
exchange union

Topics

1. Digital Asset Markets
2. Industry Pain Points
3. Vision
4. Project Intro
5. XUC
6. Use Case
7. Technology
8. Outlook

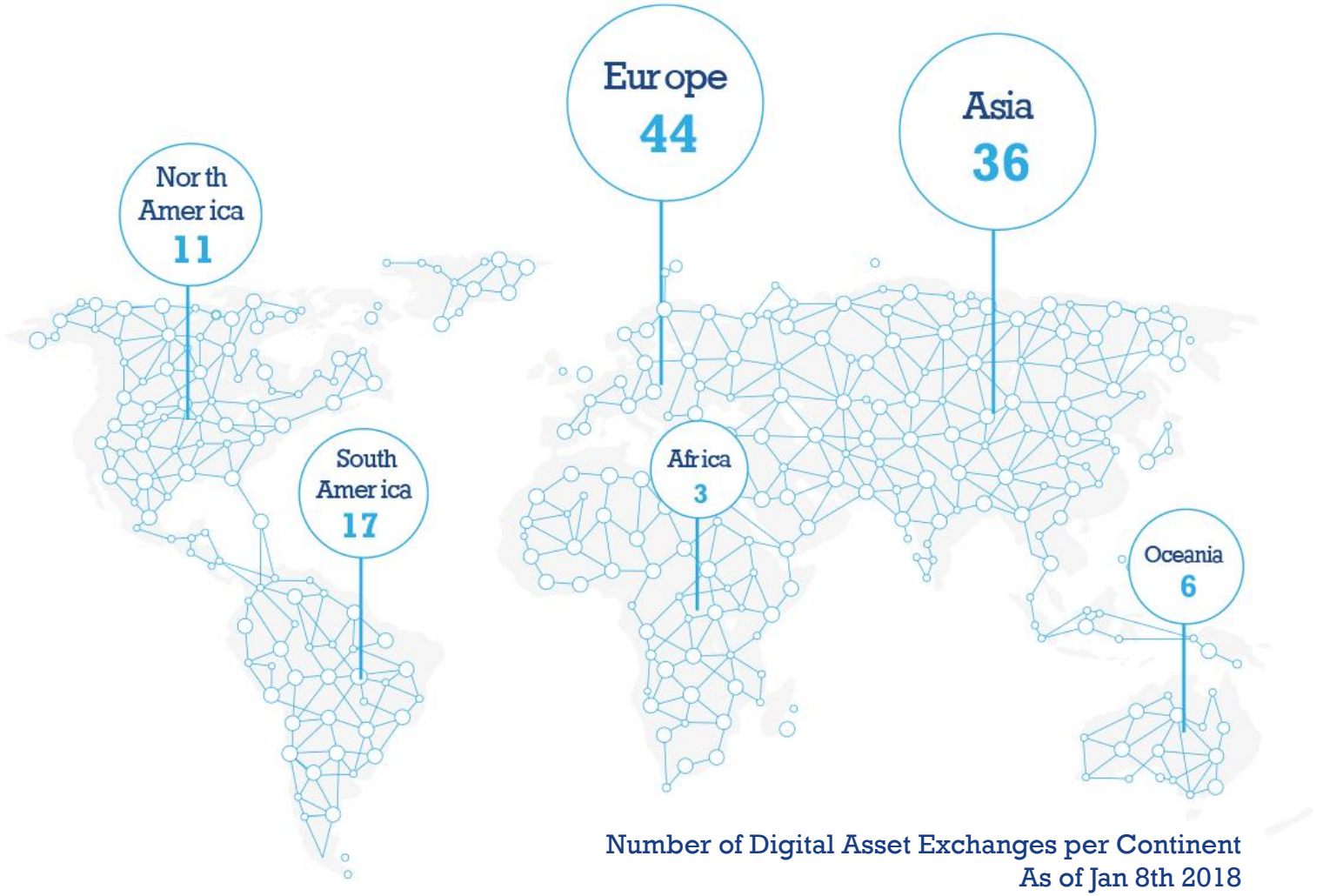
Digital Asset Markets

Types of Digital Assets:
1,300+

Market Capitalization of Digital Assets:
$700bn+

Total 24h Trading Volume:
$44bn+

Number of Digital Asset Exchanges:
100+



Number of Digital Asset Exchanges per Continent
As of Jan 8th 2018

Industry Pain Points

Exchanges:

- are localized and isolated
- have limited trading pairs
- struggle to maintain adequate liquidity

Users:

- encounter real-time price discrepancy
- face inefficient & costly cross-exchange transactions
- Need to verify multiple accounts on different exchanges (access to liquidity and new trading pairs)

Vision

*"The first **decentralized network**, which enables **instant and trustless** trades between digital asset exchanges."*

Who benefits?

Exchanges:

- larger user base
- increased volume & earnings
- increased liquidity
- robust decentralized trading infrastructure

Users:

- tighter spread
- best price
- all trading pairs
- No need for multiple verified accounts

What do we do?

- We build the software for connecting exchanges: **XU Node**
- Open-source (YES!) → Build community
- Bitcoin → the new open-source is self-sustaining
- XUC token: Fees & Incentive system
- Similar solutions:
  - Missing incentives
  - Got technology stack wrong (slow or centralized)
  - Benefits one-sided (e.g. traders, but not exchanges)

How do we realize this?

XUC

How do we realize this?

XUC = Incentive System

XUC

XUC rewards:

- Exchanges: for joining Exchange Union - allocate XUC to their users
- Users: for trading certain volume via Exchange Union
- Developers: for merged pull-requests, review, testing
- Anyone: for provide services in the union
  - Propagate Orderbooks
  - Validate Orderbooks
  - Other payment channels services like a watchtower

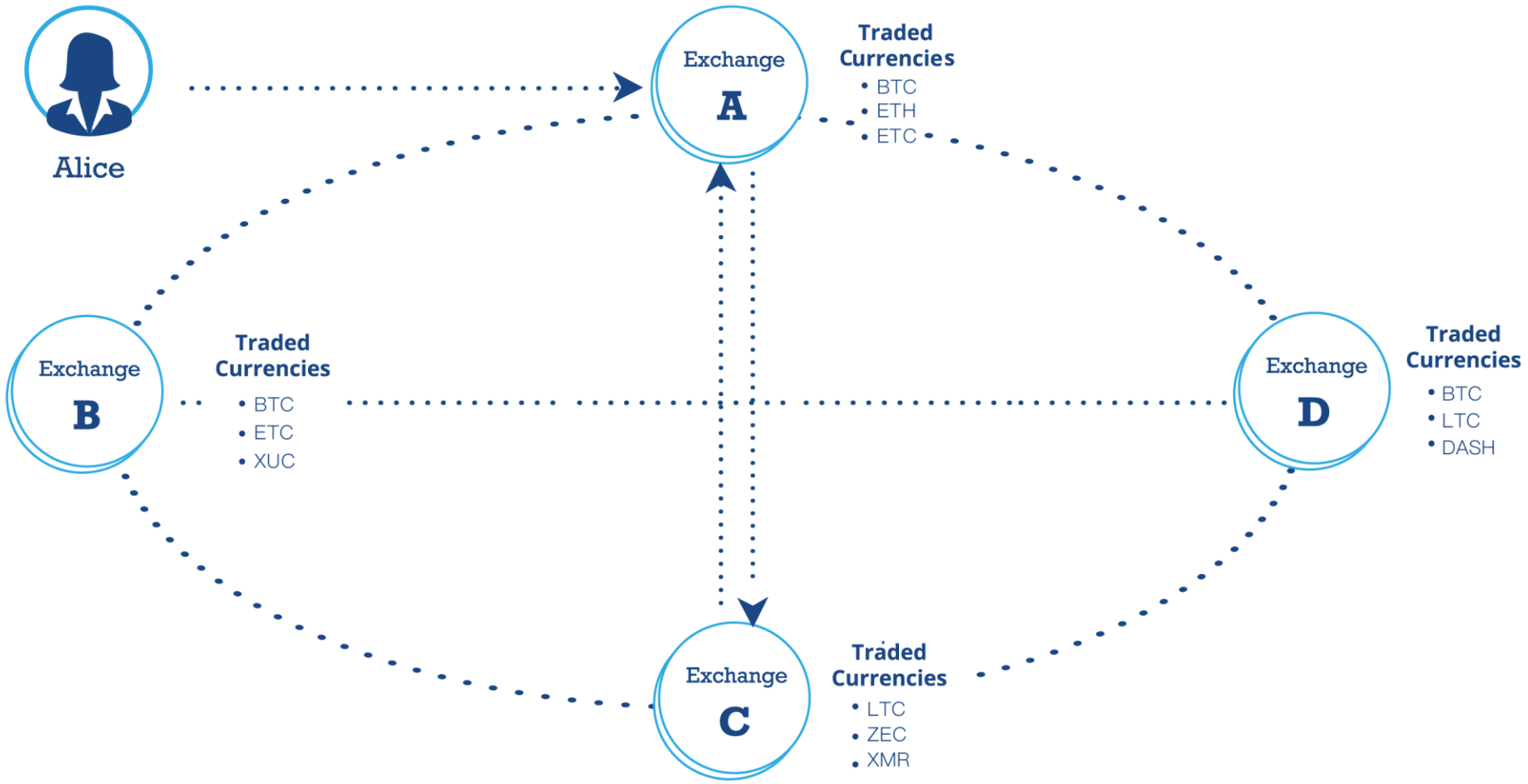
XUC

Token Data:

- Total supply: 3 billion
- Current circulation: 65 Million
- Larger parts locked long-term locked or burned
- Max. release amount per month: 5 Million (controlled by smart contract)

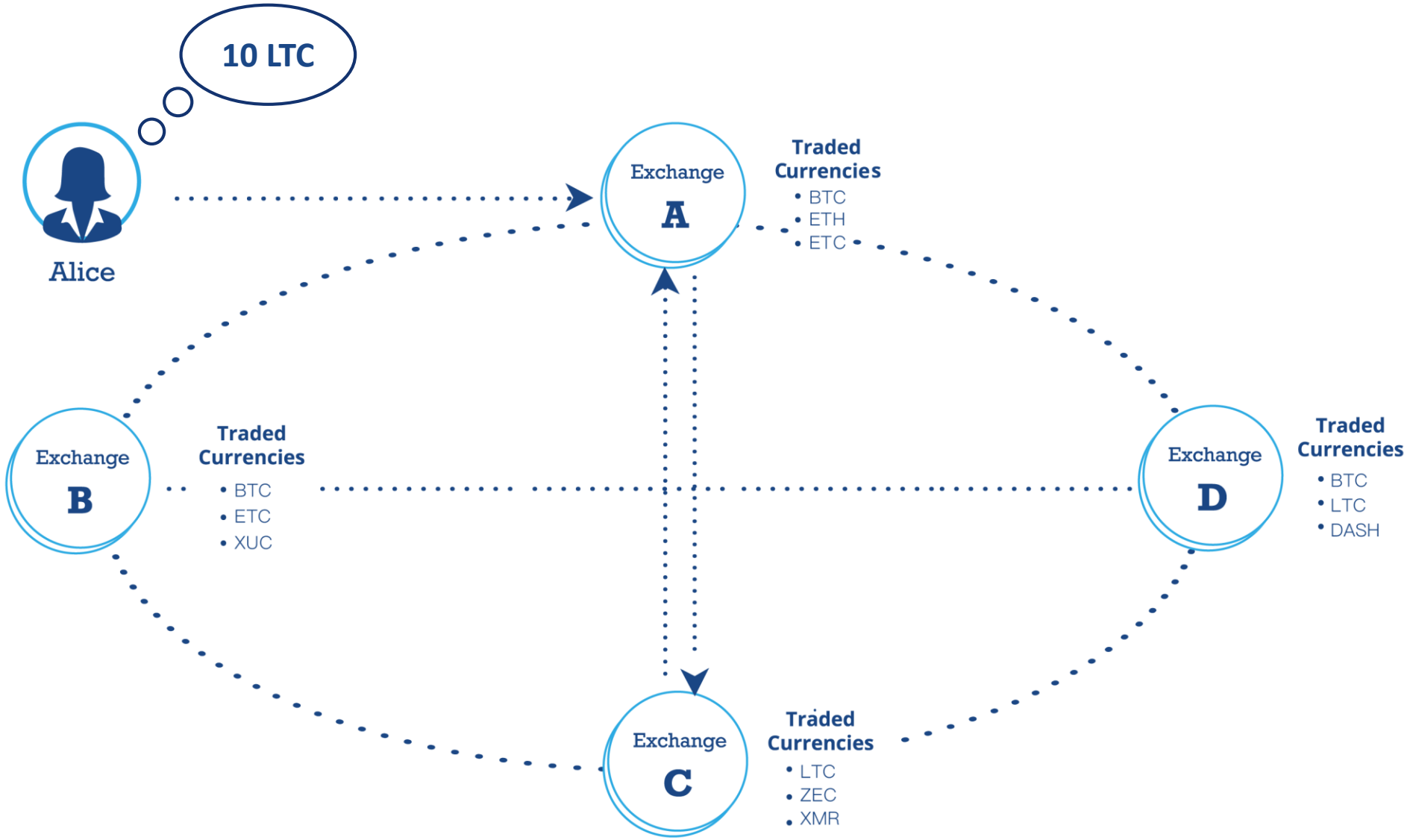
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



