Ellis & Bob

LN Dev Meetup

exchange union

What we do

@kilrau

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⚡.

@kilrau

What we do

A decentralized exchange.

Of centralized exchanges. (Why? Liquidity.)

On ⚡lightning⚡.

@kilrau

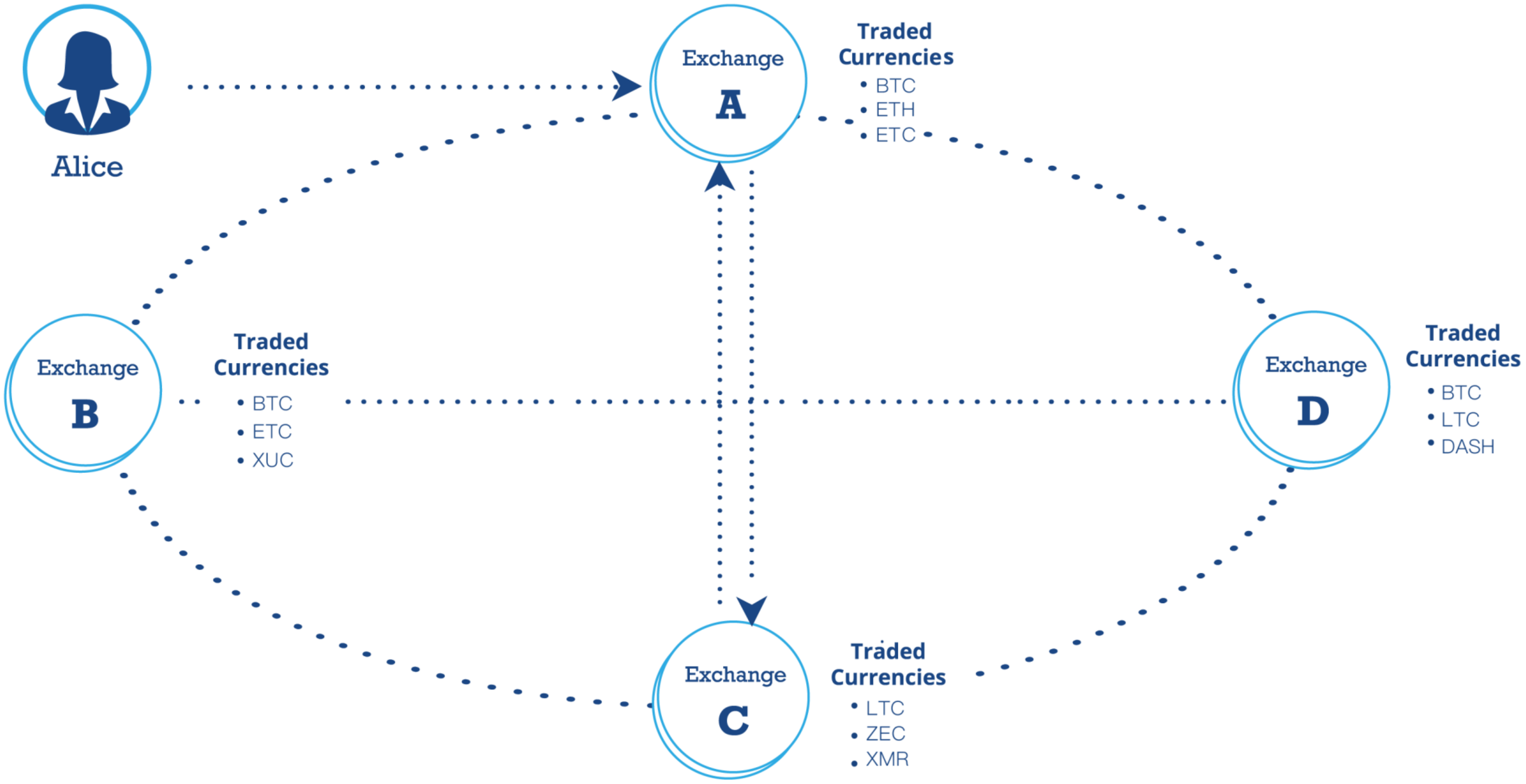
Endgame

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

@kilrau

What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



Alice

Exchange A

Traded Currencies
- BTC
- ETH
- ETC

Exchange B

Traded Currencies
- BTC
- ETC
- XUC

Exchange D

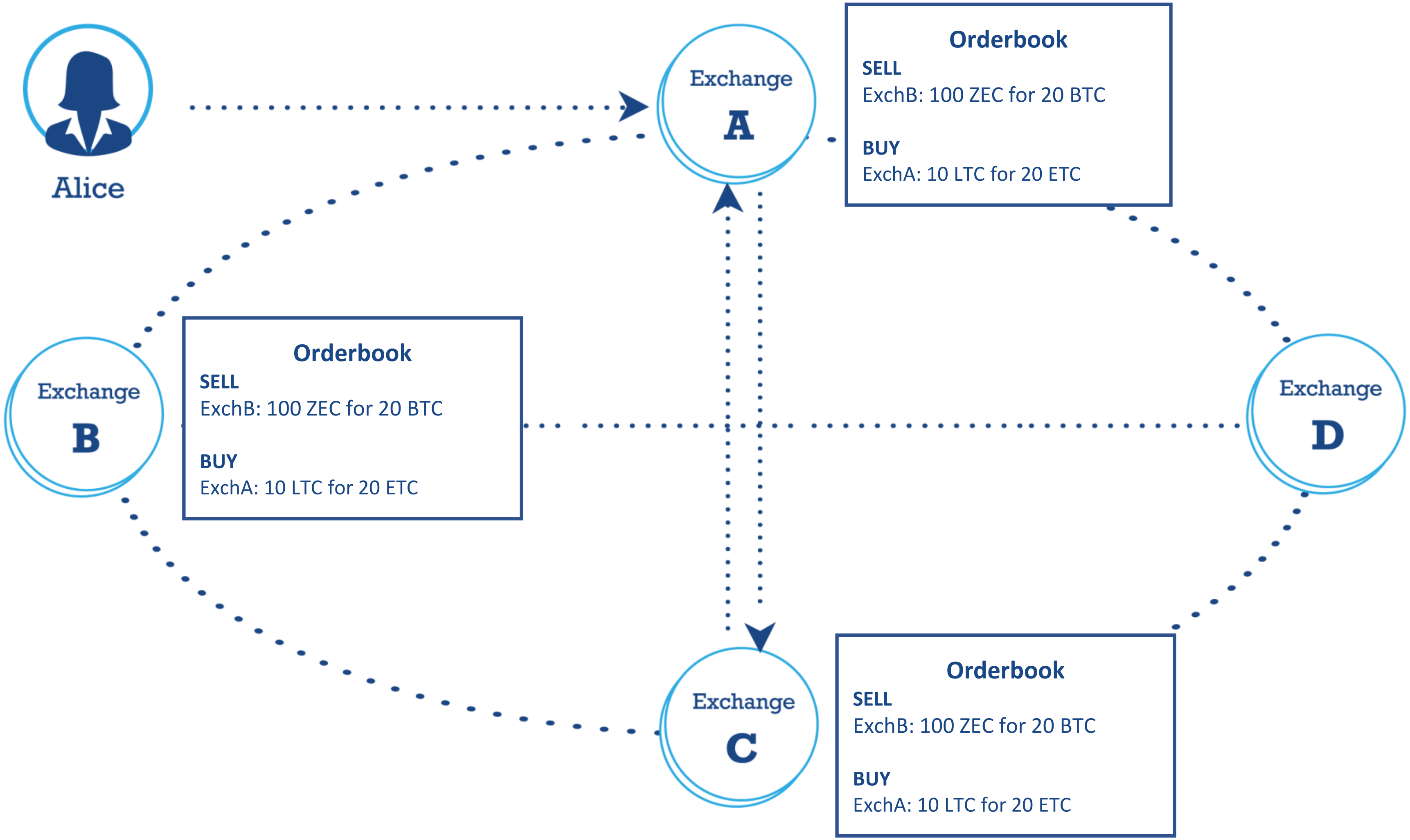
Traded Currencies
- BTC
- LTC
- DASH

Exchange C

Traded Currencies
- LTC
- ZEC
- XMR

What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



Orderbook

SELL
ExchB: 100 ZEC for 20 BTC

BUY
ExchA: 10 LTC for 20 ETC

Orderbook

SELL
ExchB: 100 ZEC for 20 BTC

BUY
ExchA: 10 LTC for 20 ETC

Orderbook

SELL
ExchB: 100 ZEC for 20 BTC

BUY
ExchA: 10 LTC for 20 ETC

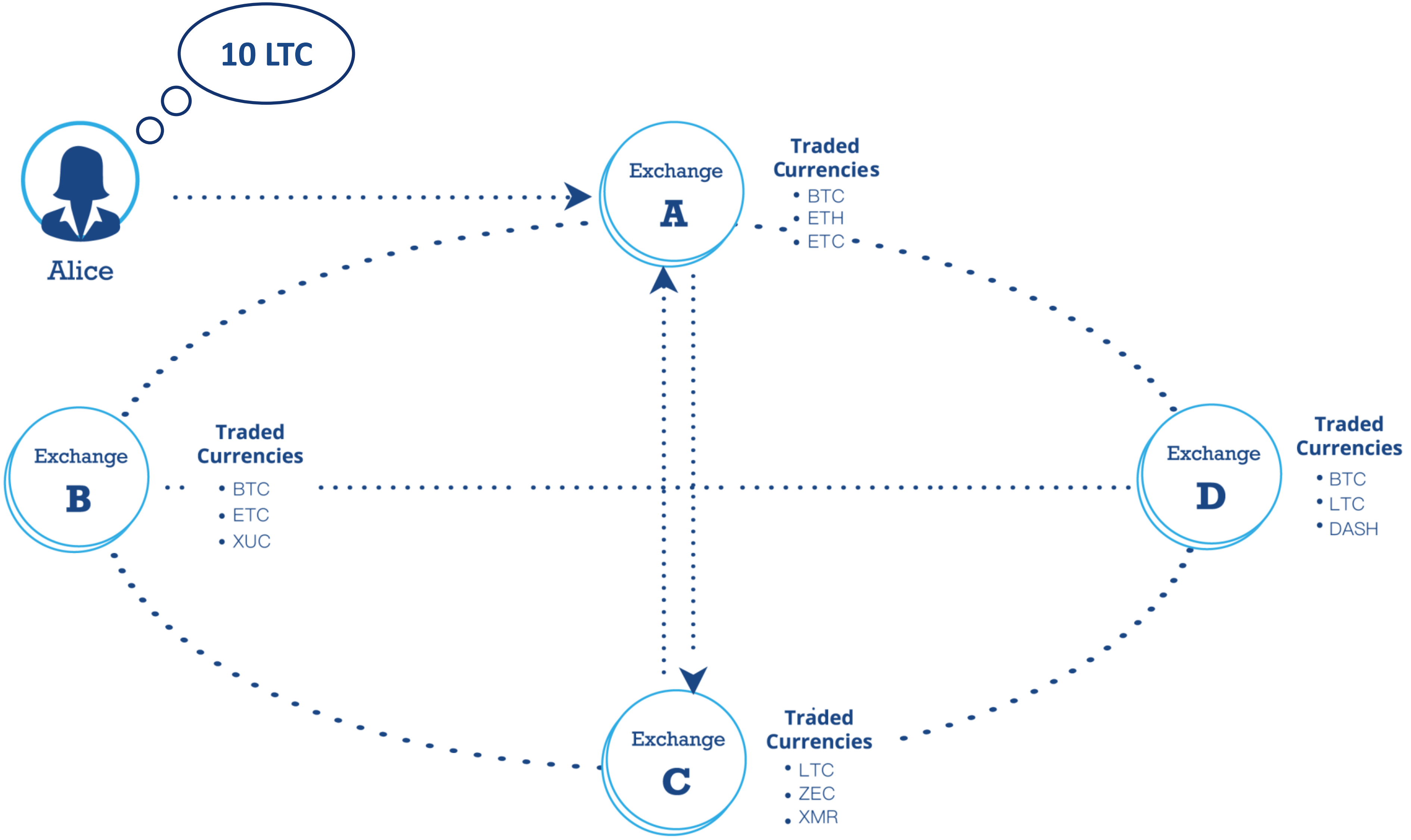
Orderbook

SELL
ExchB: 100 ZEC for 20 BTC

BUY
ExchA: 10 LTC for 20 ETC

What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



10 LTC

Alice

Exchange A

Traded Currencies
- BTC
- ETH
- ETC

Exchange B

Traded Currencies
- BTC
- ETC
- XUC

Exchange C

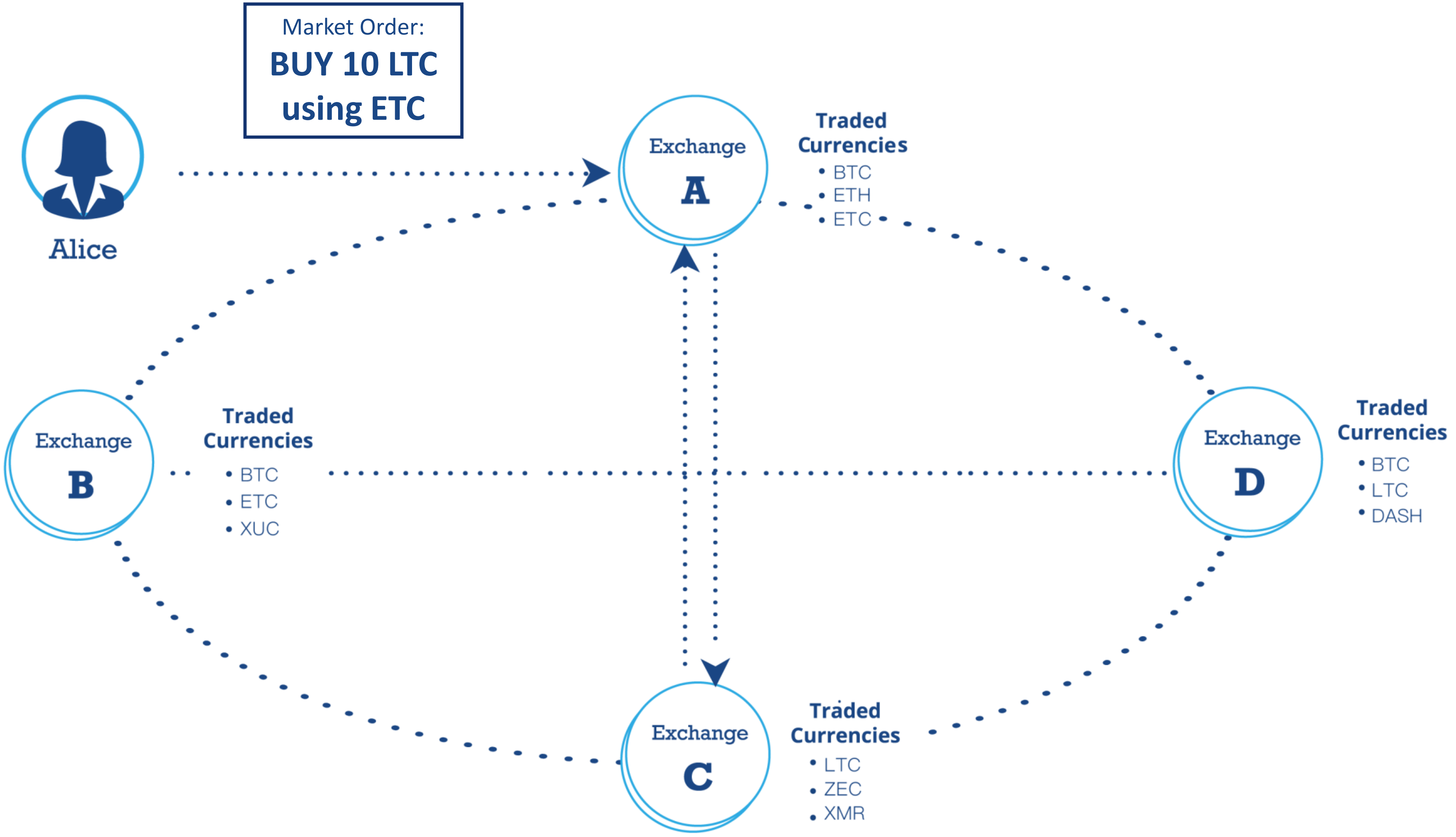
Traded Currencies
- LTC
- ZEC
- XMR

Exchange D

Traded Currencies
- BTC
- LTC
- DASH

What we do

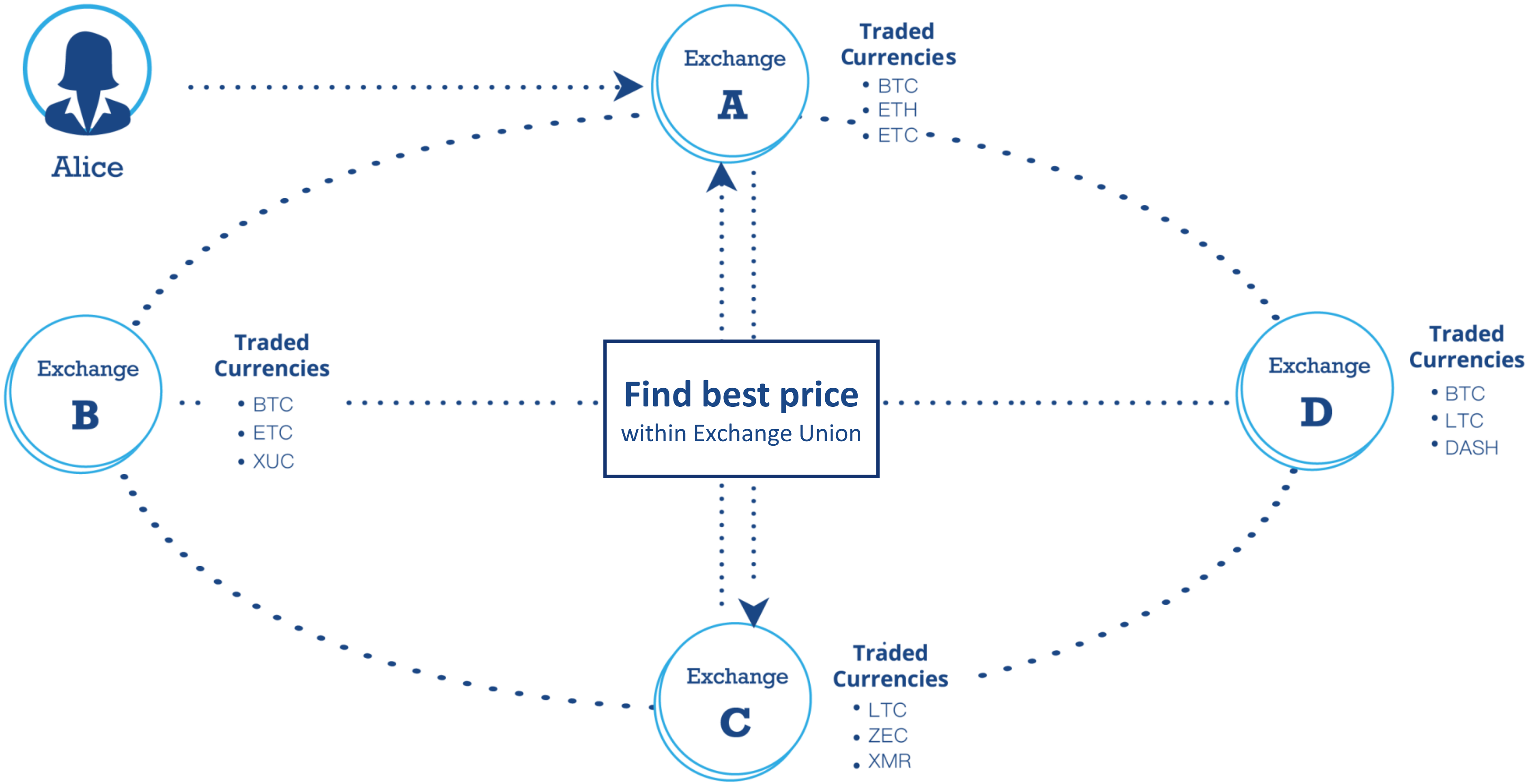
Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



