Paris P2P, January 9, 2020

Decentralized Settlement & Atomic Swaps
A simple, fair exchange protocol

Pierre Noizat
Chief Executive Officer & Founder

pierre.noizat@blockchain.io

blockchain.io
by paymium

The **trusted** exchange for crypto-actives

blockchain.io

- ▶ Delivering 3 generations of trading platforms

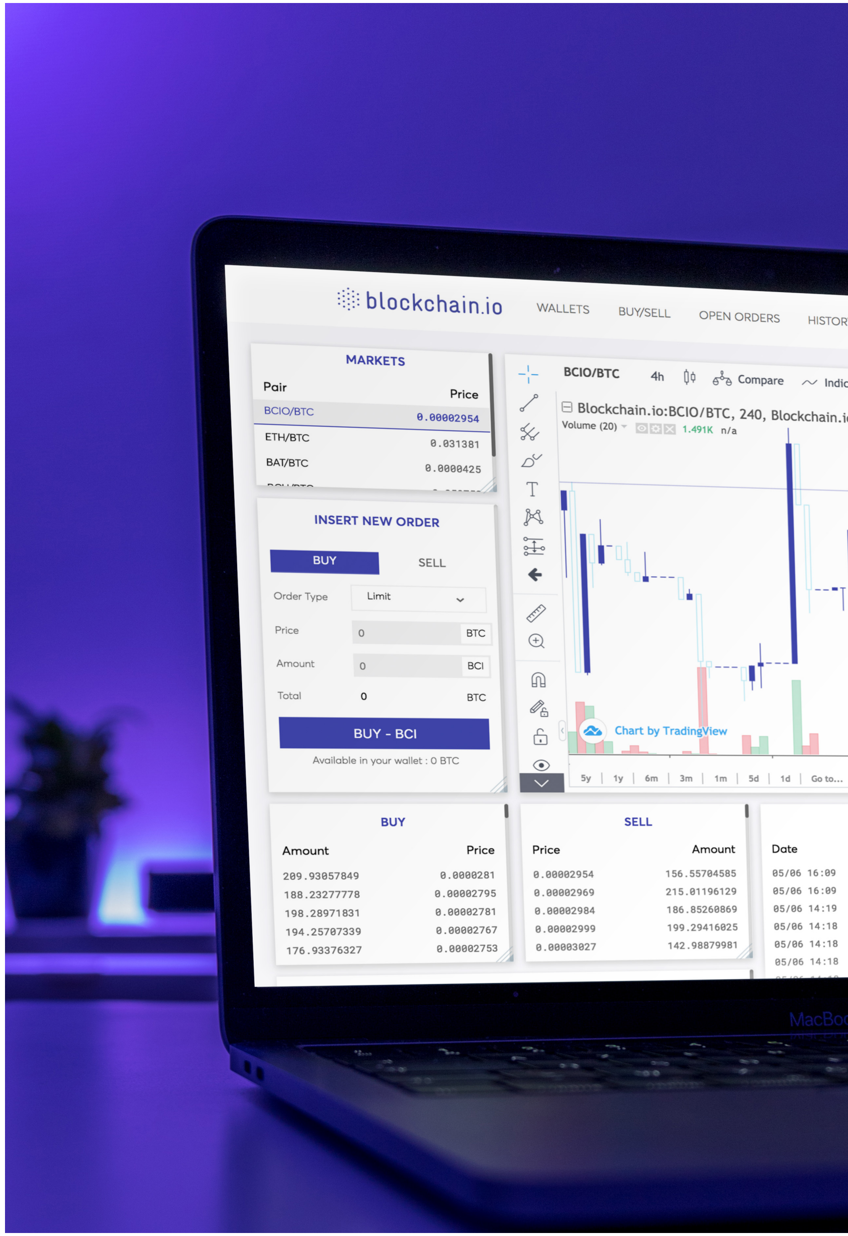
Amazing delivery since 2010

- ▶ Pioneering the ecosystem

Understanding European regulation and compliance issues

- ▶ Lowest fees on the market

Frugality as a core value



MARKETS

Pair	Price
BCIO/BTC	0.00002954
ETH/BTC	0.031381
BAT/BTC	0.0000425

INSERT NEW ORDER

BUY SELL

Order Type: Limit

Price: 0 BTC