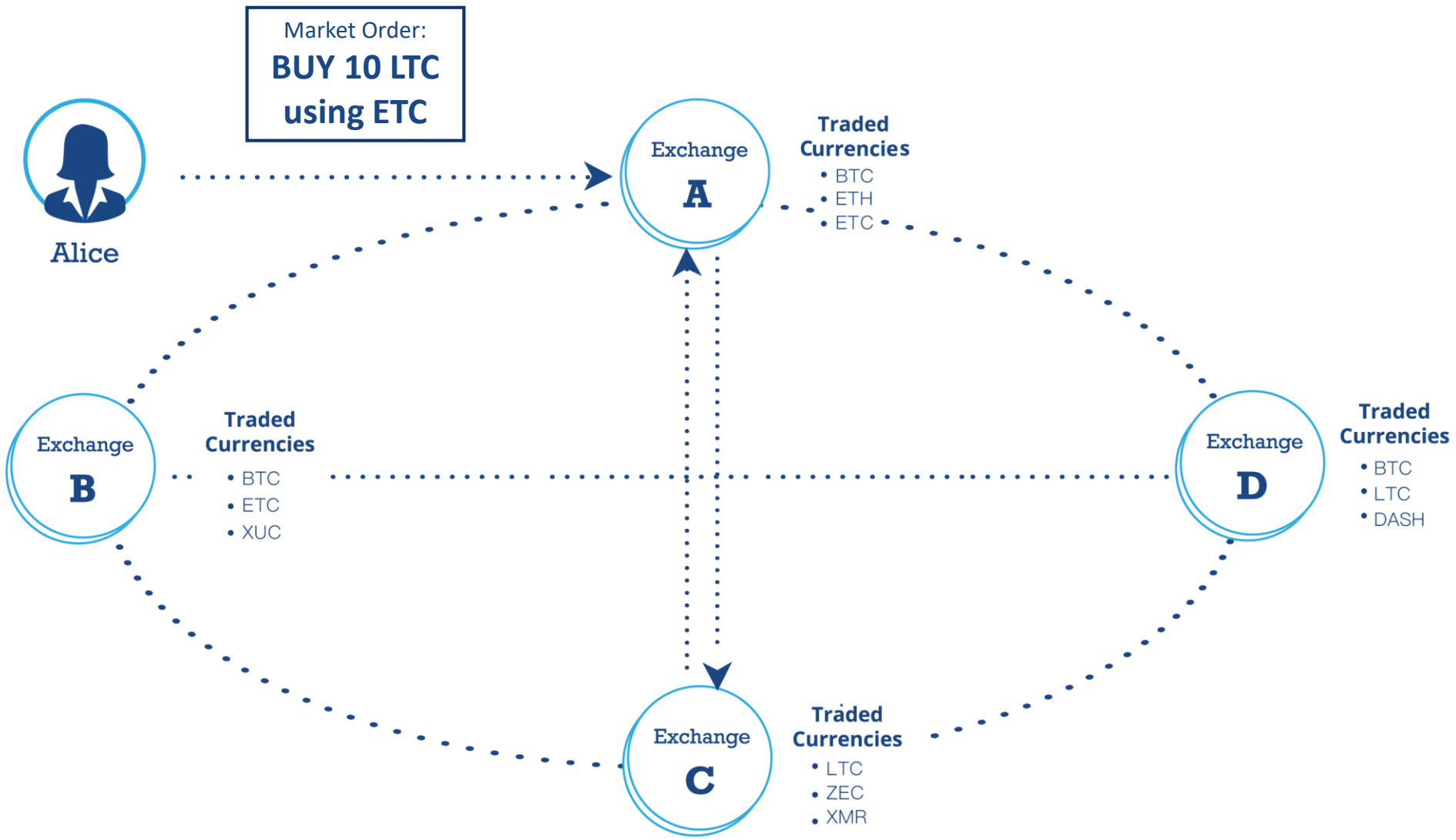
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



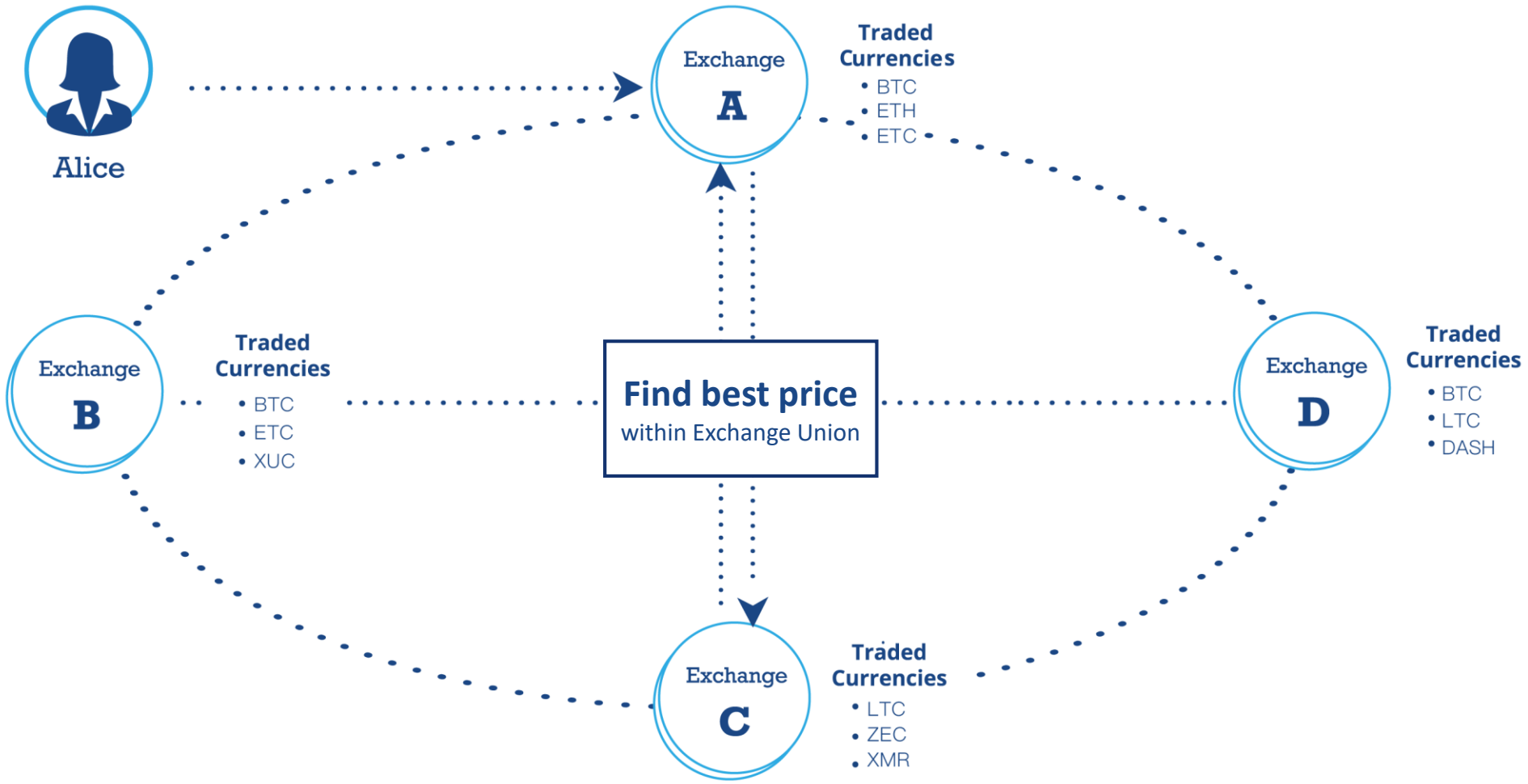
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



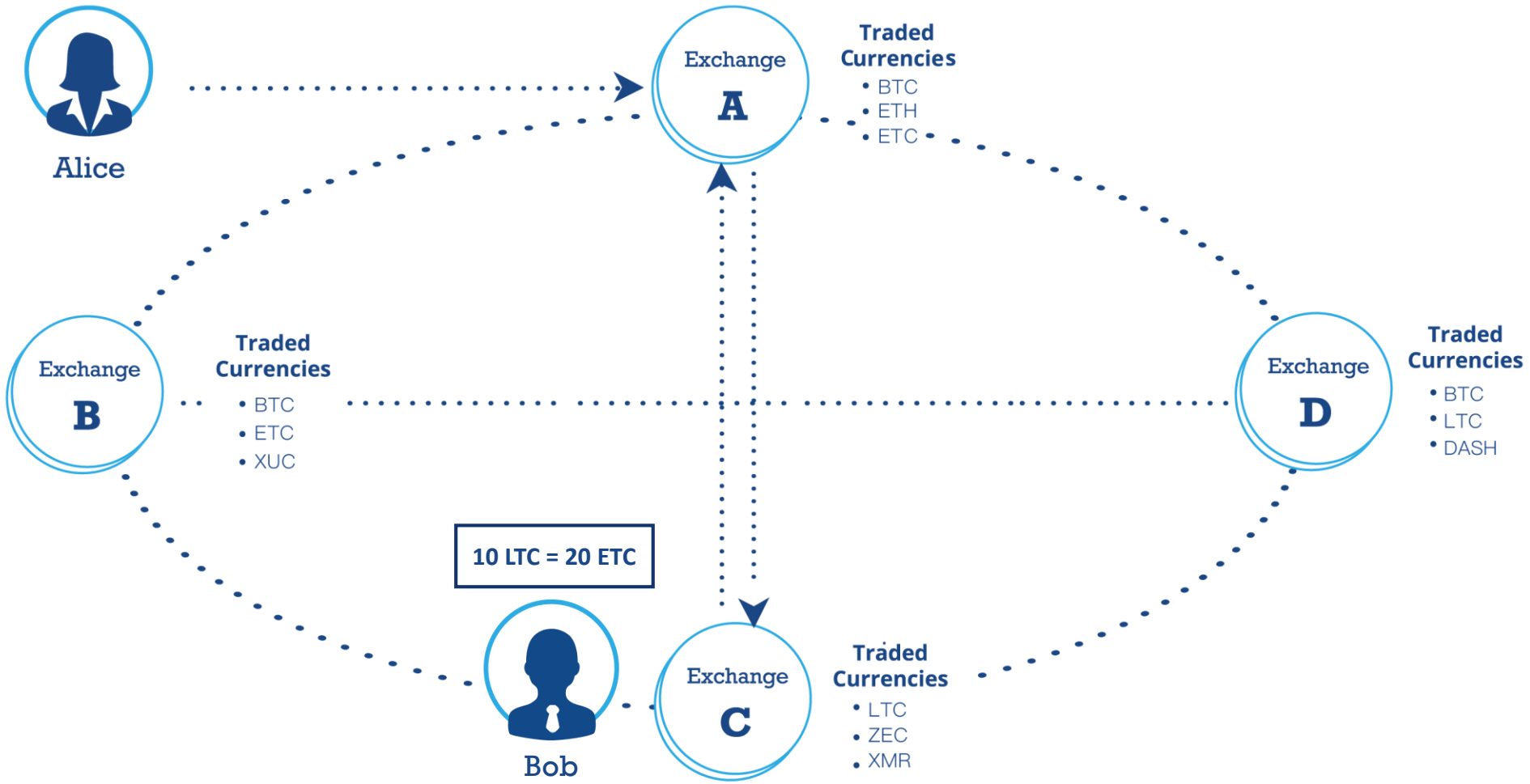
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