Market Order:
BUY 10 LTC using ETC

What we do

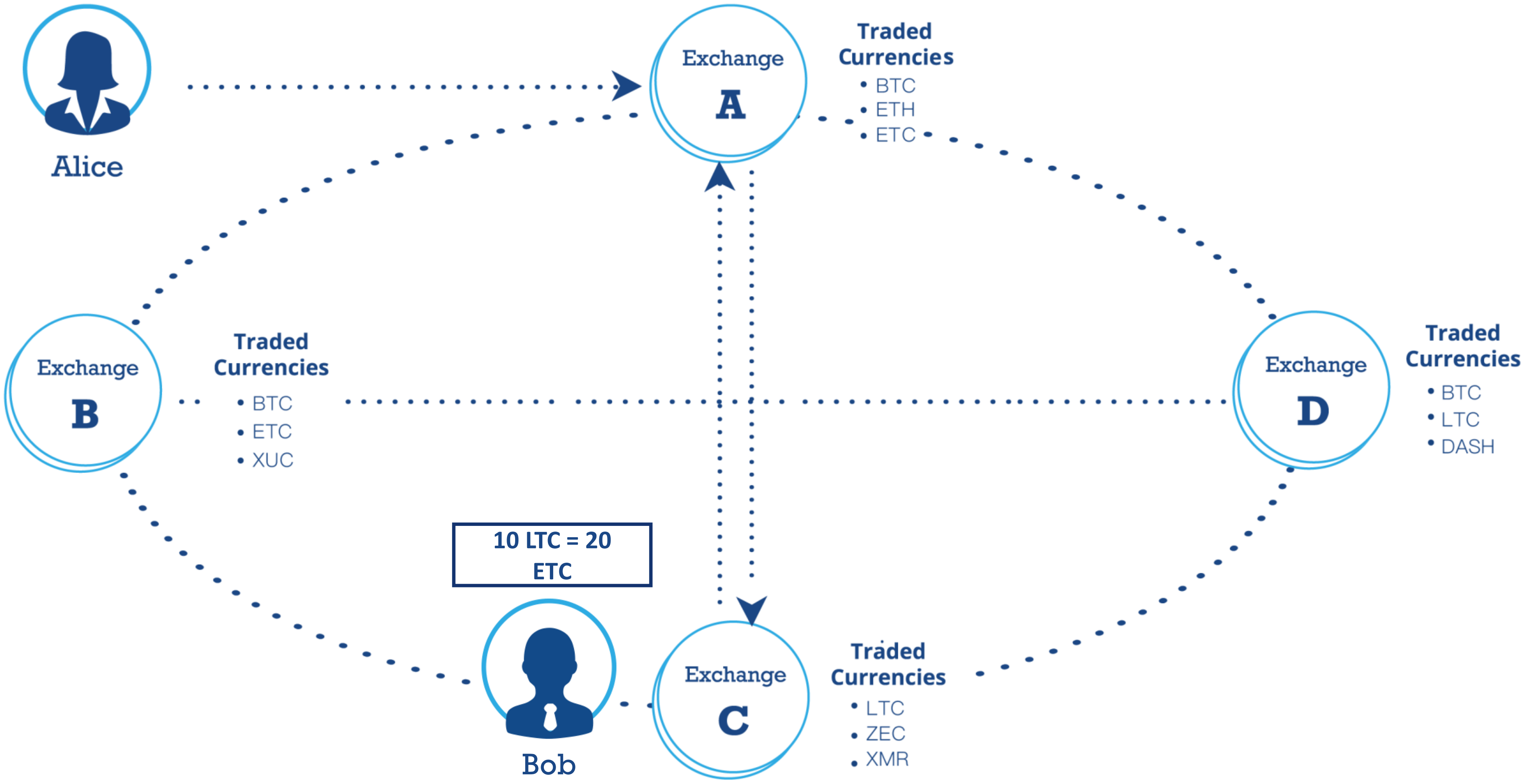
Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



Find best price
within Exchange Union

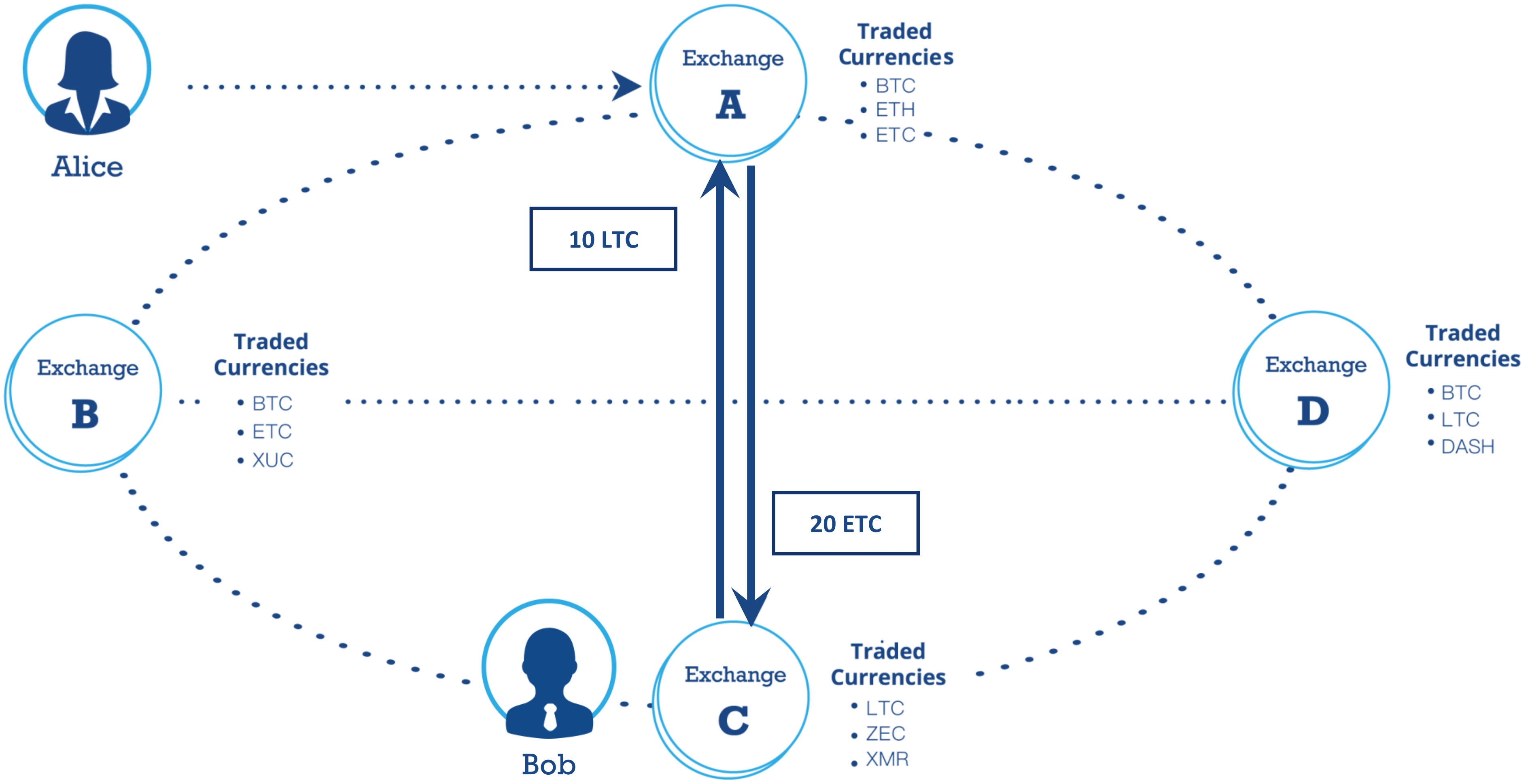
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



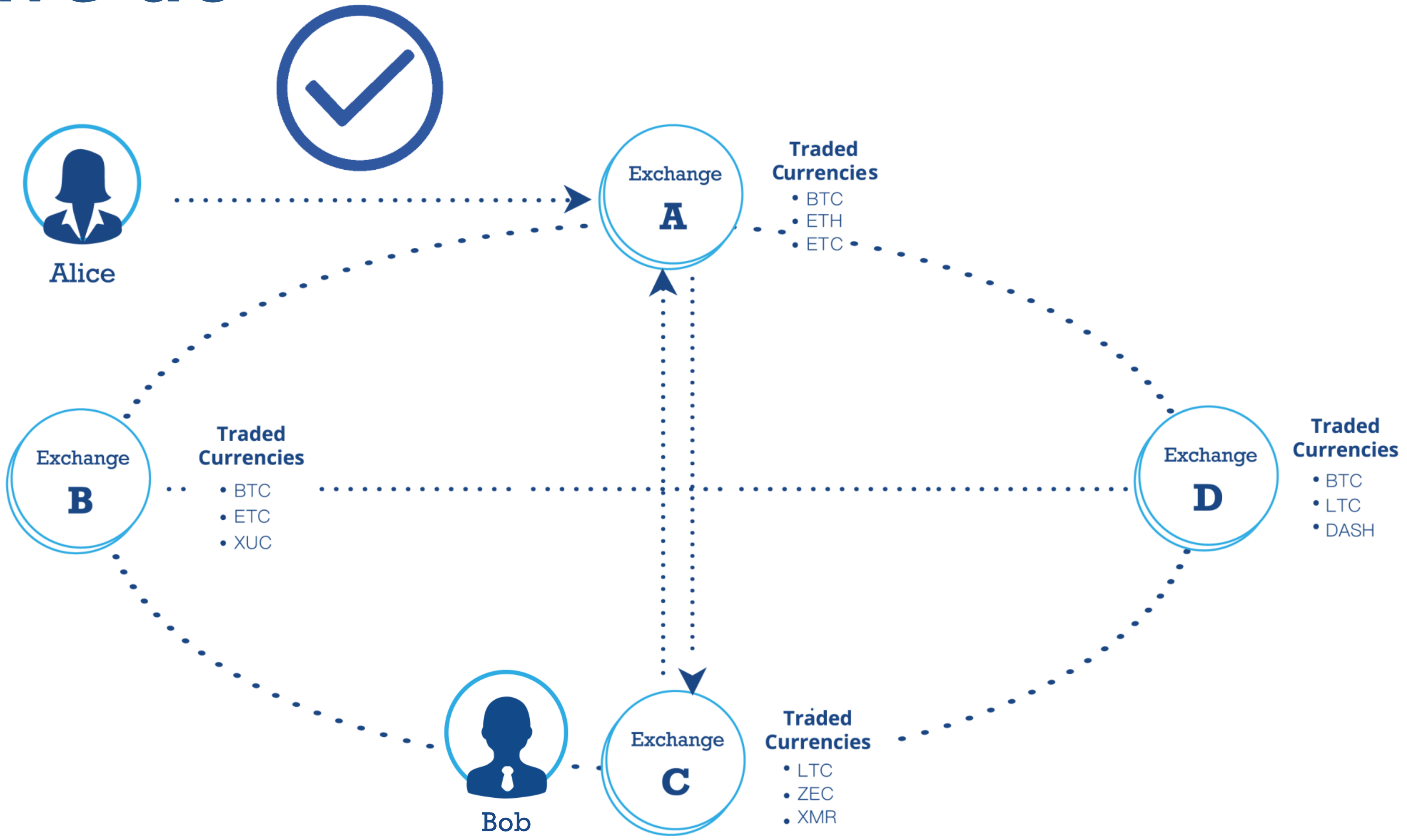
What we do

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



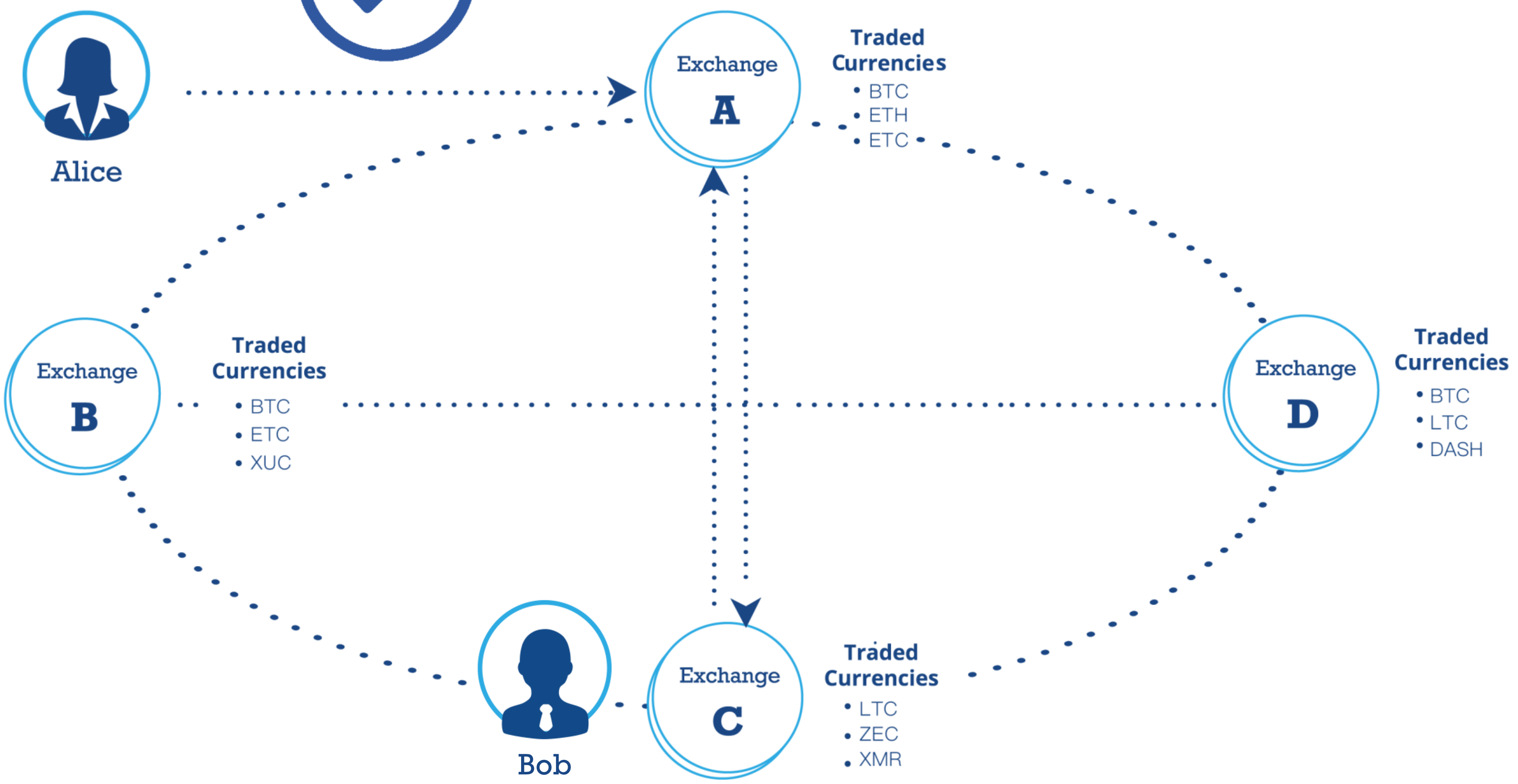
What we do

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

@kilrau

How we do

3 Key Technologies

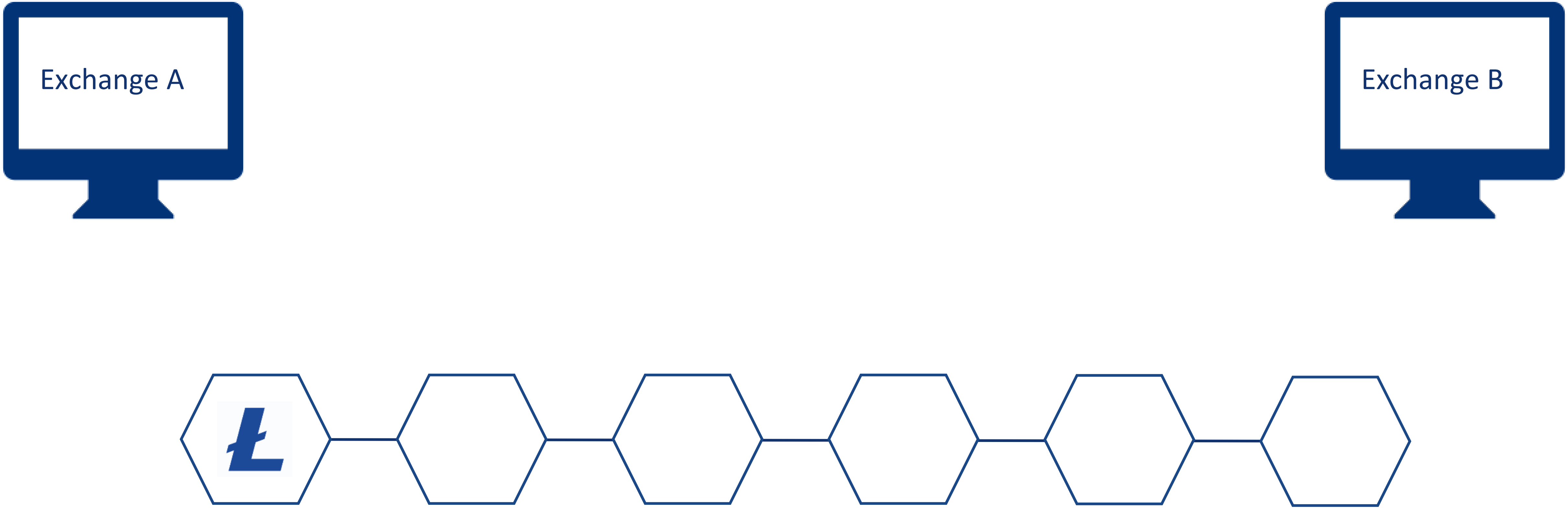
1. Payment Channels
Each trade transfers real digital assets *instantly* between exchanges

2. Atomic Swaps
Trustless trades directly between two exchanges

3. Decentralized Orderbooks
Solving the pain points of digital asset exchanges – *connecting buyer & seller*

@kilrau

Status Quo



@kilrau

Status Quo

Broadcast to everyone

Source: https://blog.bitmex.com/the-lightning-network/

Payment Channels

Payment Channels

Yes, we are talking about Lightning & Raiden!

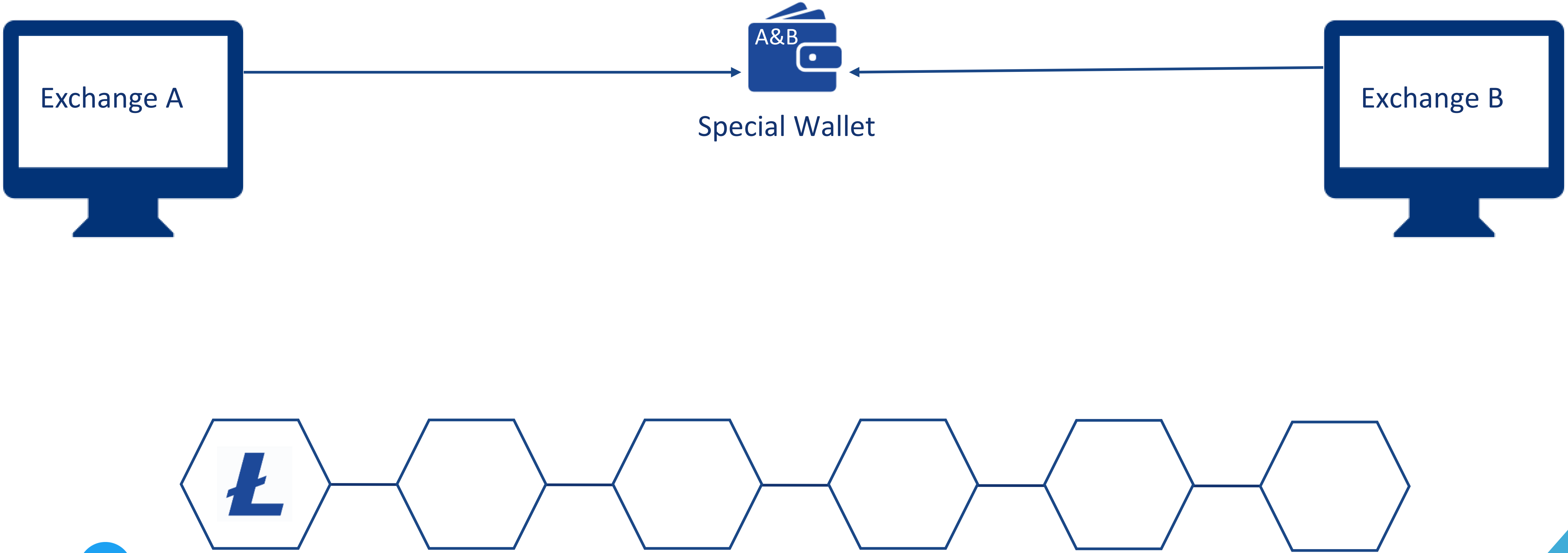
Payment Channels

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

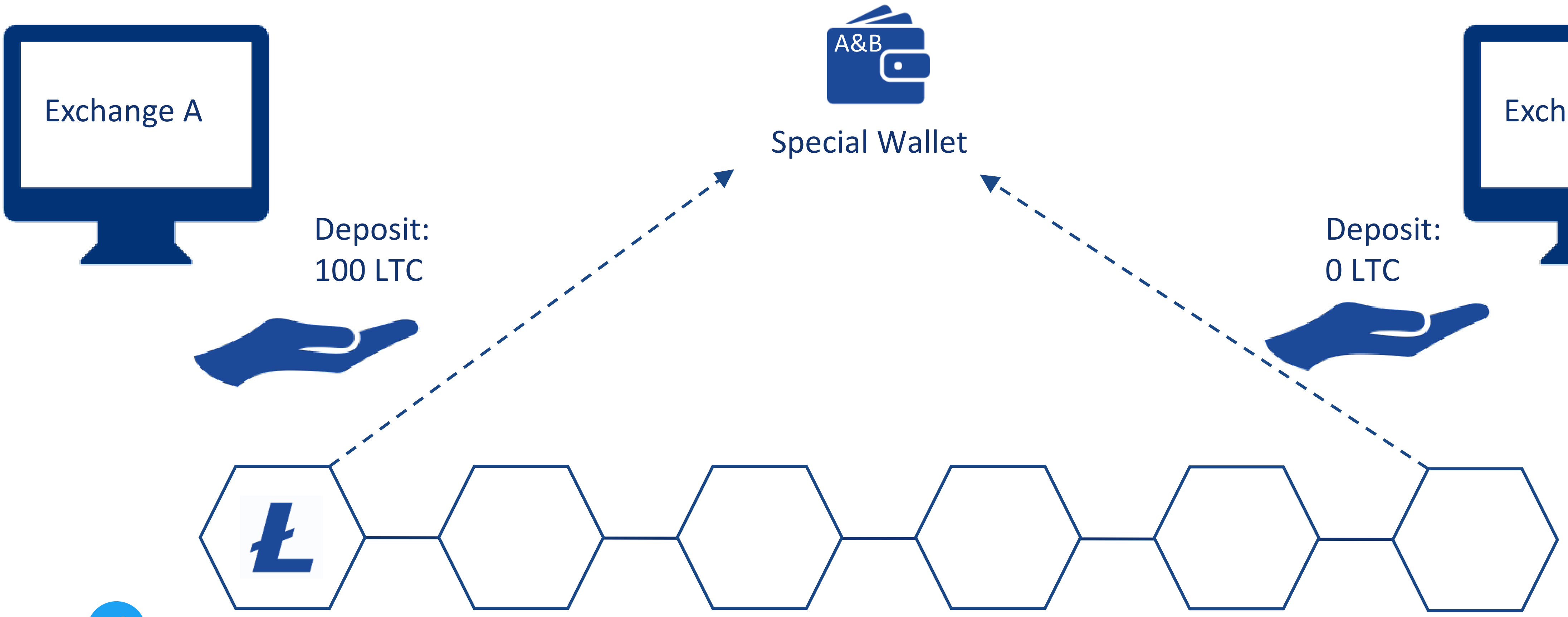
High–level:



@kilrau

Payment Channels

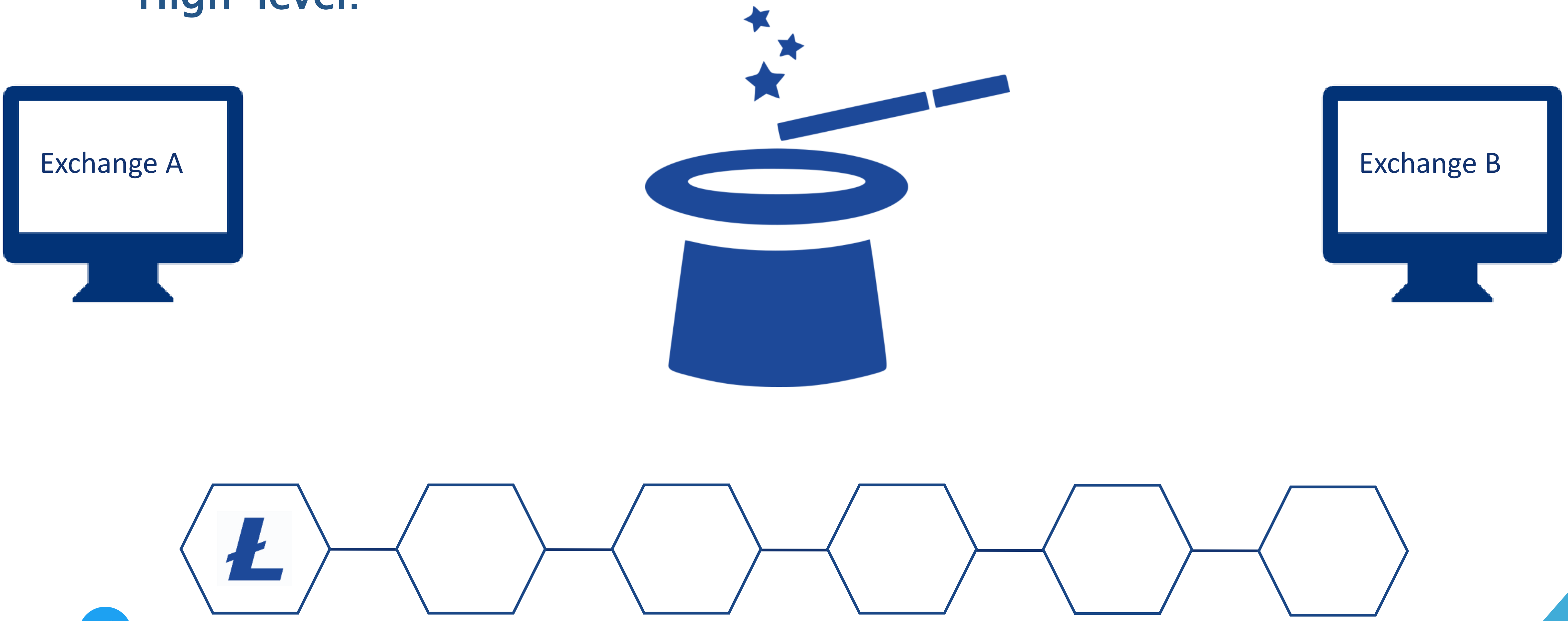
High–level:



@kilrau

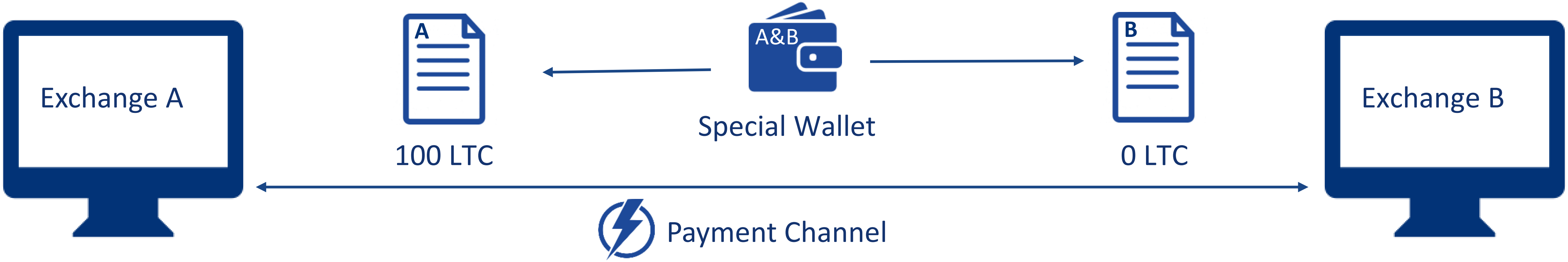
Payment Channels

High-level:



@kilrau

Payment Channels



Exchange A

A

100 LTC

A&B

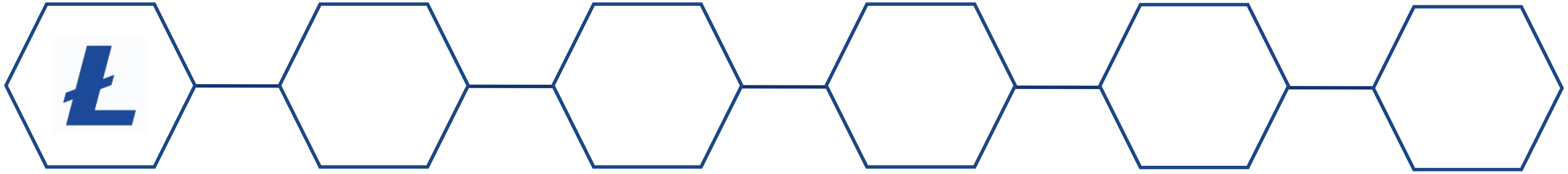
Special Wallet

B

0 LTC

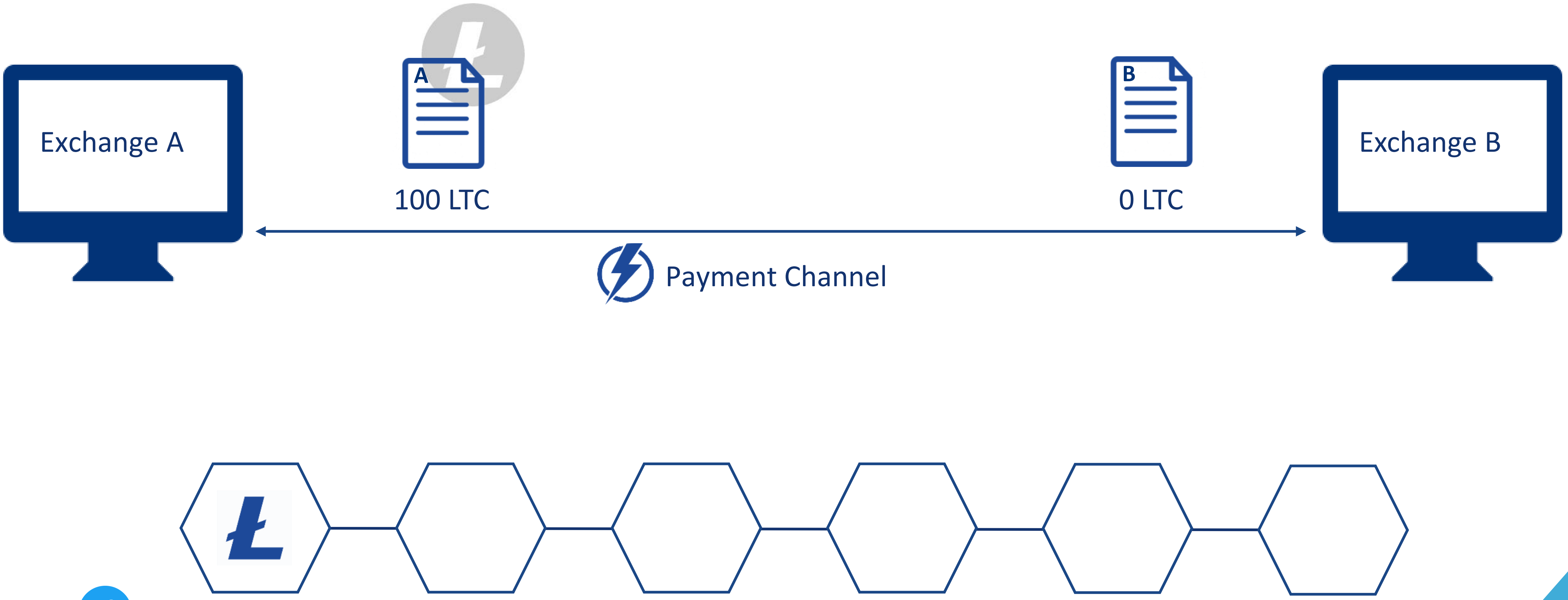
Exchange B

Payment Channel



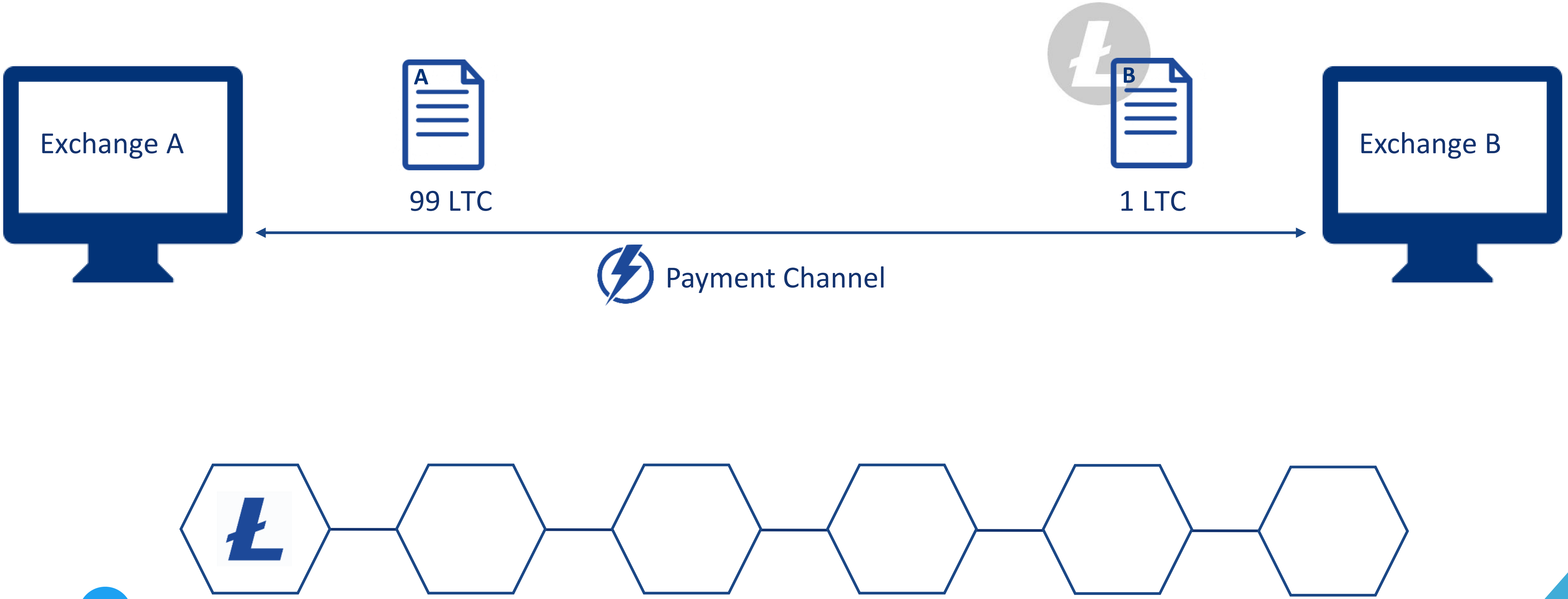
@kilrau

Payment Channels



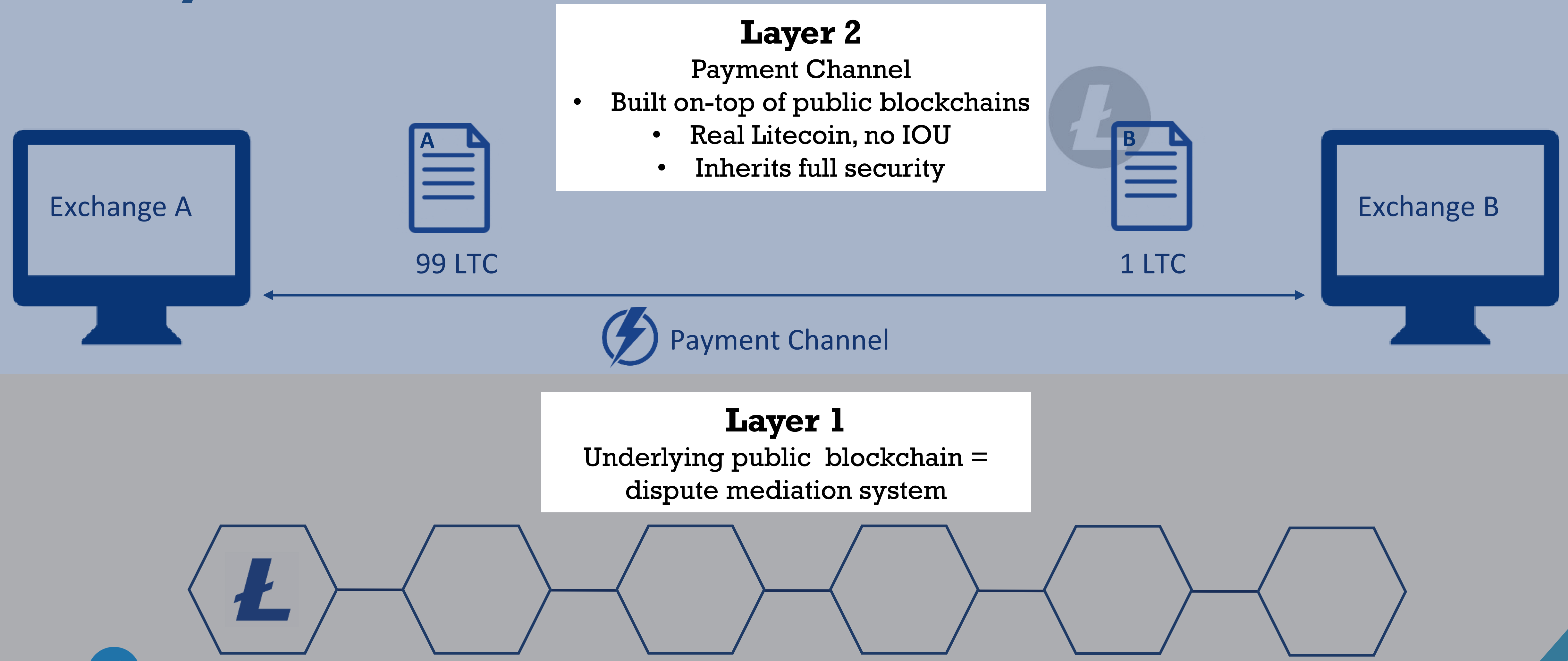
@kilrau

Payment Channels



@kilrau

Payment Channels



Layer 2

Payment Channel

- Built on-top of public blockchains
- Real Litecoin, no IOU
- Inherits full security

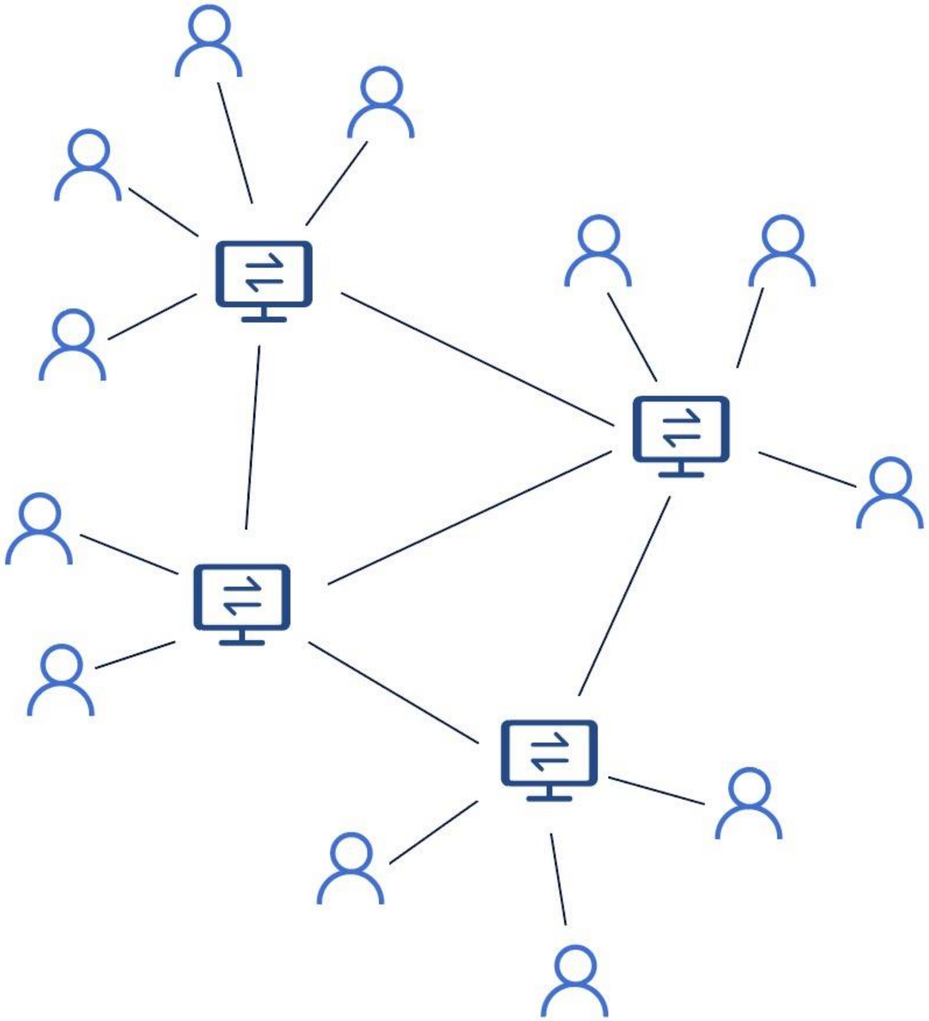
Layer 1

Underlying public blockchain =
dispute mediation system

@kilrau

Payment Channels

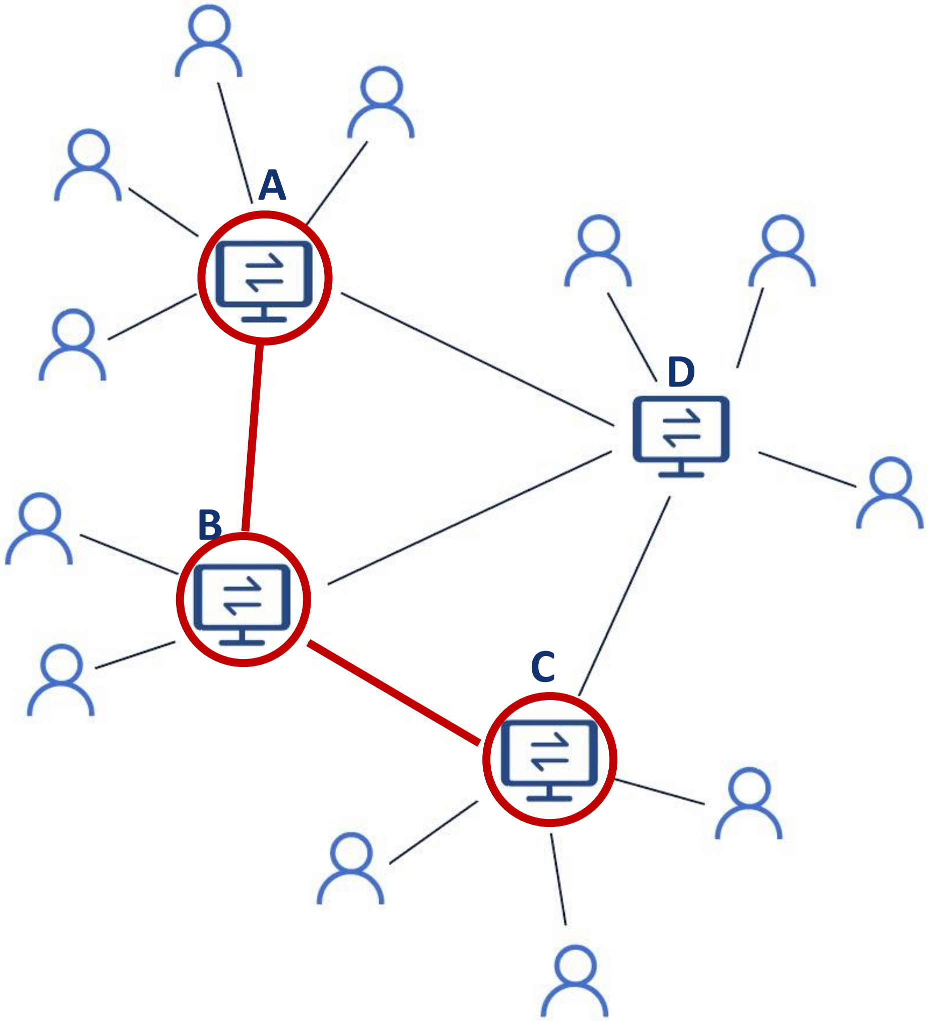
Routing:



@kilrau

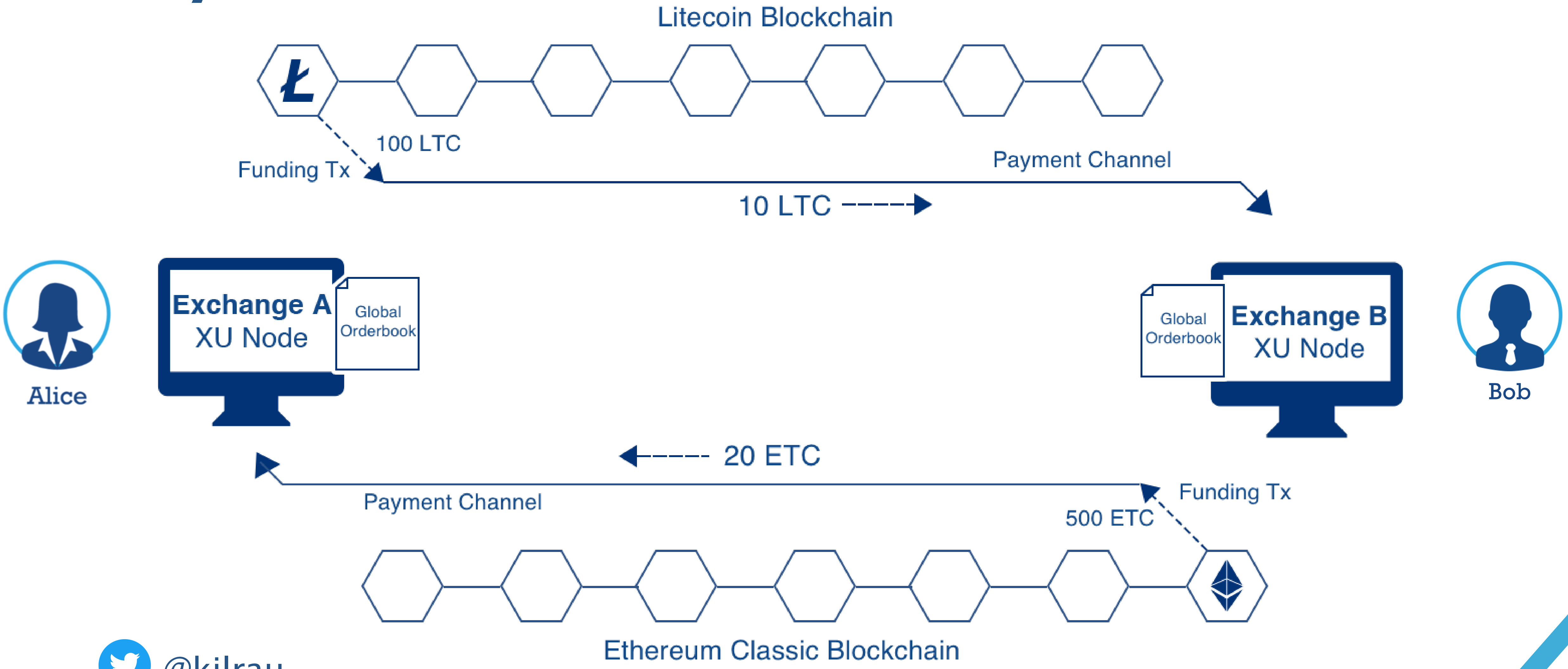
Payment Channels

Routing:



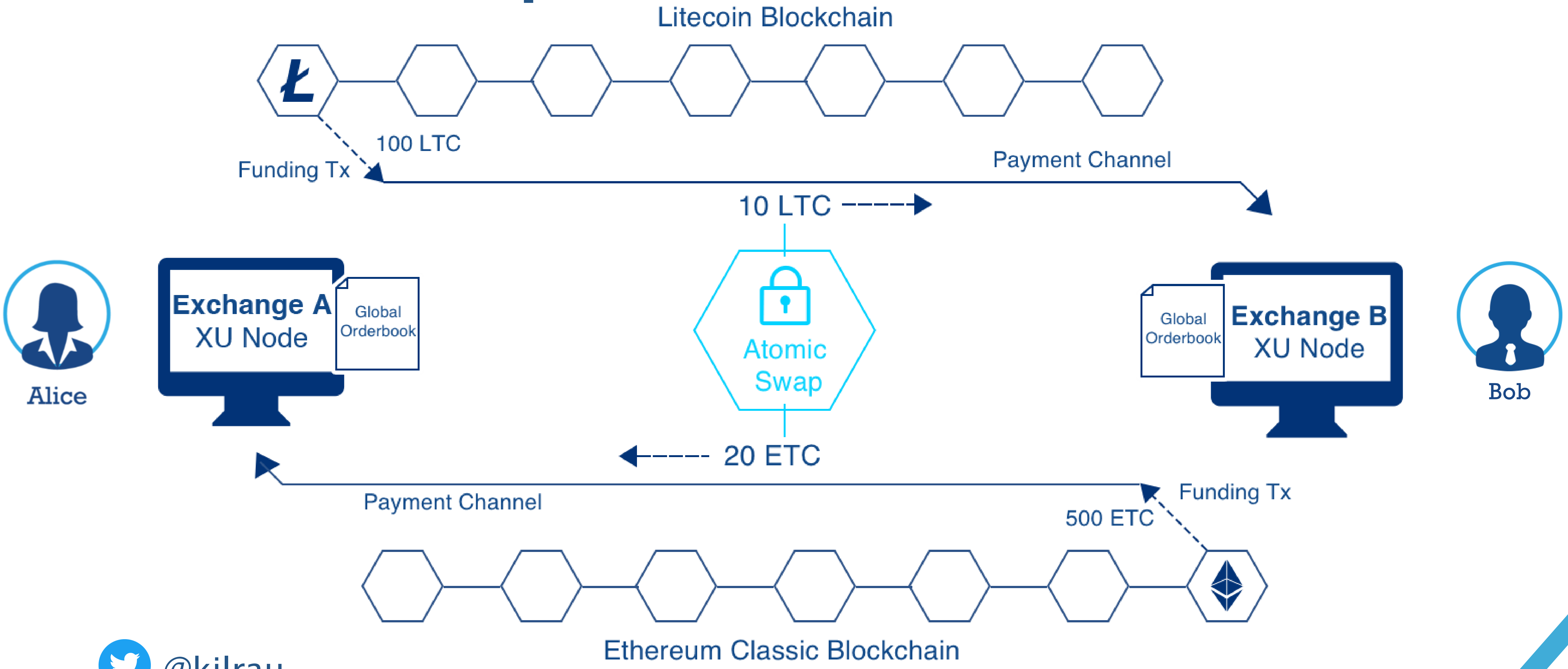
@kilrau

Payment Channels



@kilrau

Atomic Swaps



@kilrau

Atomic Swaps

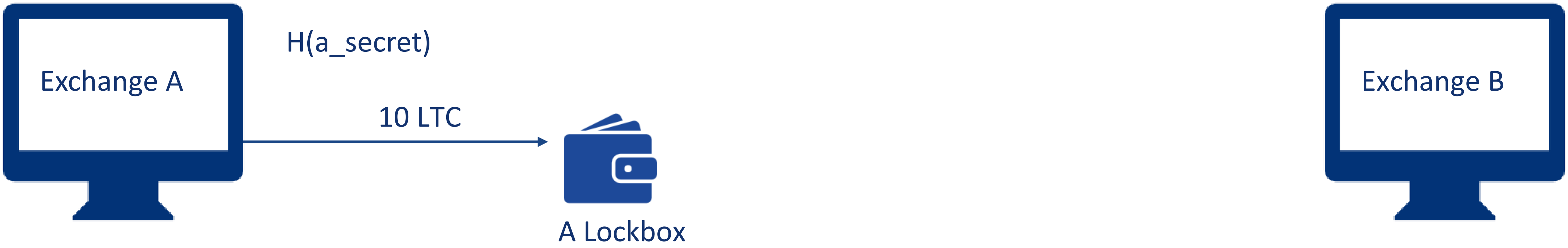
- Trustless exchange of two different assets
    - No middleman/escrow service needed
- How: guarantee atomicity
    - Both sides of the trade happen or not at all
    - Technology: Hashed TimeLock Contracts (HTLCs)

Atomic Swaps

Exchange A

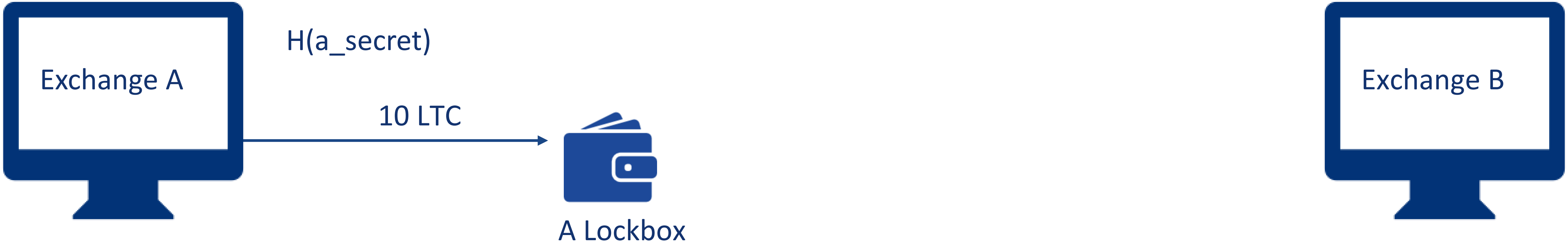
Exchange B

Atomic Swaps



@kilrau

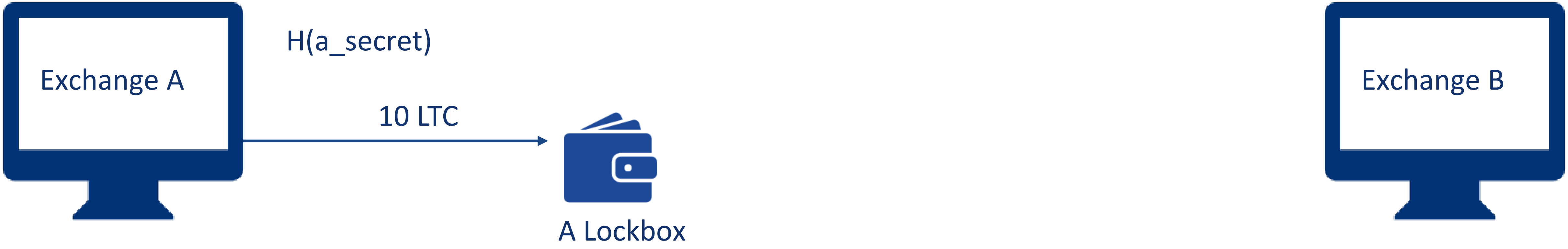
Atomic Swaps



Lockbox only opens with ‘a_secret’ + B’s signature

@kilrau

Atomic Swaps

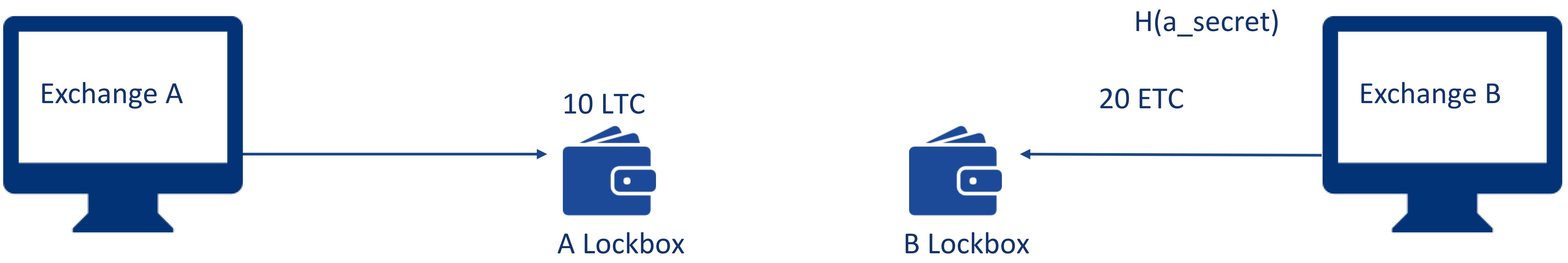


Lockbox only opens with ‘a_secret’ + B’s signature

HashLock

@kilrau

Atomic Swaps

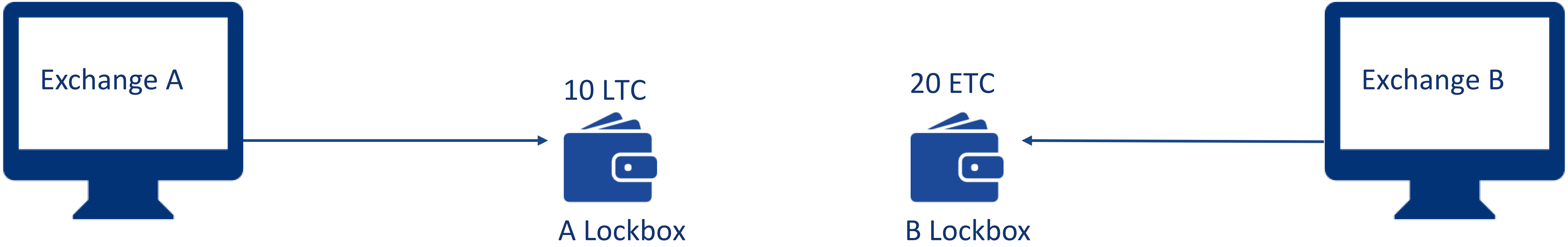


Lockbox only opens with **'a_secret'** + B's signature

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

@kilrau

Atomic Swaps



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

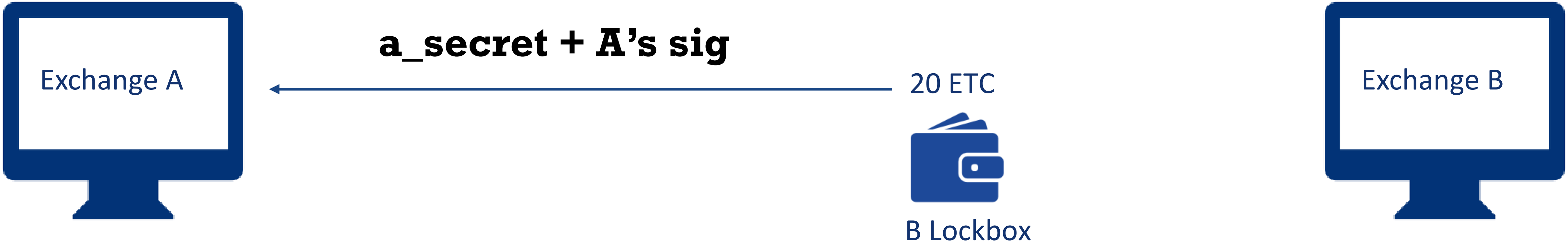
Lockbox only opens with **'a_secret'** + A's signature

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

@kilrau

Atomic Swaps

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



Exchange A

a_secret + A's sig

20 ETC

B Lockbox

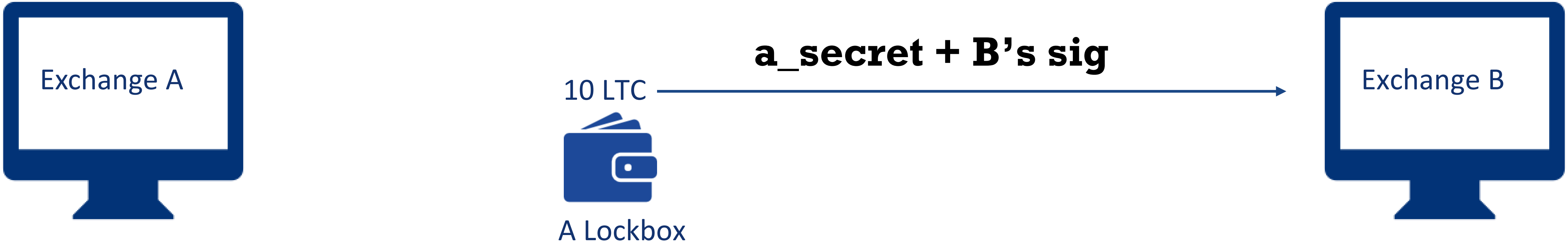
Exchange B

@kilrau

Atomic Swaps

Thx!
a_secret
Exchange A
Exchange B

Atomic Swaps



Exchange A

a_secret + B's sig

10 LTC

A Lockbox

Exchange B

@kilrau

Atomic Swaps

Exchange A

20 ETC

10 LTC

Exchange B

Atomic Swaps

Exchange A

20 ETC

10 LTC

Exchange B

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

Atomic Swaps

Exchange A

20 ETC

10 LTC

Exchange B

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

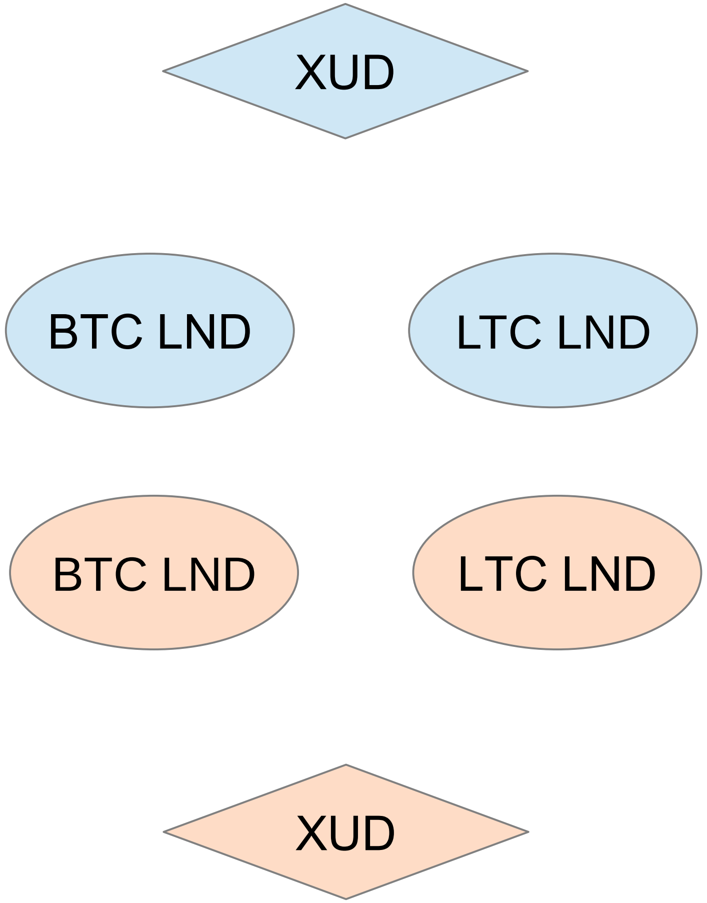
Hashed TimeLock Contracts
Via BIP199 on Bitcoin and SmartContracts on Ethereum

How XUD handles Atomic Swaps

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

@kilrau

How XUD handles Atomic Swaps

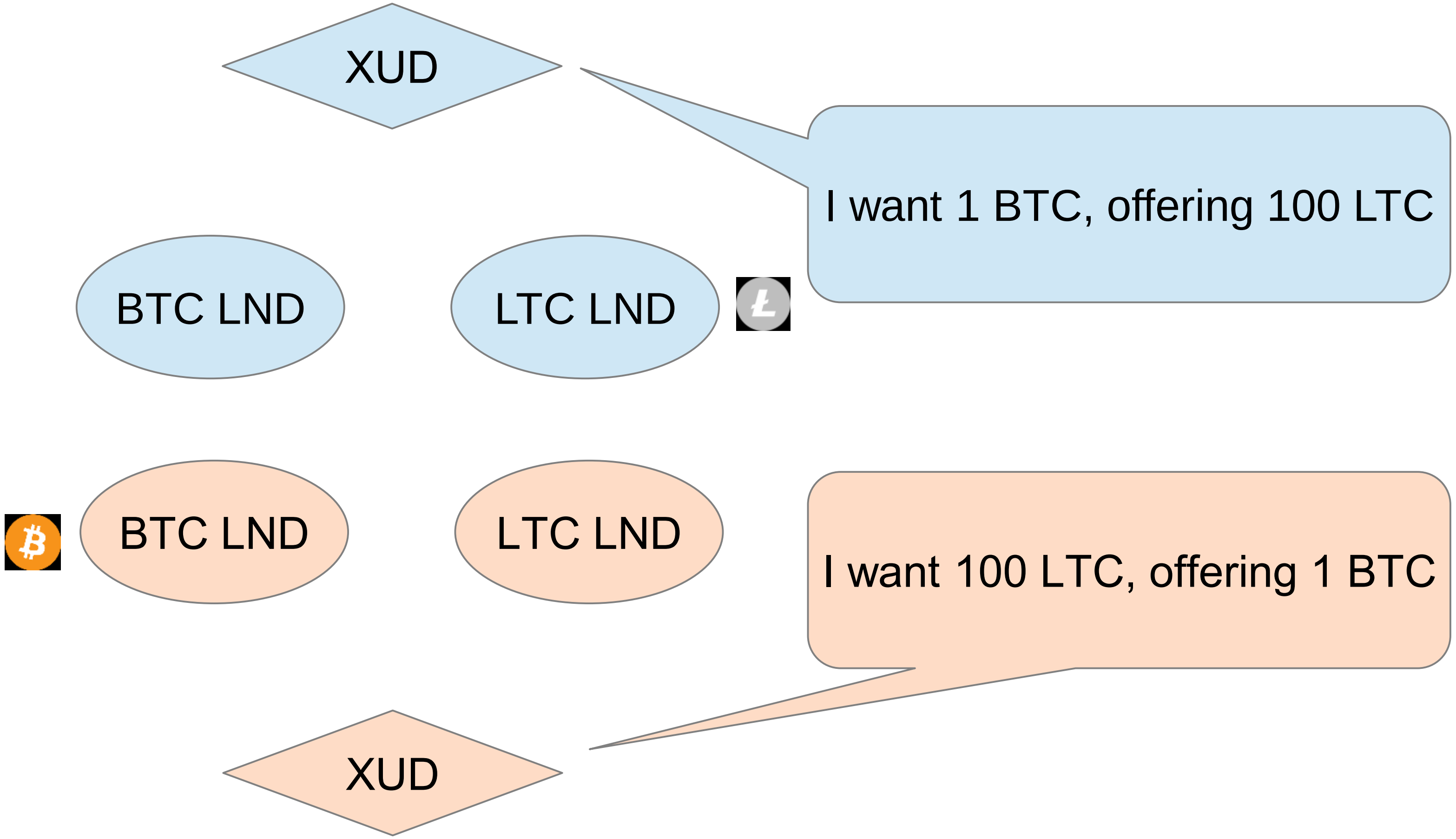


The Setup

- 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.