Amount: 0 BCI

Total: 0 BTC

Available in your wallet : 0 BTC

BUY

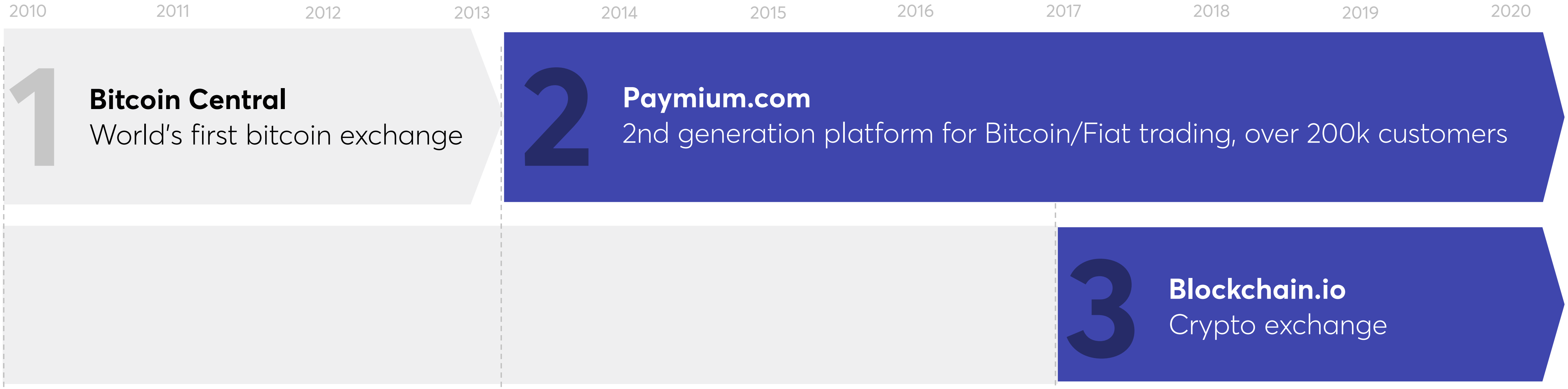
Amount	Price
209.93057849	0.0000281
188.23277778	0.00002795
198.28971831	0.00002781
194.25707339	0.00002767
176.93376327	0.00002753

SELL

Price	Amount
0.00002954	156.55704585
0.00002969	215.01196129
0.00002984	186.85260869
0.00002999	199.29416025
0.00003027	142.98879981

Date
05/06 16:09
05/06 16:09
05/06 14:19
05/06 14:18
05/06 14:18
05/06 14:18

A unique track record of delivering state of the art trading platforms **since 2010**



Bitcoin Central
World's first bitcoin exchange

Paymium.com
2nd generation platform for Bitcoin/Fiat trading, over 200k customers

