



What we do



What we do

A decentralized exchange.

What we do

A decentralized exchange.

Of centralized exchanges.

What we do

A decentralized exchange.

Of centralized exchanges.

On ⚡lightning⚡.

What we do

A decentralized exchange.

Of centralized exchanges. (Why? Liquidity.)

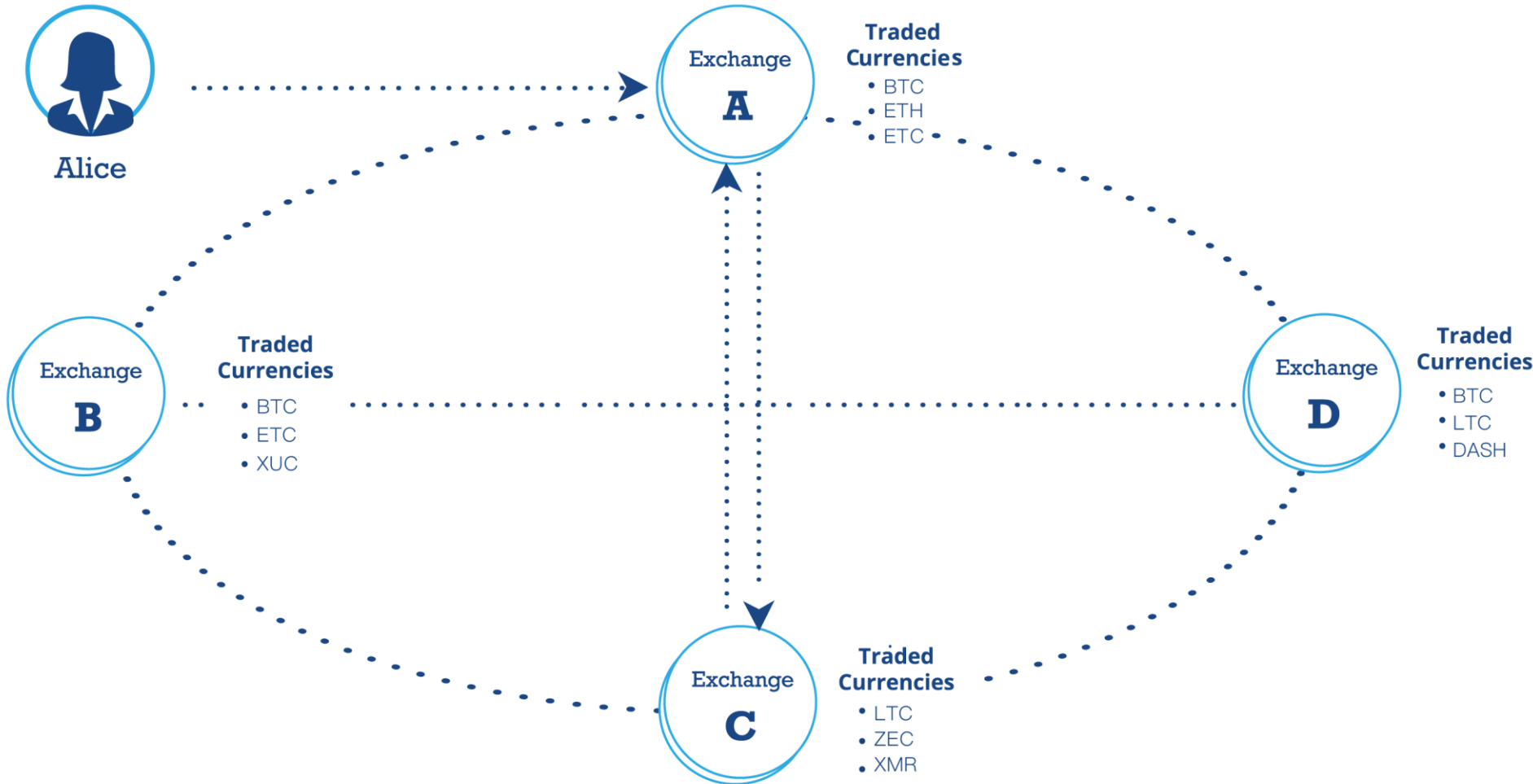
On ⚡lightning⚡.

Endgame

Individuals who run **XUD**, our open-source software, are part of the network and can trade with everyone else

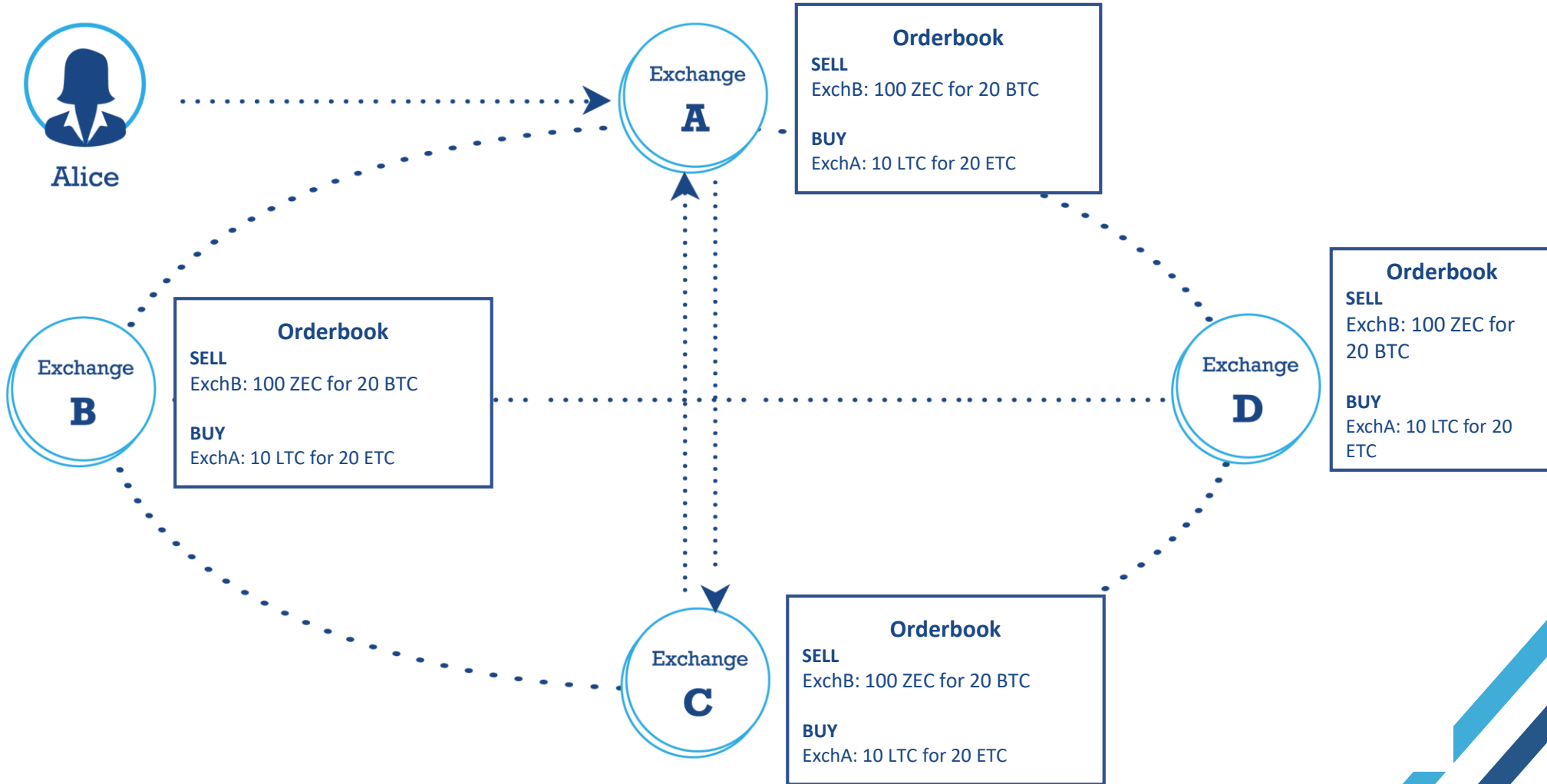
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



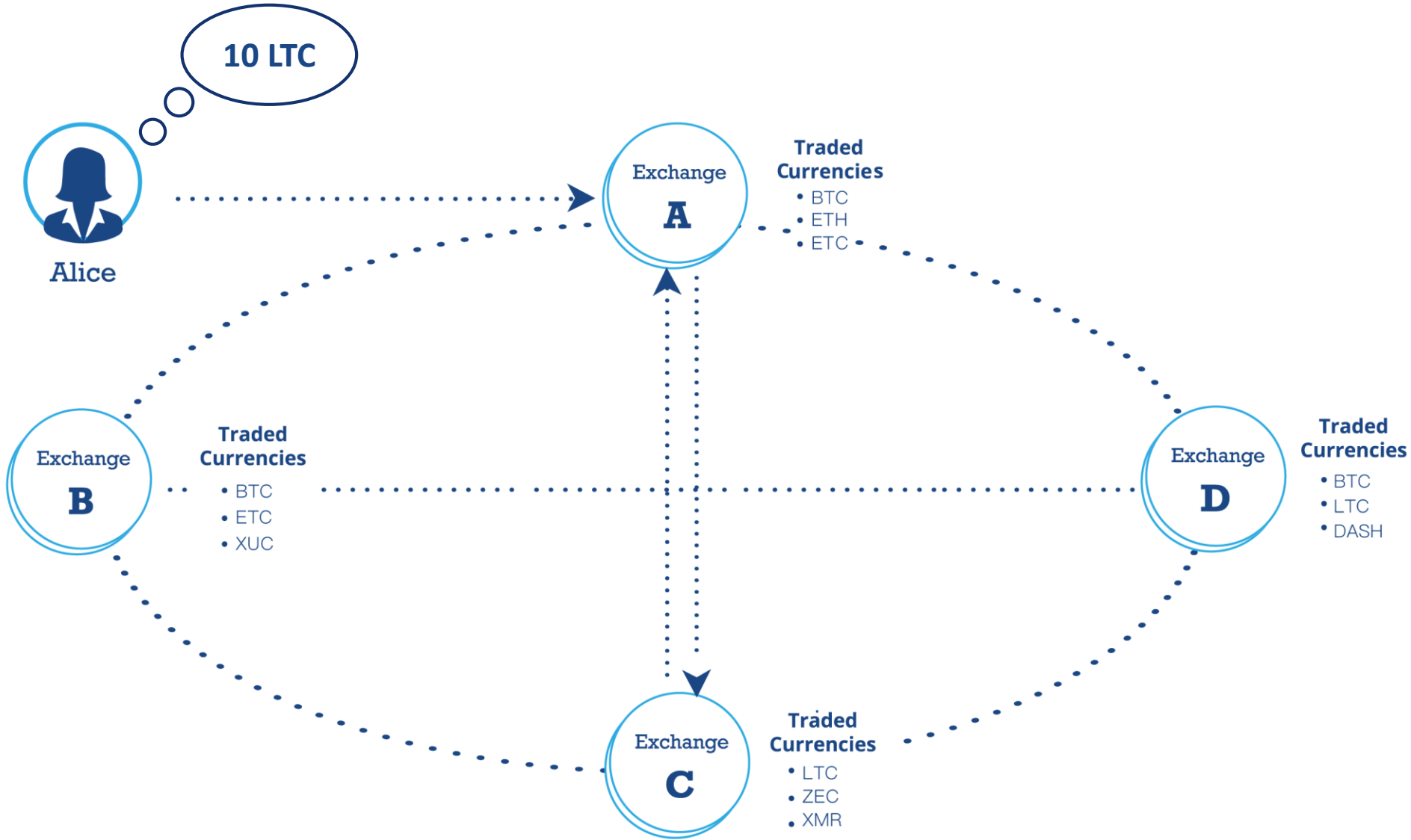
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



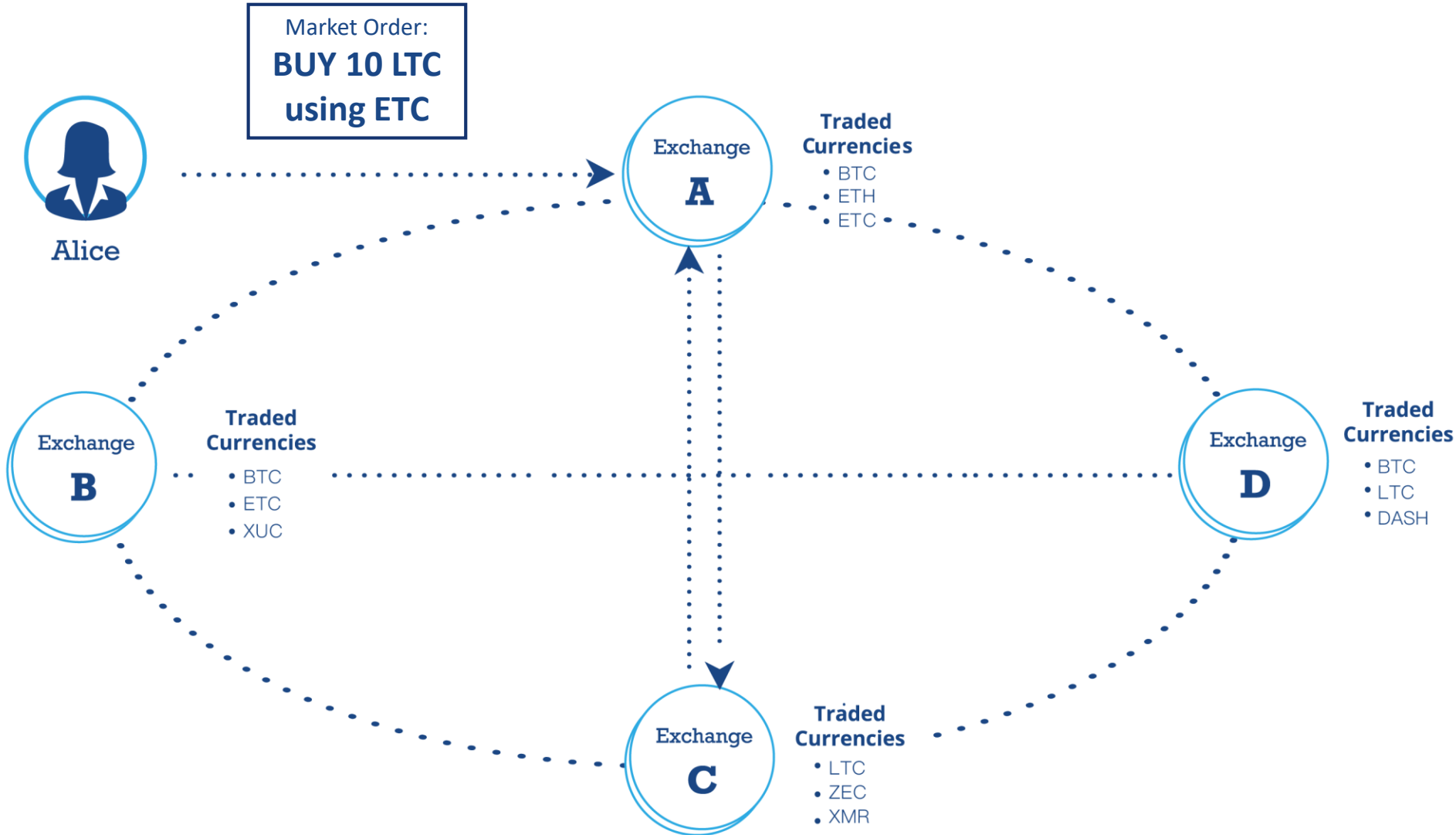
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



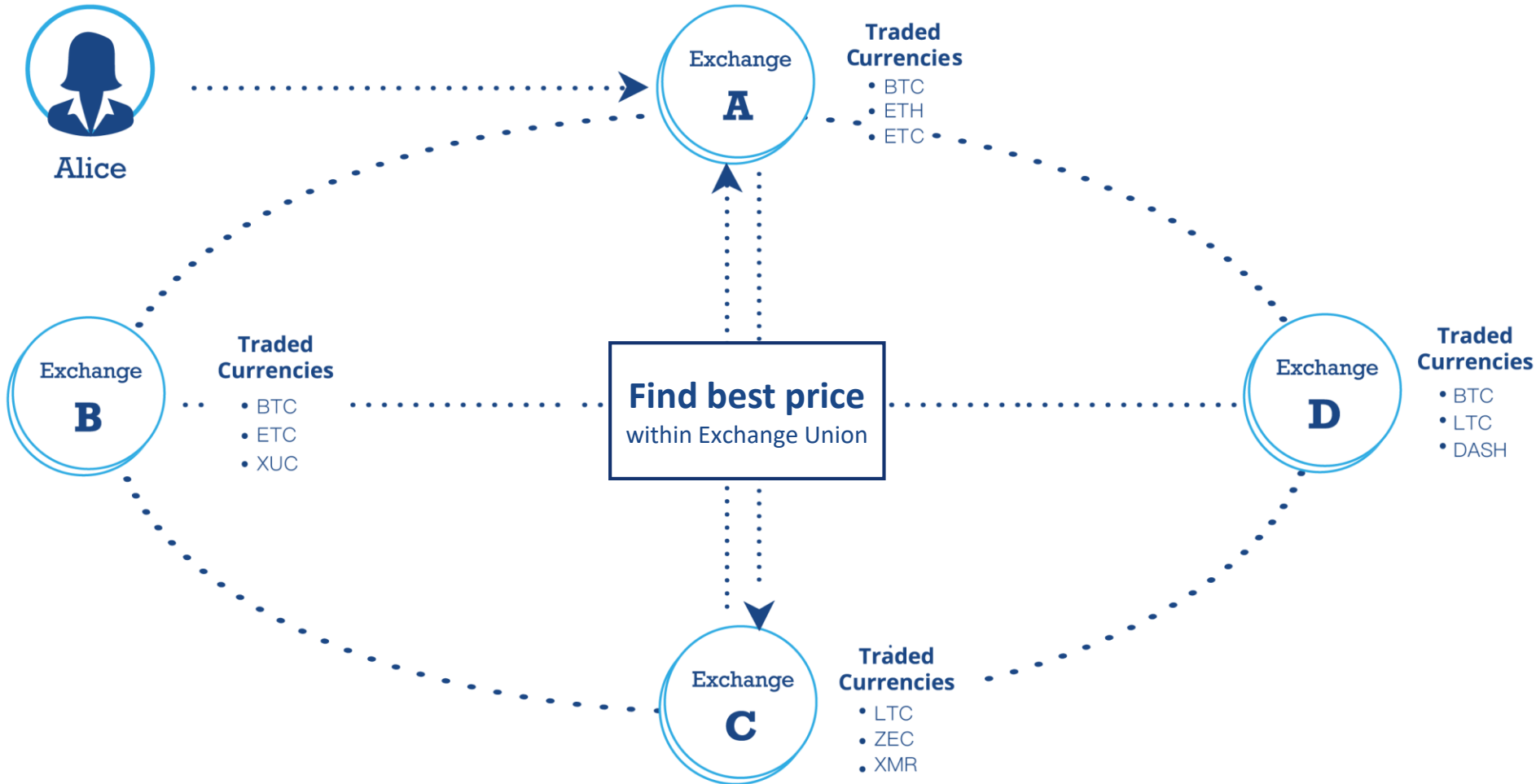
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