@kilrau

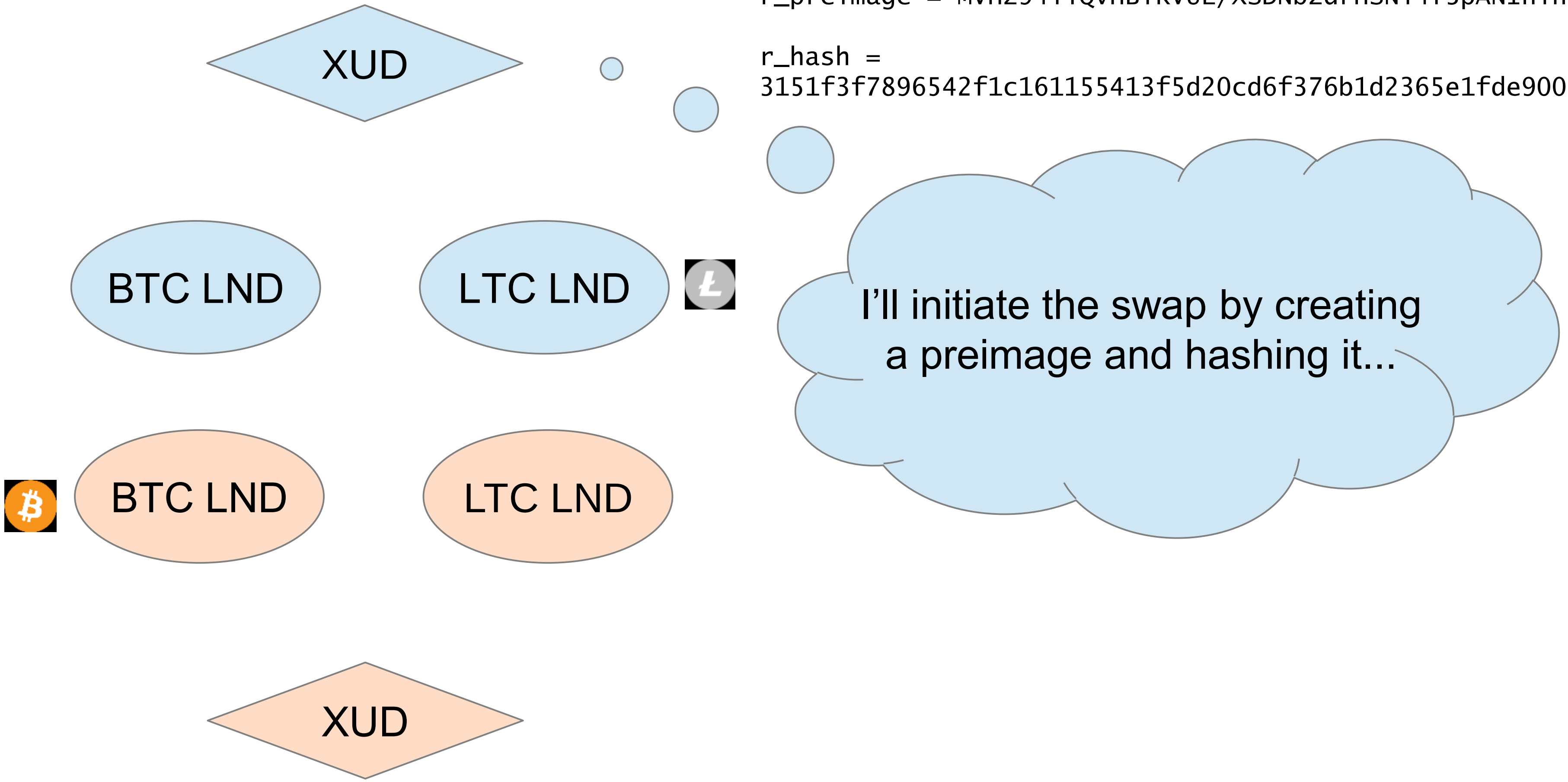
How XUD handles Atomic Swaps


XUD
I want 1 BTC, offering 100 LTC
BTC LND
LTC LND
BTC LND
LTC LND
I want 100 LTC, offering 1 BTC
XUD

@kilrau

XUD, The Software

```
r_preimage = MVHz94llQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

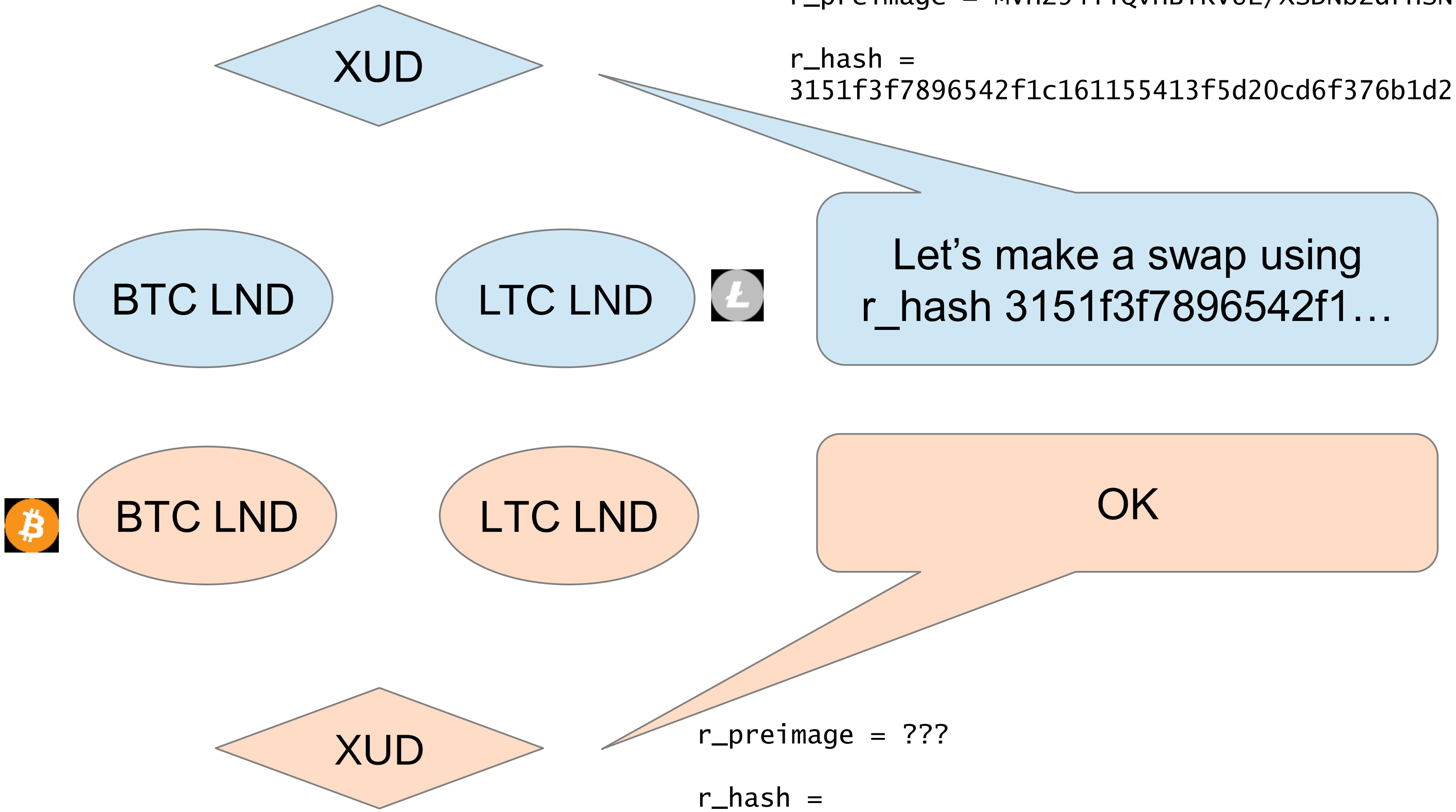


I'll initiate the swap by creating a preimage and hashing it...

@kilrau

XUD, The Software

```
r_preimage = MVHz94llQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```



XUD

BTC LND

LTC LND

Let’s make a swap using r_hash 3151f3f7896542f1…

BTC LND

LTC LND

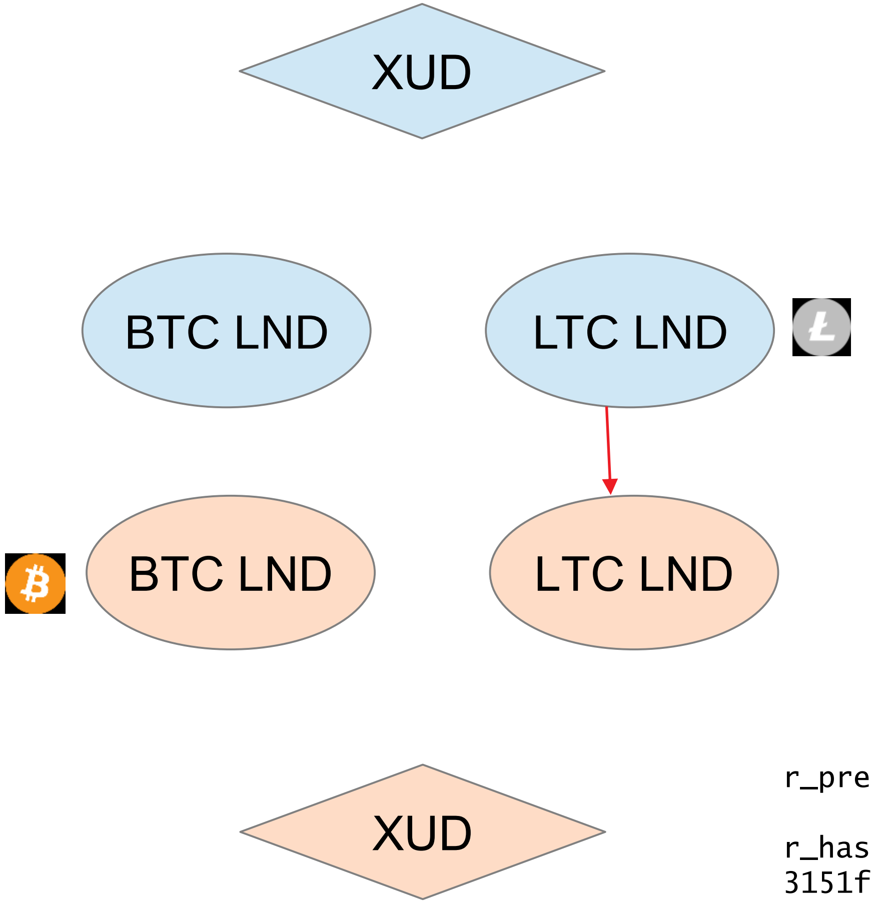
OK

XUD

```
r_preimage = ???

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

@kilrau

XUD, The Software



```
r_preimage = MVHz94llQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

Pending HTLC

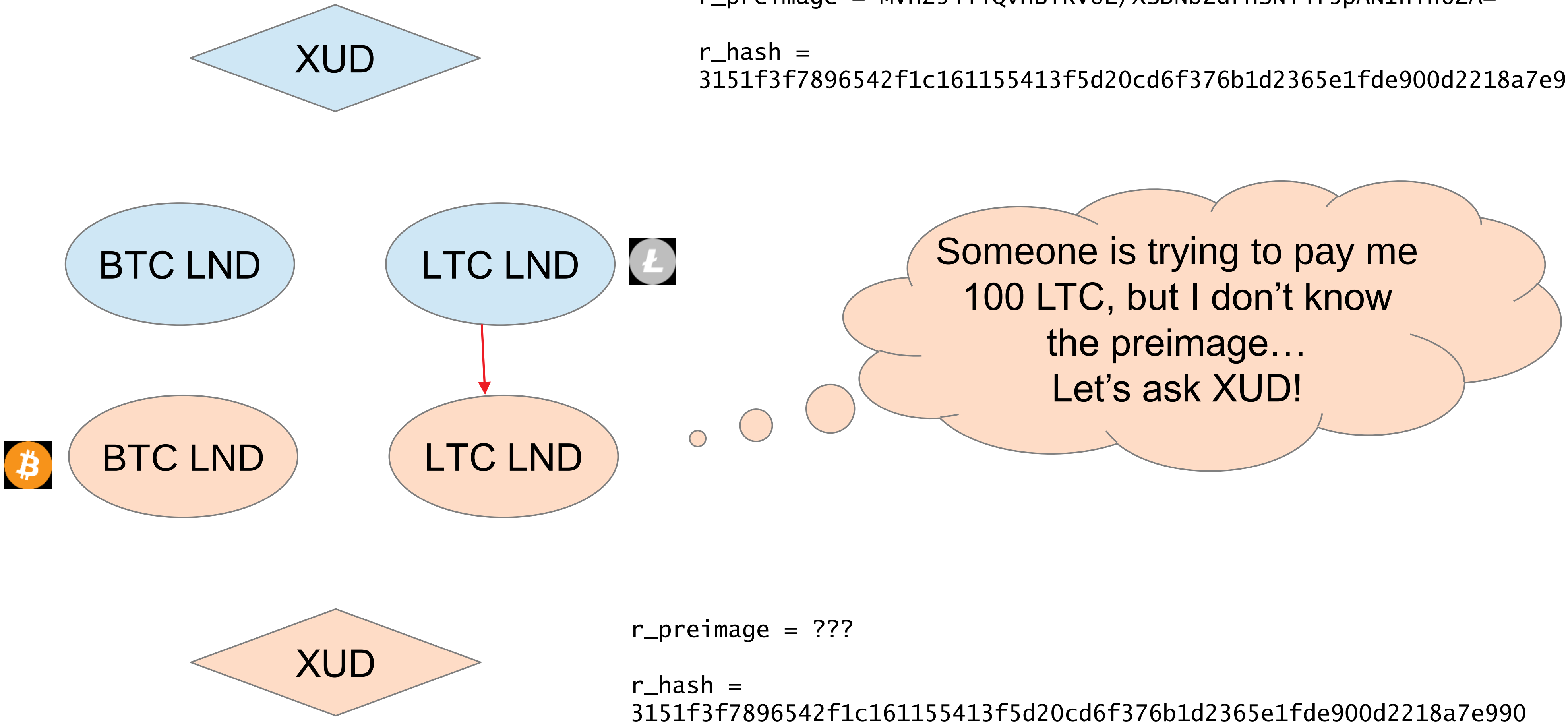
amount - 100 LTC
r_hash - 3151f3f7896542f1…

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

```
r_preimage = ???

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

@kilrau

XUD, The Software



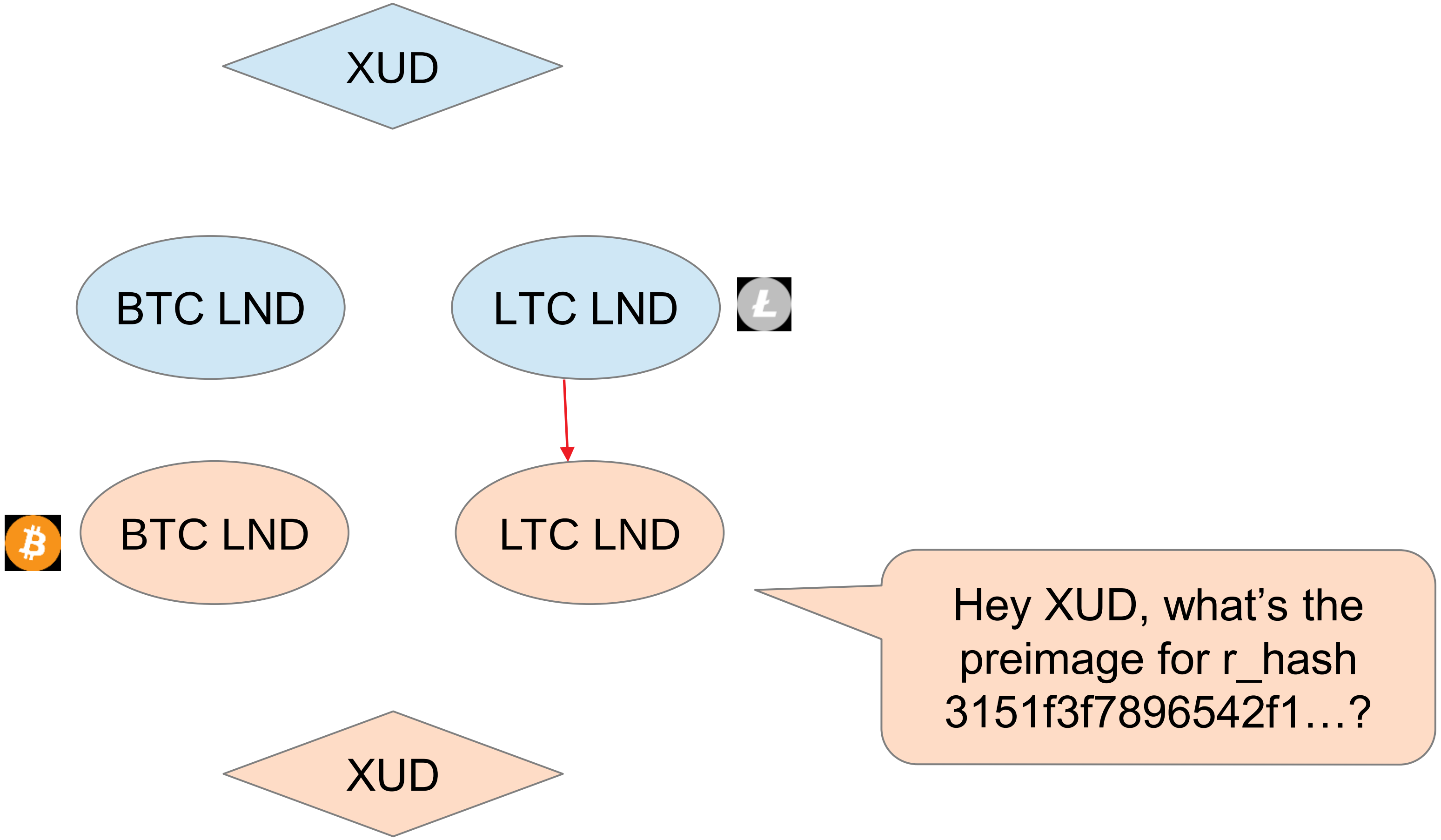
Someone is trying to pay me 100 LTC, but I don't know the preimage…
Let's ask XUD!