Blockchain.io
Crypto exchange

1st Generation

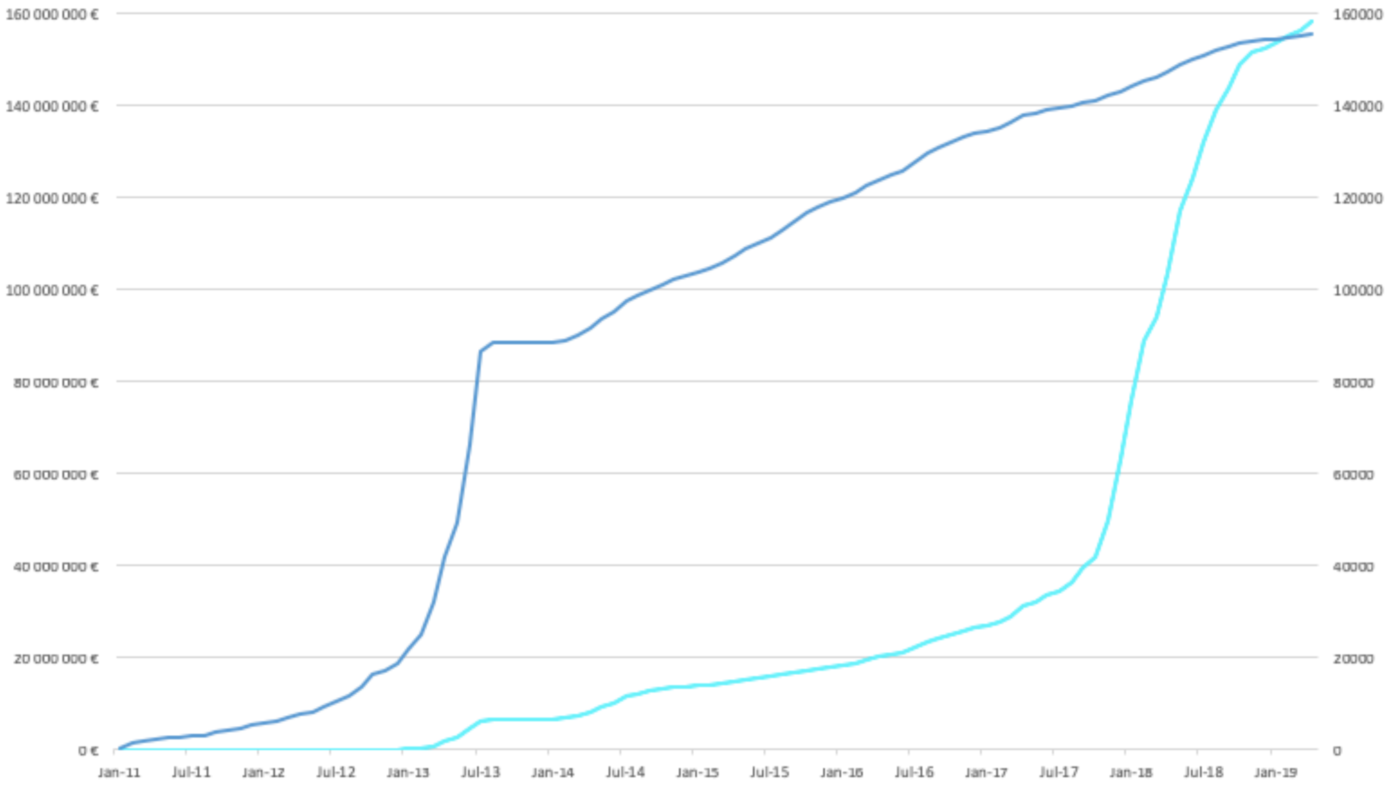
2nd Generation

- Scalability
- Improved security

3rd Generation

- Multi-currency
- Over 50 altcoin markets added

A history of **continuous growth** since 2010…
Through the ups and downs of the crypto market



155,000 BTC

Traded on our platforms

Cumulated trade volume in euros and BTC on bcio.com

▬ Cumulated BTC volume

▬ Cumulated Euros volume

A **strong user base** supported by an active community

250k+

customers

✉	🐦	✈	in	👽	f
250k	75.1k	49.7k	24k	24k	23k

The amounts indicated are cumulative. They include Paymium and Blockchain.io communities.

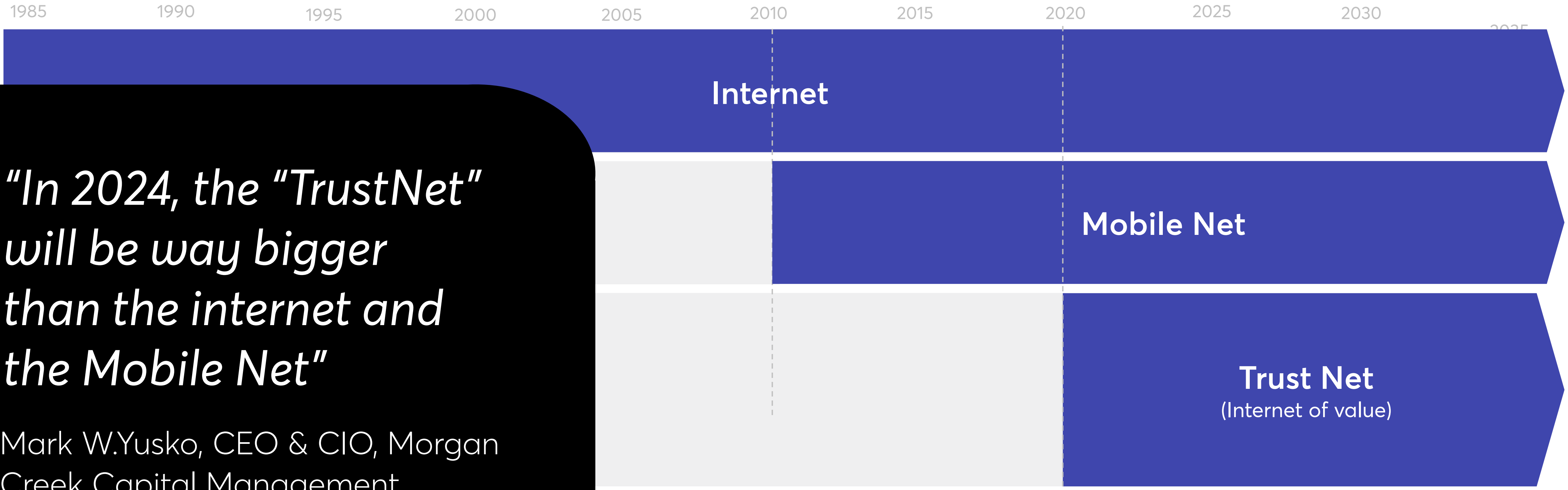
Tokenization, the next big thing?

blockchain.io
by paymium

“10% of the global GDP will be stored & transacted as digital tokens by 2025–27.”