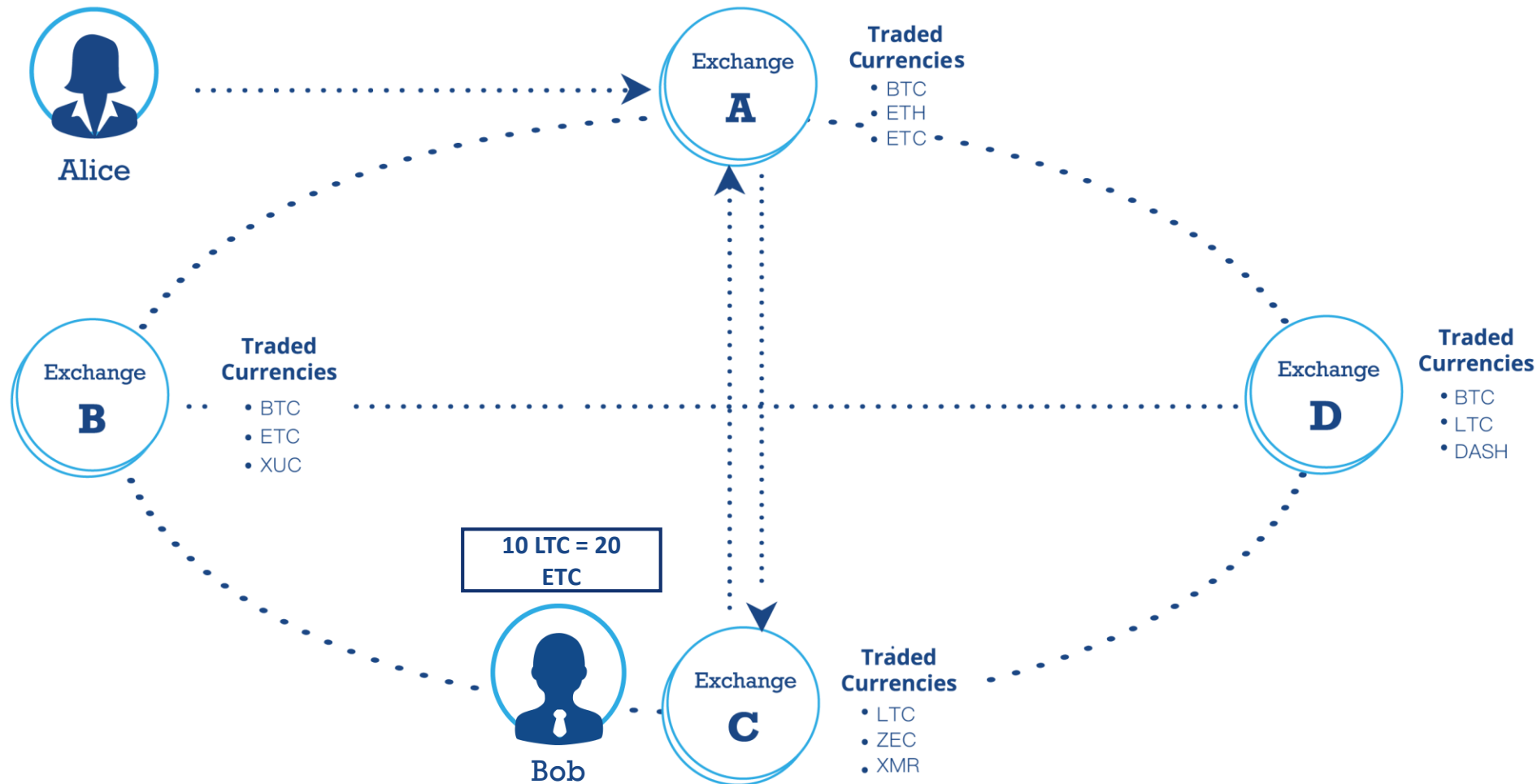
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



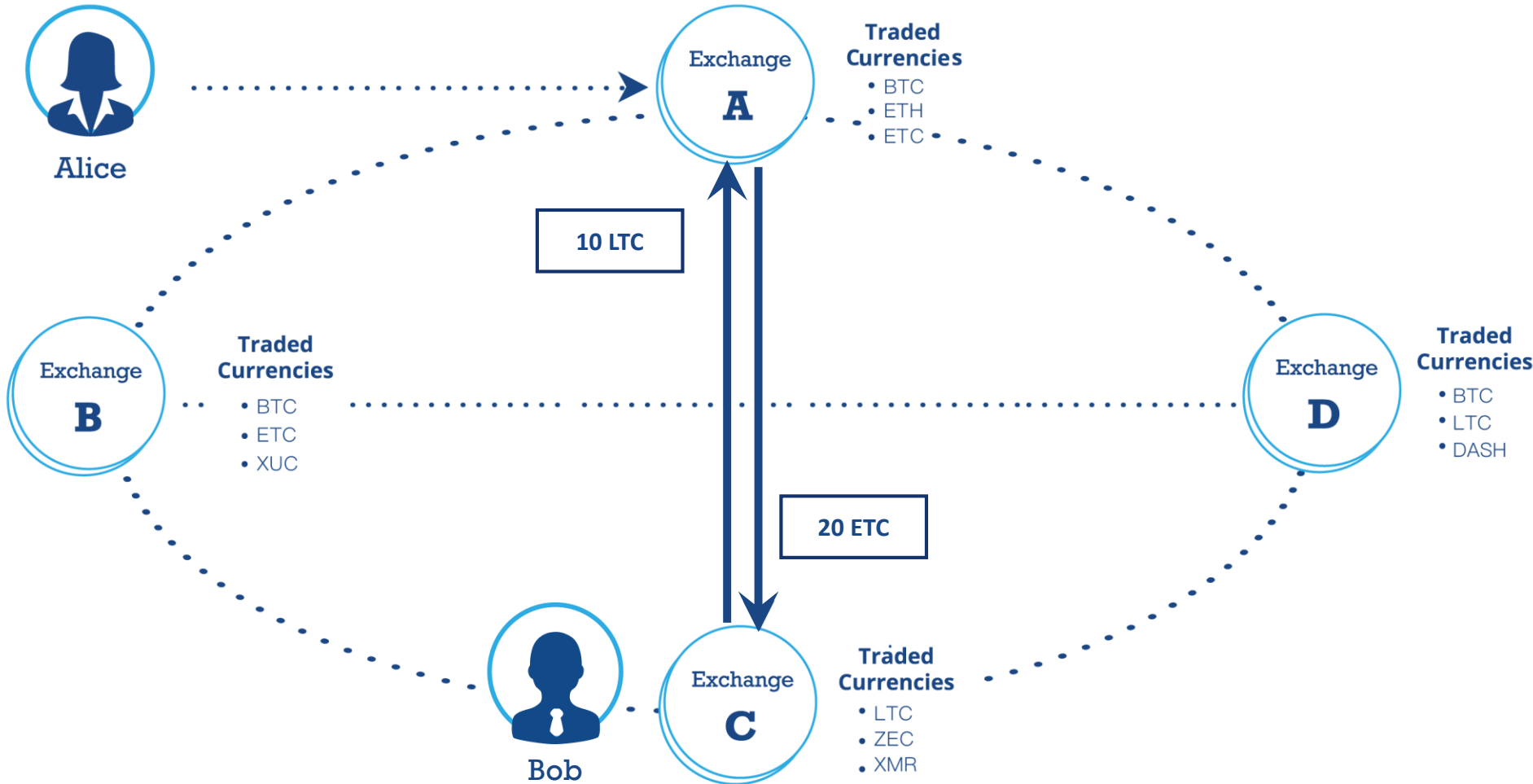
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



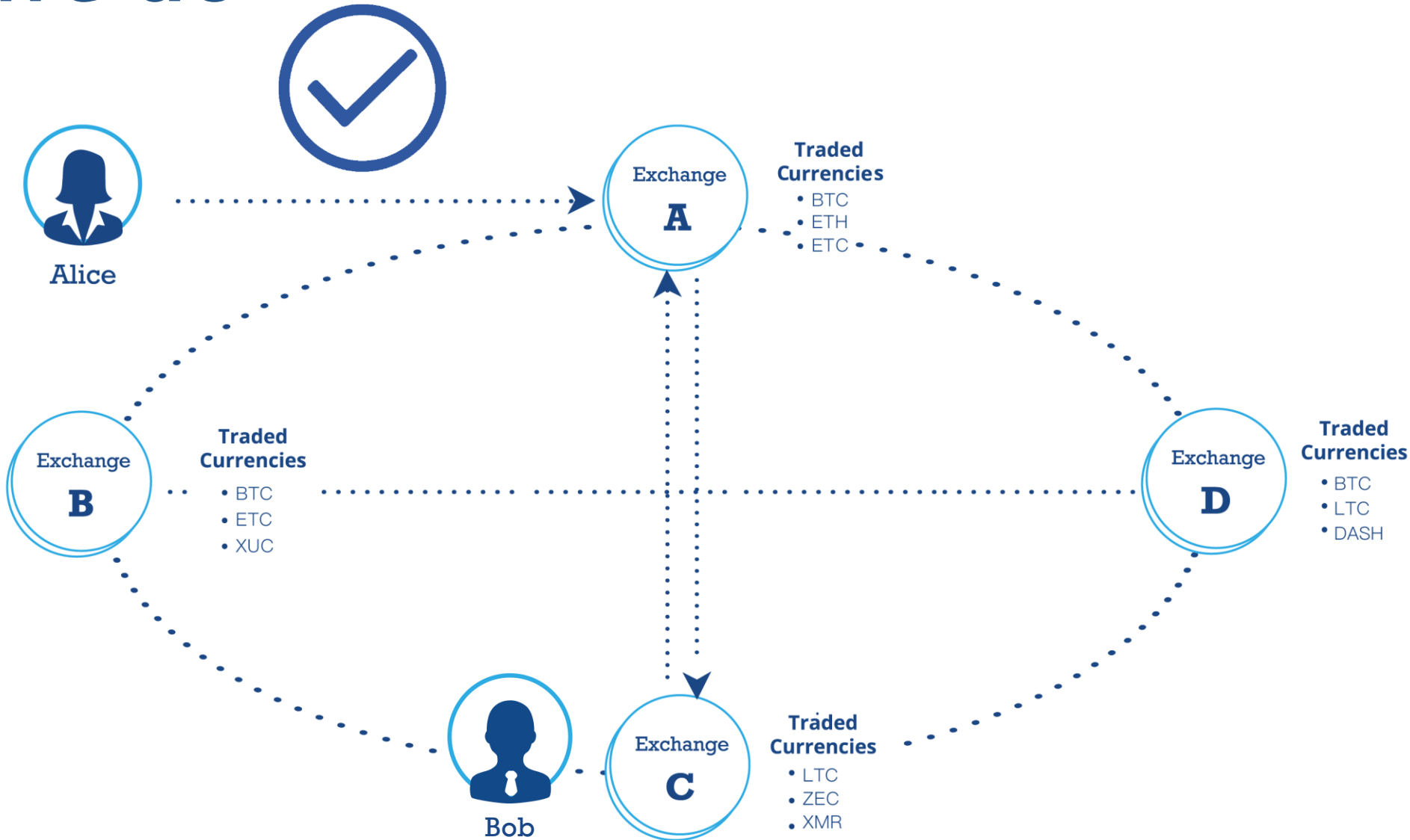
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



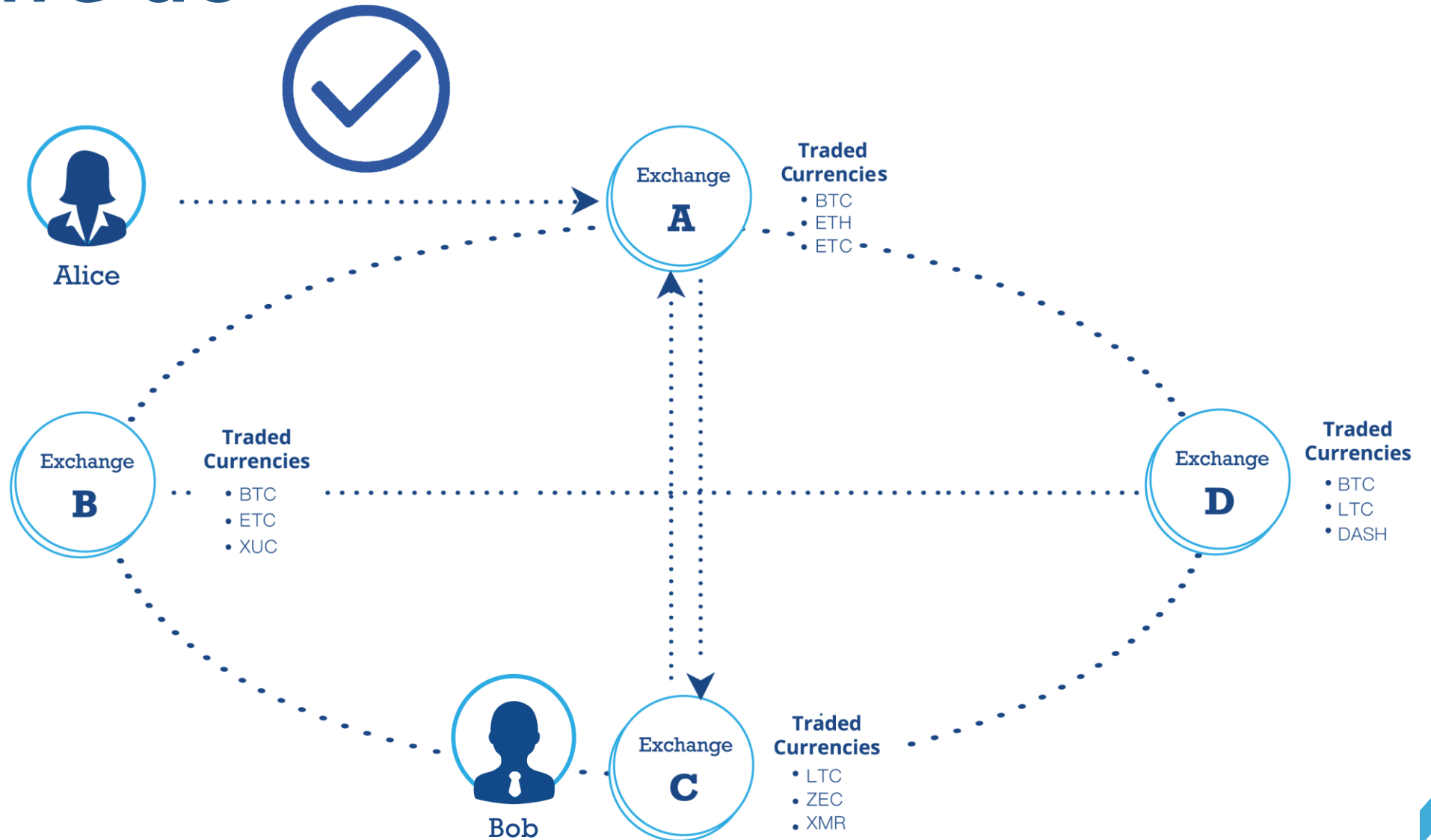
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



What we do

Portfolio		
	Before	After
BTC	2	2
LTC	0	10
ETC	100	80



Who benefits

Exchanges



Larger user base

Increased revenue & earnings

Increased liquidity



Users



Tighter spreads

Best market price

More trading pairs

One UI

How we do

3 Key Technologies



1. Payment Channels

Each trade transfers real digital assets *instantly* between exchanges



2. Atomic Swaps

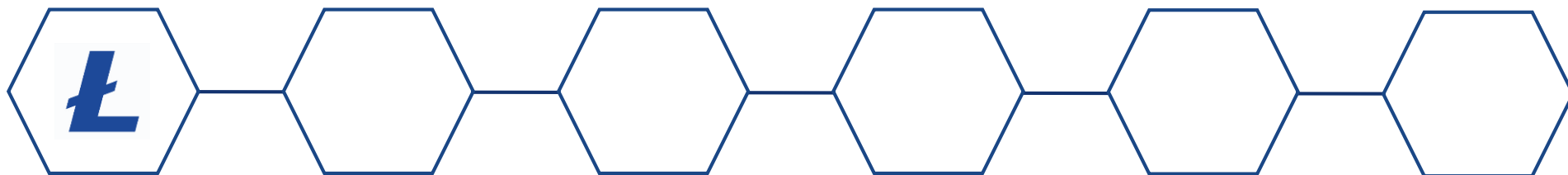
Trustless trades directly between two exchanges



3. Decentralized Orderbooks

Solving the pain points of digital asset exchanges – *connecting buyer & seller*

Status Quo



Status Quo



Payment Channels

Payment Channels

Yes, we are talking about Lightning & Raiden!