```
r_preimage = MVHz94llQvHBYRVUE/XSDNbzdrHSNl4f3pANIhin6ZA=

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

```
r_preimage = ???

r_hash =
3151f3f7896542f1c161155413f5d20cd6f376b1d2365e1fde900d2218a7e990
```

@kilrau

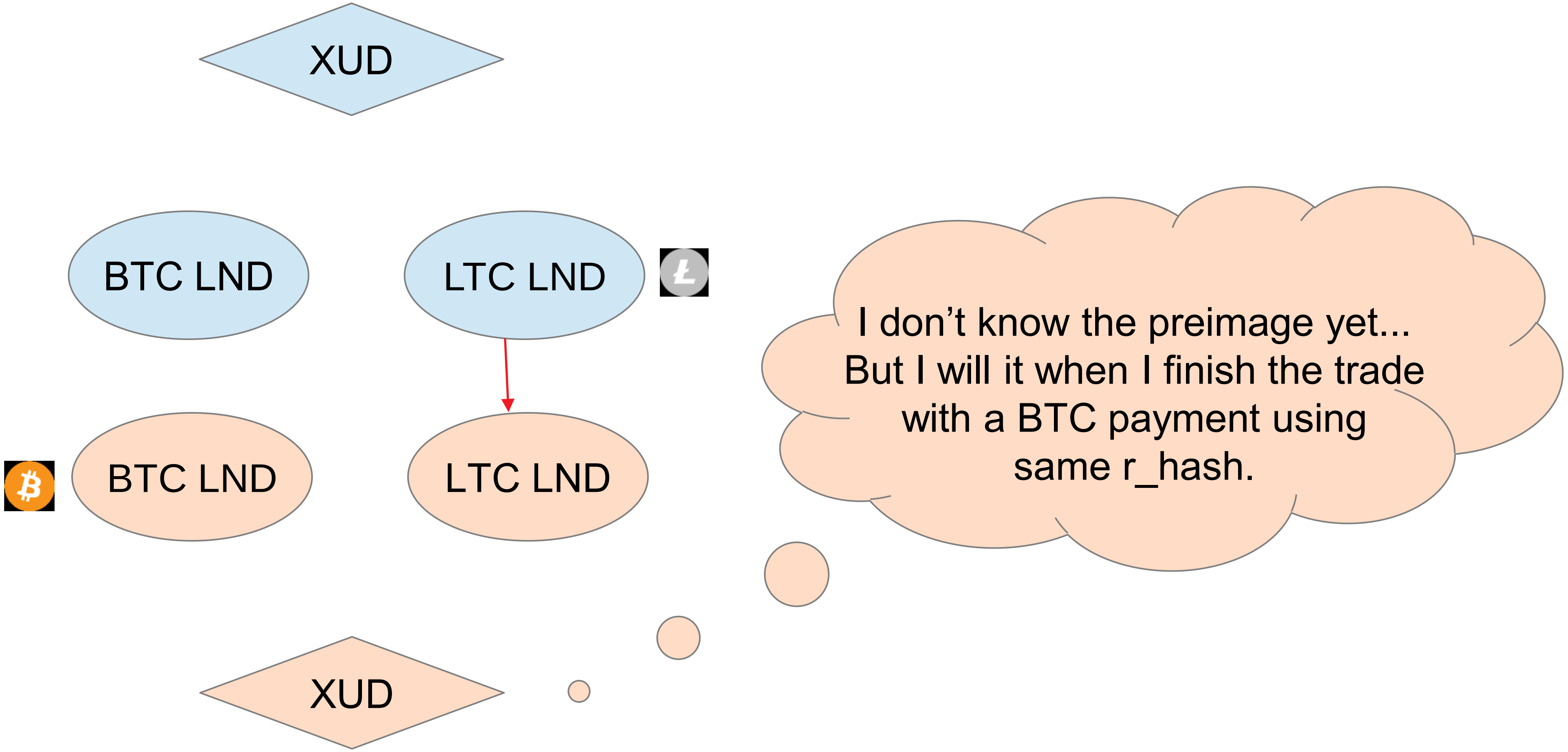
XUD, The Software



Hey XUD, what’s the preimage for r_hash 3151f3f7896542f1…?

@kilrau

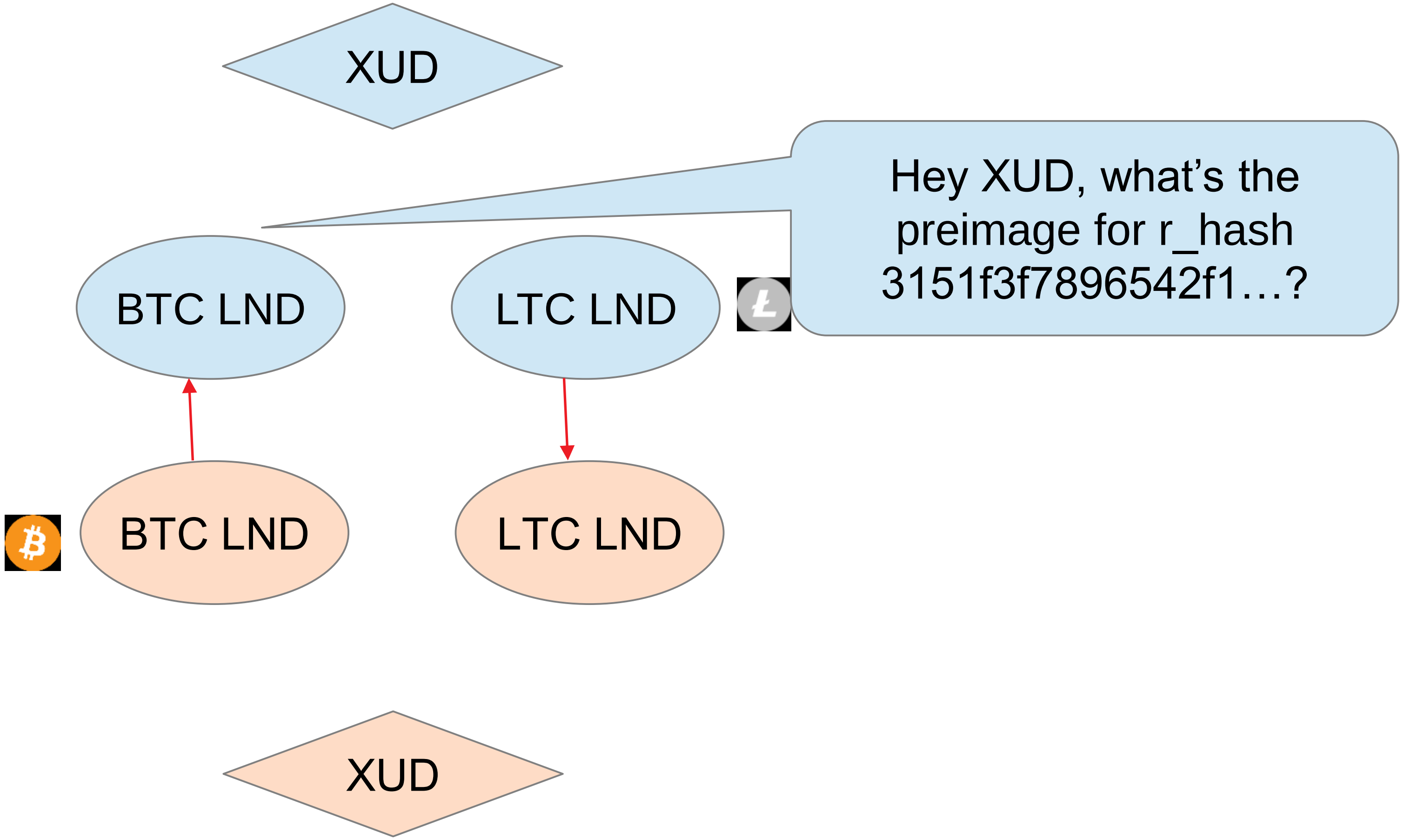
XUD, The Software



I don’t know the preimage yet...
But I will it when I finish the trade
with a BTC payment using
same r_hash.

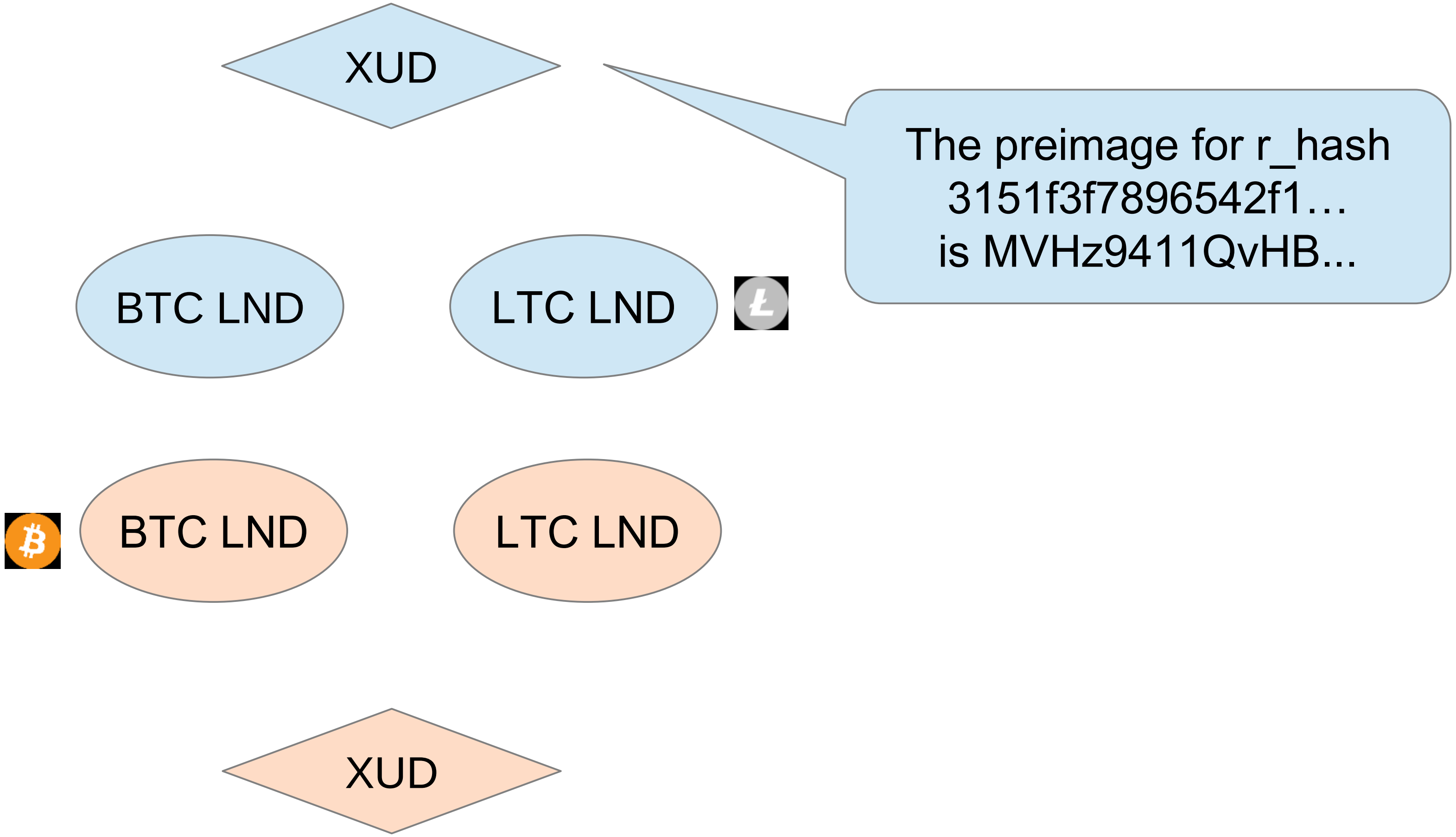
@kilrau

XUD, The Software



@kilrau

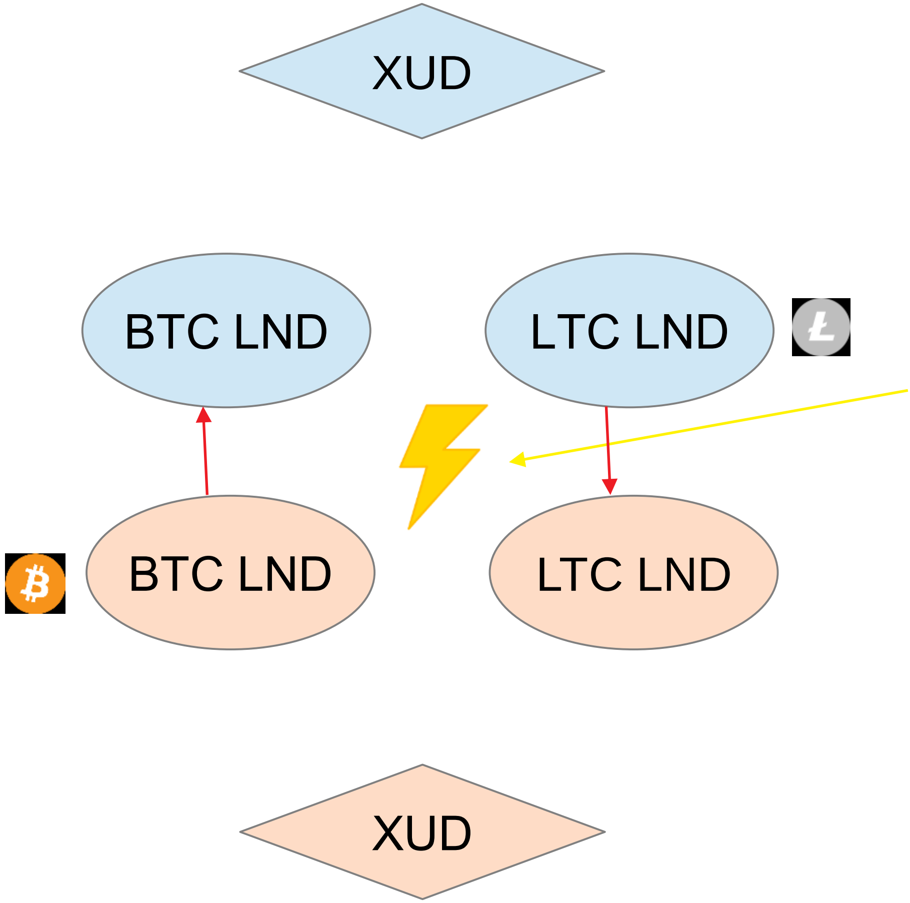
XUD, The Software



The preimage for r_hash
3151f3f7896542f1…
is MVHz9411QvHB...

