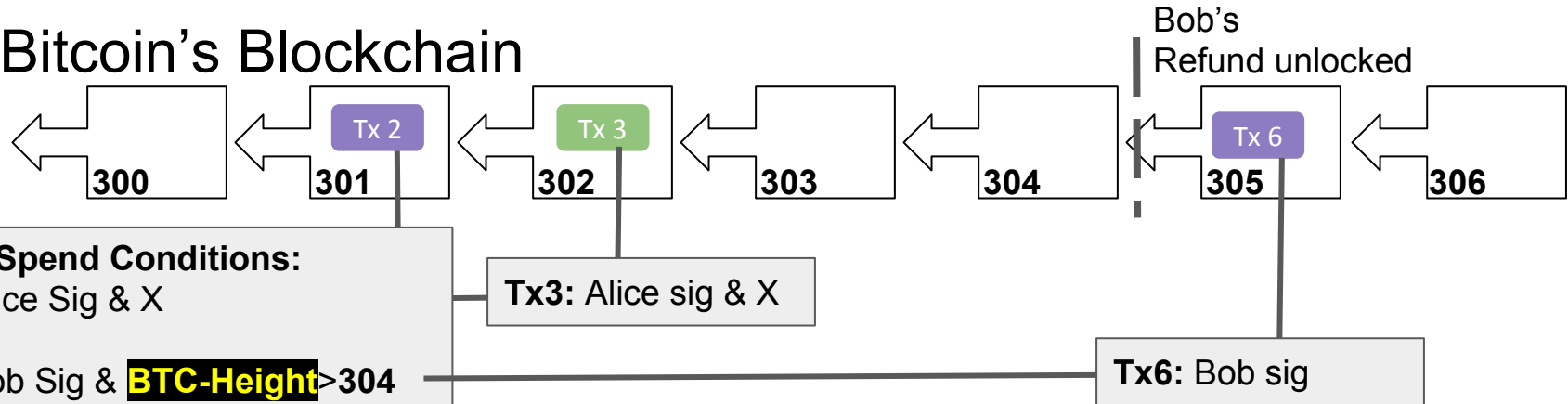Full Tier-Nolan Atomic Trade Protocol
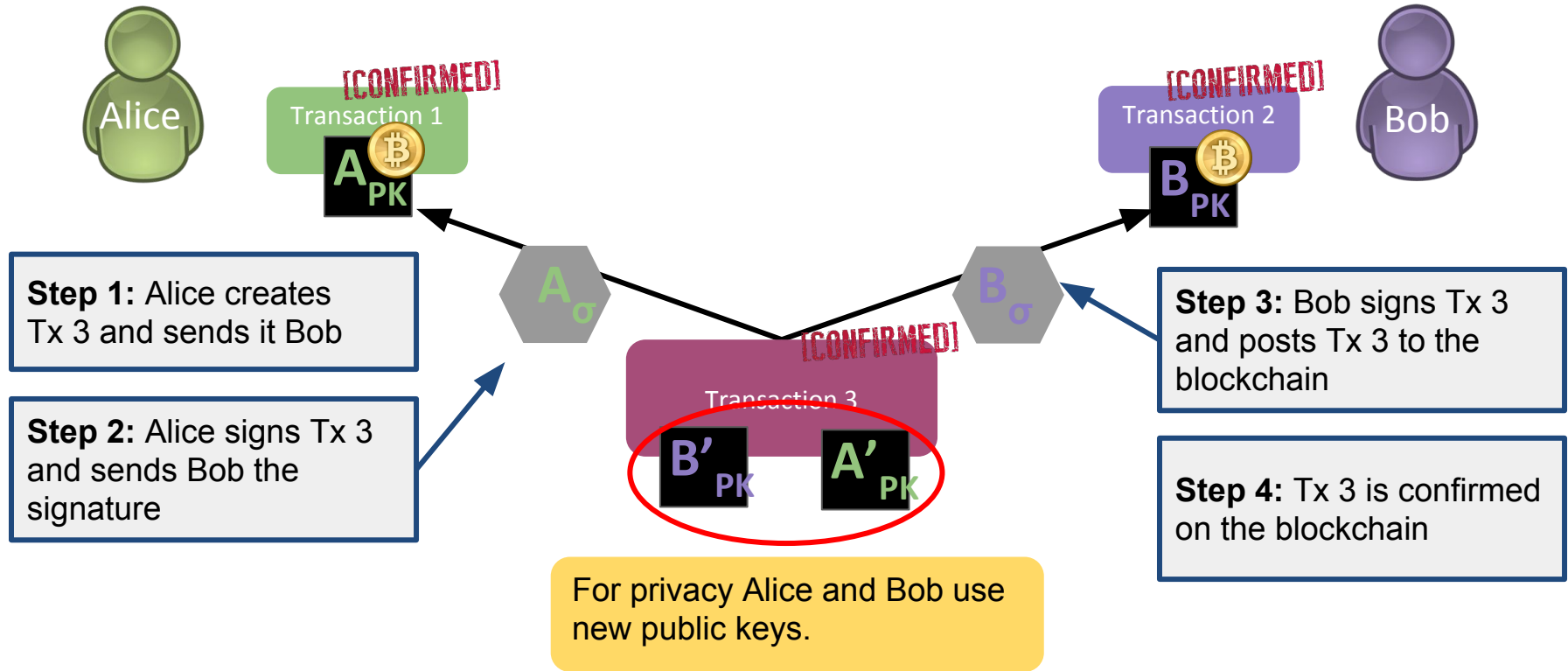
Full Tier-Nolan Atomic Trade Protocol