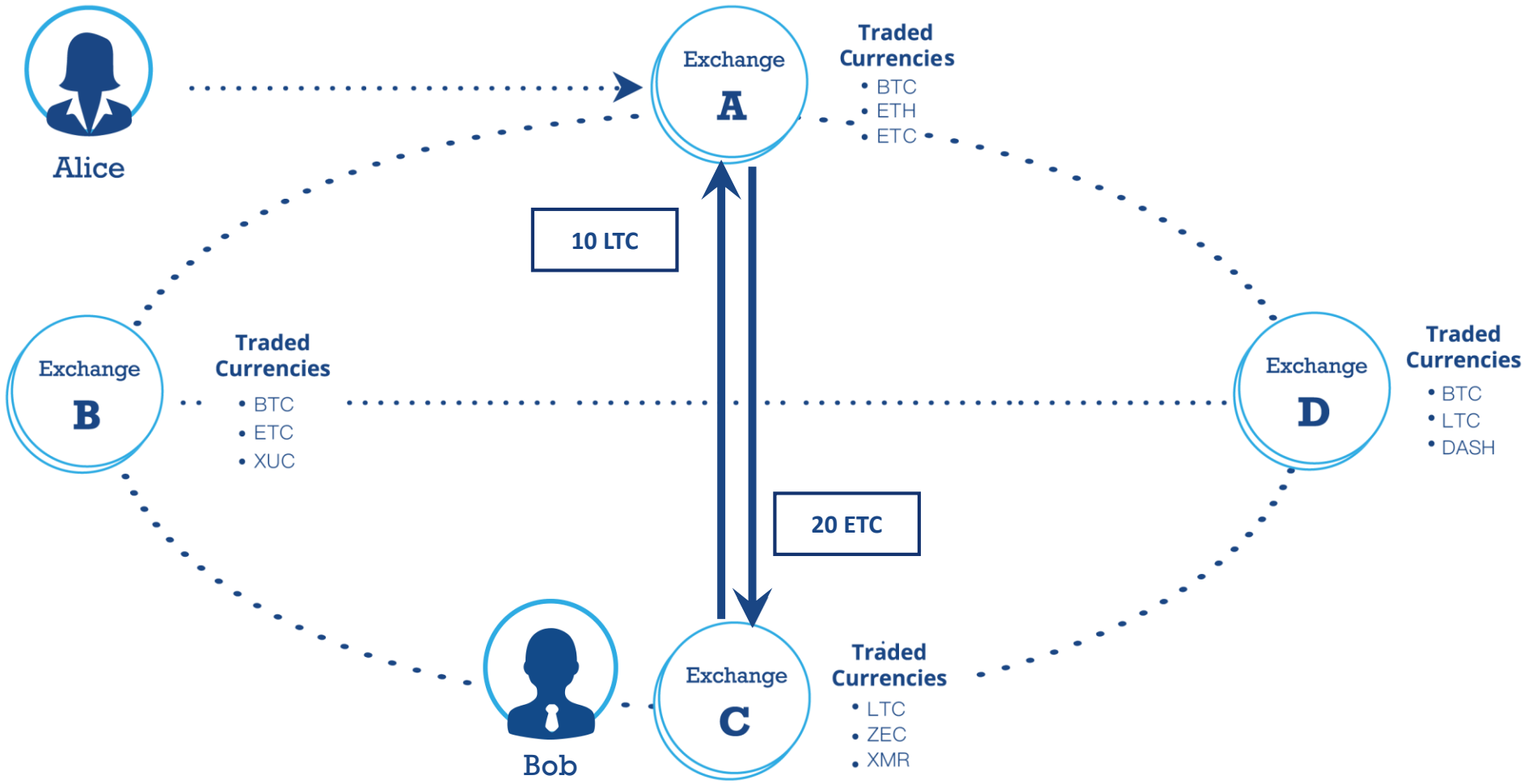
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



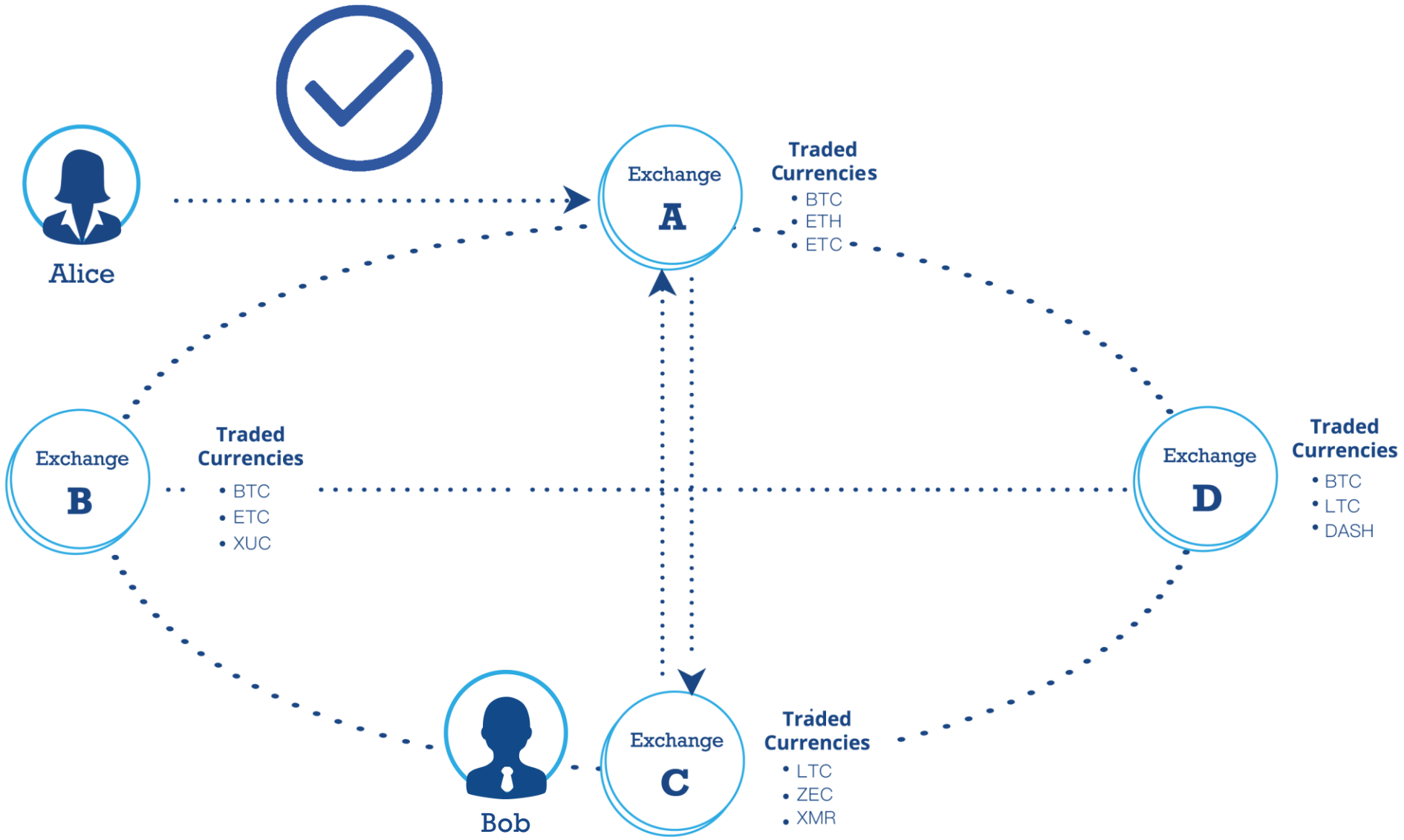
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



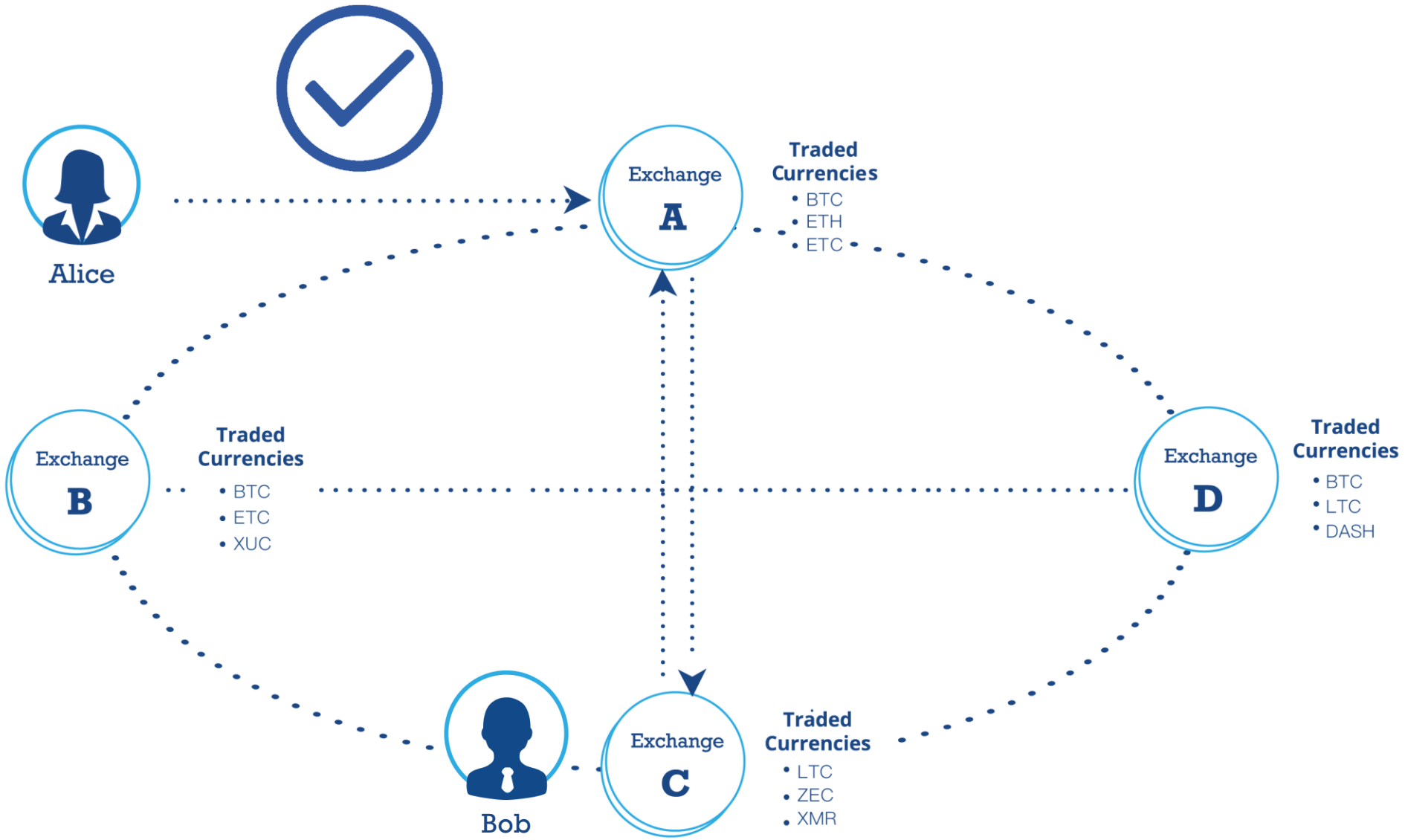
Use Case

Portfolio		
	Before	After
BTC	2	
LTC	0	
ETC	100	



Use Case

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



Technical Architecture

3 Key Technologies

Technical Architecture

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

3 Key Technologies

Technical Architecture

3 Key Technologies

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

2. Atomic Swaps
Trustless trades directly between two exchanges

Technical Architecture

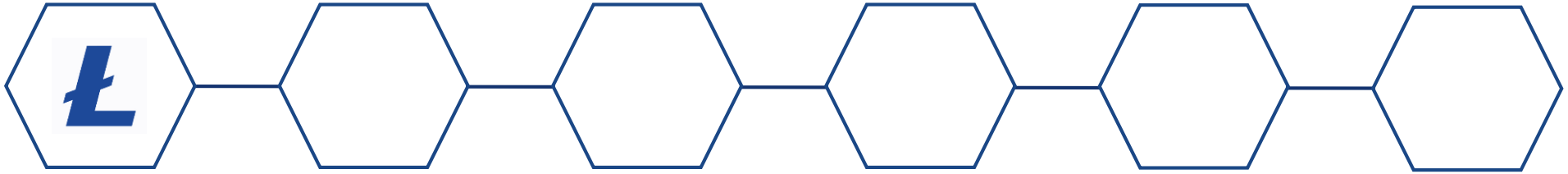
3 Key Technologies

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 – *connect buyer & seller*

Status Quo



Status Quo

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

1. Payment Channels

Yes, we are talking about Lightning & Raiden!