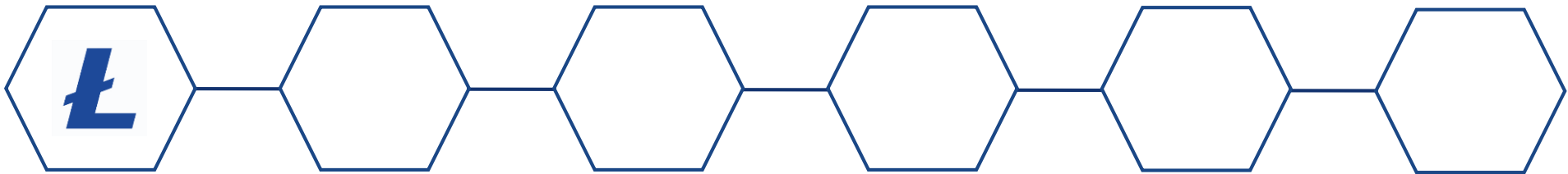
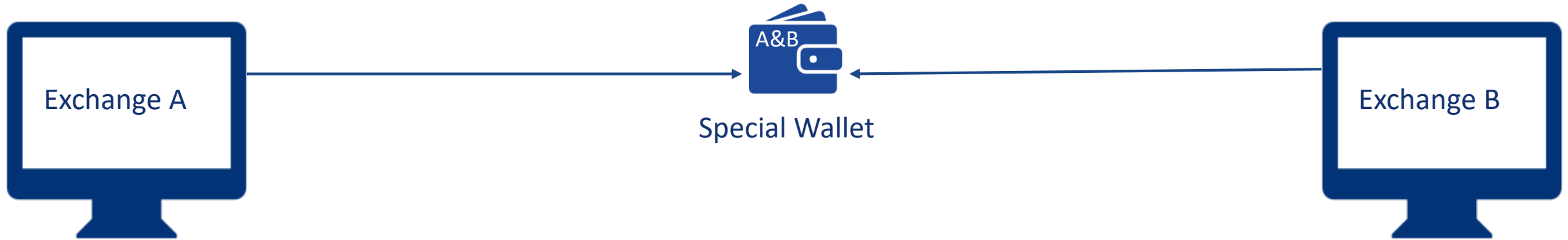
Payment Channels

Old idea, obviously Satoshi already came up with the basics:

*One use of nLockTime is **high frequency trades** between a set of parties. They can **keep updating a tx** by unanimous agreement. The party giving money would be the first to sign the next version. If one party stops agreeing to changes, then the last state will be recorded at nLockTime.*

Payment Channels

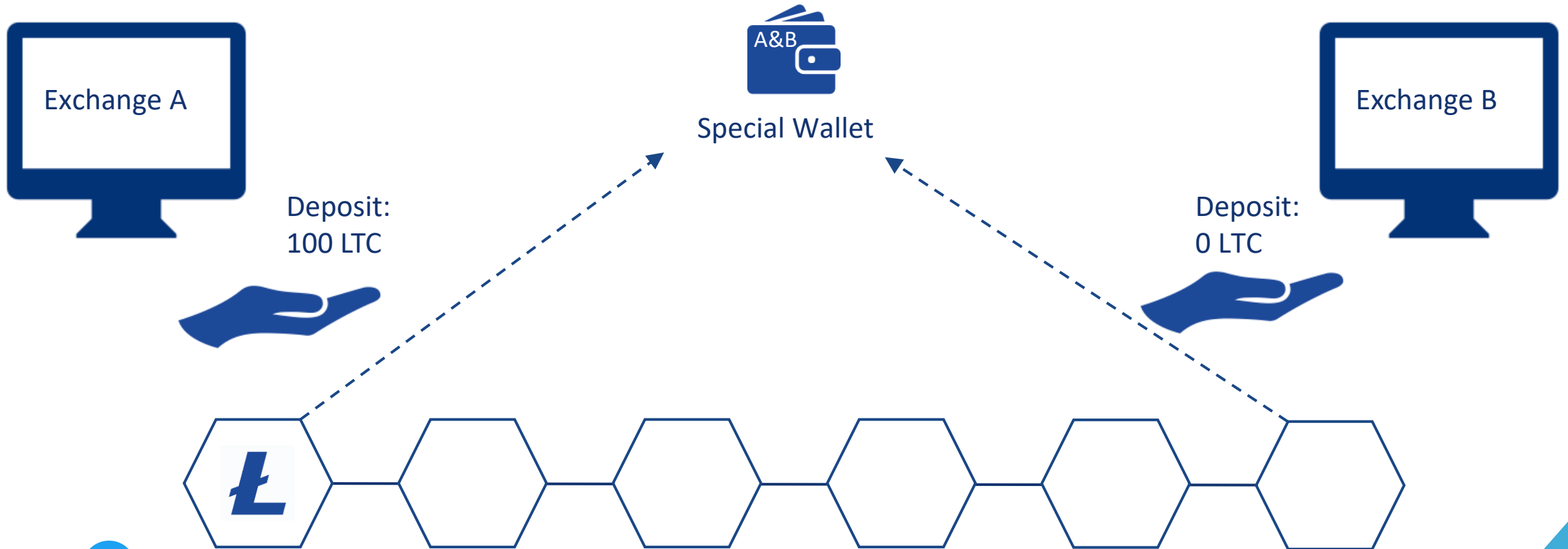
High-level:



@kilrau

Payment Channels

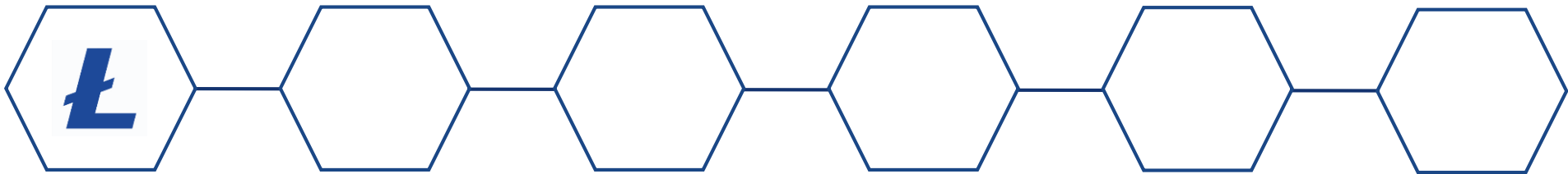
High-level:



@kilrau

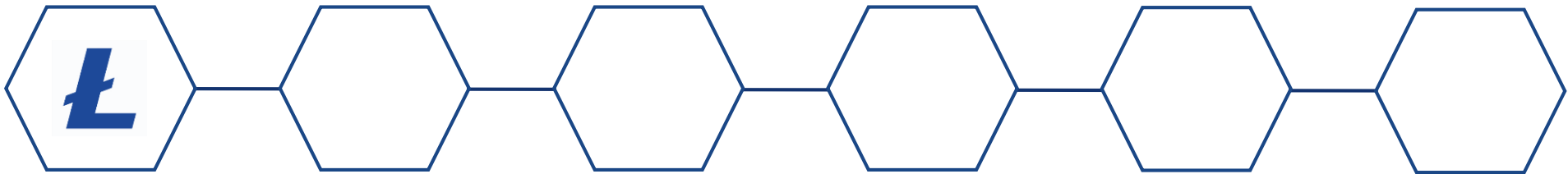
Payment Channels

High-level:

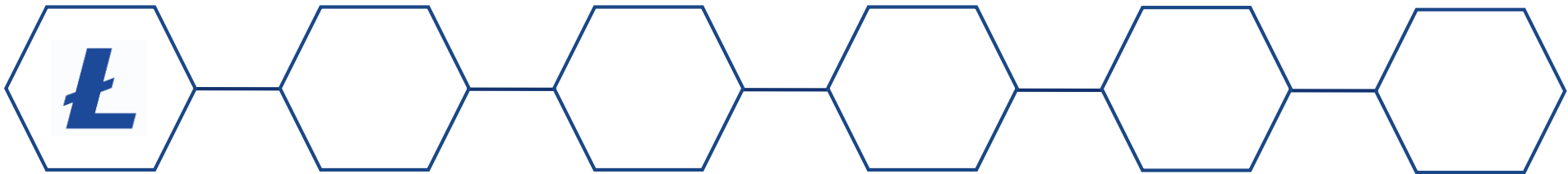


@kilrau

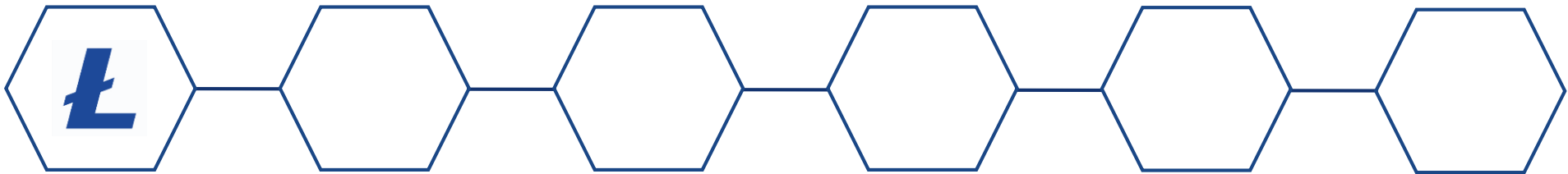
Payment Channels



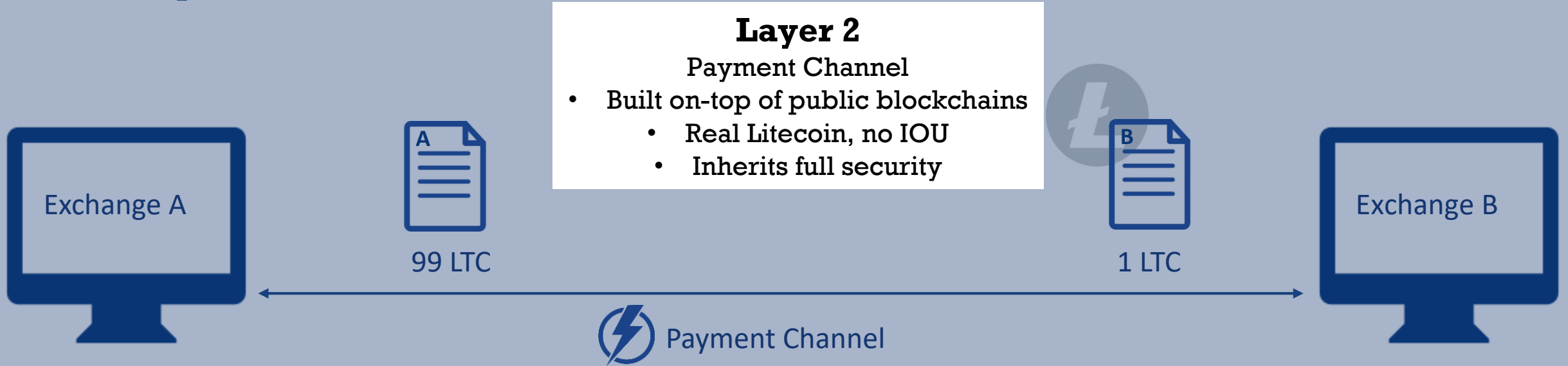
Payment Channels



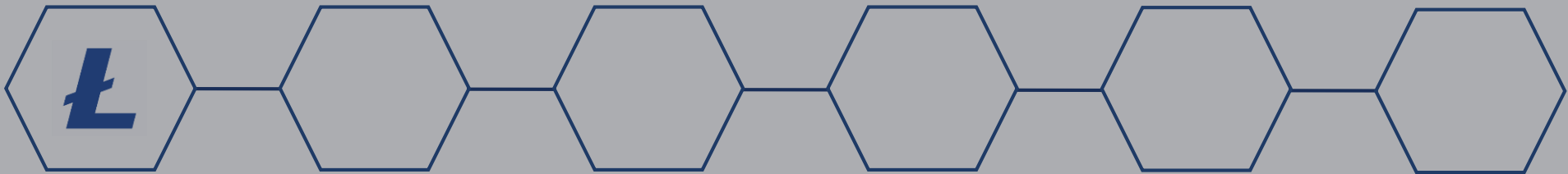
Payment Channels



Payment Channels

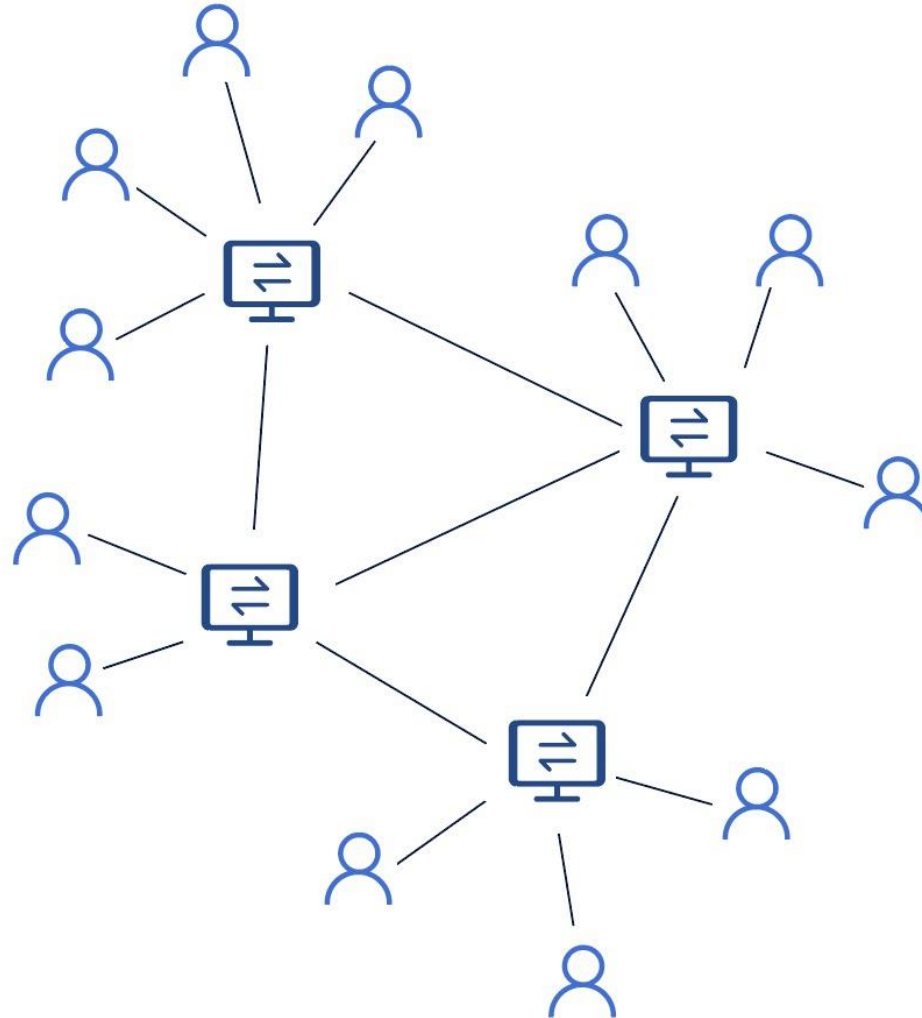


Layer 1
Underlying public blockchain =
dispute mediation system



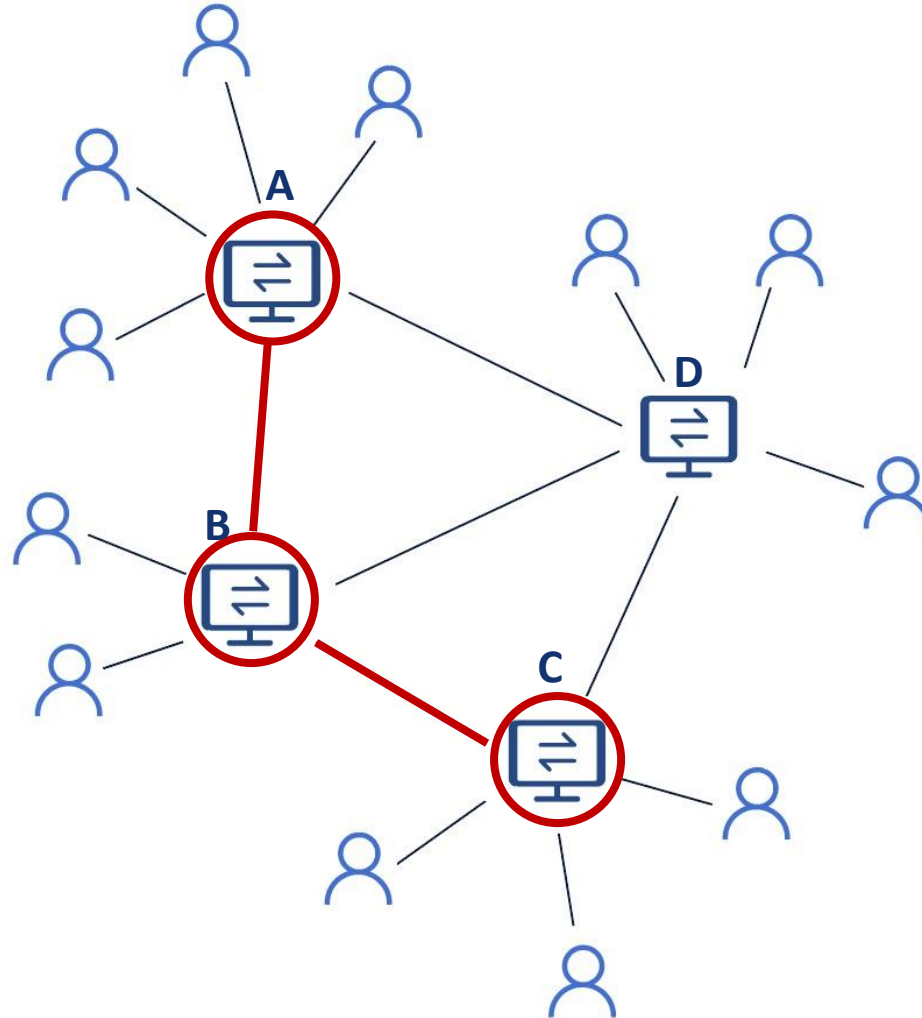
Payment Channels

Routing:

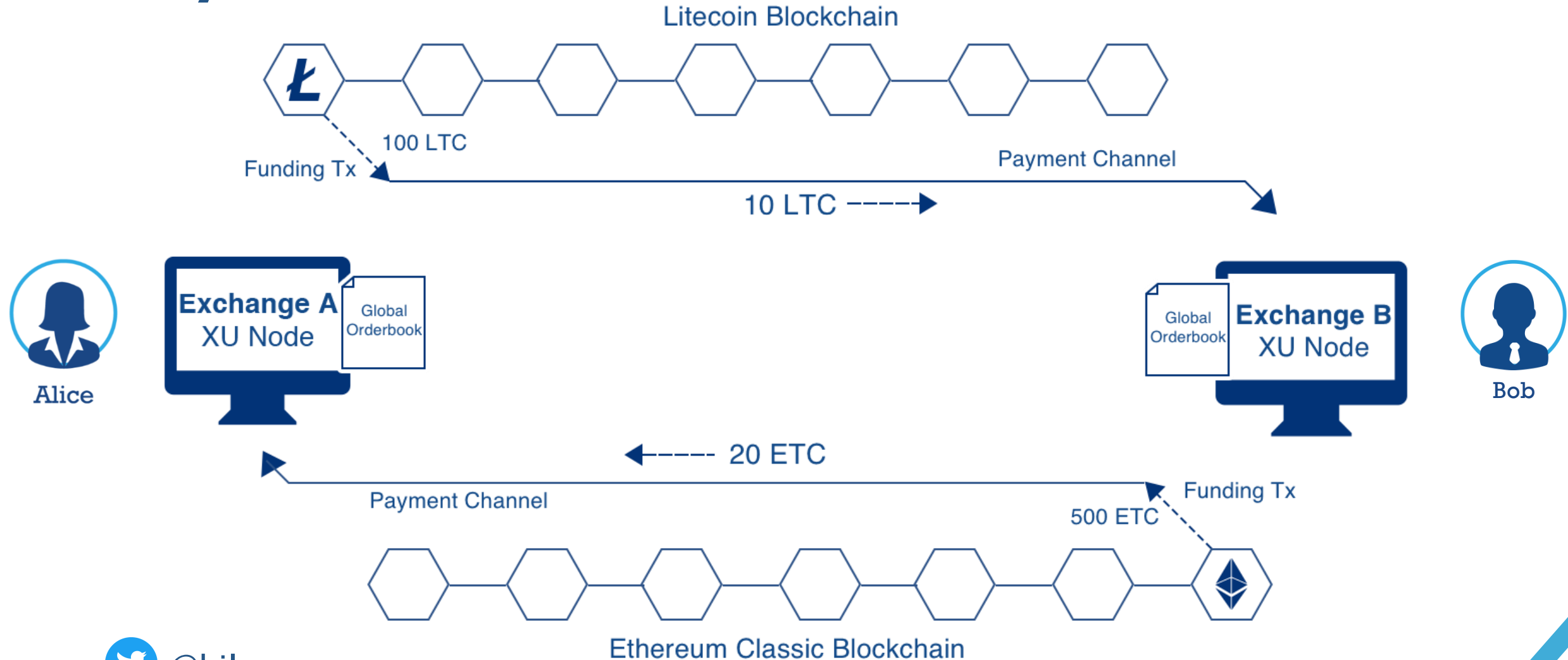


Payment Channels

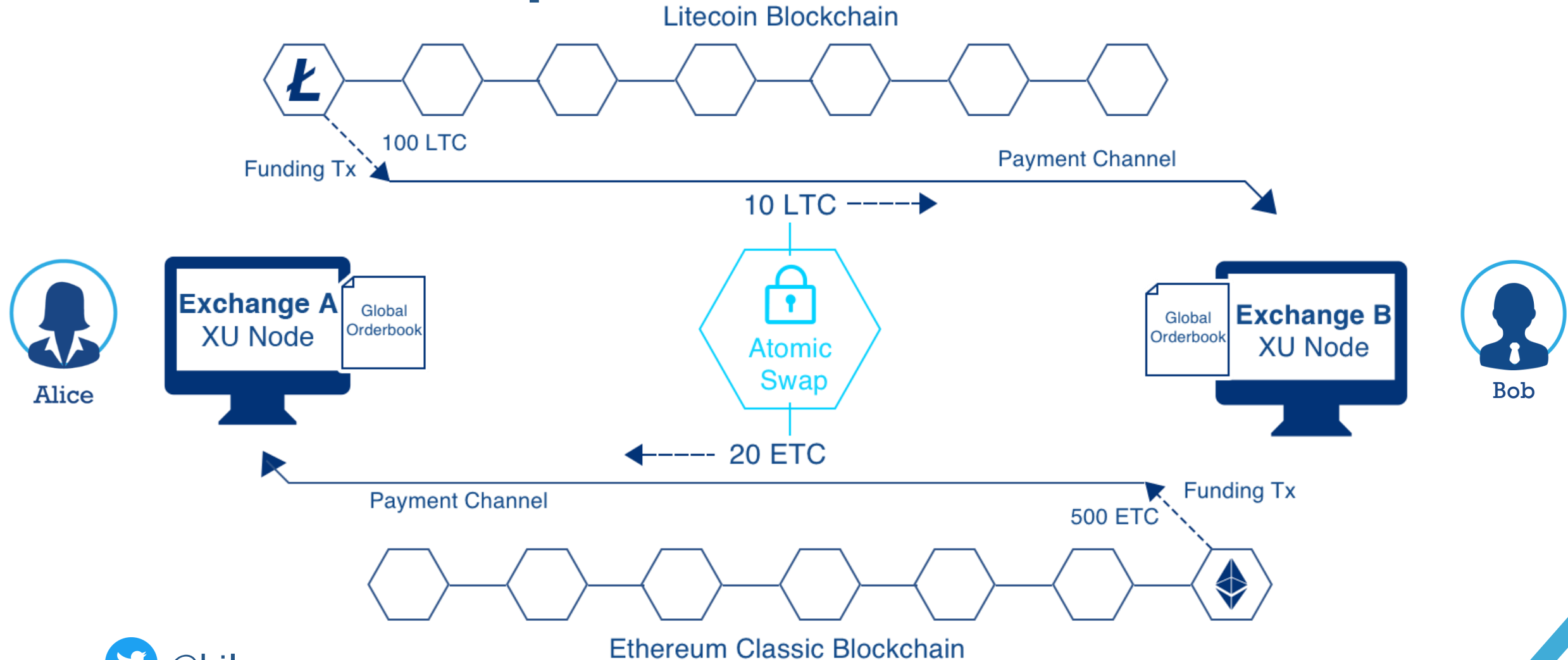
Routing:



Payment Channels



Atomic Swaps



Atomic Swaps

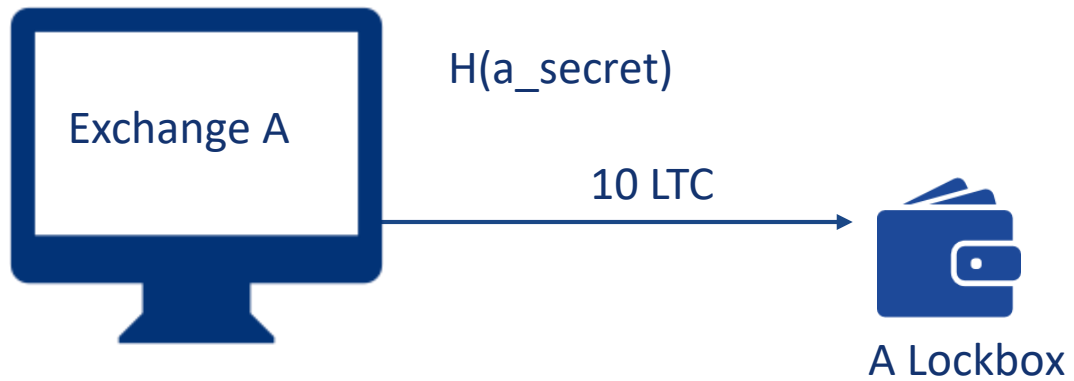
- ◆ Trustless exchange of two different assets
 - ◆ No middleman/escrow service needed
- ◆ How: guarantee atomicity
 - ◆ Both sides of the trade happen or not at all
 - ◆ Technology: Hashed TimeLock Contracts (HTLCs)



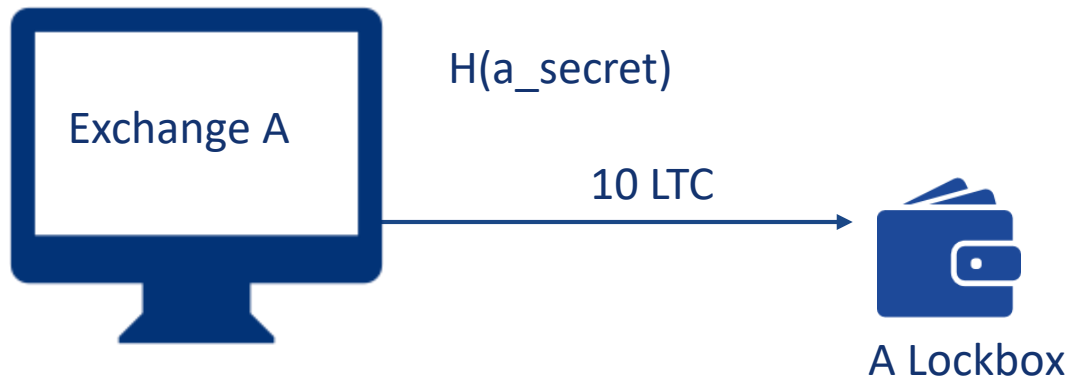
Atomic Swaps



Atomic Swaps

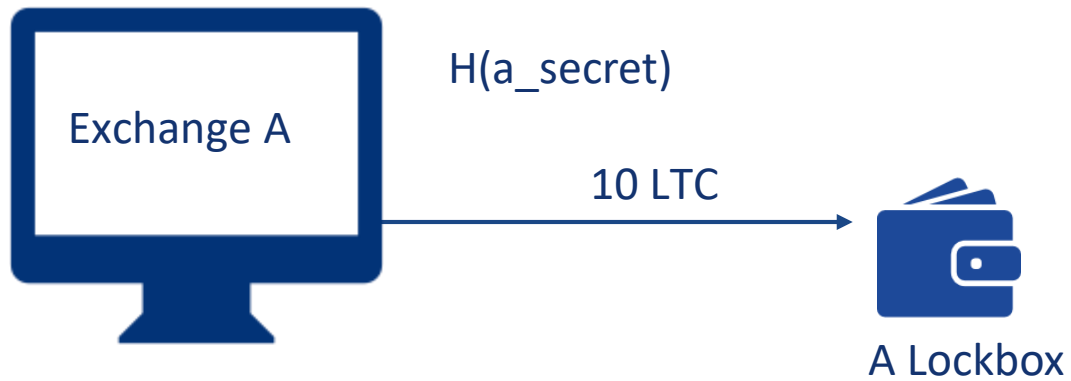


Atomic Swaps



Lockbox only opens with 'a_secret' + B's signature

Atomic Swaps



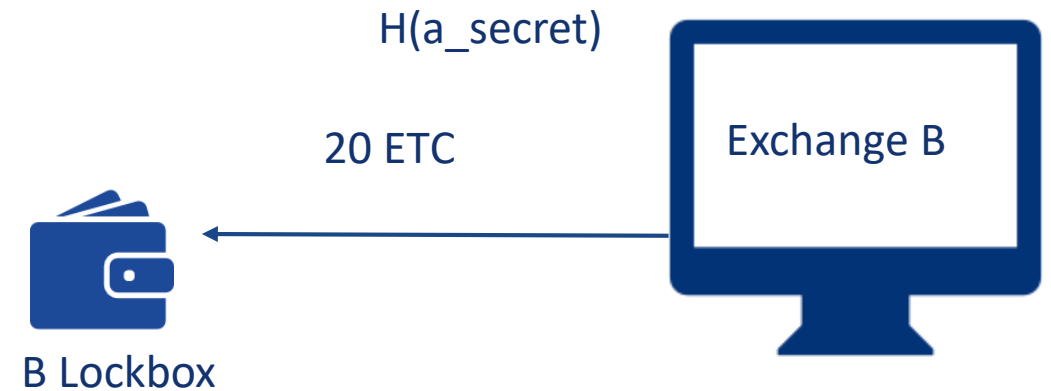
Lockbox only opens with 'a_secret' + B's signature

HashLock

Atomic Swaps



Lockbox only opens with '**a_secret**' + B's signature



Lockbox only opens with '**a_secret**' + A's signature

Atomic Swaps



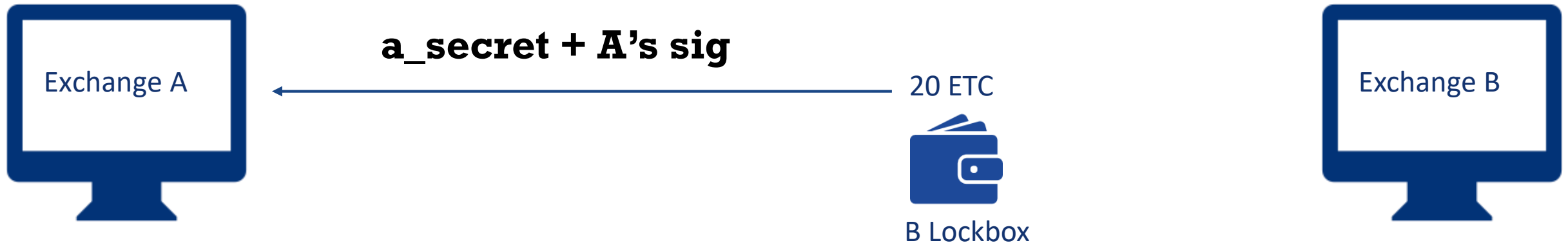
Lockbox only opens with '**a_secret**' + B's signature

Lockbox only opens with '**a_secret**' + A's signature

Both lockboxes need the **same "a_secret"** to be opened!

Atomic Swaps

If now A wants to open B's lockbox it has to reveal it's a_secret on the payment channel



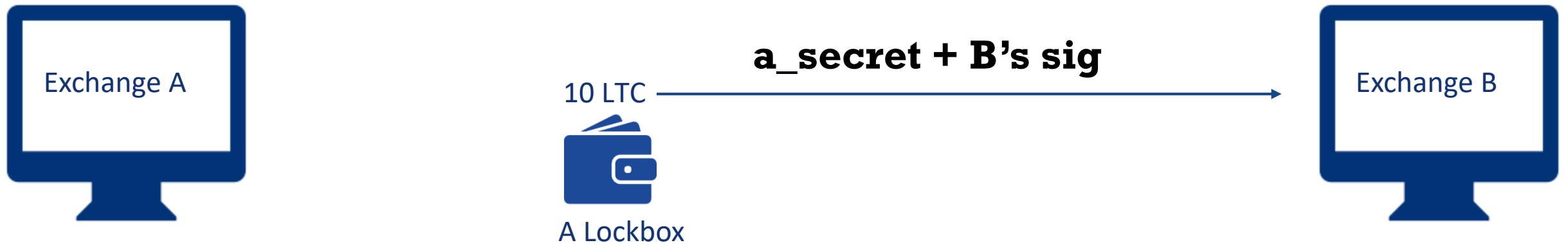
Atomic Swaps



a_secret



Atomic Swaps



Atomic Swaps



20 ETC



10 LTC



Atomic Swaps



TimeLock:

If something goes wrong, 10 LTC go back to A and 20 ETC back to B after certain time interval

Atomic Swaps



TimeLock:

If something goes wrong, 10 LTC go back to A and 20 ETC back to B after certain time interval