Litecoin's Blockchain

Alice's Refund unlocked

| Tx 1 | | | Tx 4 | | | Tx 5 |
| 200 | 201 | 202 | 203 | 204 | 205 | 206 |

Tx1 Spend Conditions:
1. Bob Sig & X
Or
2. Alice Sig & LTC-Height>205

Tx4: Bob sig & X

Tx5: Alice sig

Bitcoin's Blockchain

Bob's Refund unlocked

| | Tx 2 | Tx 3 | | | Tx 6 | |
| 300 | 301 | 302 | 303 | 304 | 305 | 306 |

Tx2 Spend Conditions:
1. Alice Sig & X
Or
2. Bob Sig & BTC-Height>304

Tx3: Alice sig & X

Tx6: Bob sig

Simple Two Party CoinJoin Protocol

Step 1: Alice creates Tx 3 and sends it Bob

Step 2: Alice signs Tx 3 and sends Bob the signature

Step 3: Bob signs Tx 3 and posts Tx 3 to the blockchain

Step 4: Tx 3 is confirmed on the blockchain

For privacy Alice and Bob use new public keys.

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

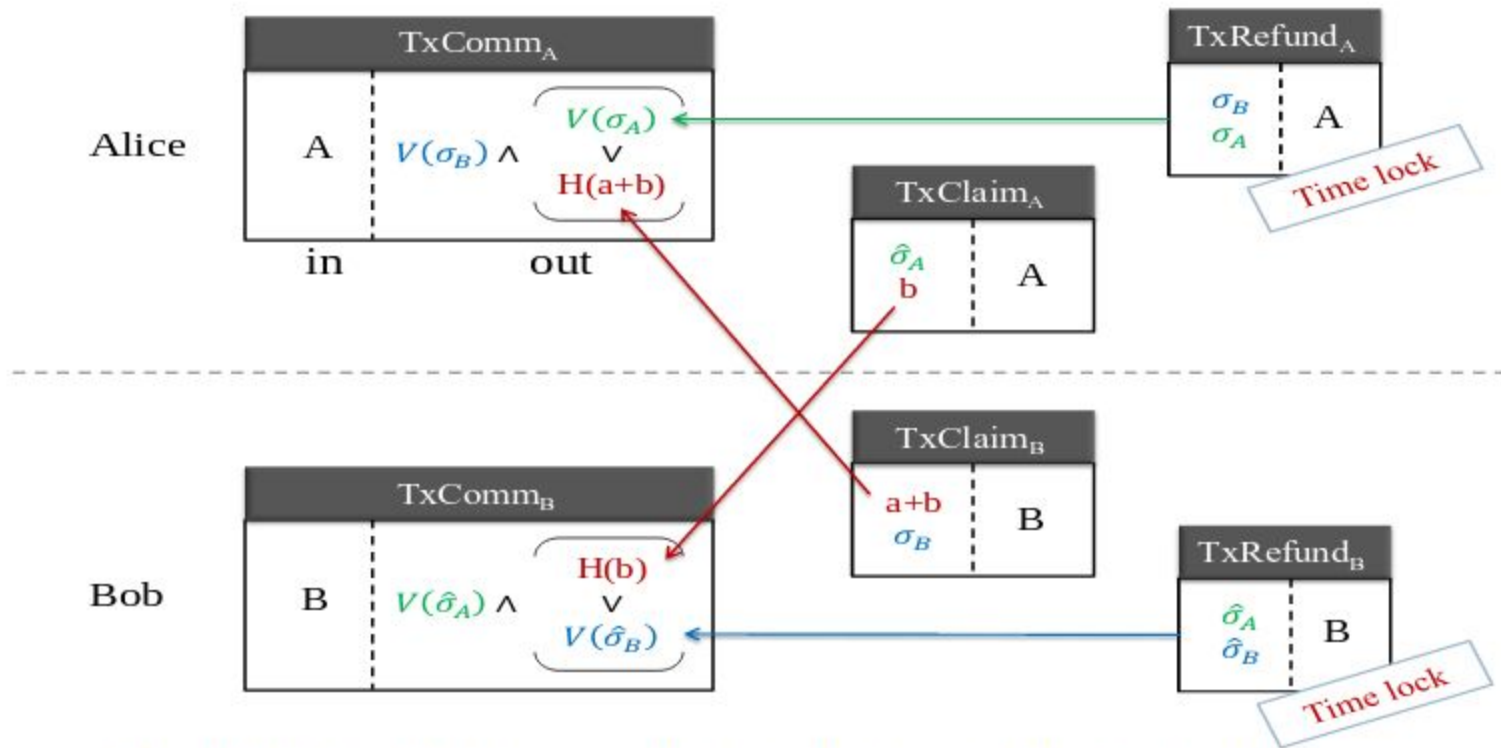# Barber Protocol
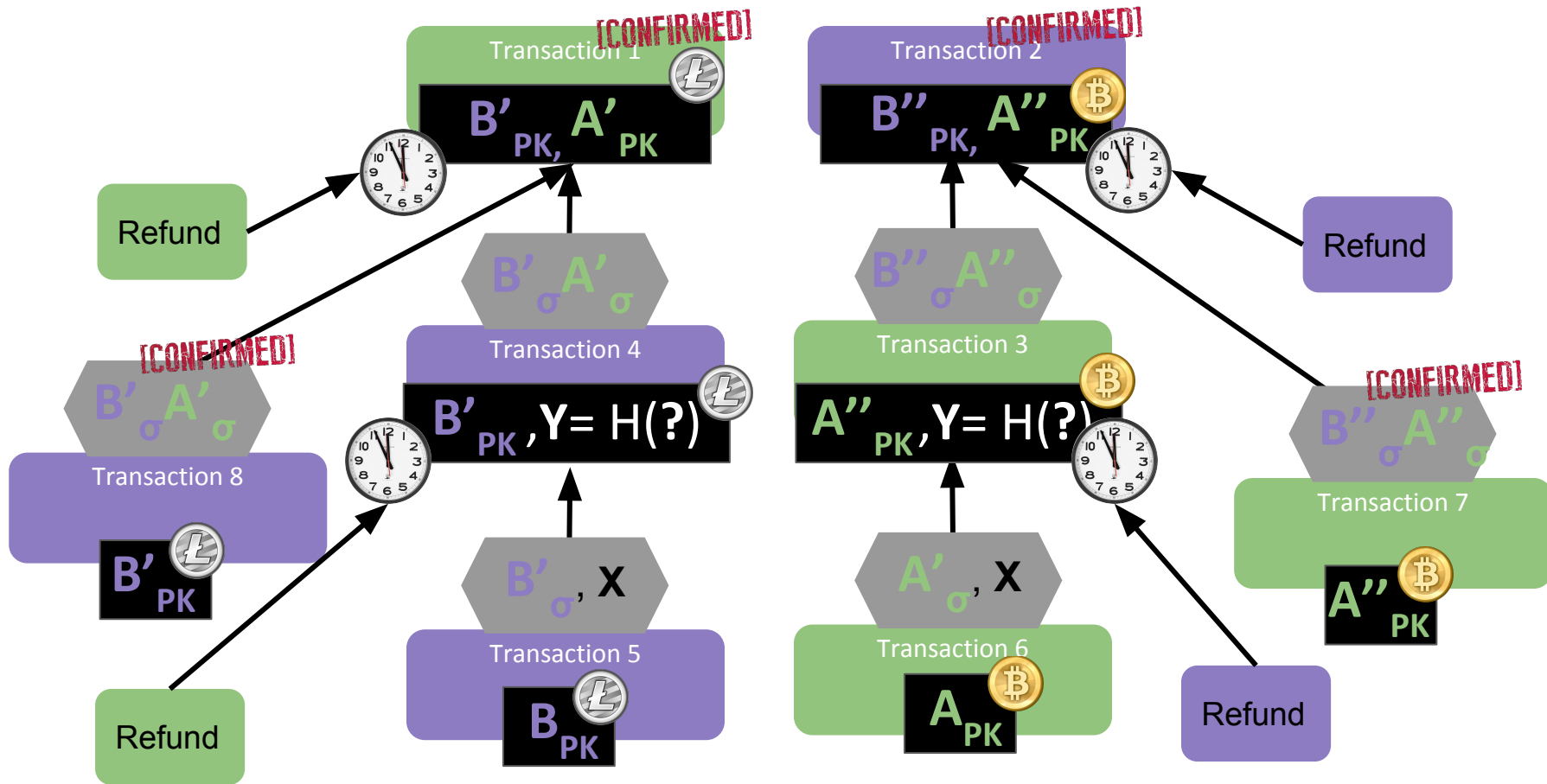
Barber et al's Fair-Exchange Protocol

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.