1. Payment Channels

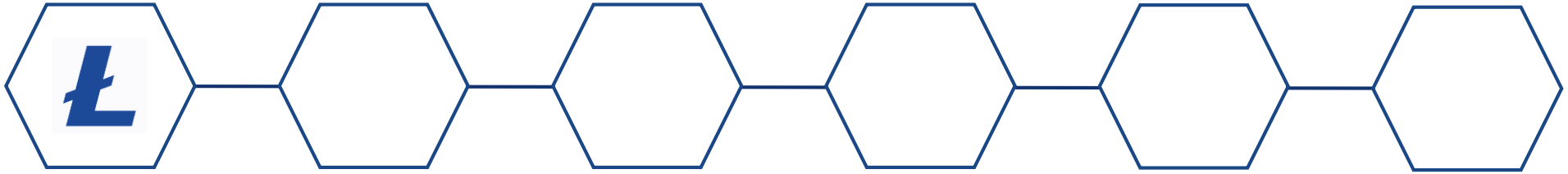
Old idea, obviously Satoshi already came up with the basics:

*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.*

Source: https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2013-April/002417.html

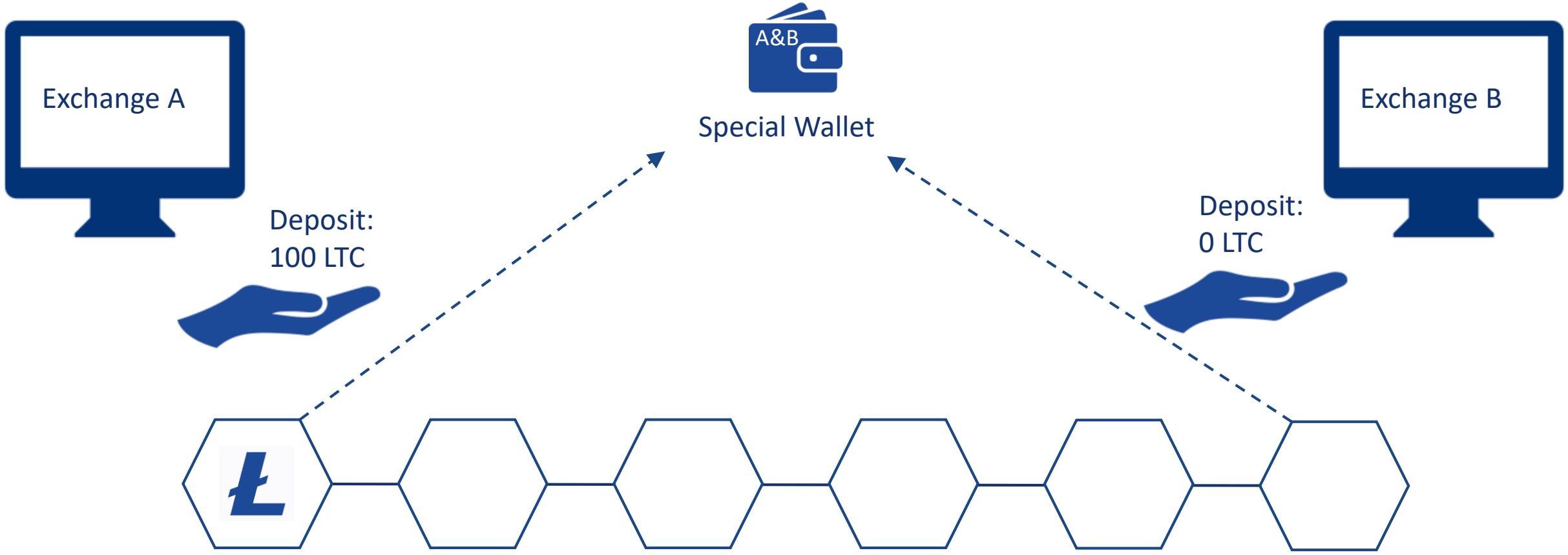
1. Payment Channels

High-level:



1. Payment Channels

High-level:

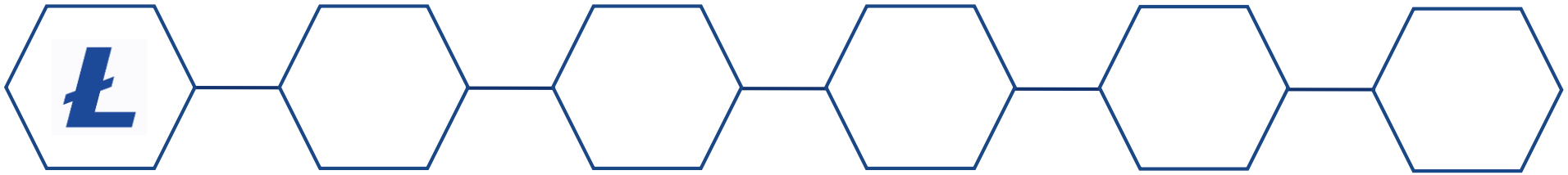


1. Payment Channels

High-level:

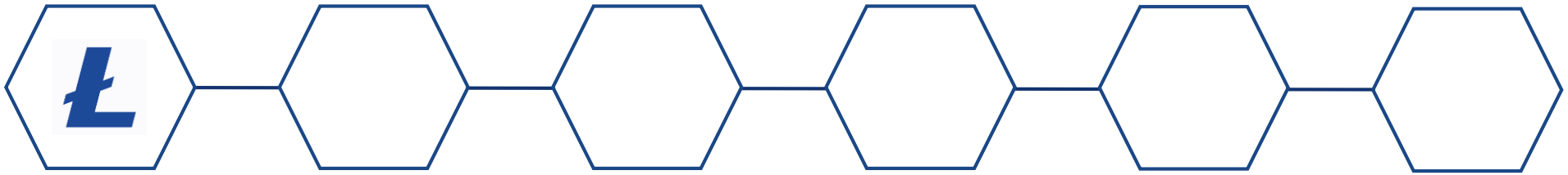
1. Payment Channels

High-level:



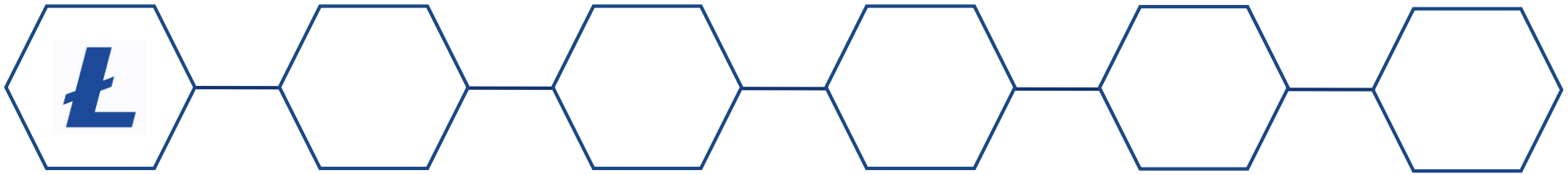
1. Payment Channels

High-level:



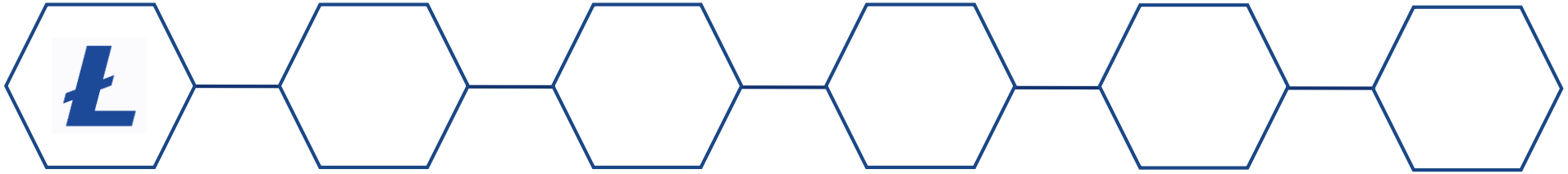
1. Payment Channels

High-level:



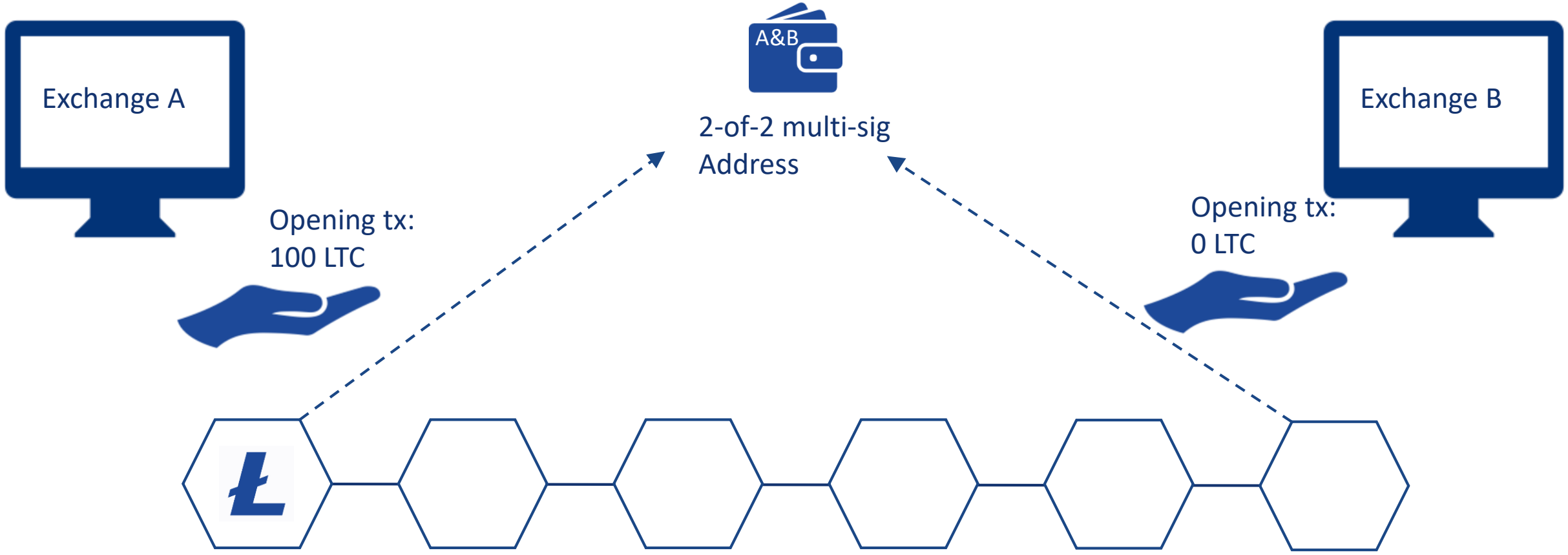
1. Payment Channels

Bi-Directional Channel:



1. Payment Channels

Bi-Directional Channel:

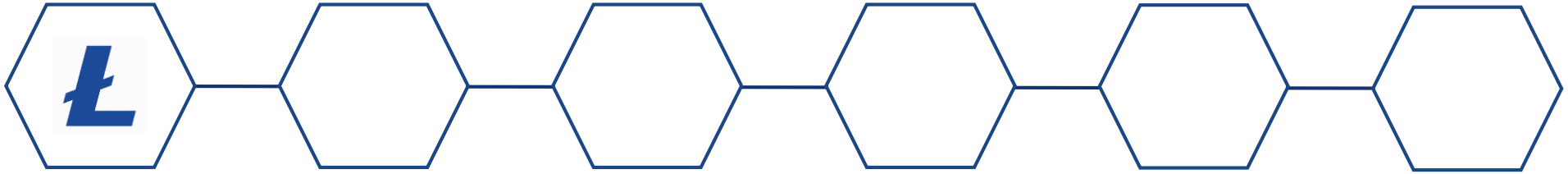


1. Payment Channels

Bi-Directional Channel:

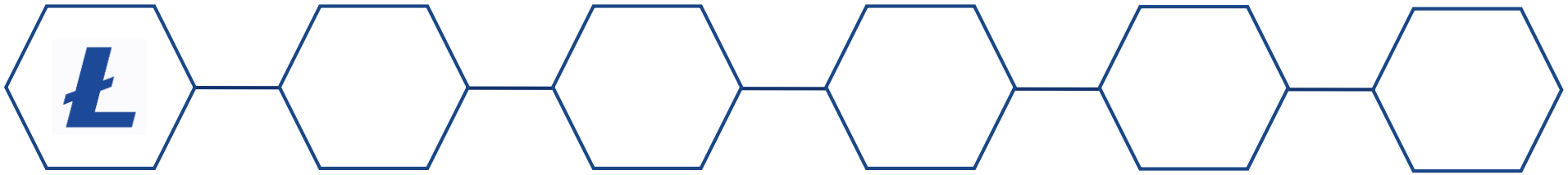
H(a_secret)

H(b_secret)



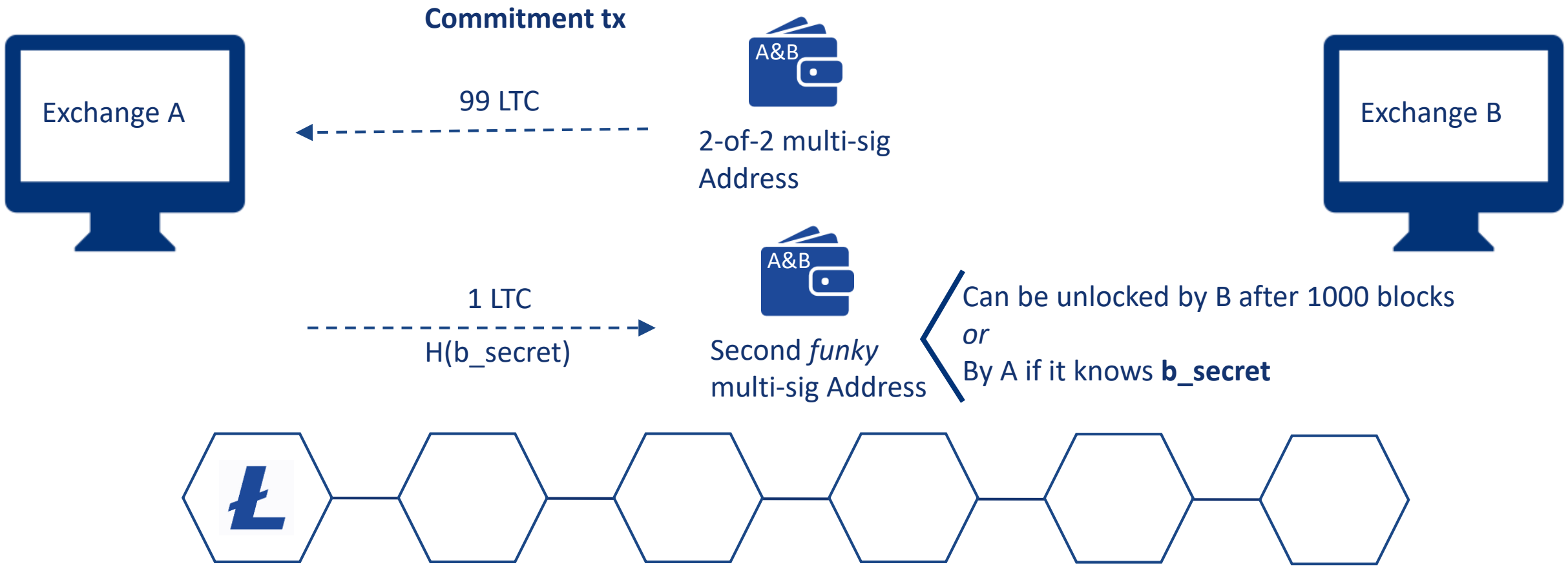
1. Payment Channels

Bi-Directional Channel:



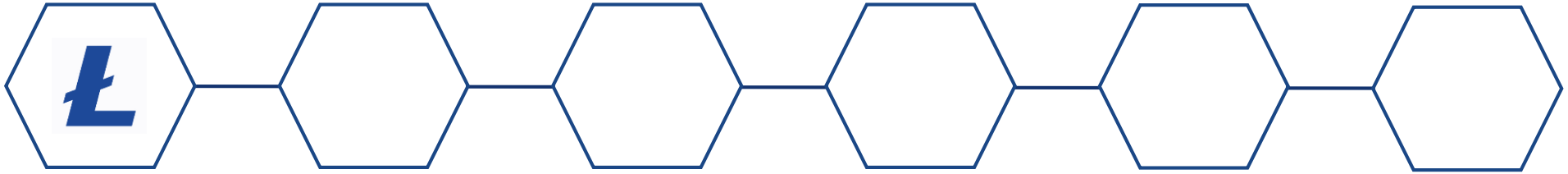
1. Payment Channels

Bi-Directional Channel:



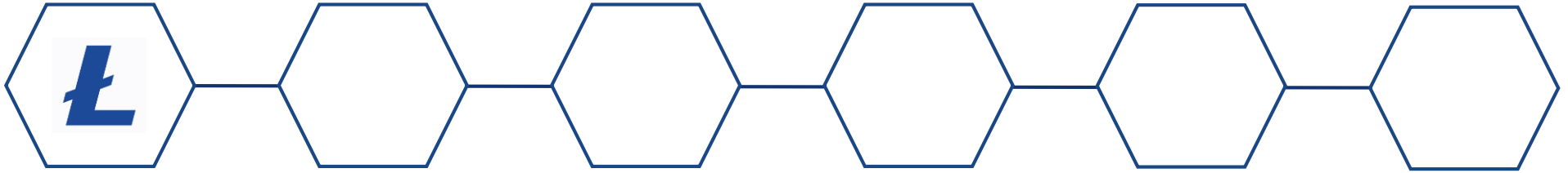
1. Payment Channels

Bi-Directional Channel:



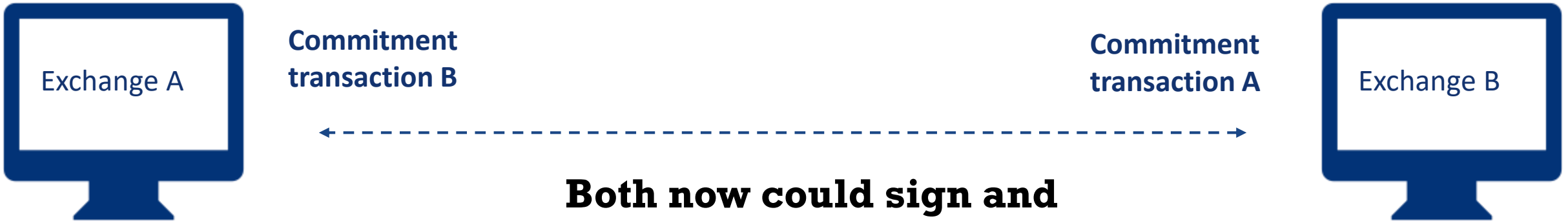
1. Payment Channels

Bi-Directional Channel:

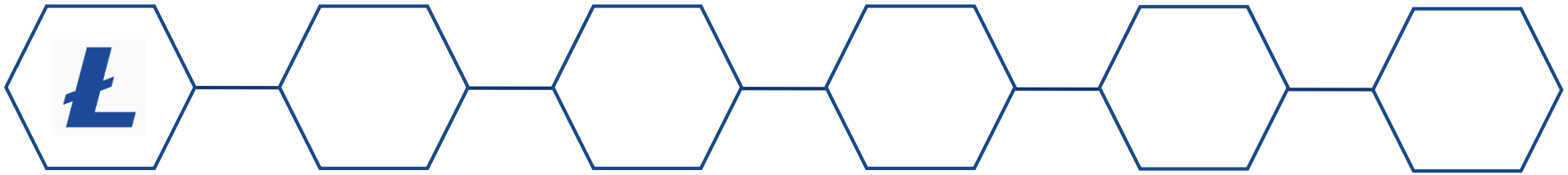


1. Payment Channels

Bi-Directional Channel:



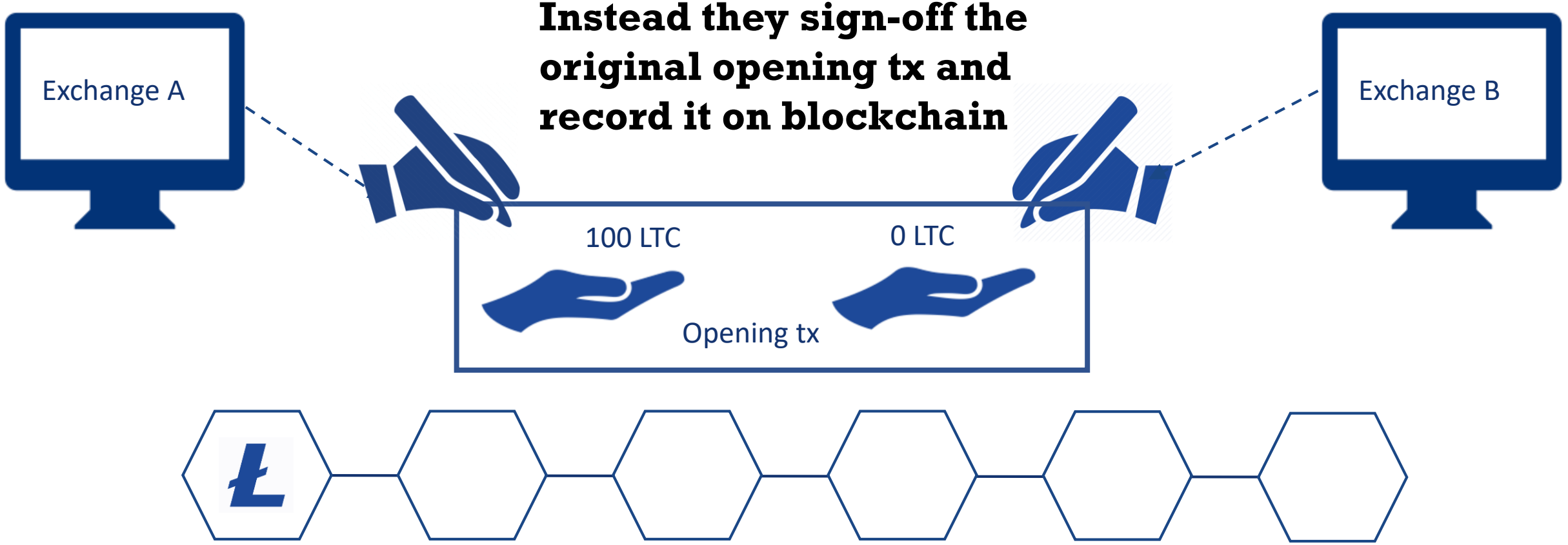
Both now could sign and broadcast these tx, but… they don't