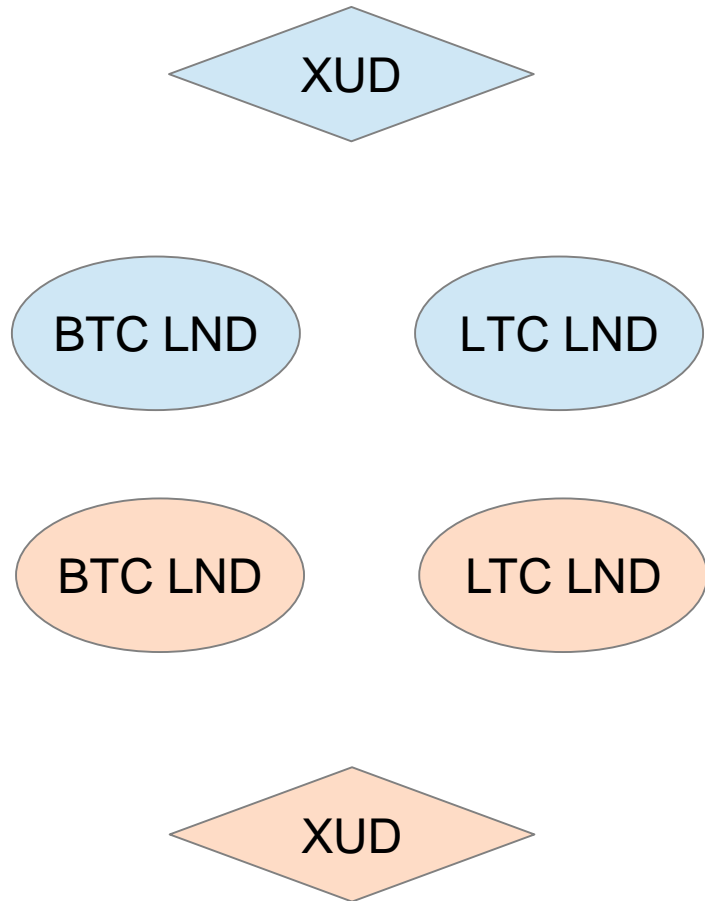
Hashed TimeLock Contracts

Via BIP199 on Bitcoin and SmartContracts on Ethereum

How XUD handles Atomic Swaps

Goal: minimal changes to LND,
make it part of official LND master

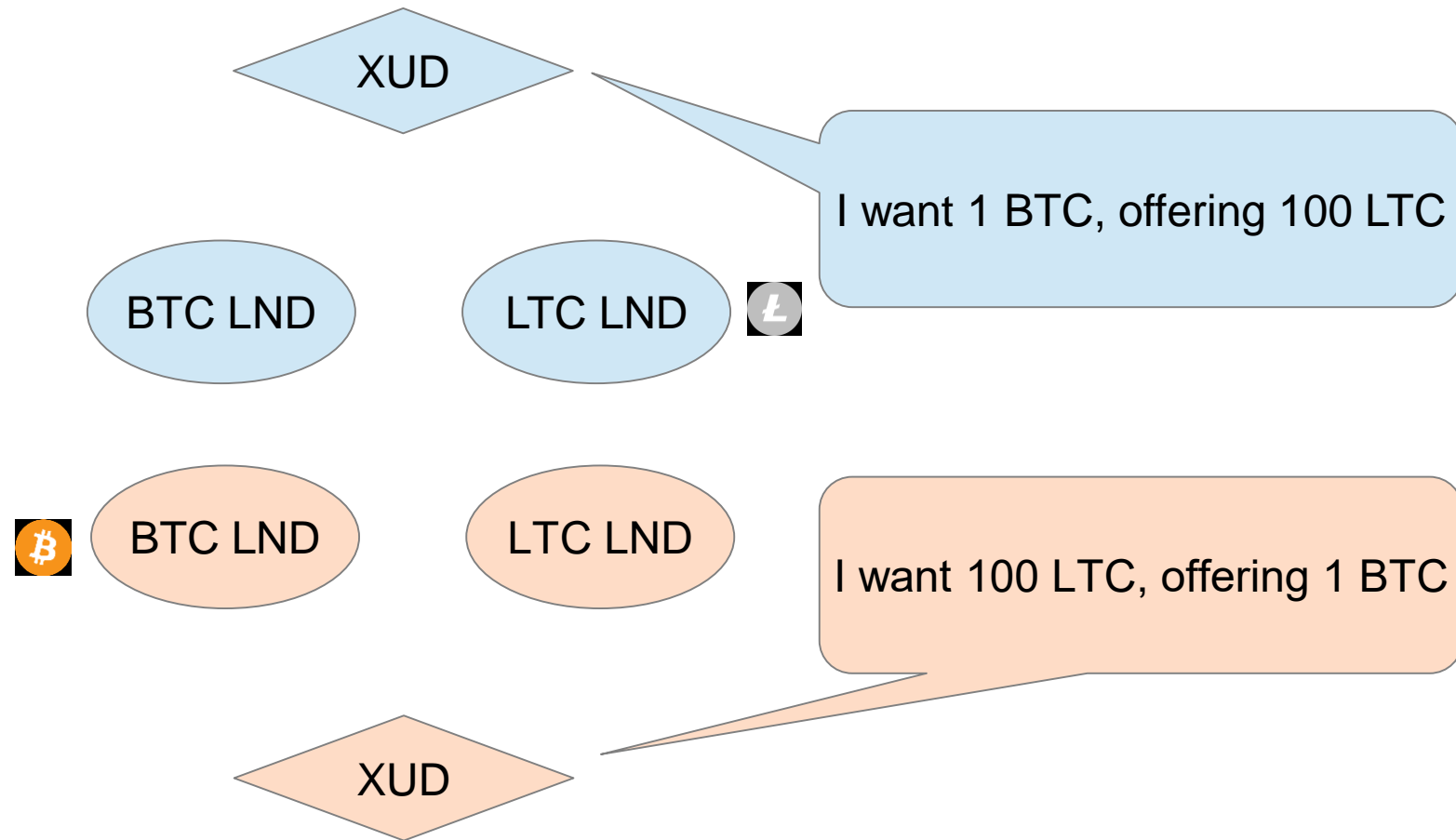
How XUD handles Atomic Swaps



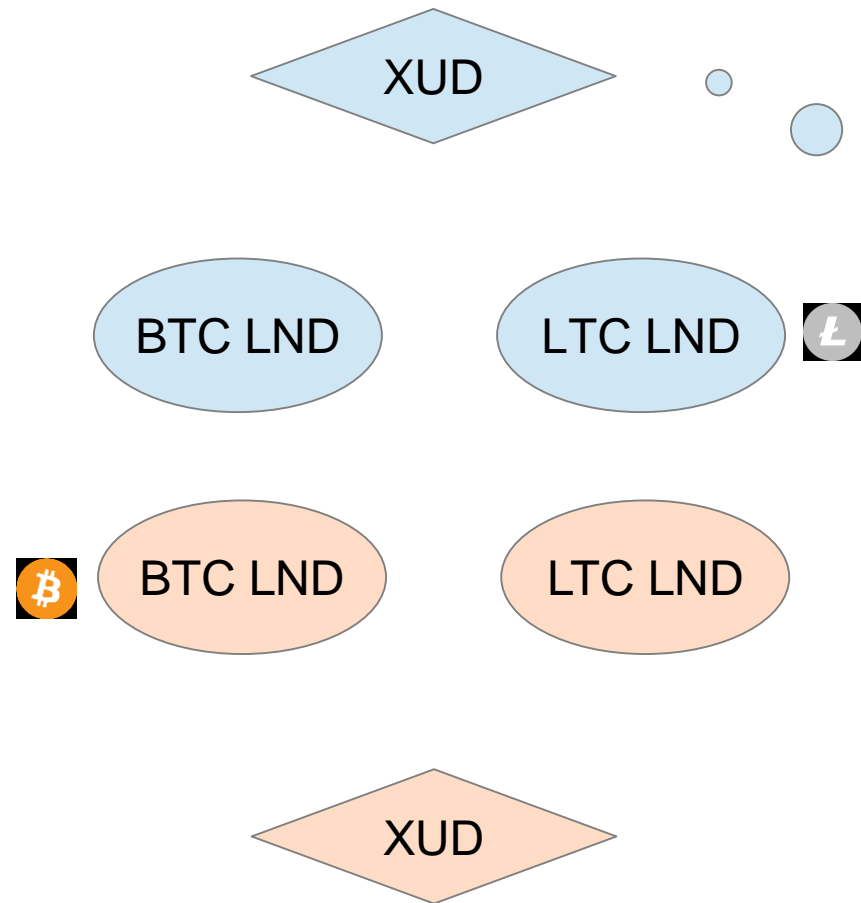
The Setup

- Two XUDs that each manage two LND clients, one on BTC and one on LTC.
- LNDs configured to query XUD when they are recipients of a payment with an unknown hash/preimage.
- Routes with sufficient capacity exist between the BTC LND nodes and the LTC LND nodes.
- XUDs are aware of each others' LND pub keys and can communicate with each other.

How XUD handles Atomic Swaps



XUD, The Software

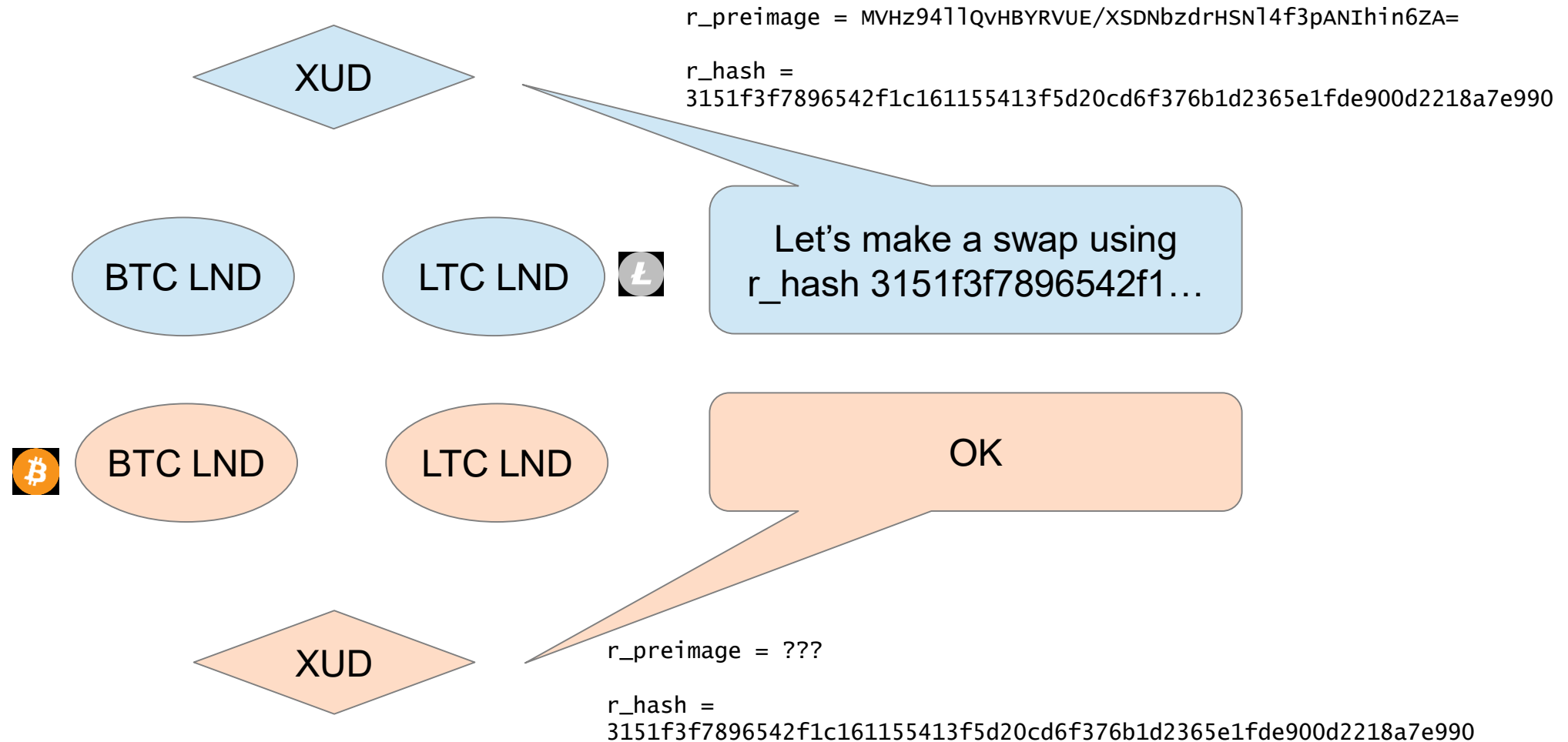


```
r_preimage = MVHz941lQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=
```