@kilrau

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

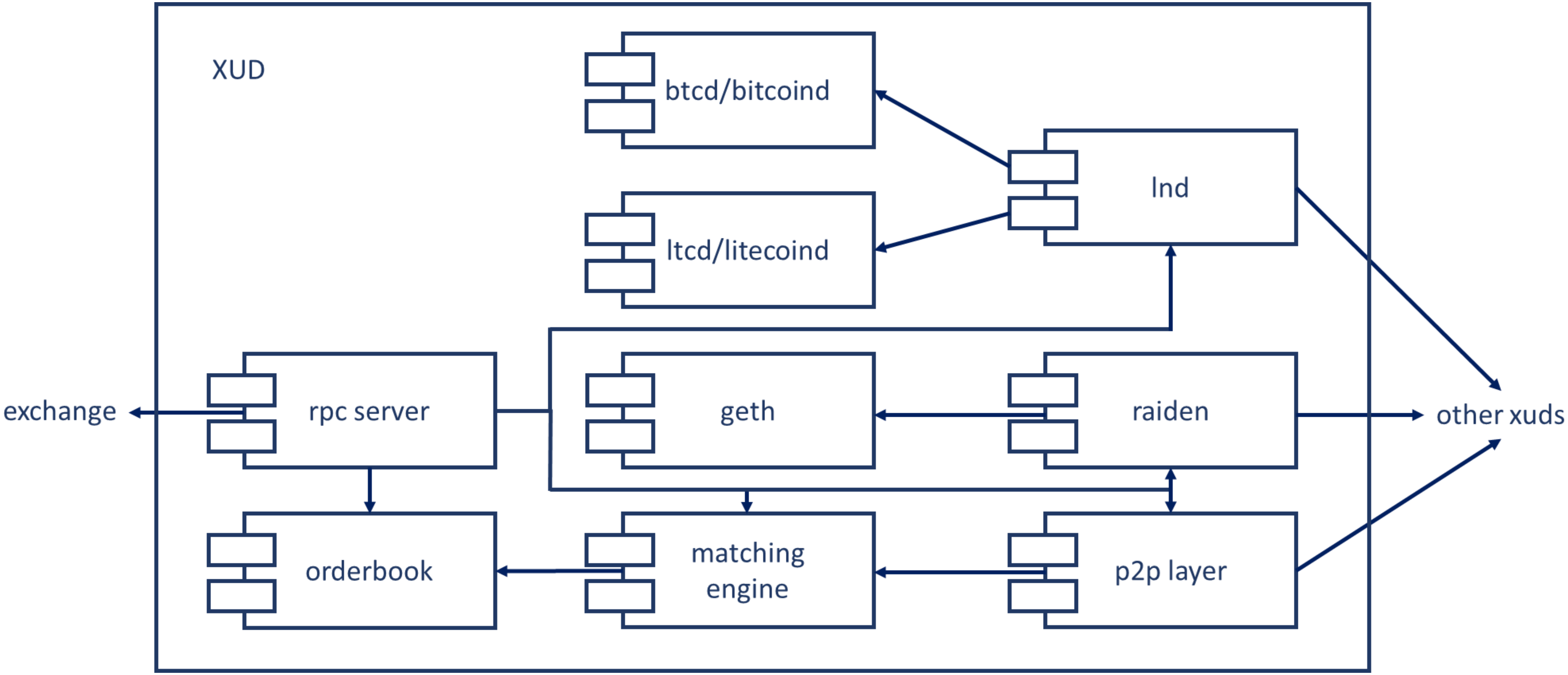
@kilrau

DIY

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

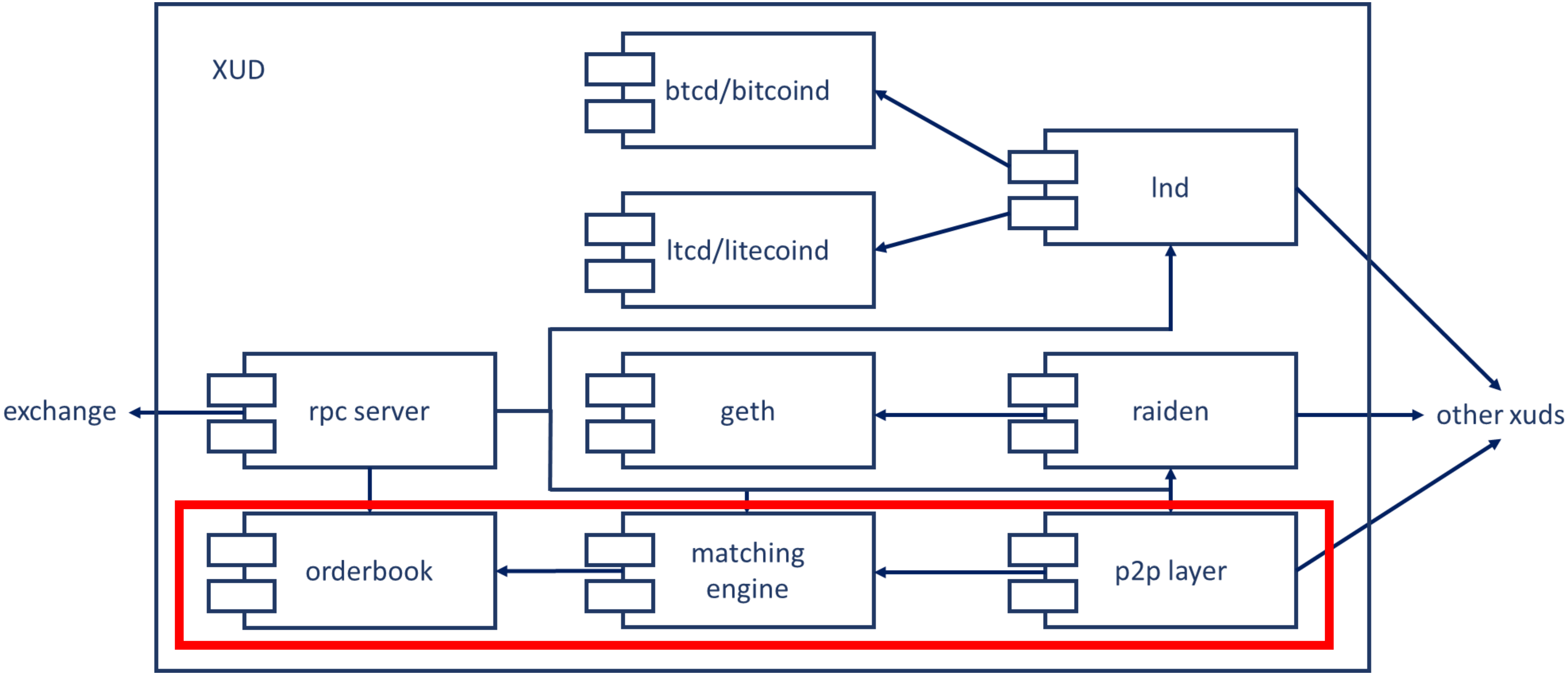
@kilrau

XUD, The Software



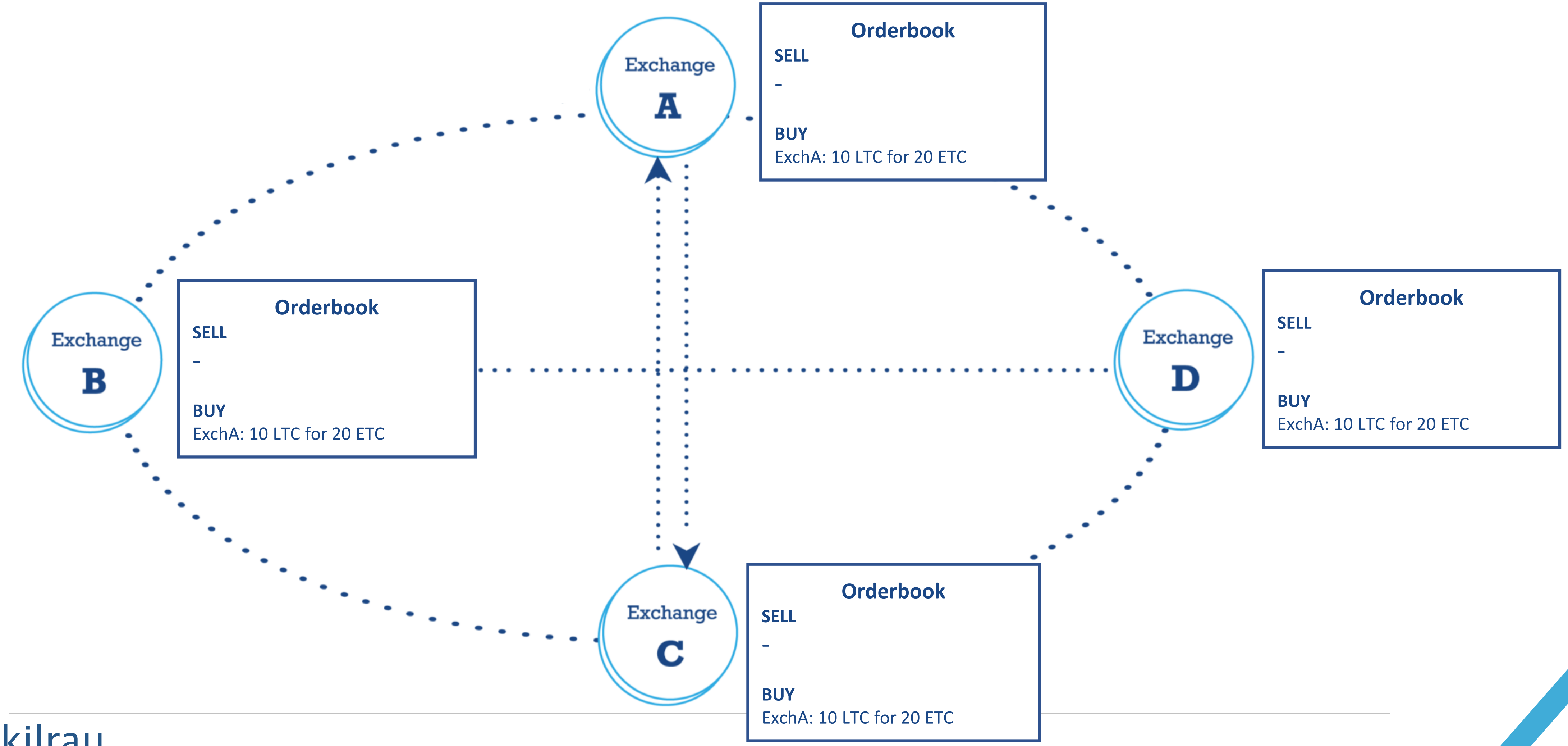
@kilrau

XUD, The Software



@kilrau

Decentralized Orderbook



Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

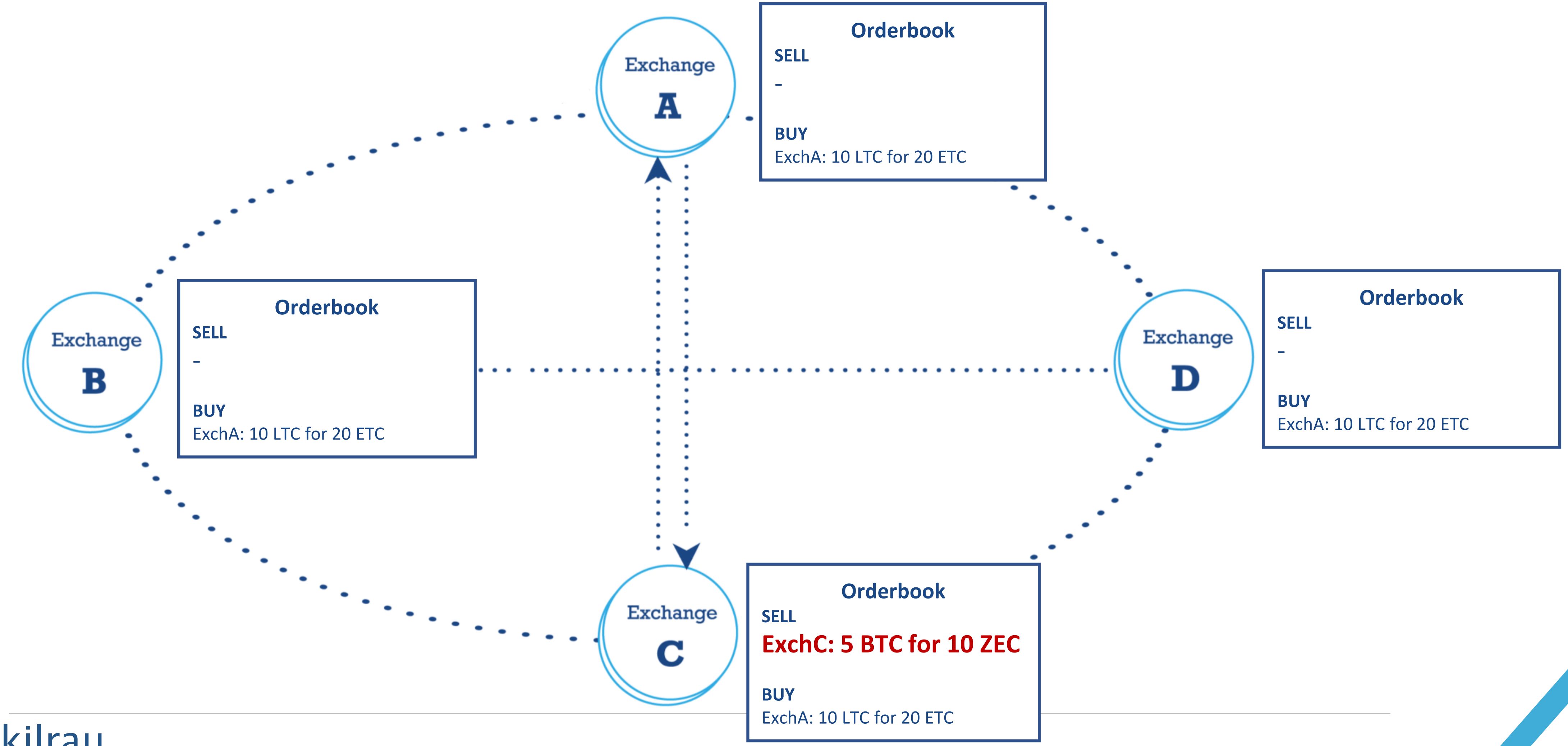
SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Decentralized Orderbook



Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

–

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

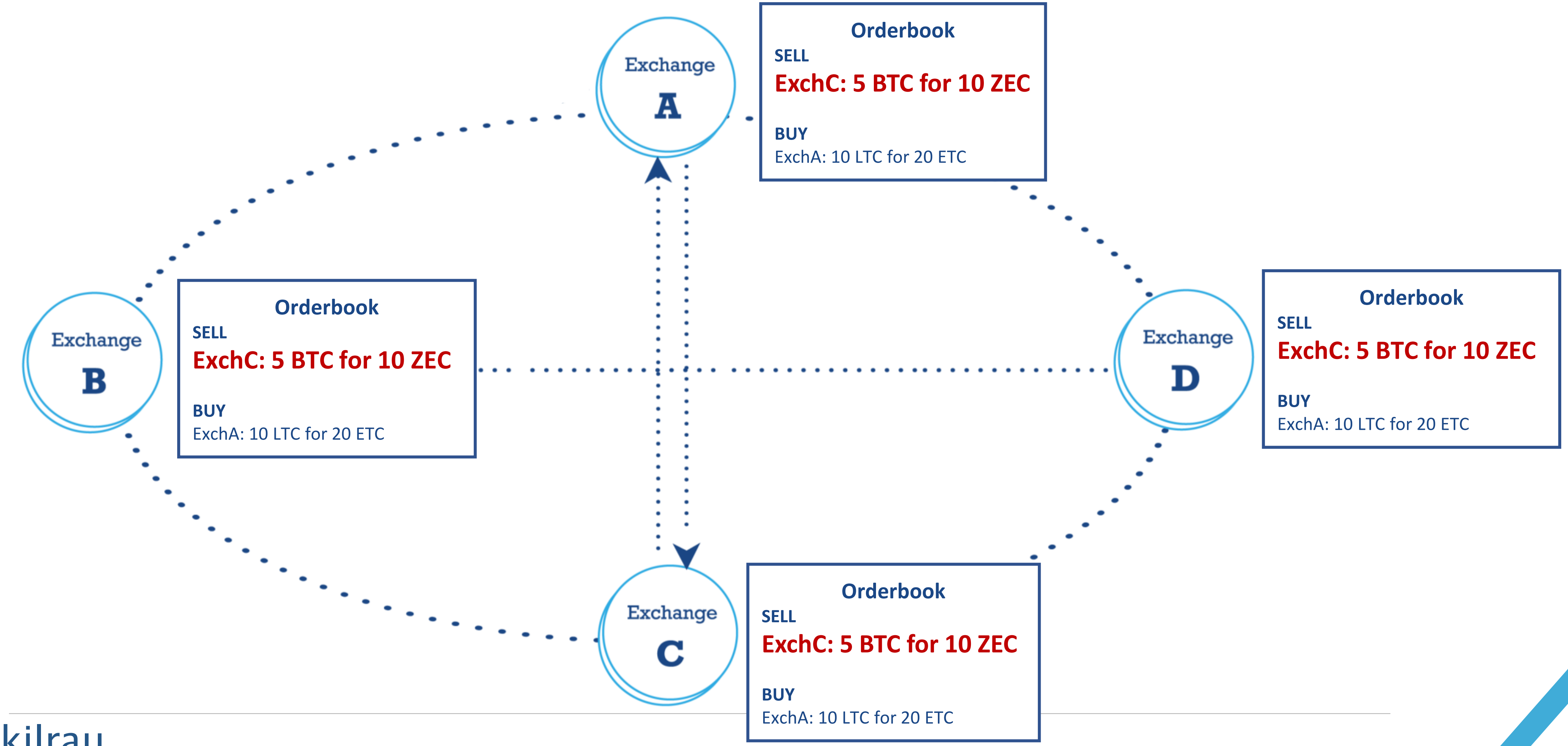
SELL

ExchC: 5 BTC for 10 ZEC

BUY

ExchA: 10 LTC for 20 ETC

Decentralized Orderbook



Orderbook

SELL

ExchC: 5 BTC for 10 ZEC

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

ExchC: 5 BTC for 10 ZEC

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

ExchC: 5 BTC for 10 ZEC

BUY

ExchA: 10 LTC for 20 ETC

Orderbook

SELL

ExchC: 5 BTC for 10 ZEC

BUY

ExchA: 10 LTC for 20 ETC

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

@kilrau

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.

@kilrau

We are hiring

exchangeunion.com

gitter.im/exchangeunion

github.com/exchangeunion

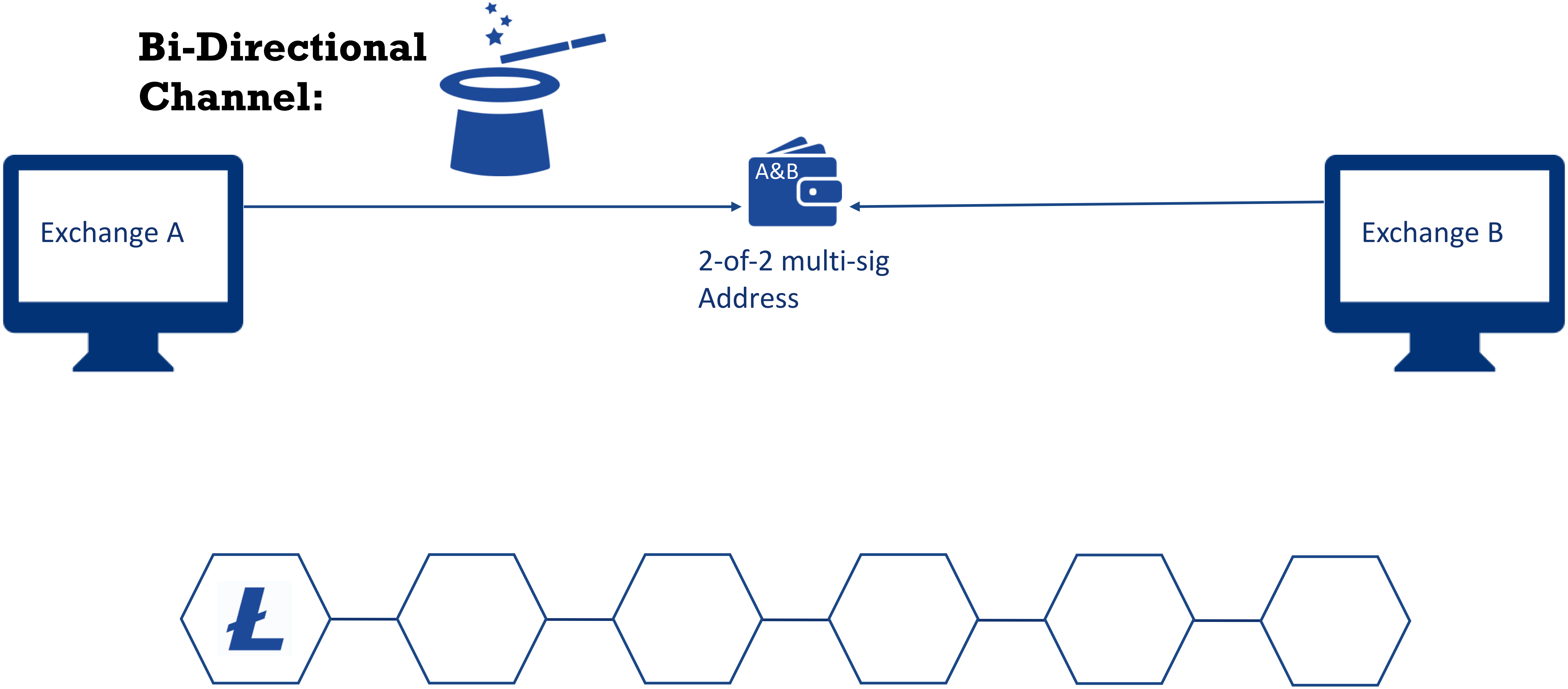
@exchange_union

BitcoNNEEECT!

Backup

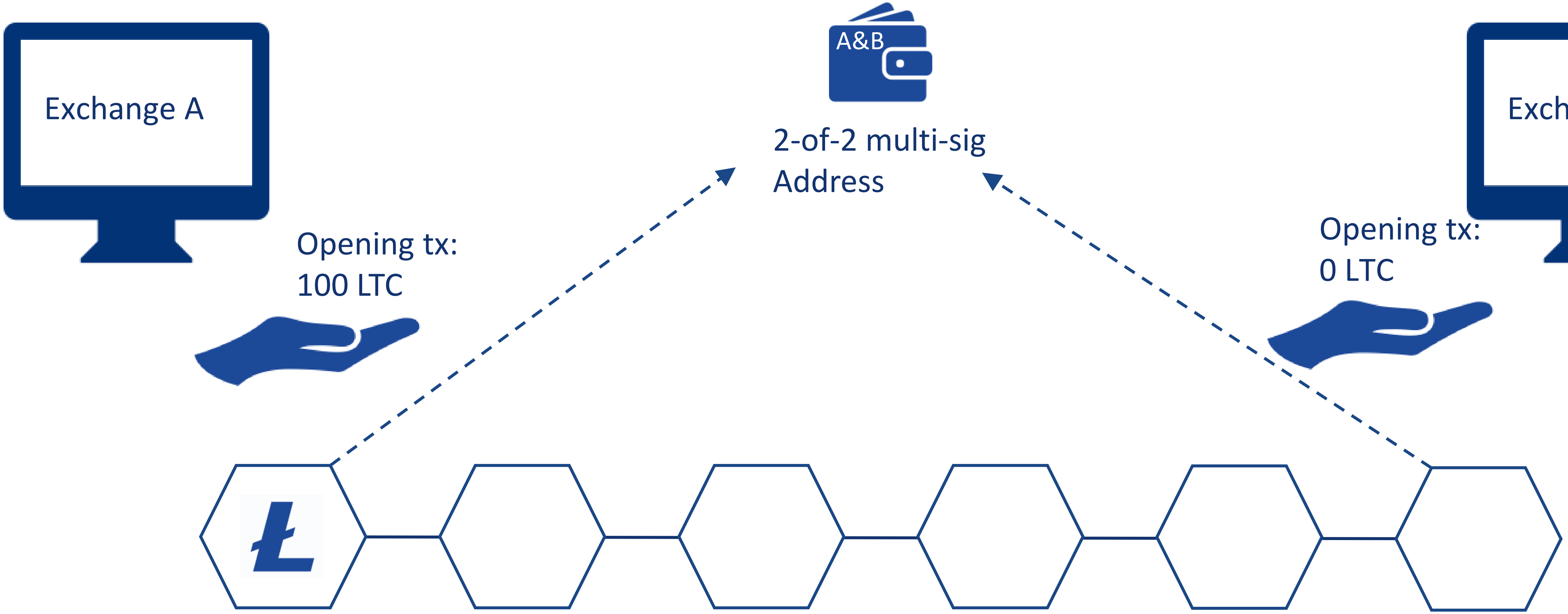
1. Payment Channels

Bi-Directional Channel:



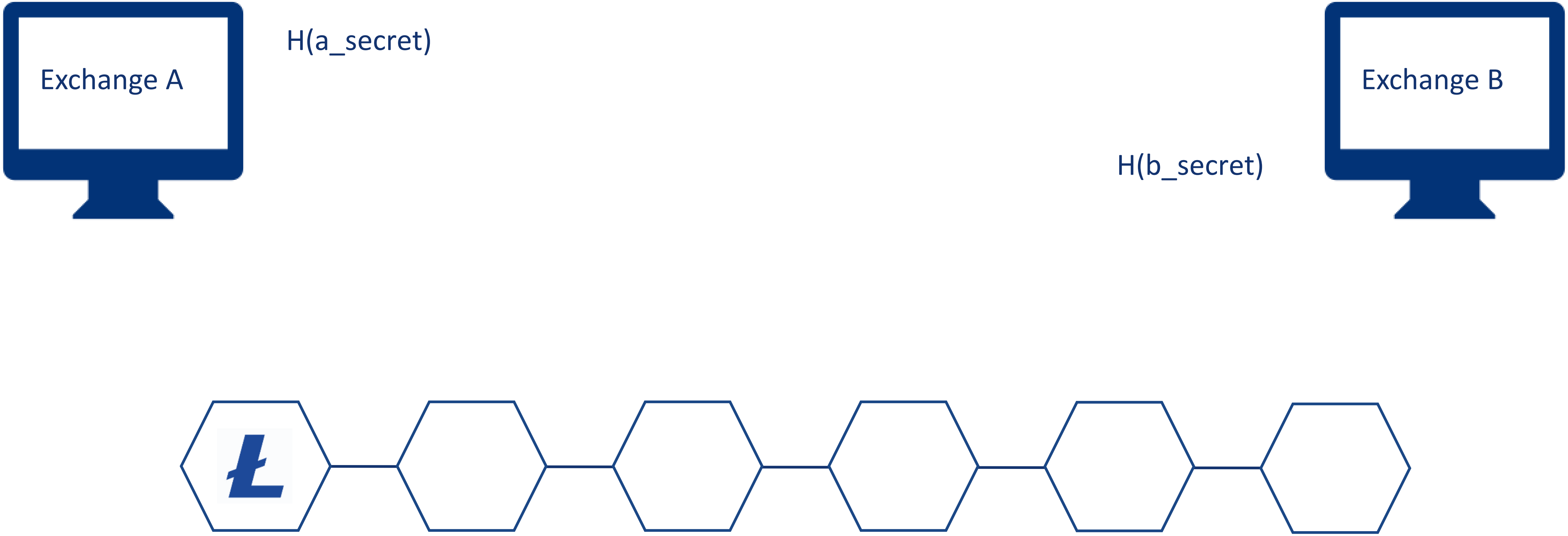
1. Payment Channels

Bi-Directional Channel:



1. Payment Channels

Bi-Directional Channel:



Exchange A

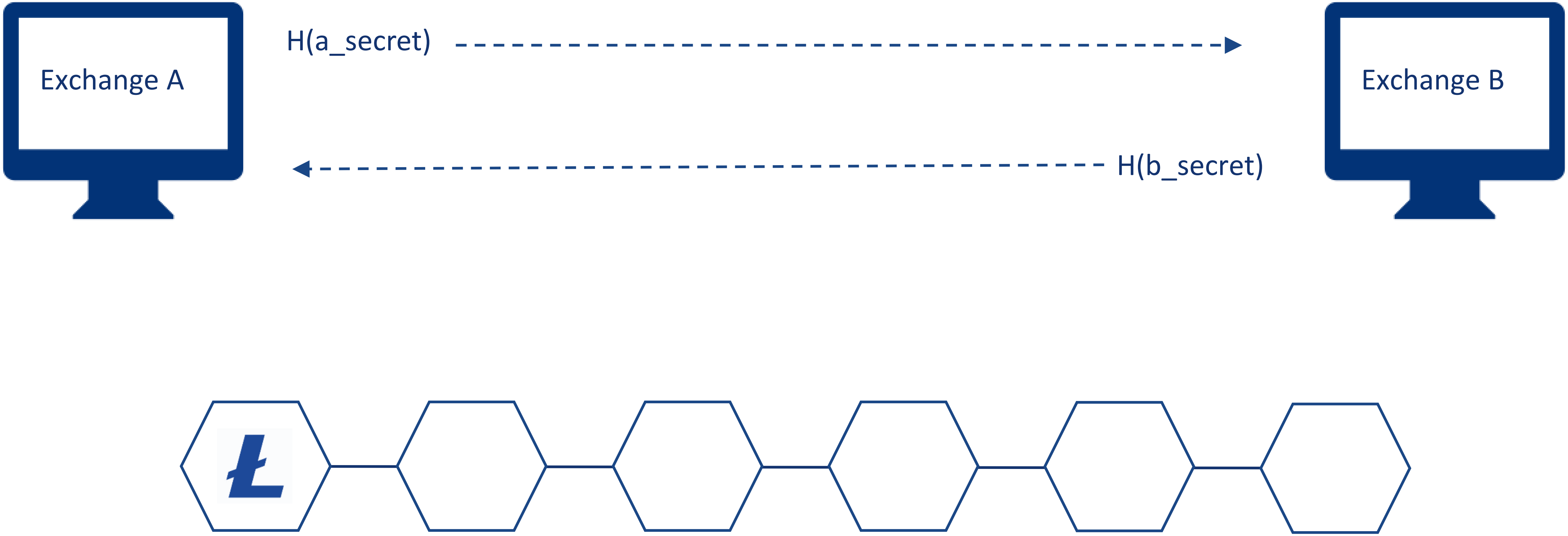
H(a_secret)