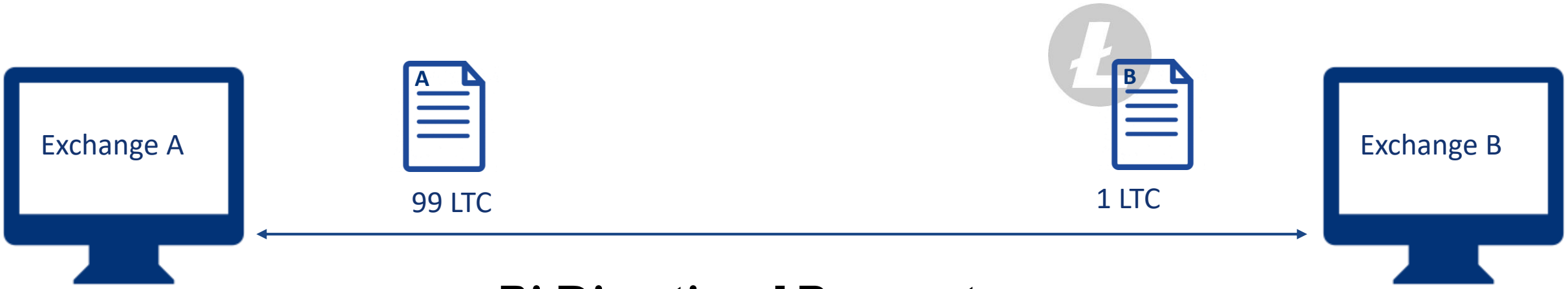
1. Payment Channels

Bi-Directional Channel:

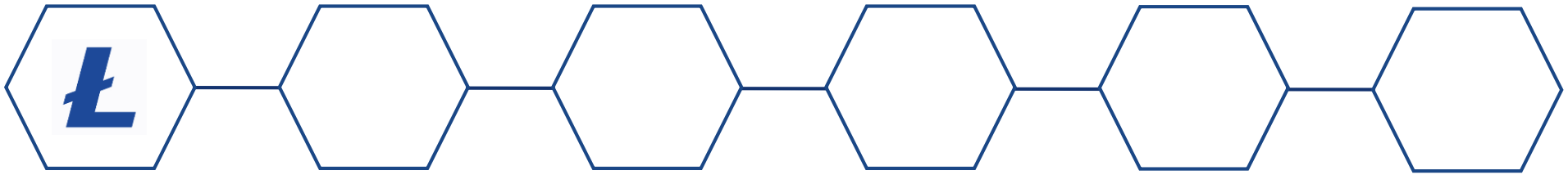
Instead they sign-off the original opening tx and record it on blockchain



1. Payment Channels



Bi-Directional Payment Channel is now officially open

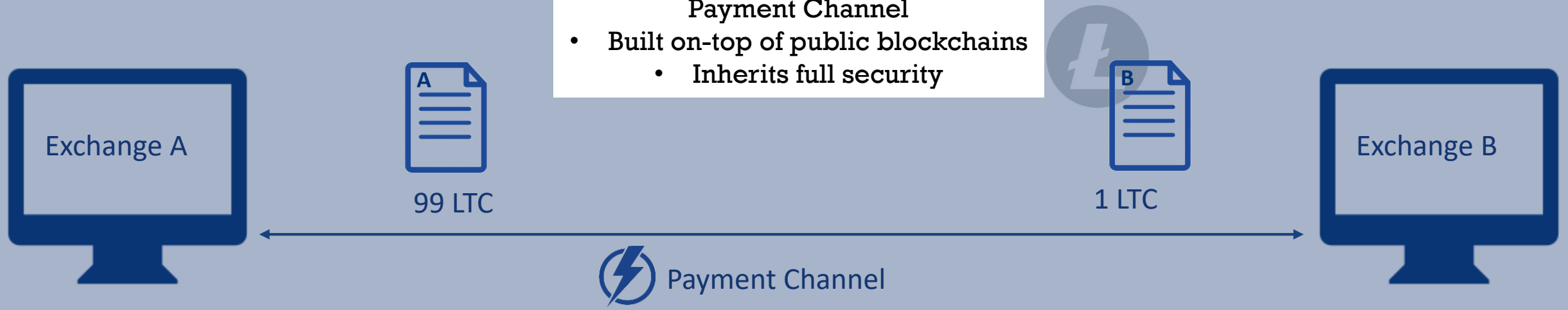


1. Payment Channels

Layer 2

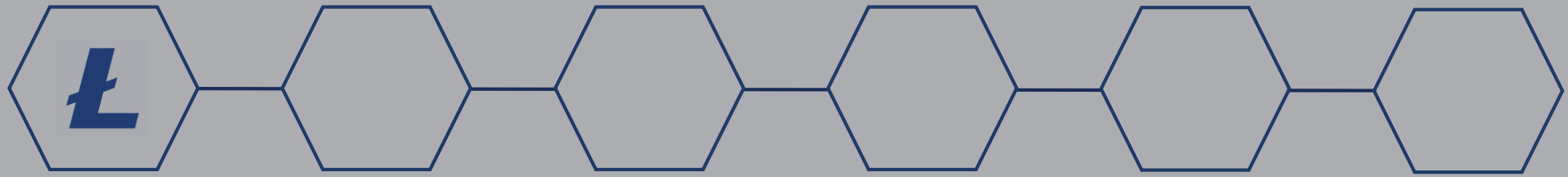
Payment Channel

- Built on-top of public blockchains
- Inherits full security



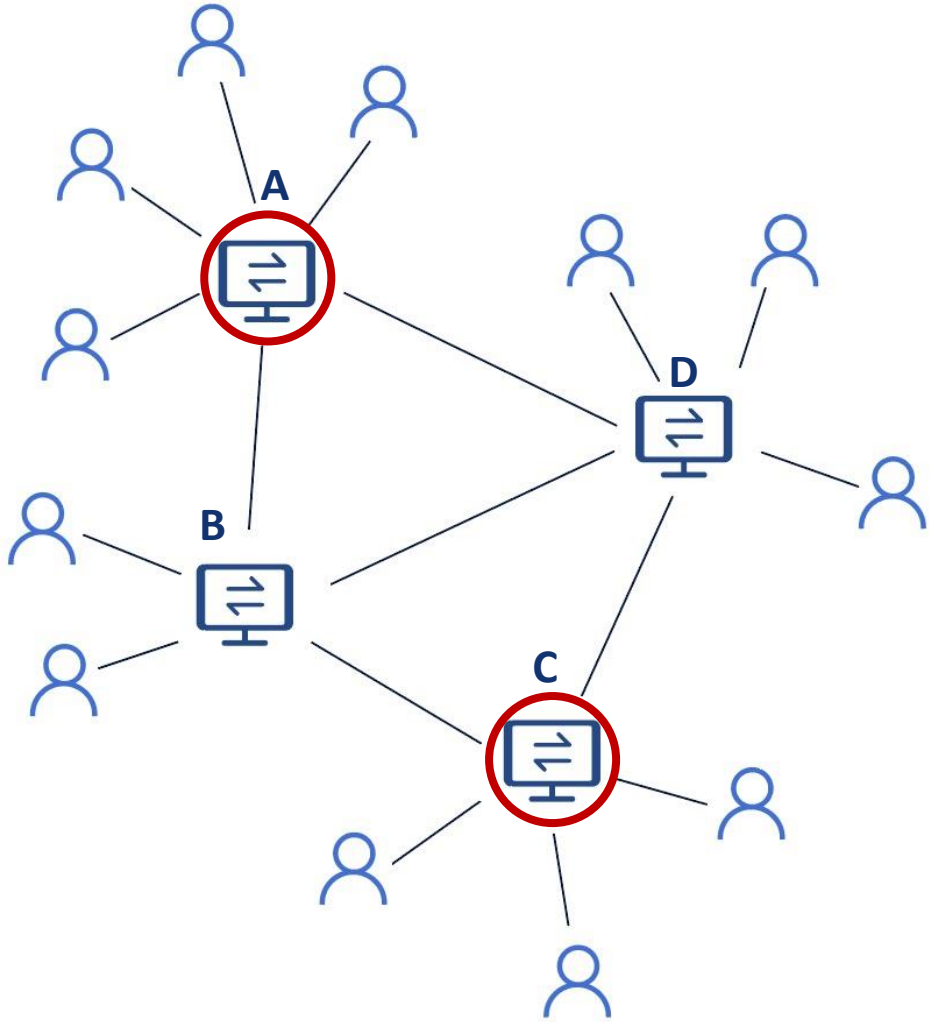
Layer 1

Underlying public blockchain = dispute mediation system



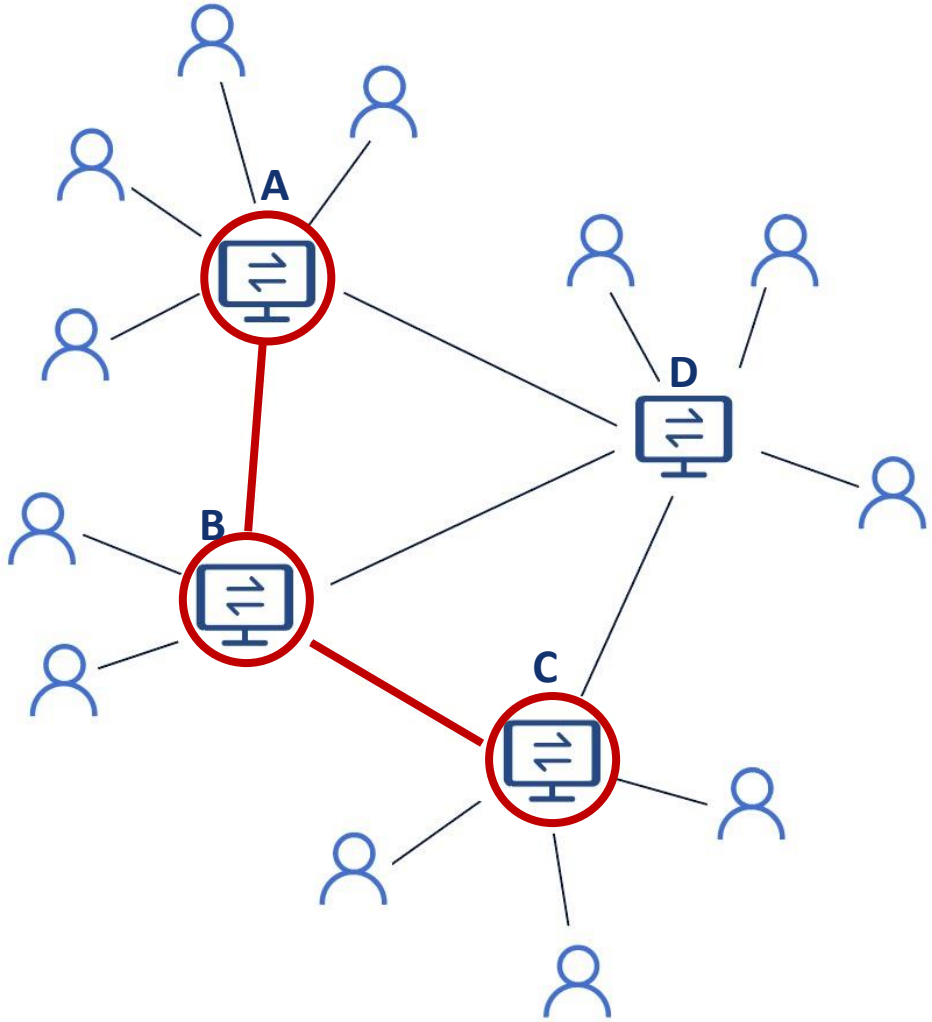
1. Payment Channels

Routing:

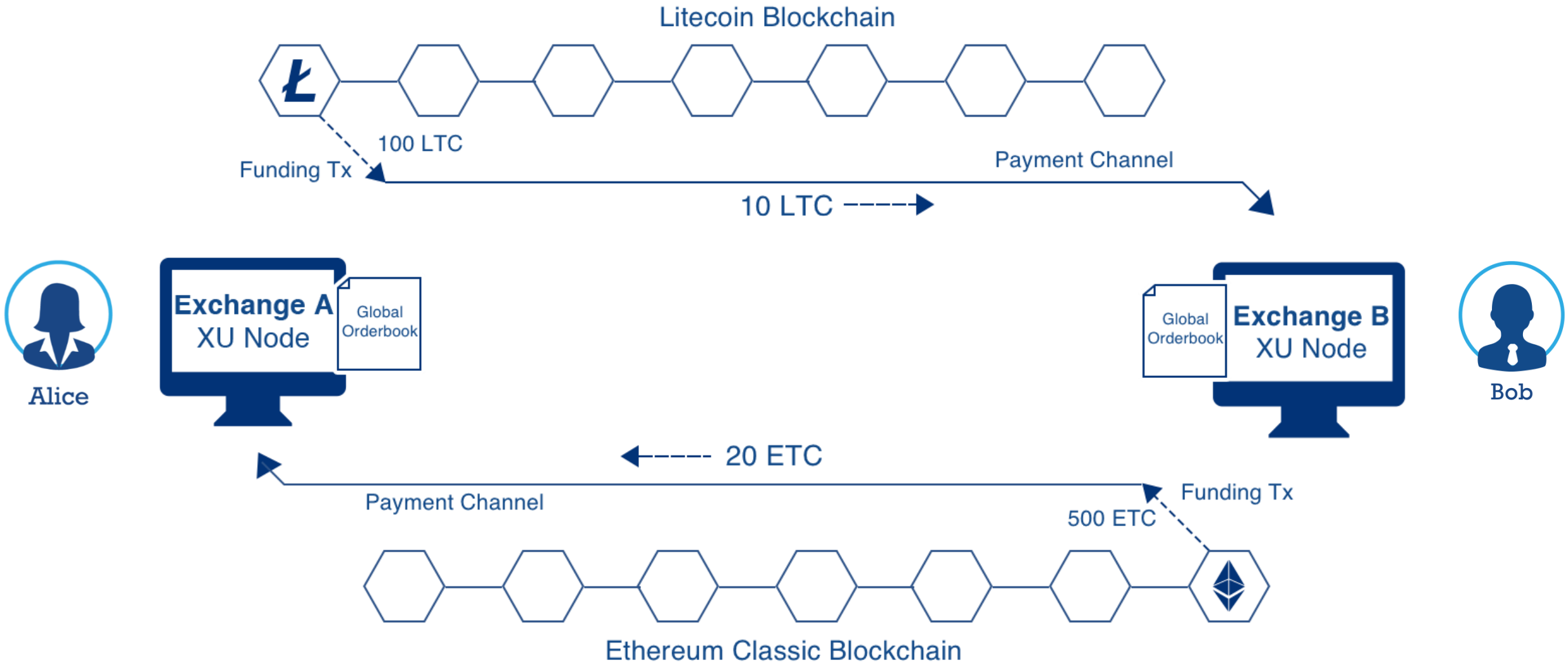


1. Payment Channels

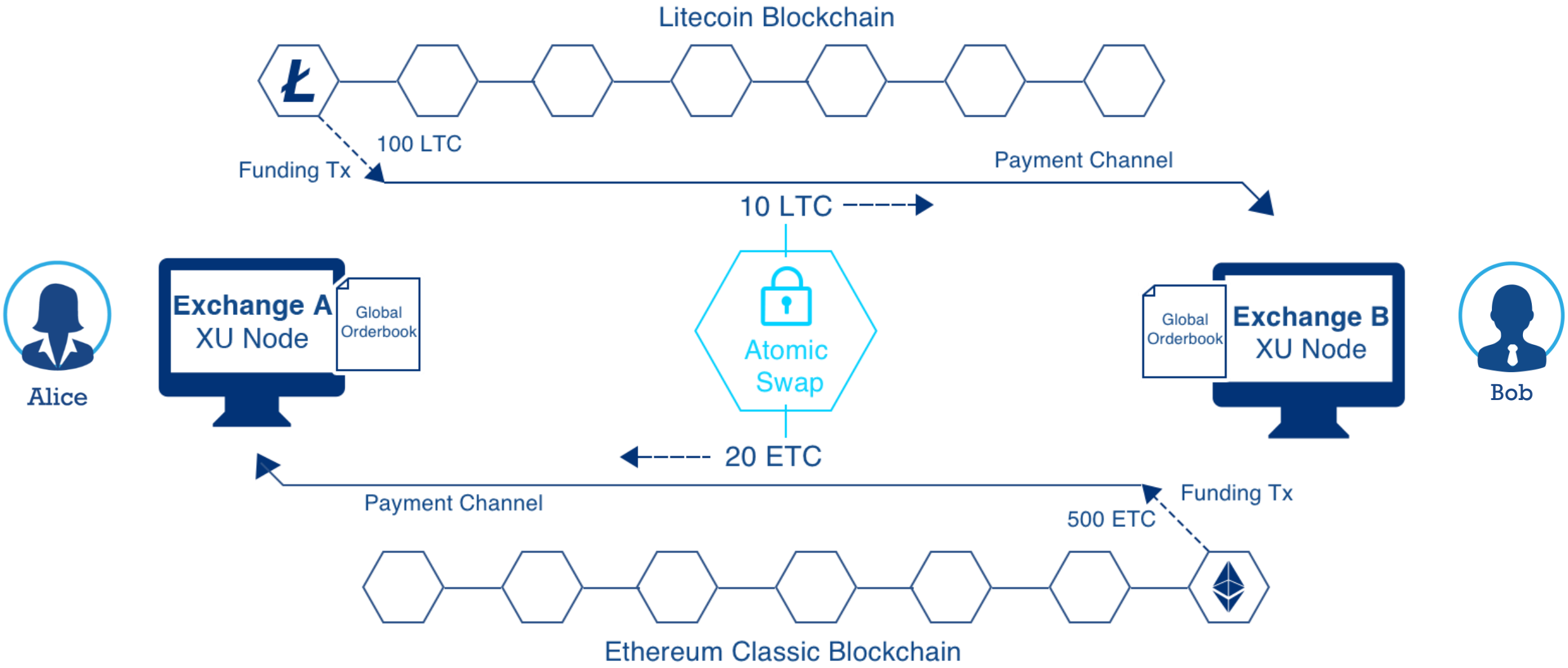
Routing:



1. Payment Channels



2. Atomic Swaps



2. Atomic Swaps

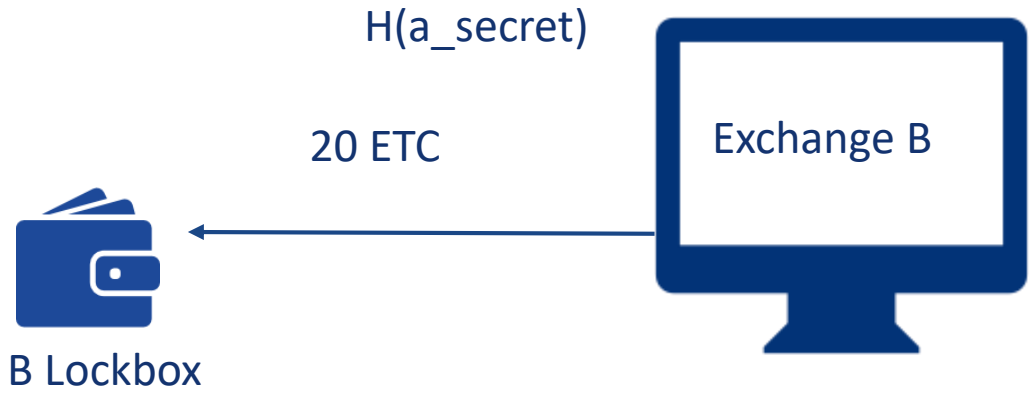
- Trustless exchange of two different assets
  - No middleman/escrow service needed
- How: guarantee atomicity
  - Either both sides of the trade happen or none
  - Technology: Hashed TimeLock Contracts (HTLCs)

2. Atomic Swaps

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

2. Atomic Swaps

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



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

2. Atomic Swaps

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

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

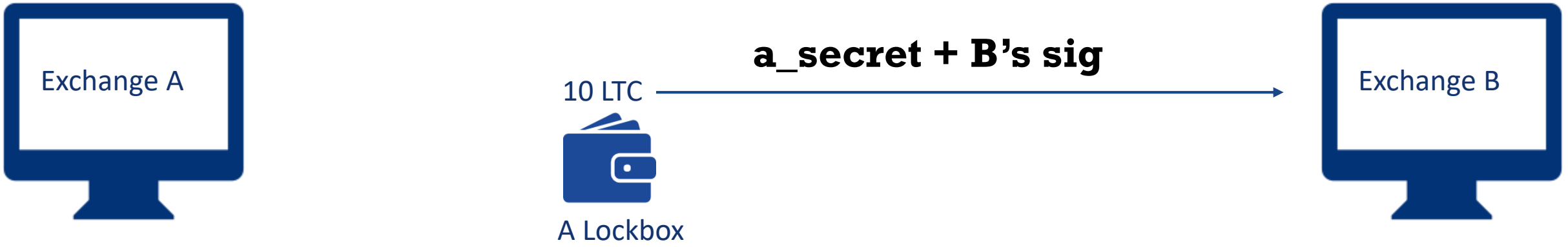
Both lockboxes need the **same "a_secret"** to be opened!