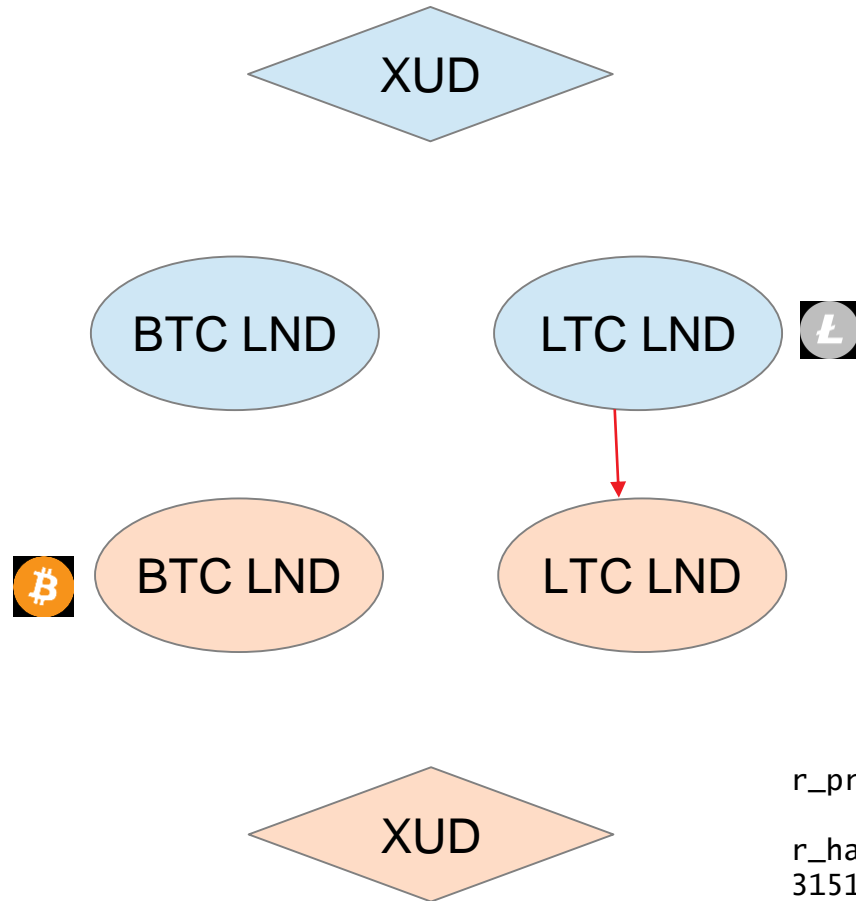
```
r_hash =  
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

I'll initiate the swap by creating
a preimage and hashing it...

XUD, The Software



XUD, The Software



`r_preimage = MVHz941lQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=`

`r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990`

Pending HTLC

amount - 100 LTC

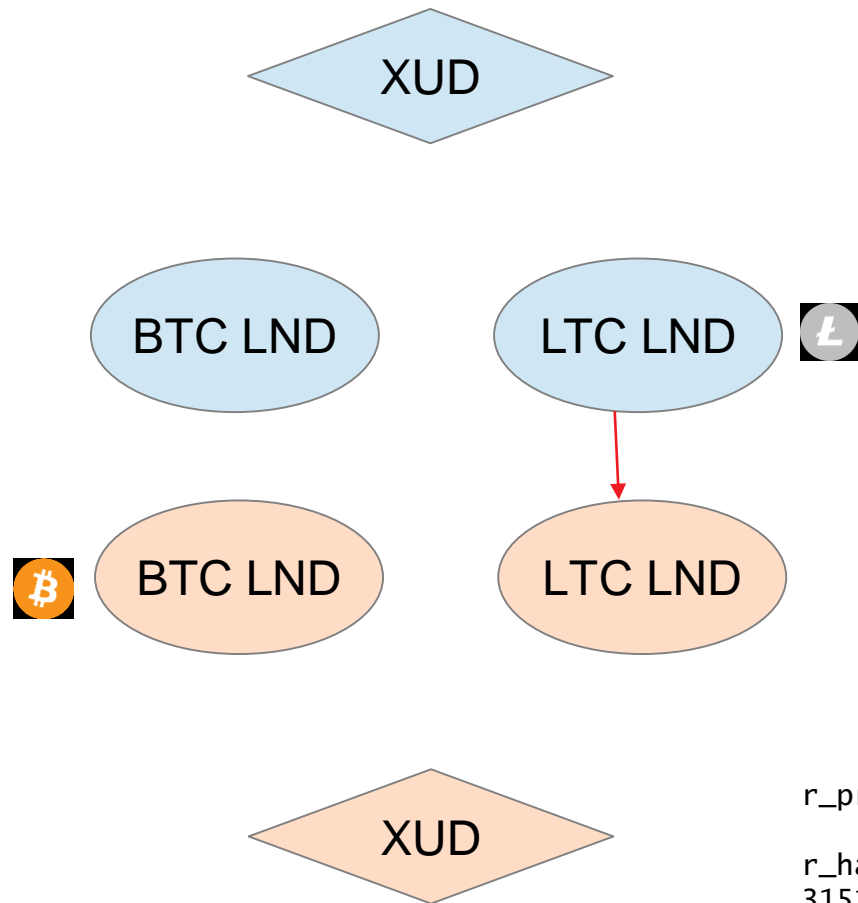
`r_hash - 3151f3f7896542f1...`

Note: This payment can route through any number of intermediary nodes on the LTC lightning network

`r_preimage = ???`

`r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990`

XUD, The Software



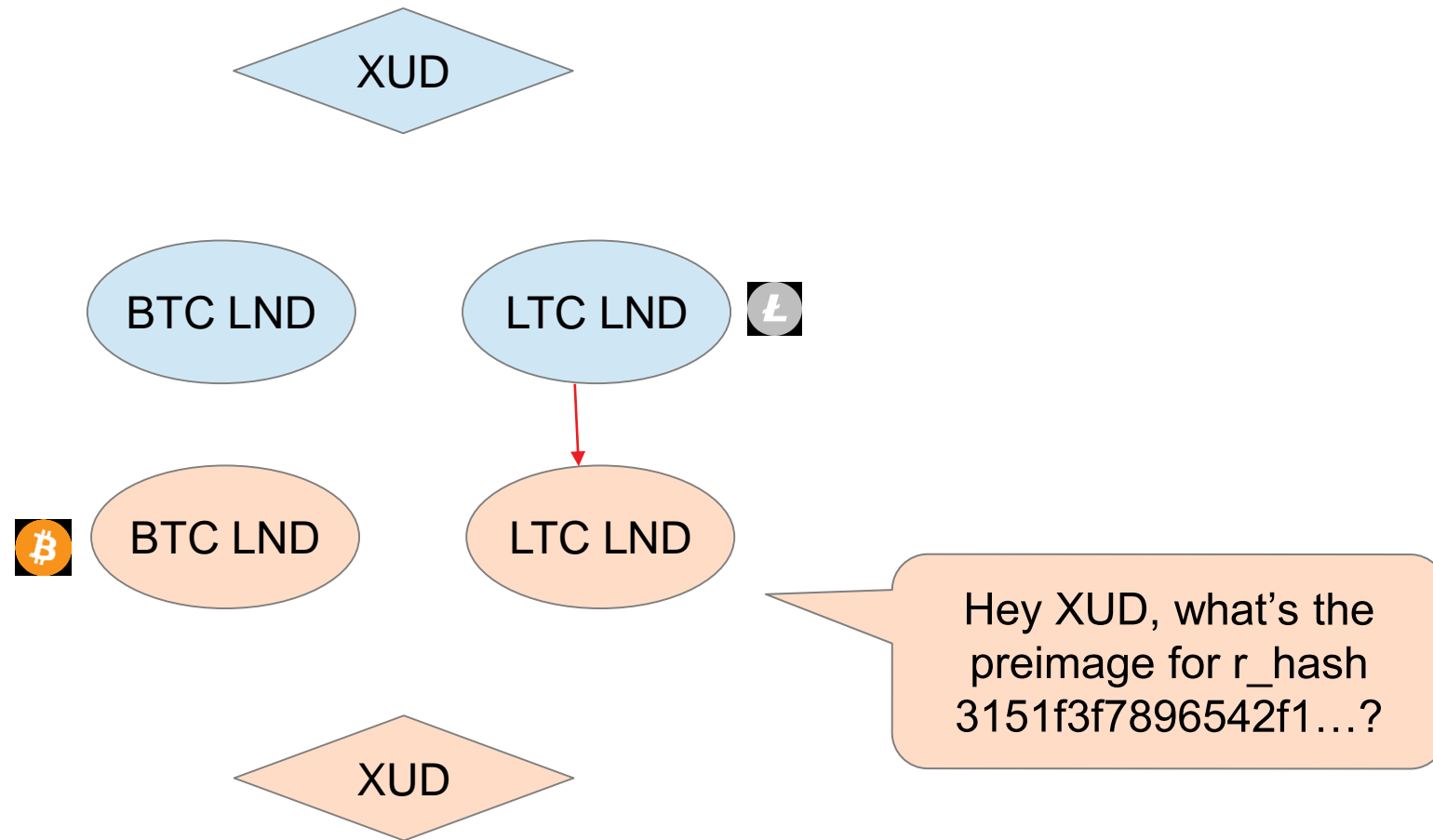
`r_preimage = MVHz941lQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=`

`r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990`

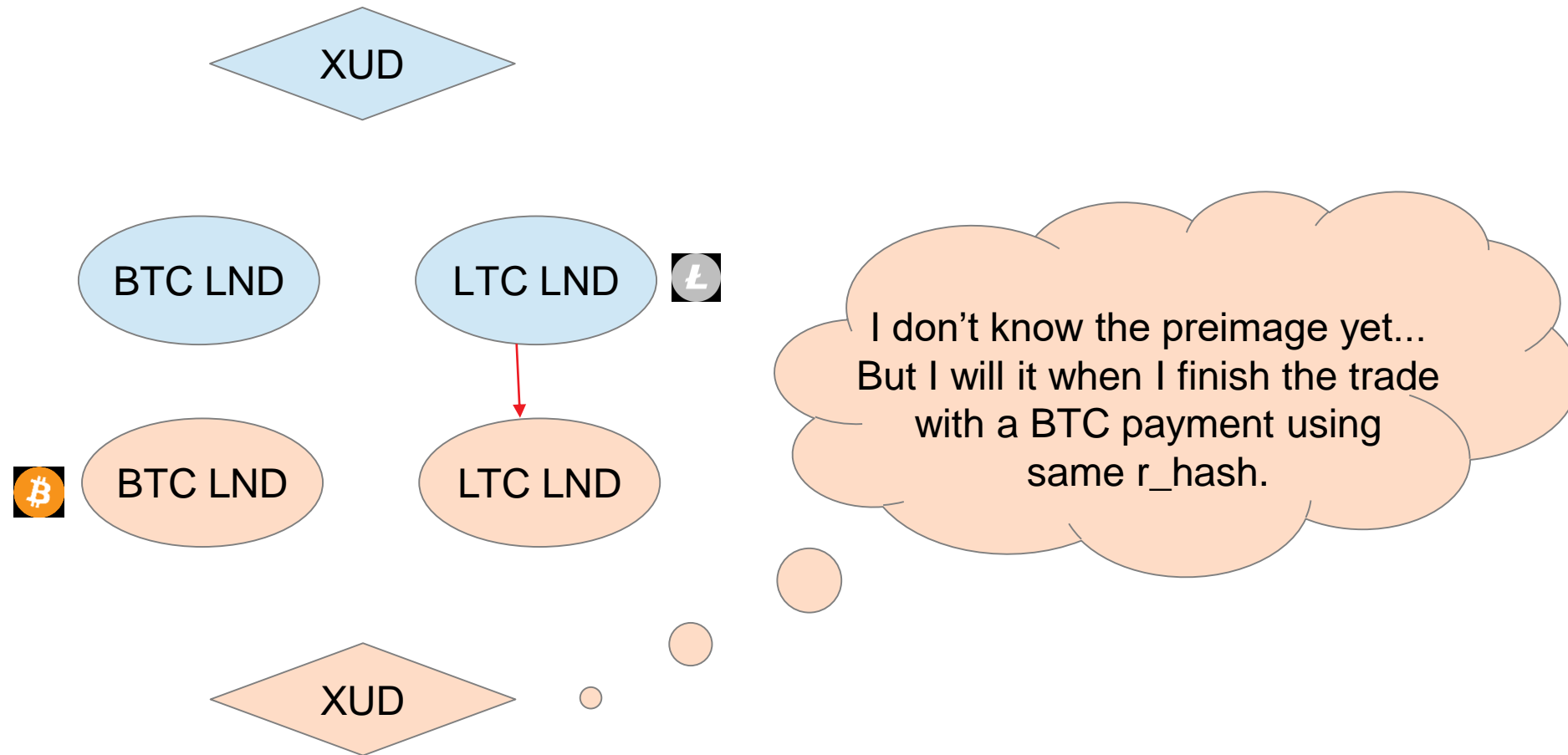
`r_preimage = ???`

`r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990`

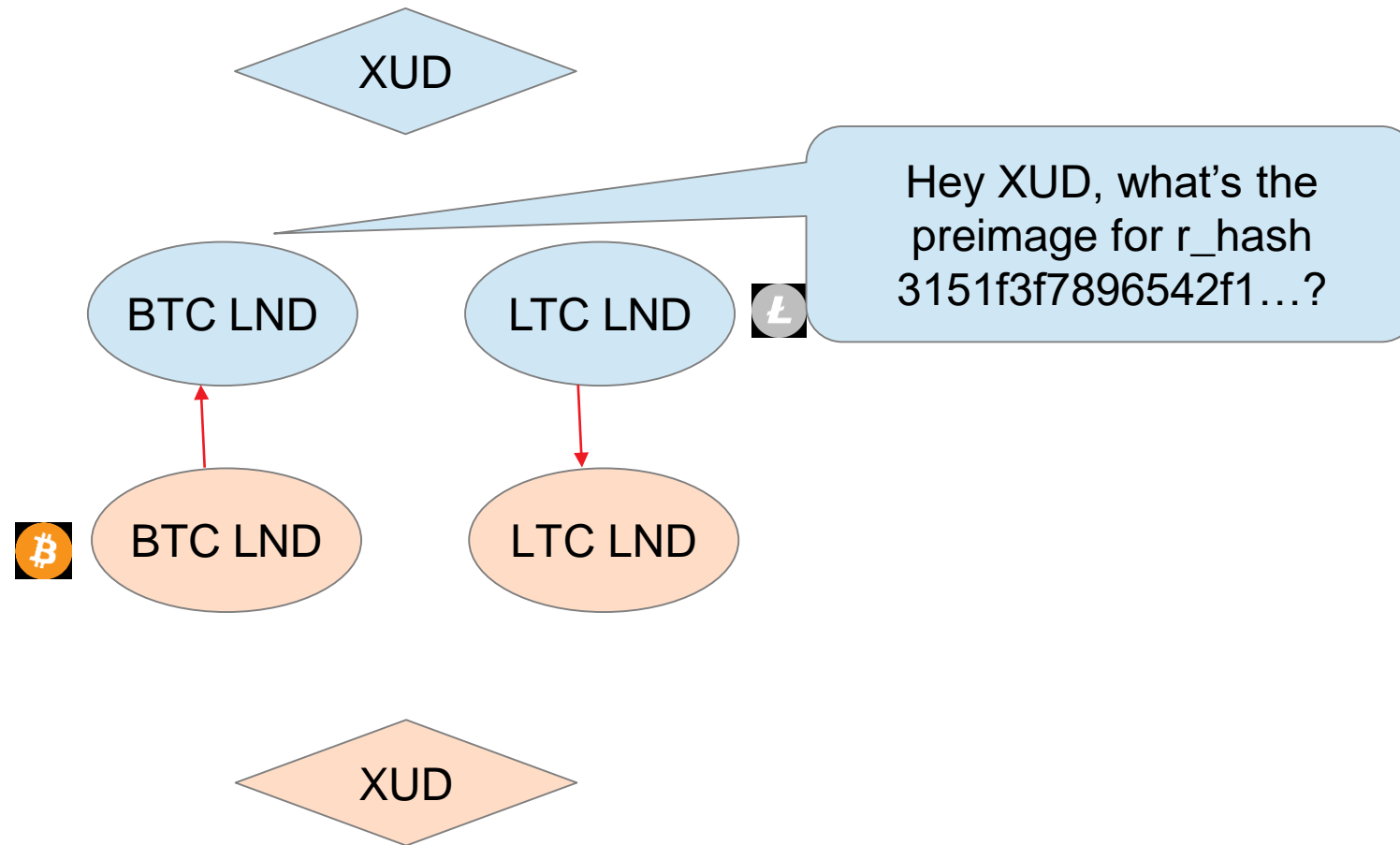
XUD, The Software



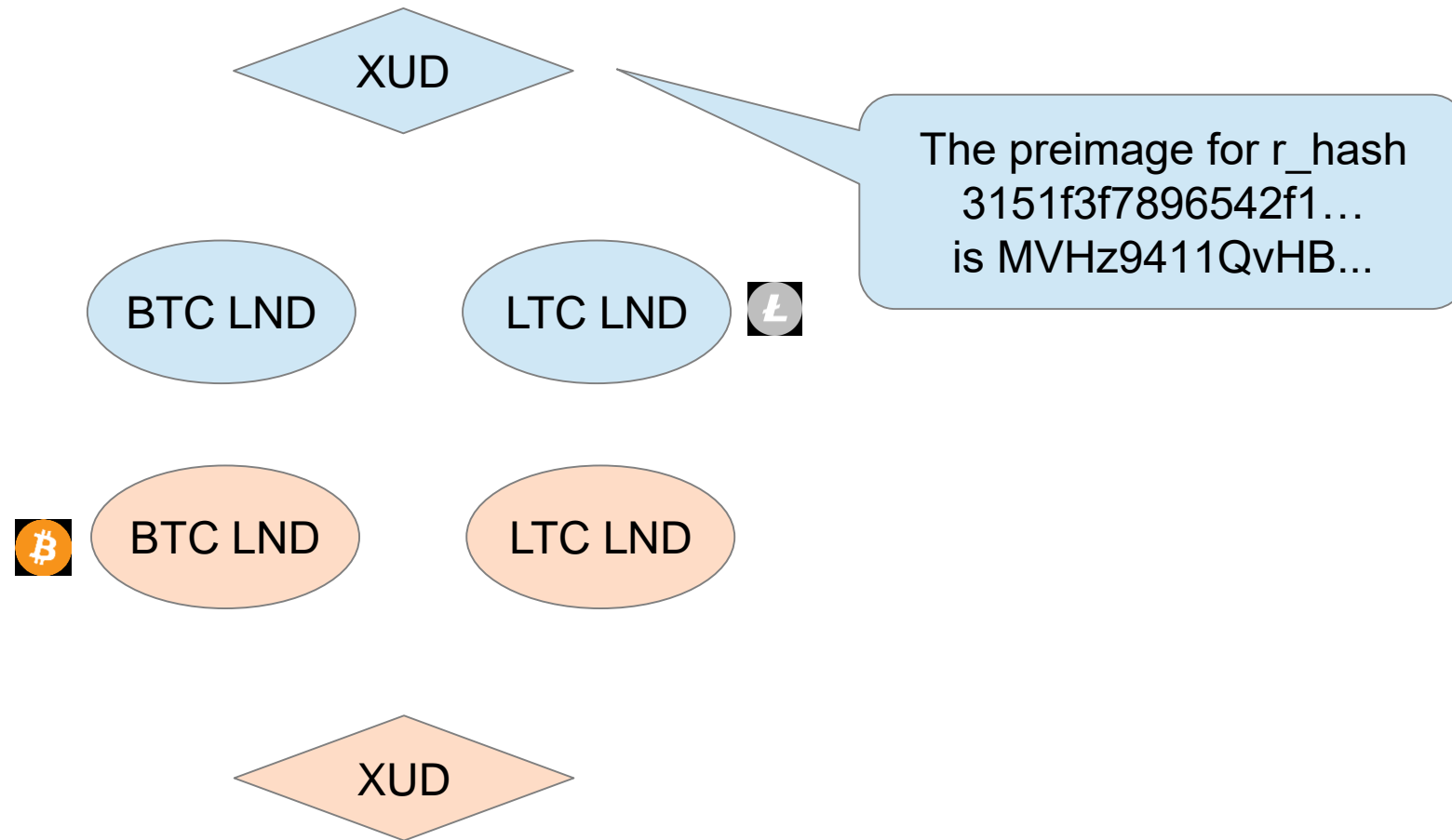
XUD, The Software



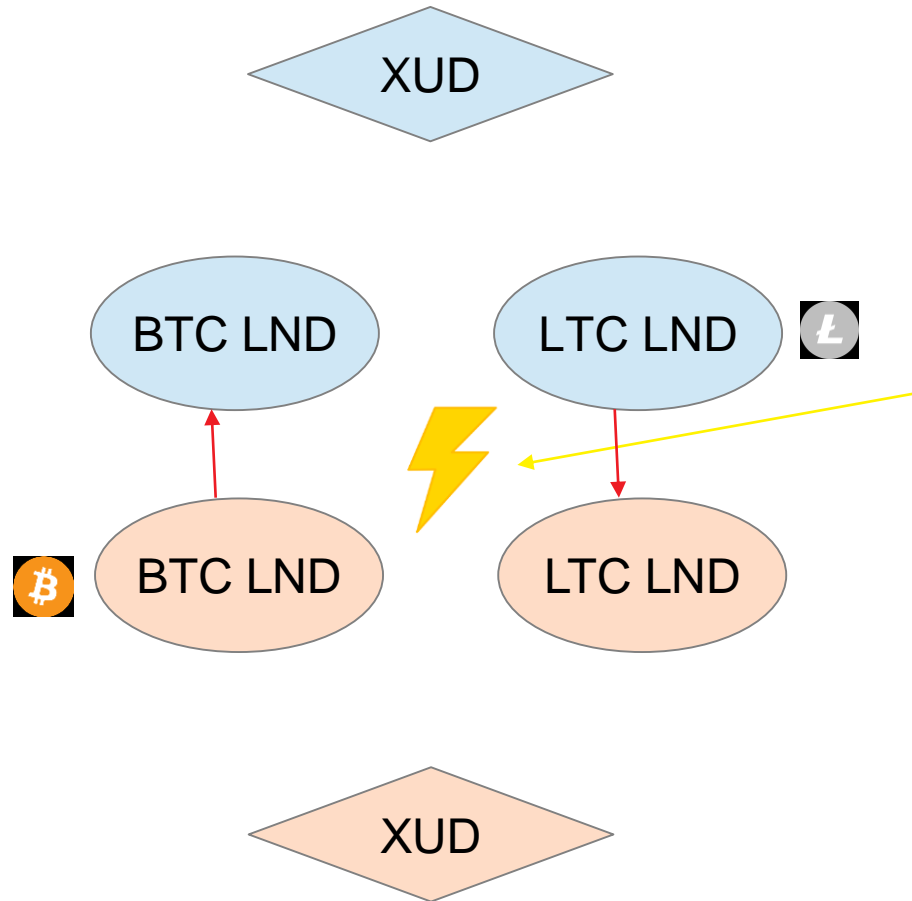
XUD, The Software



XUD, The Software



XUD, The Software



Preimage revealed

BTC & LTC Lightning payment settled!

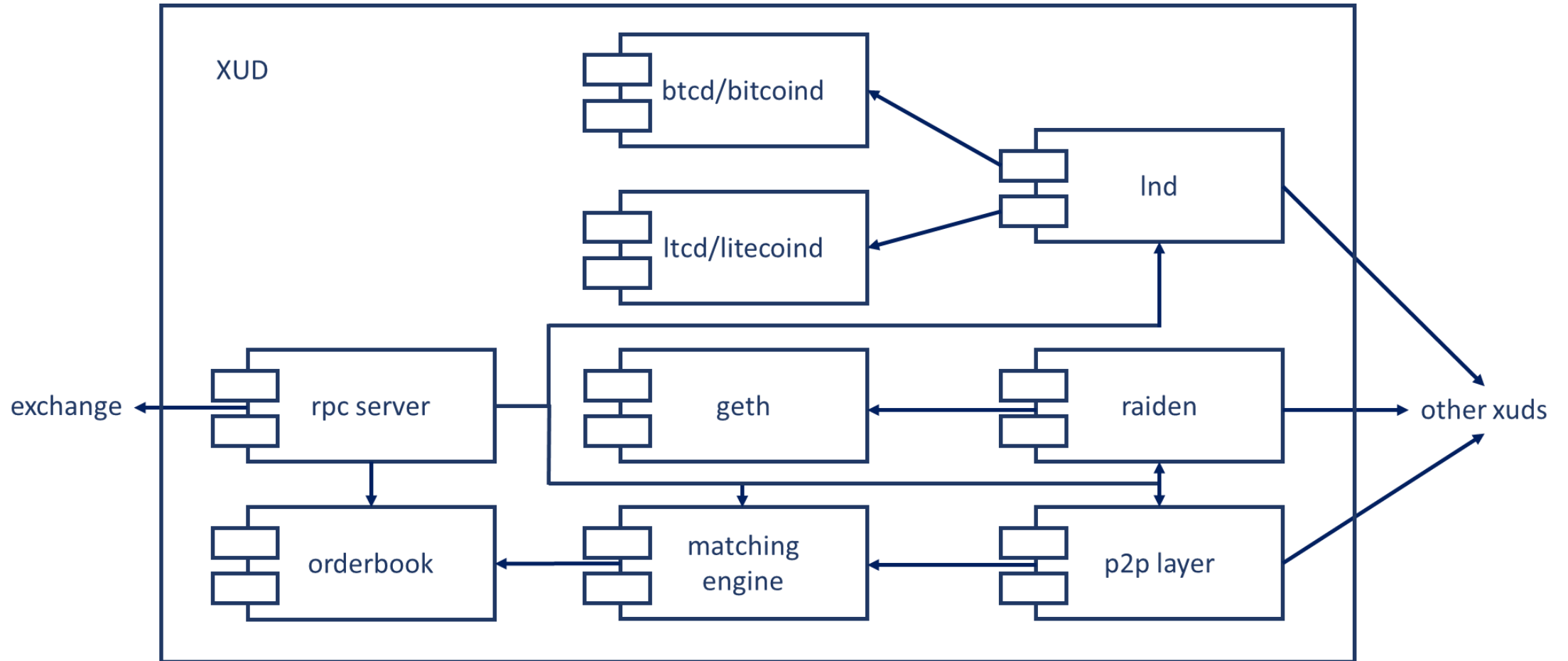
Note: This payment can route through any number of intermediary nodes on the BTC lightning network

DIY

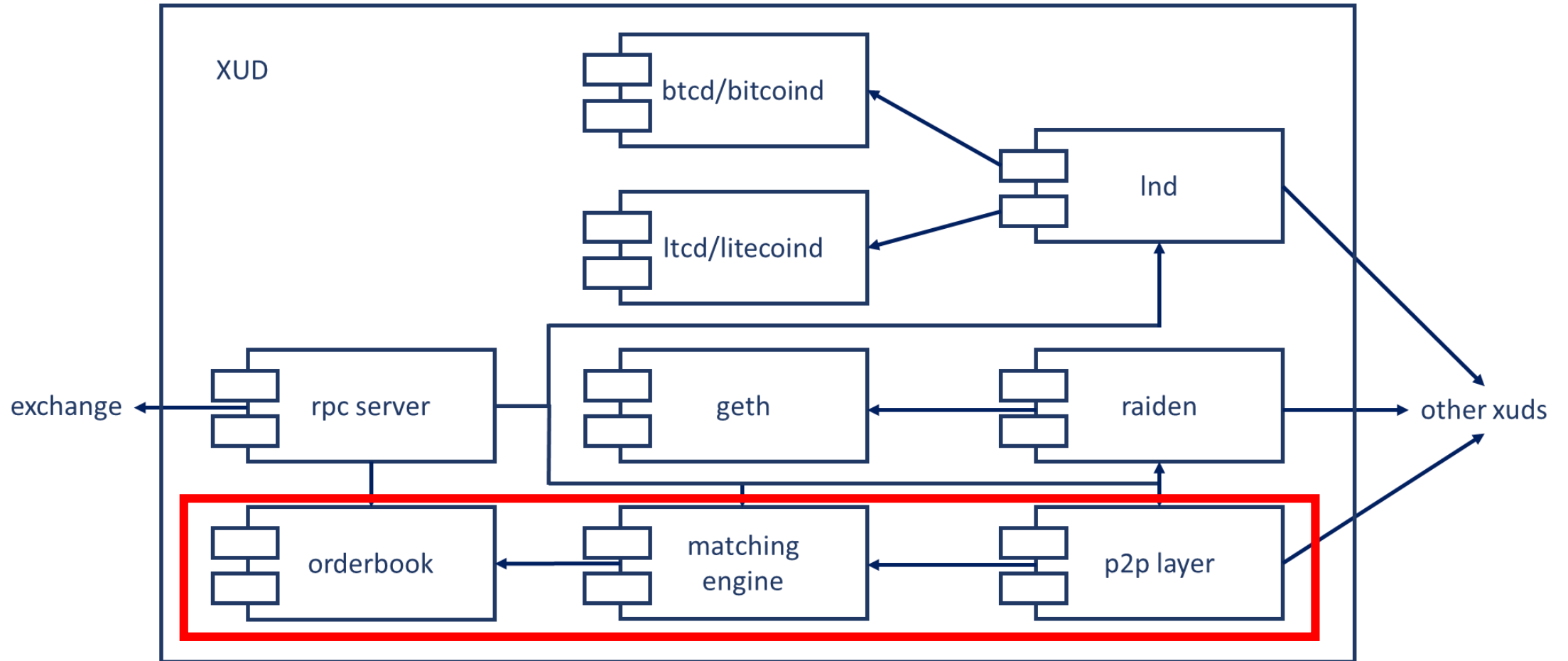
<https://github.com/ExchangeUnion/Lightning-Swap-PoC-v2>



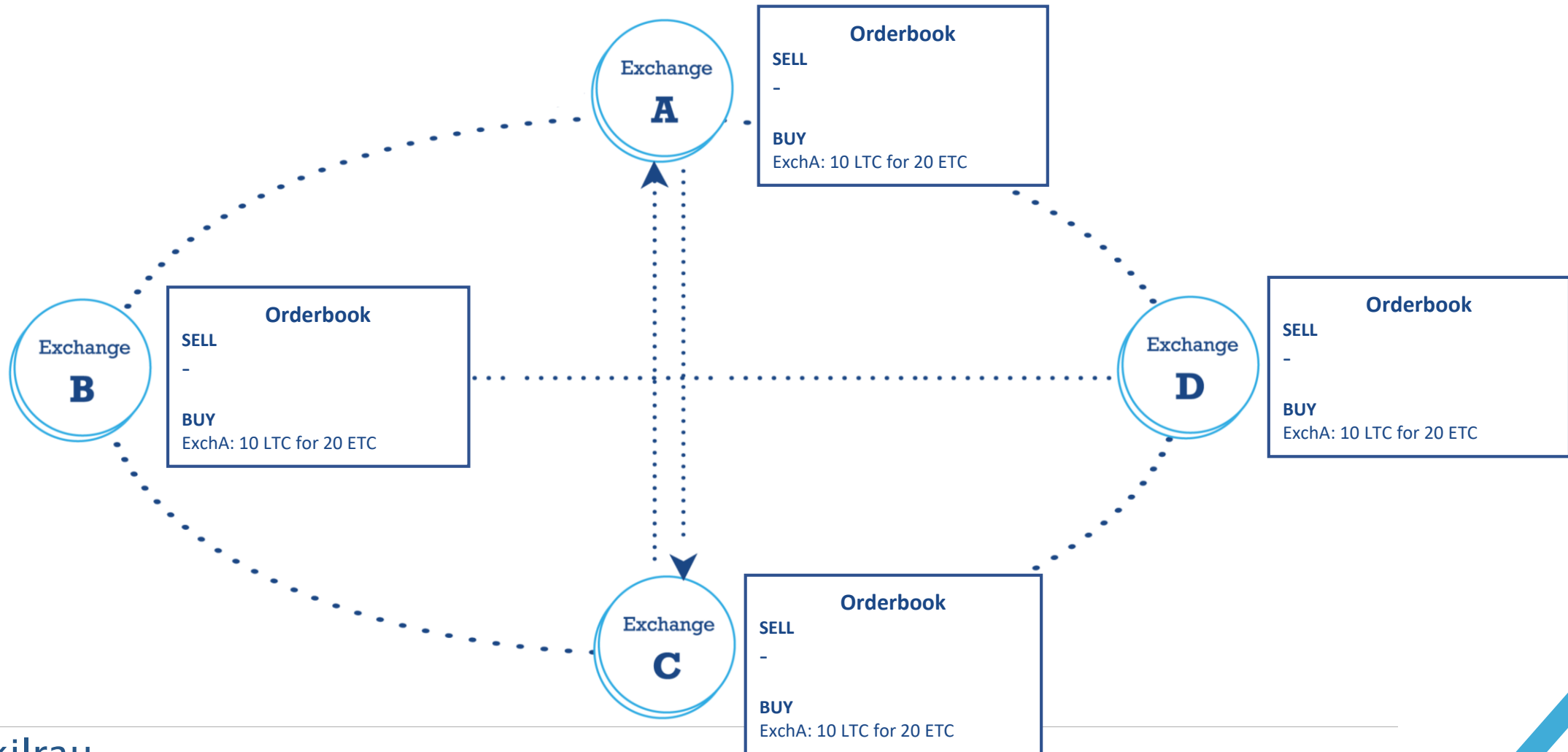
XUD, The Software



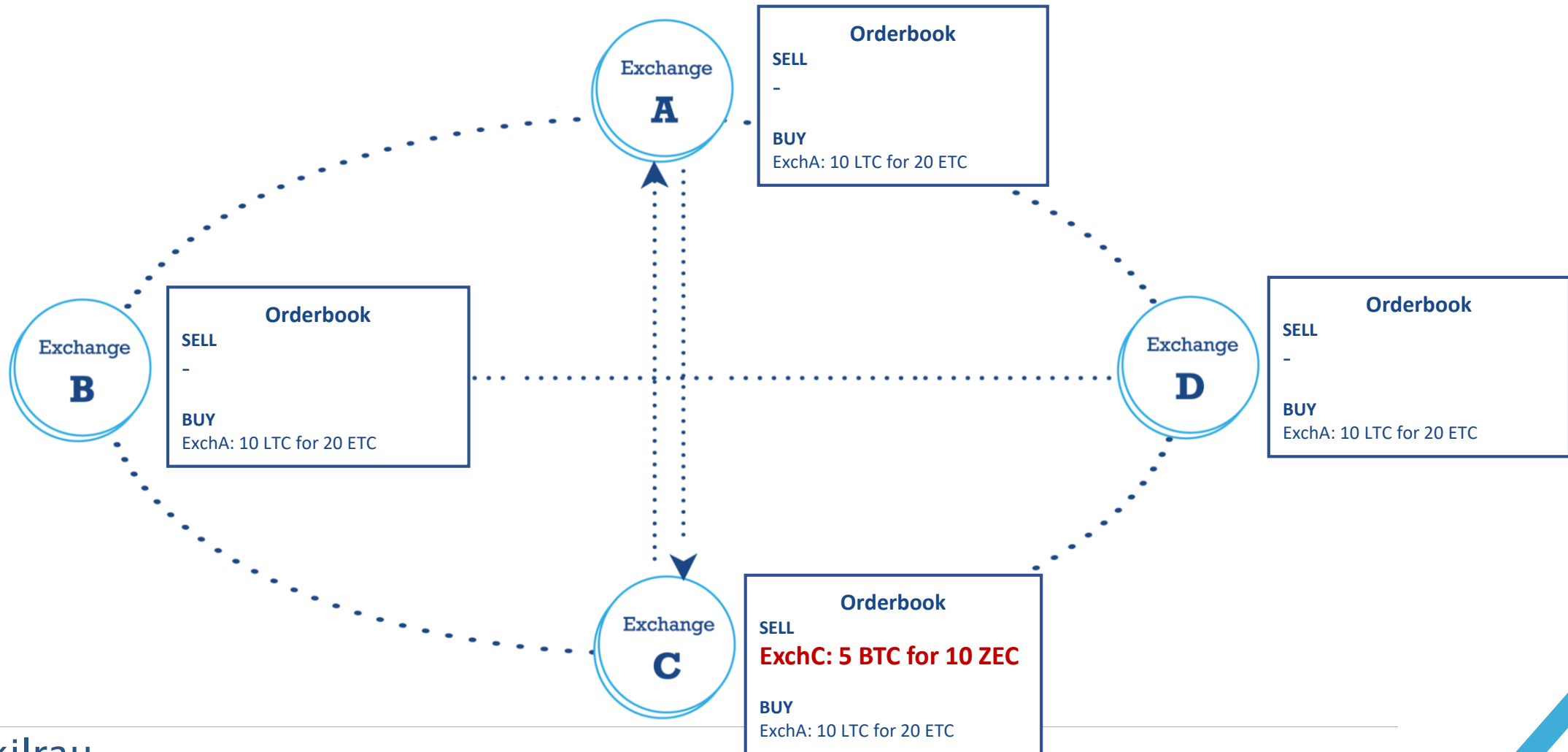