Exchange B

H(b_secret)

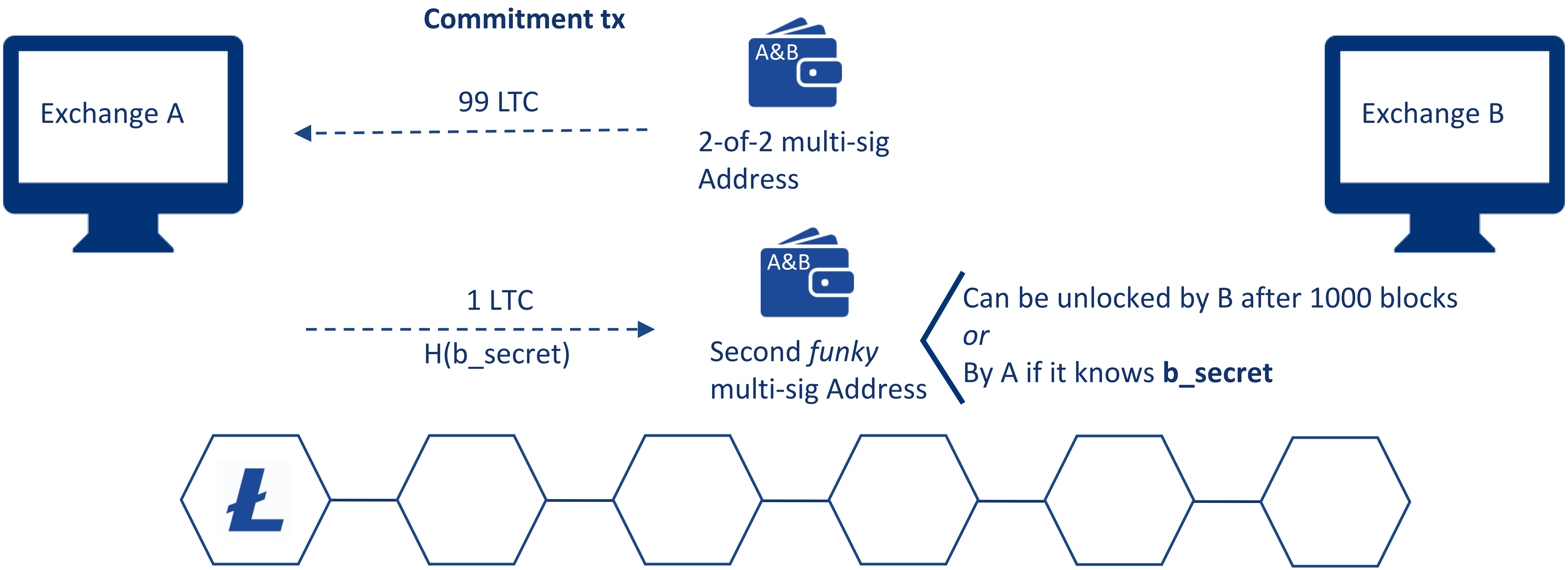
1. Payment Channels

Bi-Directional Channel:



1. Payment Channels

Bi-Directional Channel:



Commitment tx

Exchange A

99 LTC

2-of-2 multi-sig Address

Exchange B

1 LTC

H(b_secret)

Second *funky* multi-sig Address

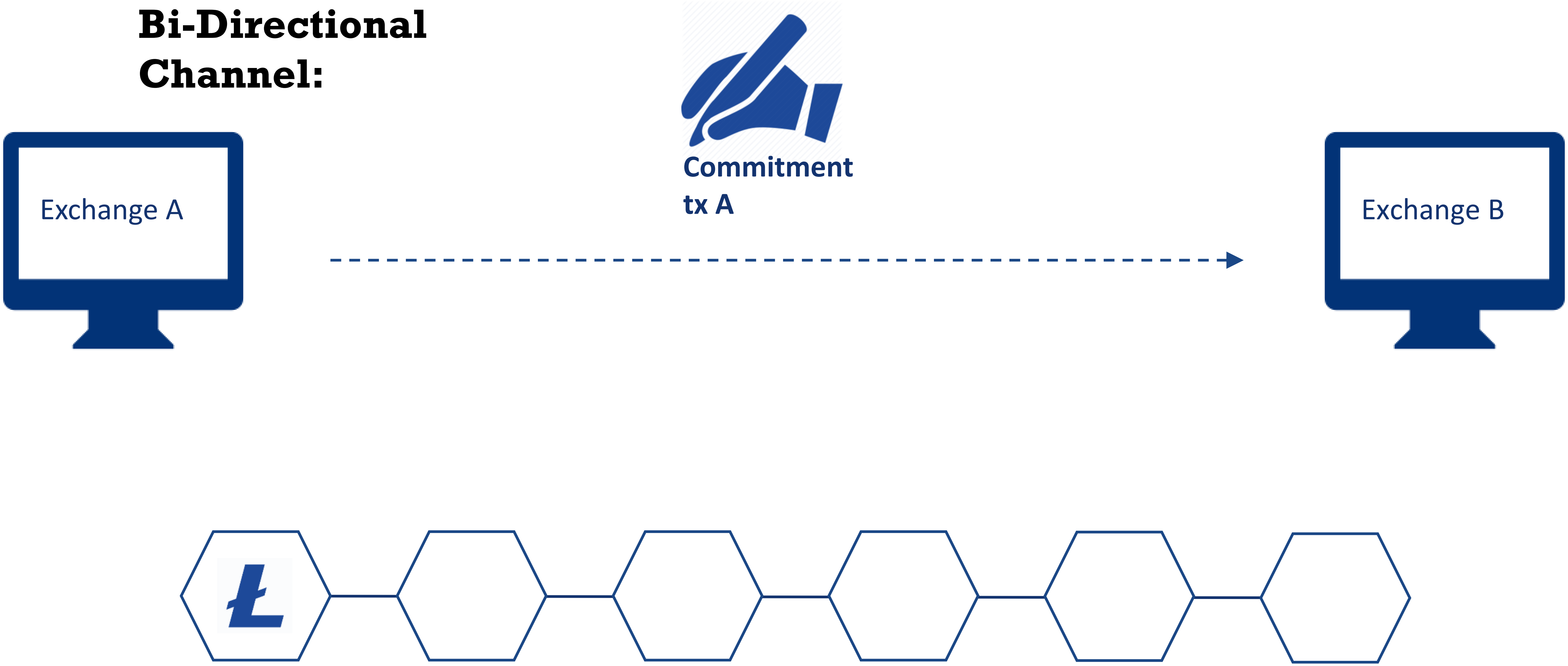
Can be unlocked by B after 1000 blocks

or

By A if it knows **b_secret**

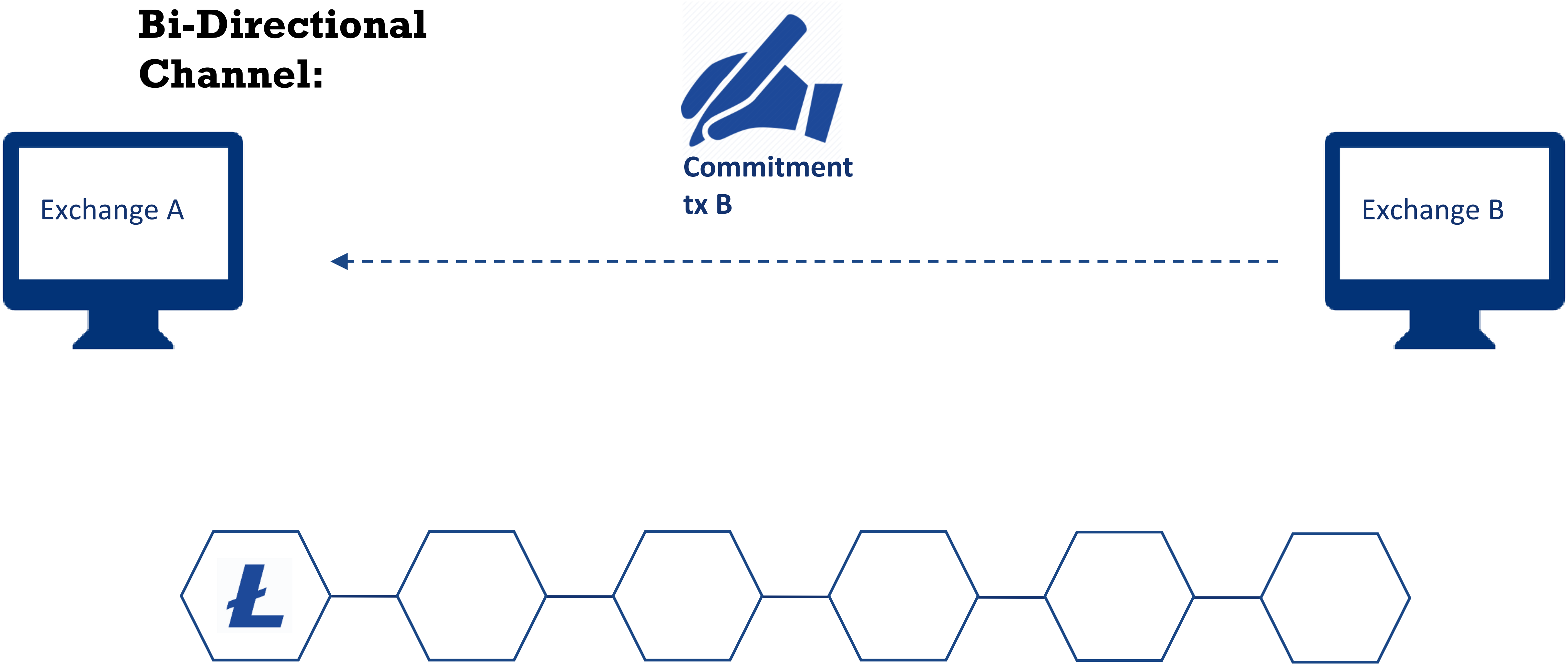
1. Payment Channels

Bi-Directional Channel:



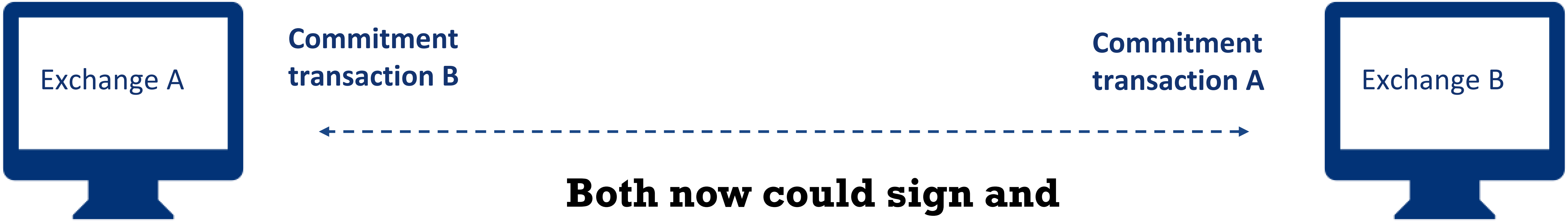
1. Payment Channels

Bi-Directional Channel:



1. Payment Channels

Bi-Directional Channel:



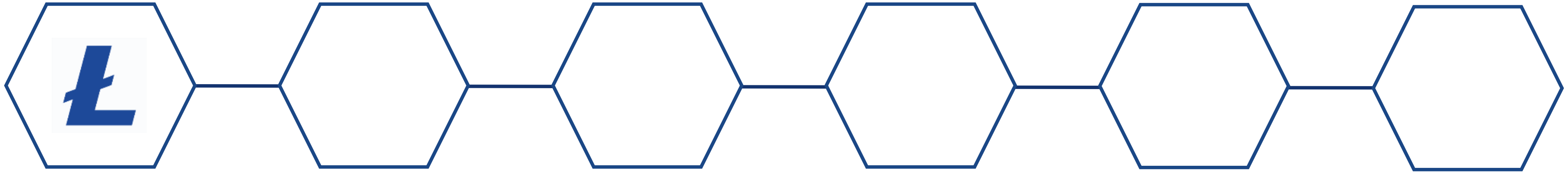
Exchange A

Commitment transaction B

Commitment transaction A

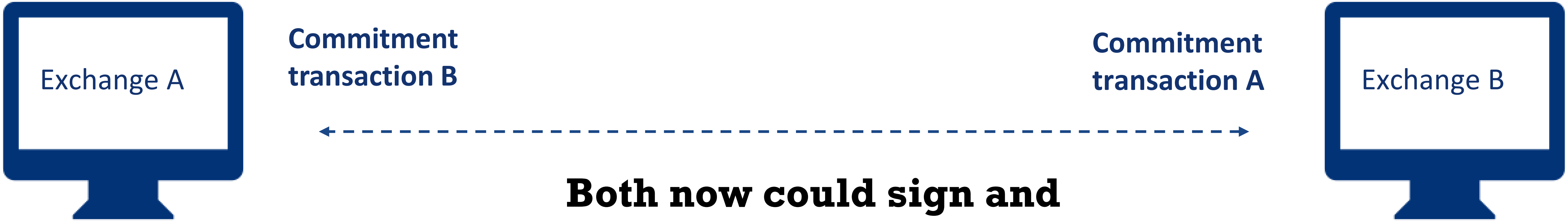
Exchange B

Both now could sign and broadcast these tx, but…

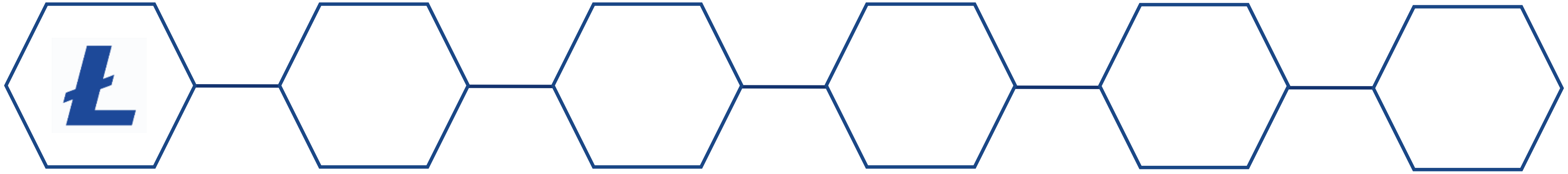


1. Payment Channels

Bi-Directional Channel:



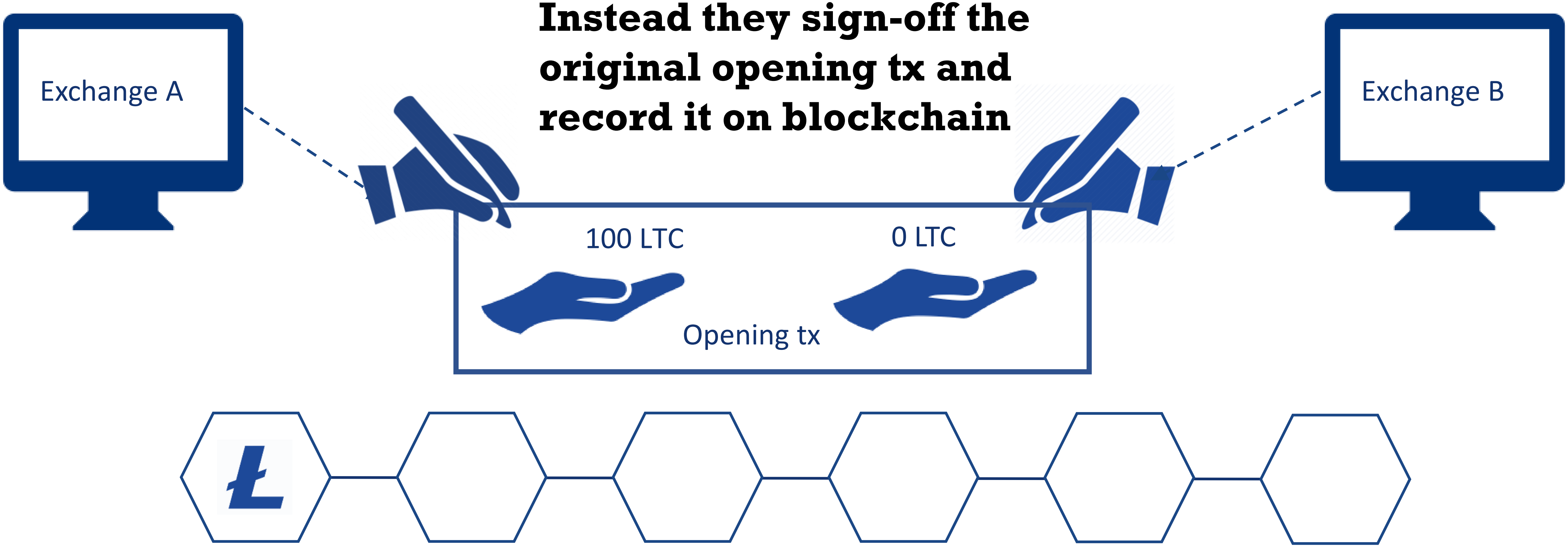
Both now could sign and broadcast these tx, but… they don’t



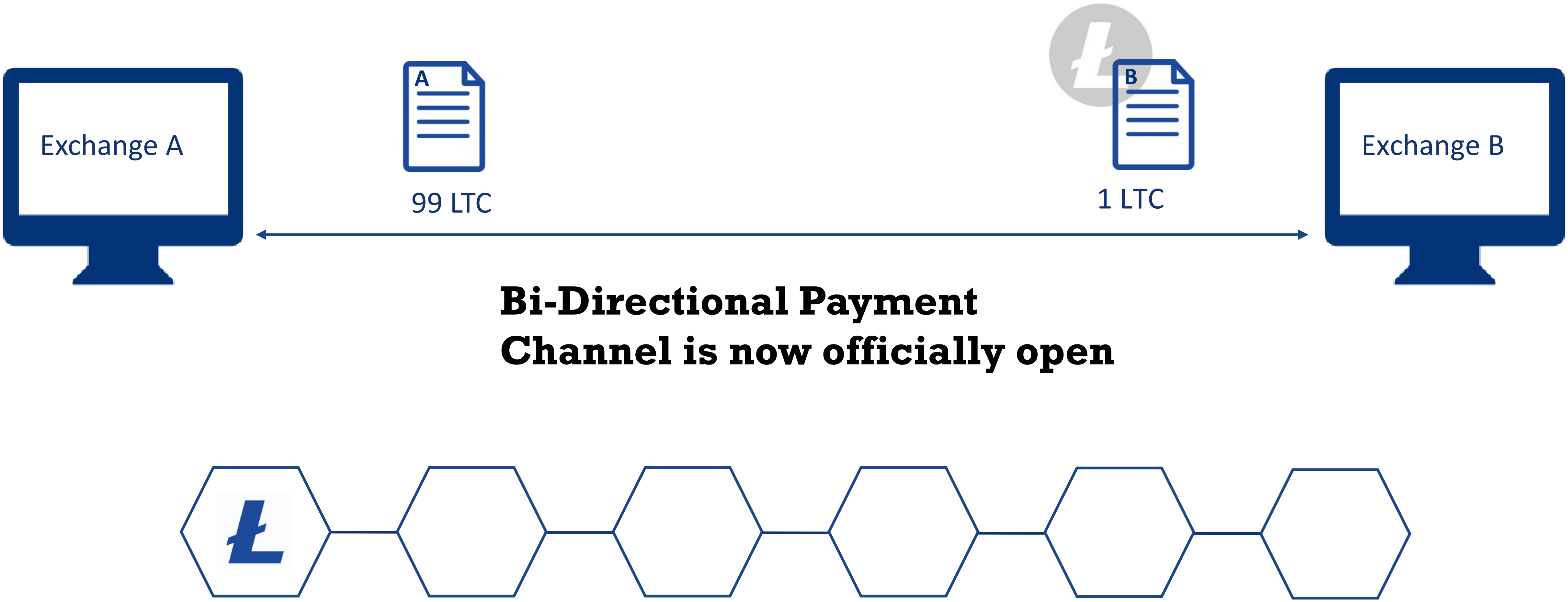
1. Payment Channels

Bi-Directional Channel:

Instead they sign-off the original opening tx and record it on blockchain



1. Payment Channels



Bi-Directional Payment Channel is now officially open