2. Atomic Swaps

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

2. Atomic Swaps

2. Atomic Swaps



2. Atomic Swaps

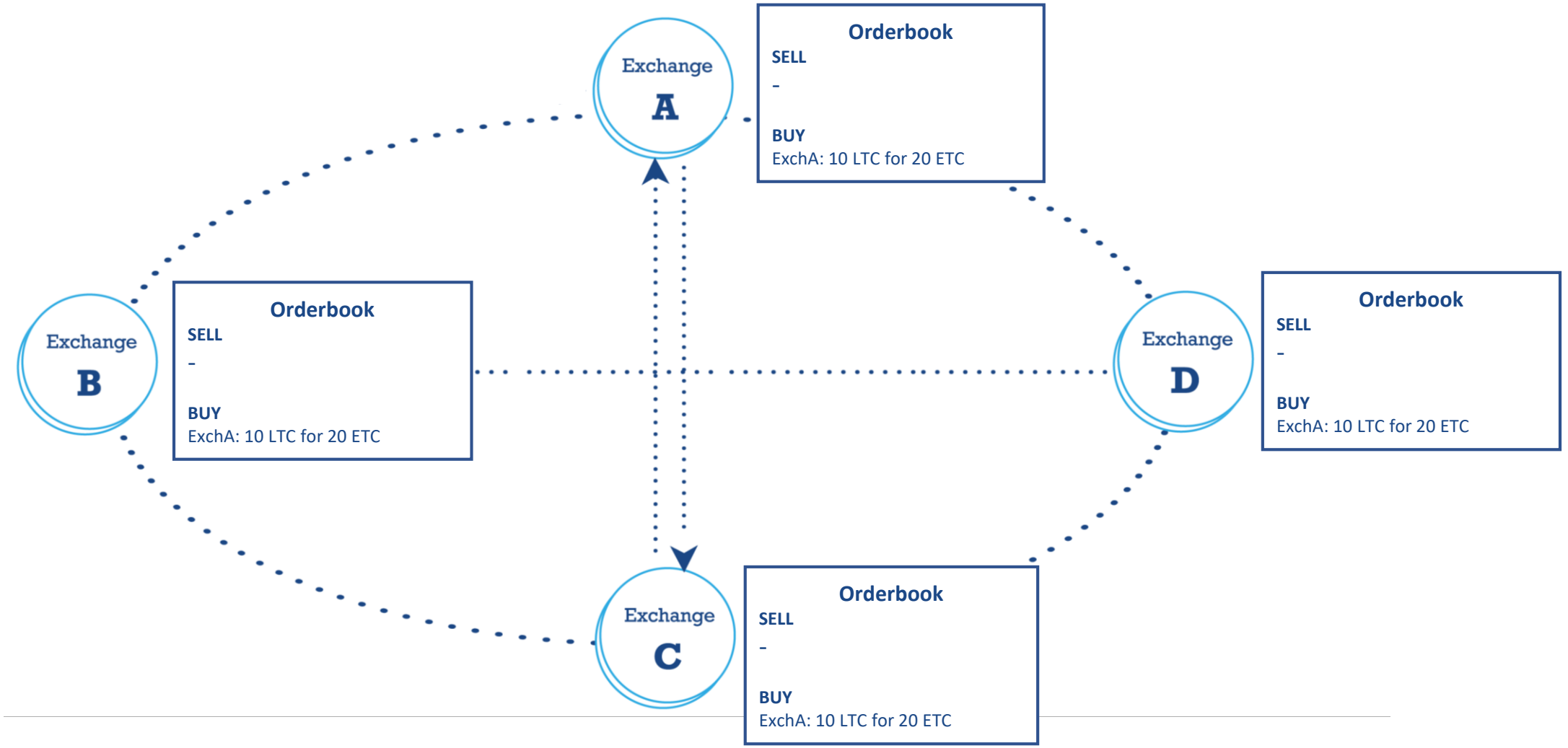
20 ETC

10 LTC

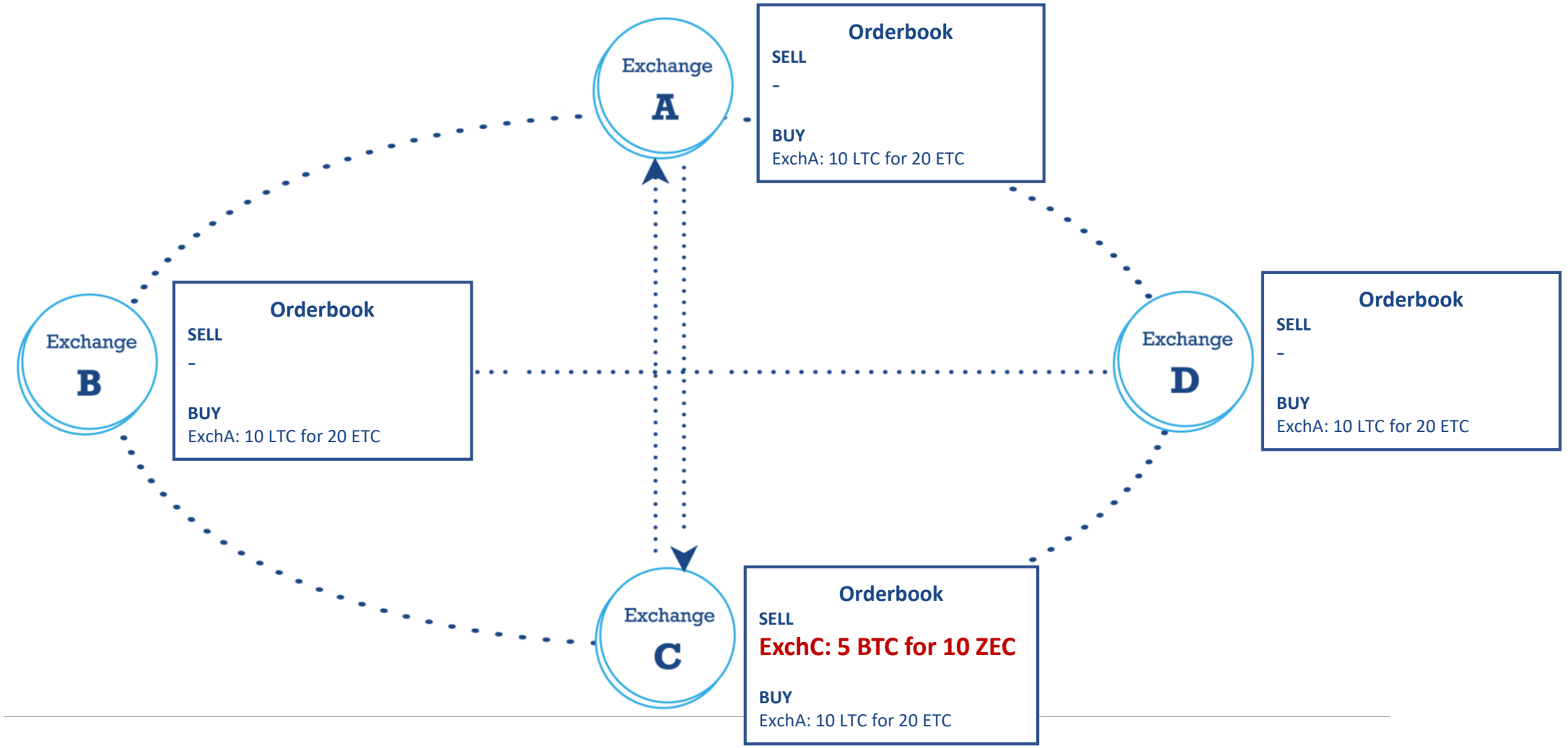
2. Atomic Swaps

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

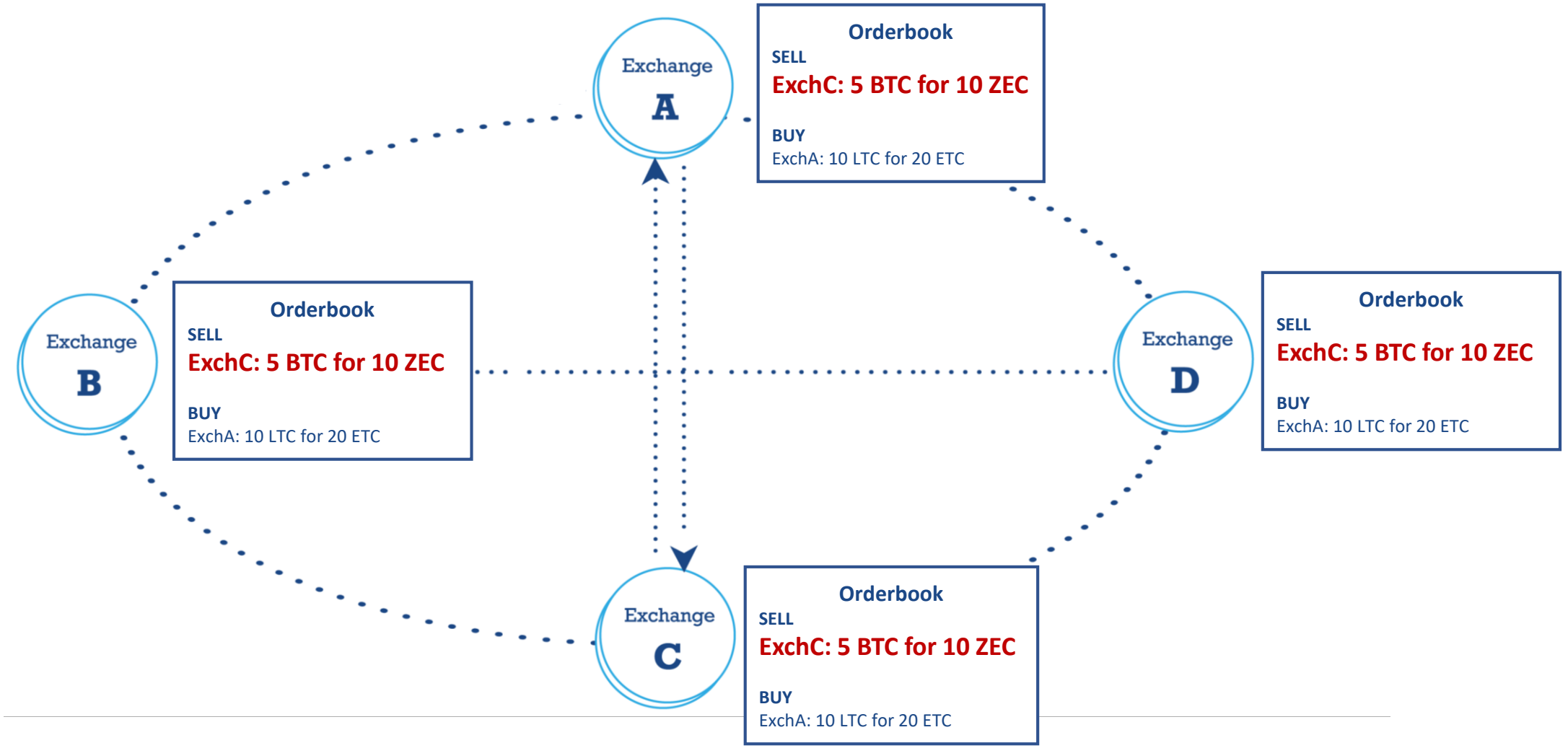
3. Decentralized Orderbook



3. Decentralized Orderbook



3. Decentralized Orderbook



3. Decentralized Orderbook

- XU node software will propagate order updates to peers
  → XUC reward for relaying orders
- Orders may be signed by known key to prove authenticity
- Takers ping maker node to ensure validity and create invoice & swap route

Summary

Decentralized & Open Source

Technology:

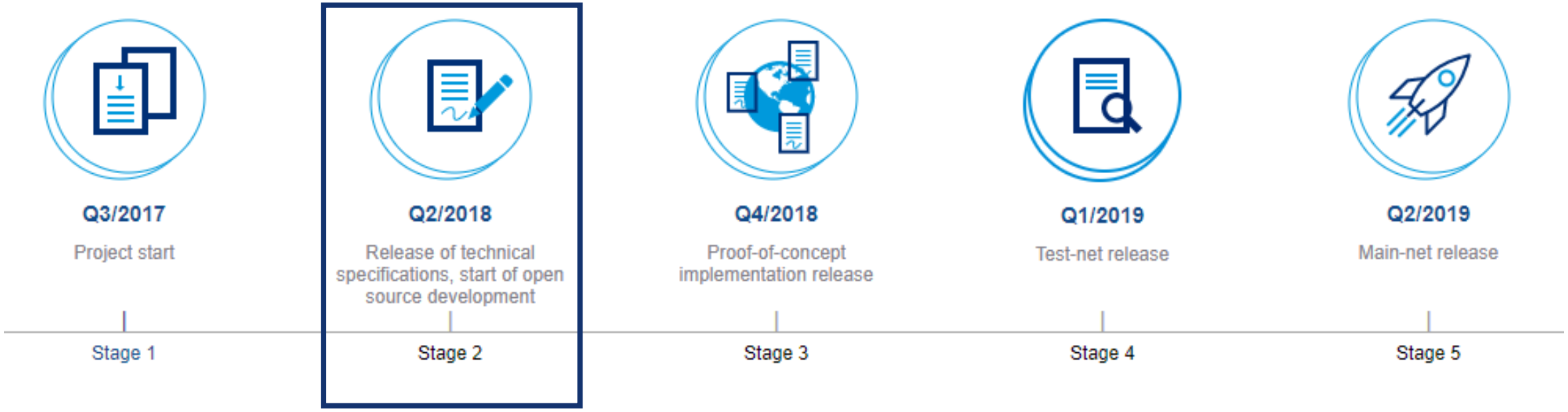
- Payment Channels
- Atomic Swaps
- Decentralized Orderbooks

Benefits:

- Exchanges: increased revenue & liquidity
- Users: trade from one account & best price

XUC: fee and incentive system

Where are we?


Q3/2017
Project start
Stage 1
Q2/2018
Release of technical specifications, start of open source development
Stage 2
Q4/2018
Proof-of-concept implementation release
Stage 3
Q1/2019
Test-net release
Stage 4
Q2/2019
Main-net release
Stage 5

Outlook

Exchange Union is infrastructure

Exchanges as first ‘users’, endgame: individuals

Base for entire new products:

- Wallets
- Merchant PoS

How to get involved?

We need YOU!

- Open Source Lightning/Raiden Developer
- Blockchain developer /Cryptographer

exchangeunion.com
/jobs

Participate!

github.com/ExchangeUnion

t.me/exchangeunioncoin

twitter.com/exchange_union

Shape the way we exchange digital assets in future