XUD, The Software



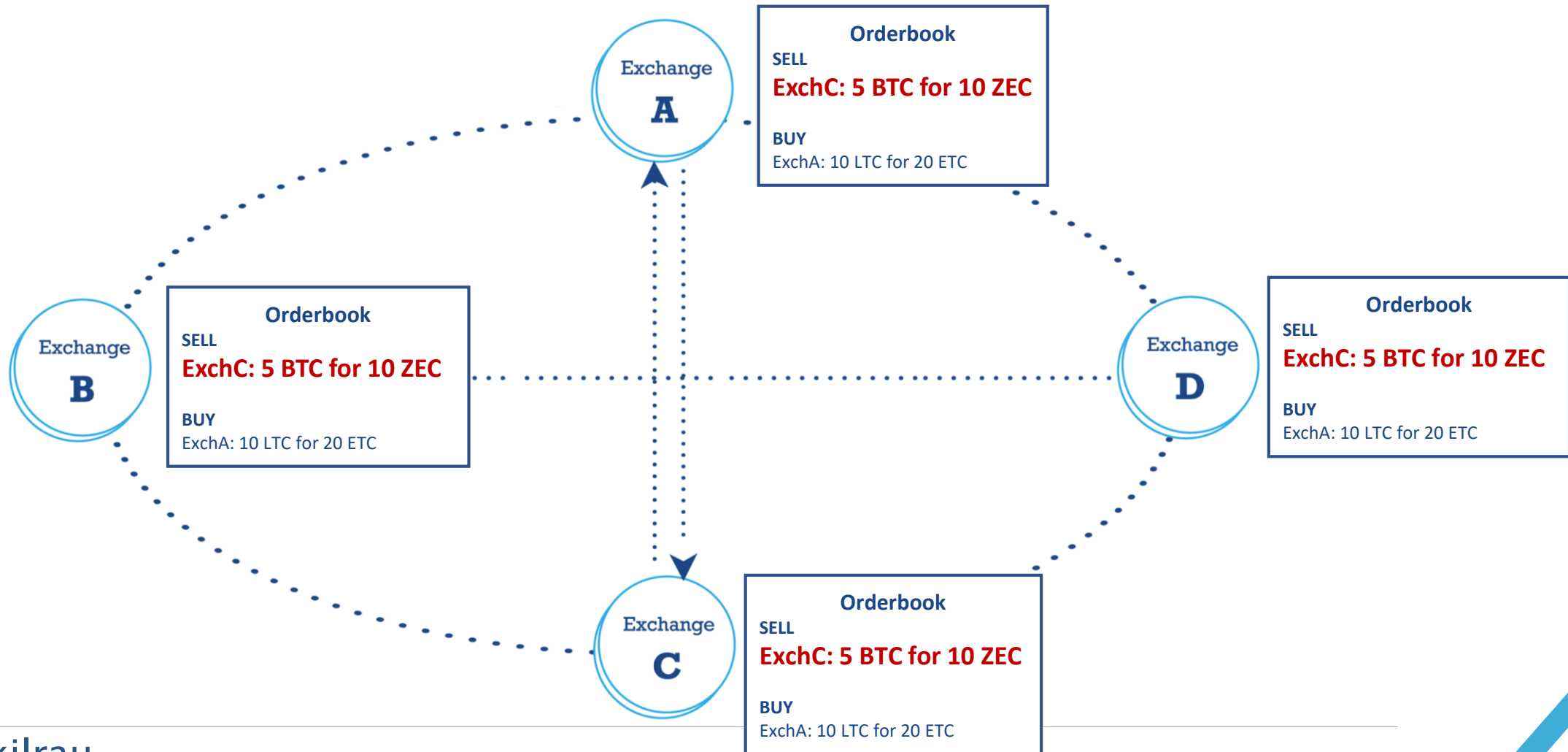
Decentralized Orderbook



Decentralized Orderbook



Decentralized Orderbook



Who we are

Crypto. Startup. Decentralized.



Who we are

Crypto. Startup. Decentralized.

Not searching for funding.



Problems we are working on

DOB

Cross-chain compatibility

Staking and Punishing

The LN future we are excited about

- Watchtowers & Neutrino: safe mobile usage (receive!)
- Dual-funded Channels: fairer!
- Advanced Autopilot: Look ma no hands
- Submarine Swaps & Splicing: never close channels
- AMP: One payment via multiple channels
- Atomic Swaps: Cross-chain compatibility

The LN future we are excited about

- Watchtowers & Neutrino: safe mobile usage (receive!) → <https://github.com/lightningnetwork/lnd/pull/1579>
- Dual-funded Channels: fairer!
- Advanced Autopilot: Look ma no hands
→ <https://github.com/ElementsProject/lightning/pull/1888>
- Submarine Swaps & Splicing: never close channels
→ <https://github.com/submarineswaps/swaps-service>
- AMP: One payment via multiple channels
- Atomic Swaps: Cross-chain compatibility
→ <https://github.com/lightningnetwork/lnd/pull/1820>



@kilrau

Summary

Exchange Union is not a blockchain.

Summary

Exchange Union is not a blockchain.

It uses layer 2 payment channels on top of Bitcoin, Litecoin, Ethereum, Ethereum Classic ...

Summary

**Exchange Union is not a regular
Exchange.**

Summary

Exchange Union is not a regular Exchange.

Don't ask us to list your token.

Summary

Exchange Union is not a regular Exchange.

It's a decentralized exchange. Run XUD, our node and you listed your token yourself.

Our Philosophy: Open Source



XUD is infrastructure.

Open & free for everyone to use.

We open-source everything. Like this PPT.

We are hiring

exchangeunion.com



gitter.im/exchangeunion



github.com/exchangeunion



[@exchange_union](https://twitter.com/exchange_union)

BitcoNNEECT!



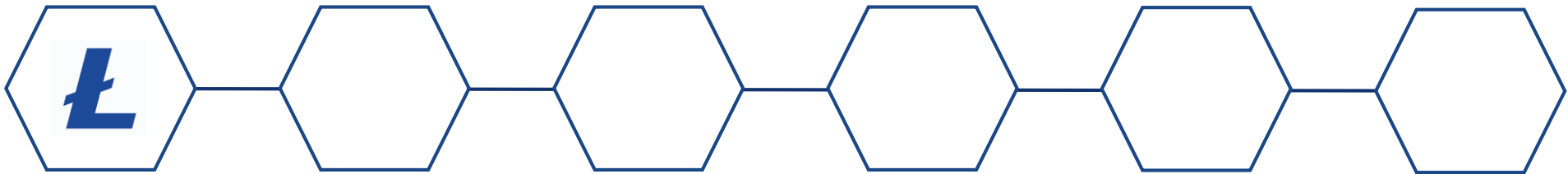
Backup

1. Payment Channels

**Bi-Directional
Channel:**

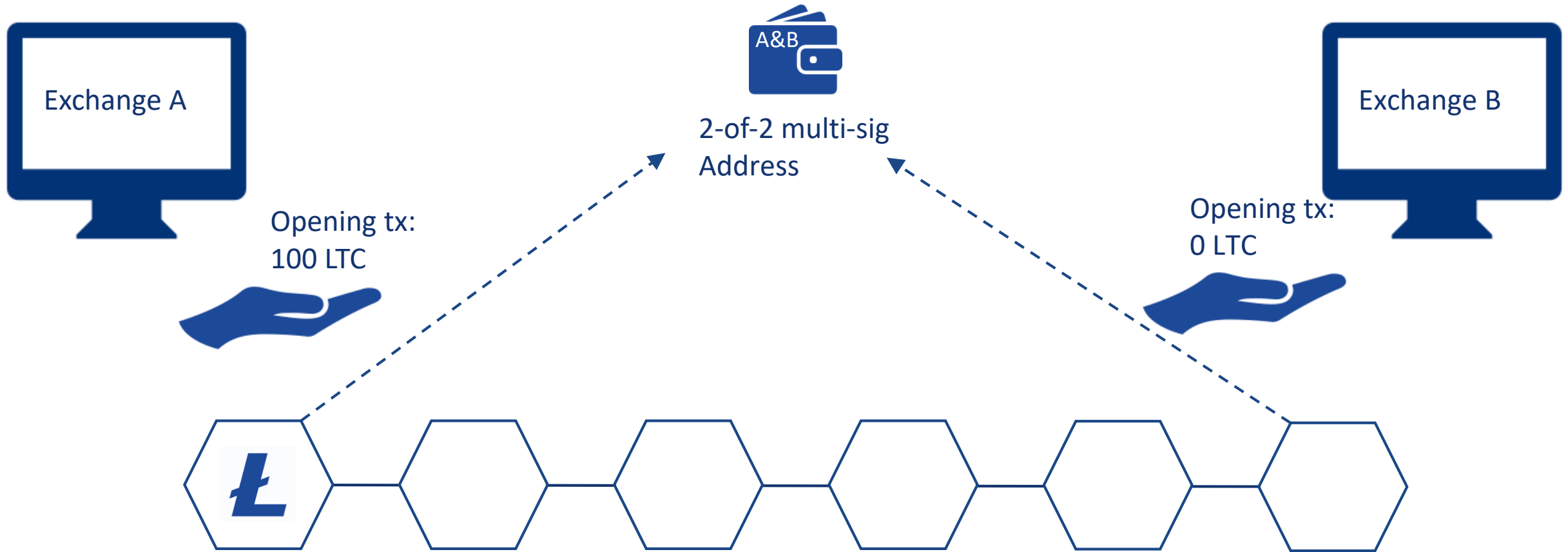


2-of-2 multi-sig
Address



1. Payment Channels

Bi-Directional Channel:



1. Payment Channels

Bi-Directional Channel:



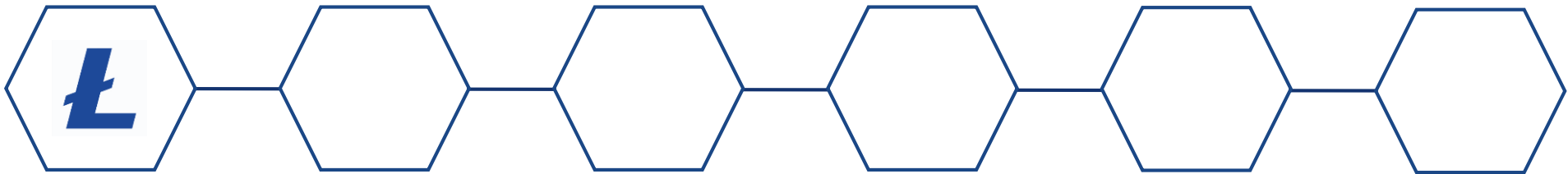
Exchange A

$H(a_secret)$



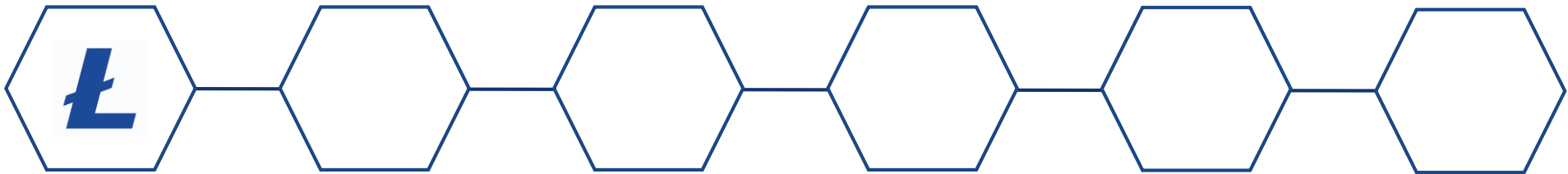
Exchange B

$H(b_secret)$



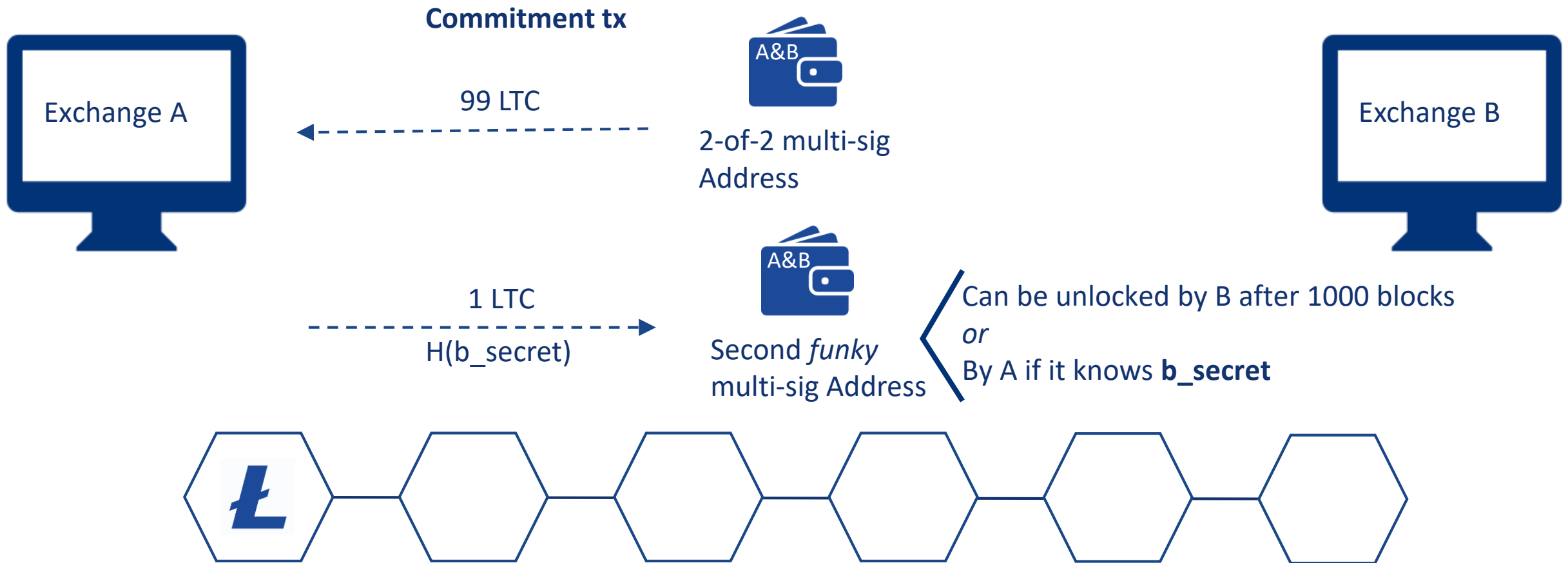
1. Payment Channels

Bi-Directional Channel:



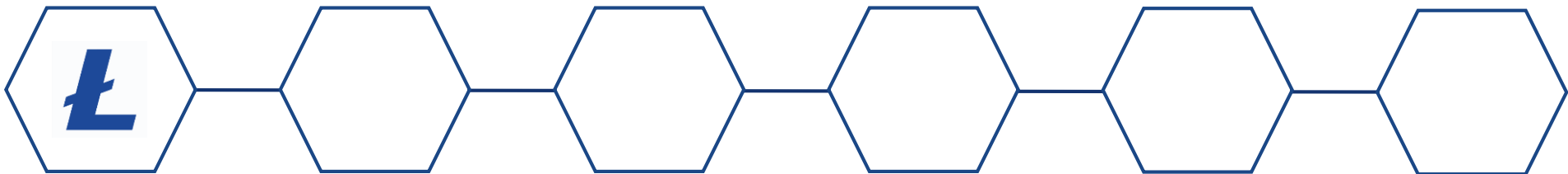
1. Payment Channels

Bi-Directional Channel:



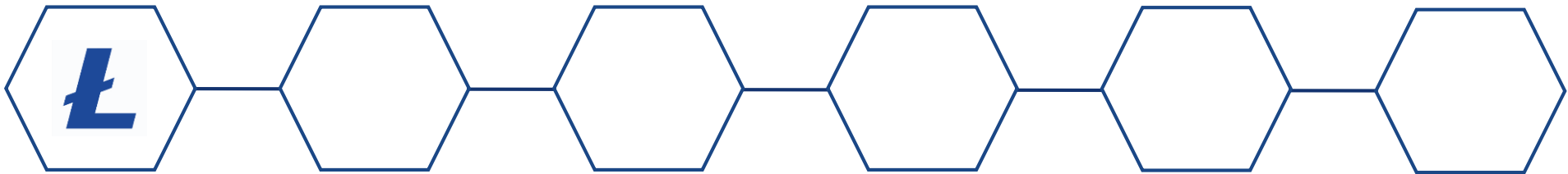
1. Payment Channels

Bi-Directional Channel:



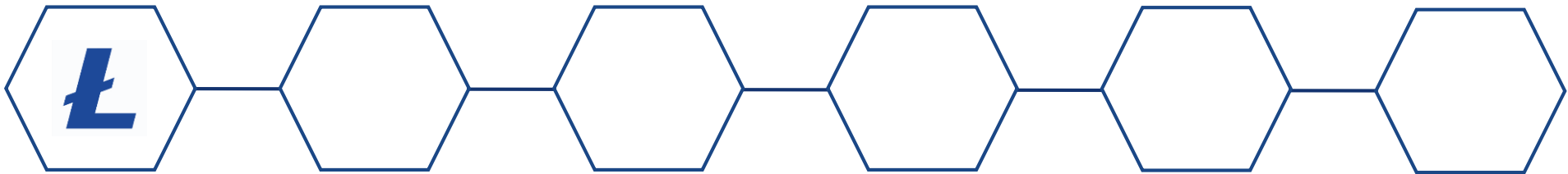
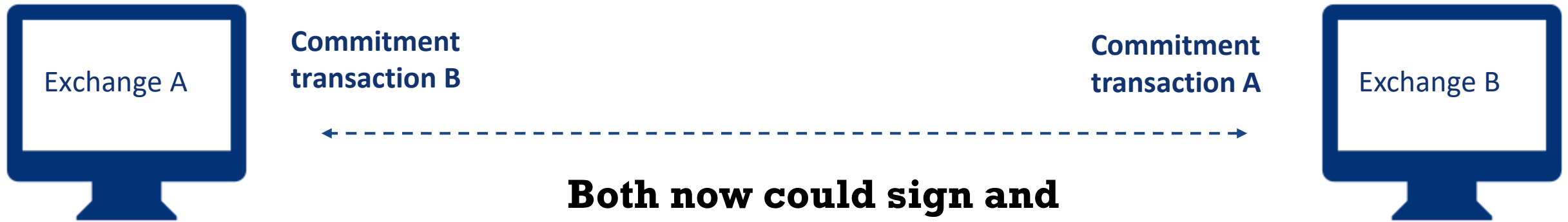
1. Payment Channels

Bi-Directional Channel:



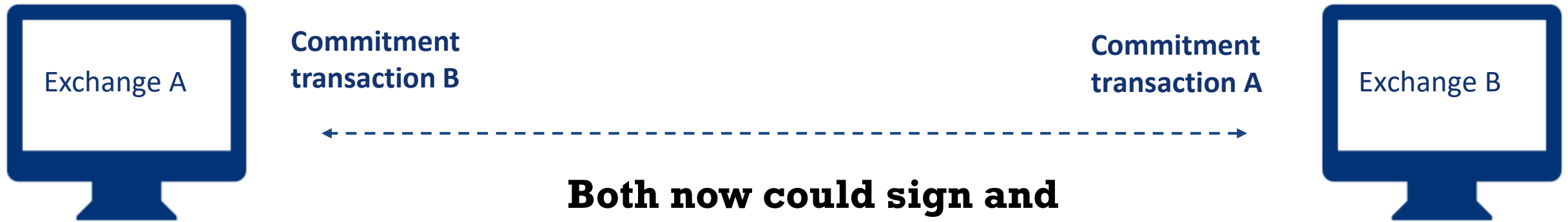
1. Payment Channels

Bi-Directional Channel:

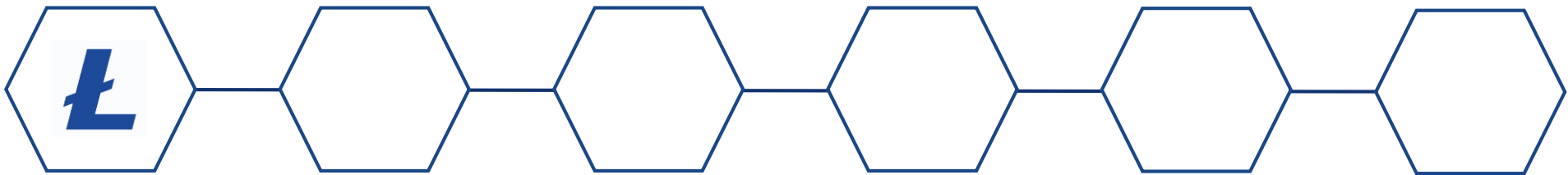


1. Payment Channels

Bi-Directional Channel:

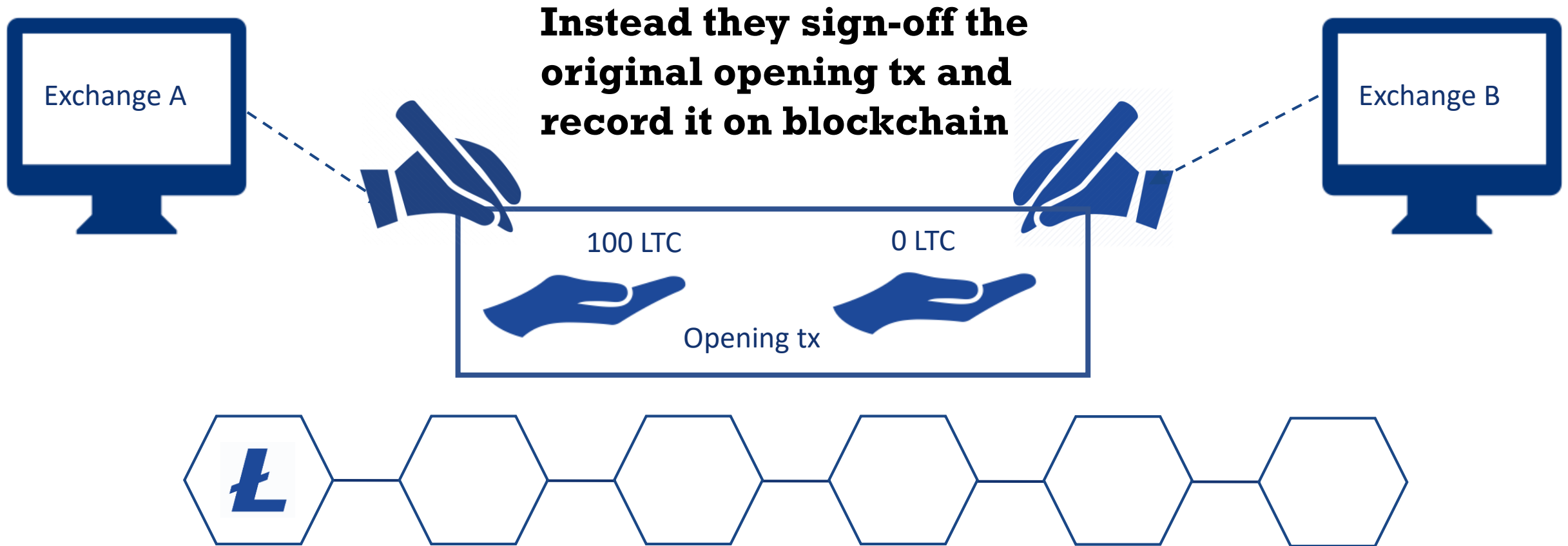


Both now could sign and broadcast these tx, but... they don't

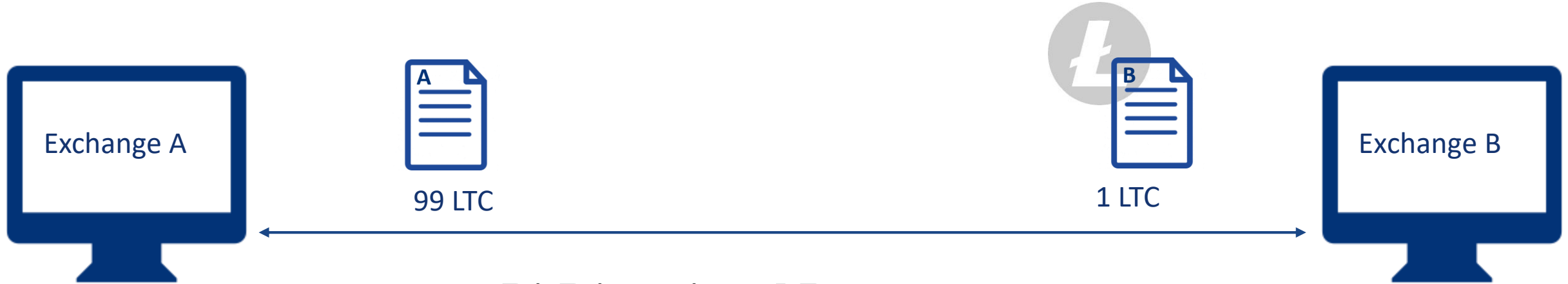


1. Payment Channels

Bi-Directional Channel:



1. Payment Channels



**Bi-Directional Payment
Channel is now officially open**