Projection from World Economic Forum, Deloitte & McKinsey

The internet of value: **a natural evolution**

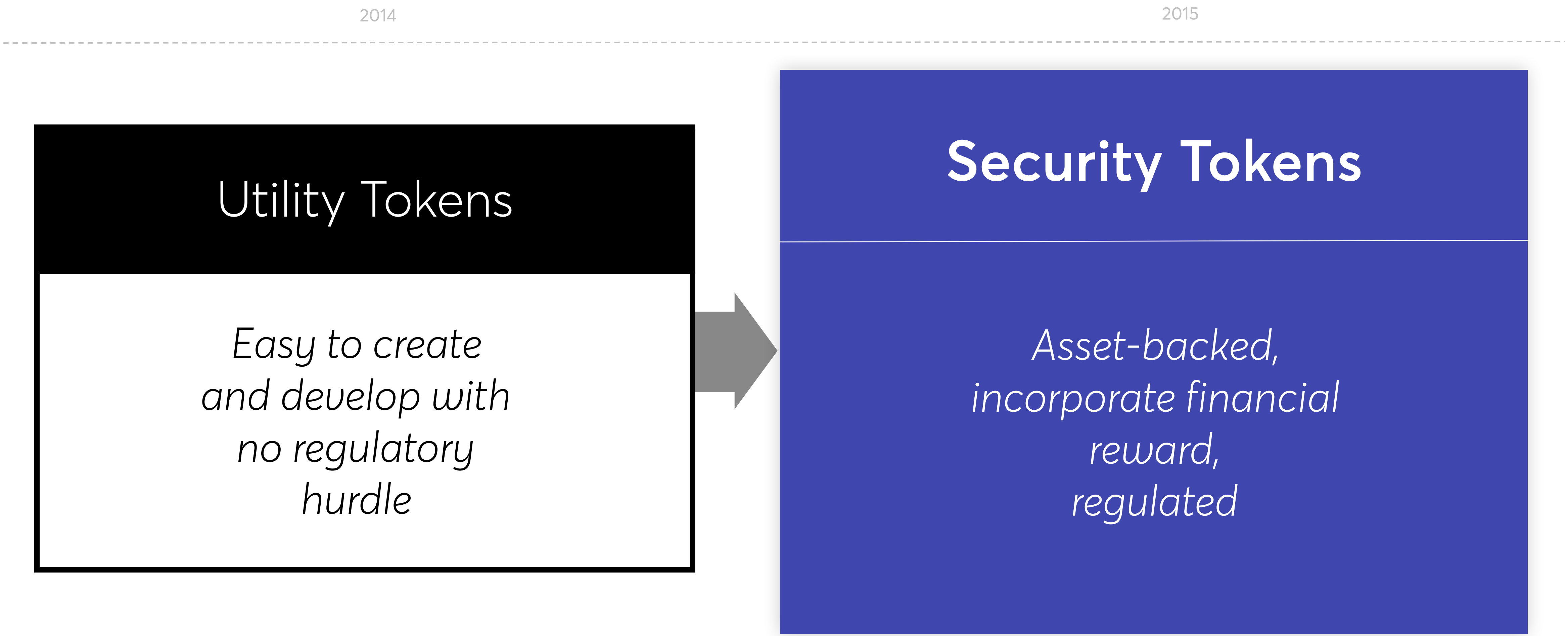


> *"In 2024, the "TrustNet" will be way bigger than the internet and the Mobile Net"*

Mark W.Yusko, CEO & CIO, Morgan Creek Capital Management

Source: https://www.newsbtc.com/2019/03/28/analyst-trading-crypto-on-coinbase-is-48x-more-expensive-than-stock-exchange/

The history of **Tokenization**



2014

2015

Utility Tokens

Easy to create and develop with no regulatory hurdle

Security Tokens

Asset-backed, incorporate financial reward, regulated

Unlimited creativity: **Any assets can be tokenized**

Applying to

Physical assets

Arts

Luxury Products

Cars

Real Estate

Gold

Financial assets:

Mortgages

Derivative Securities

Loans Equity

Funds

Bonds

Private Company Shares

How will asset owners benefit **from tokenization?**

Divisibility

Global Reach

Blockchain Custody

- Can be used as payment means just like traditional money
- No minimum investment amount
- Investors, issuers, and operators are not locked into a single pool of liquidity.
- Streamlined, low-cost issuance and transaction processing

What's needed to help **develop tokenization?**

Education

Link between tokenized asset and token legally recognized

Usage of tokens as payment means by merchants and consumers

Why is there is a **need for crypto exchanges?**

Multi-lateral Trading Facilities (MTF) **workflows are not adapted** to the crypto ecosyster

MTFs are the equivalent of Alternative Trading Systems (ATS) in the USA

Location: about:

Netscape Navigator™
Version 3.0
Copyright © 1994-1996 Netscape Communications Corporation, All rights reserved.

This software is subject to the license agreement set forth in the license. Please read and agree to all terms before using this software.

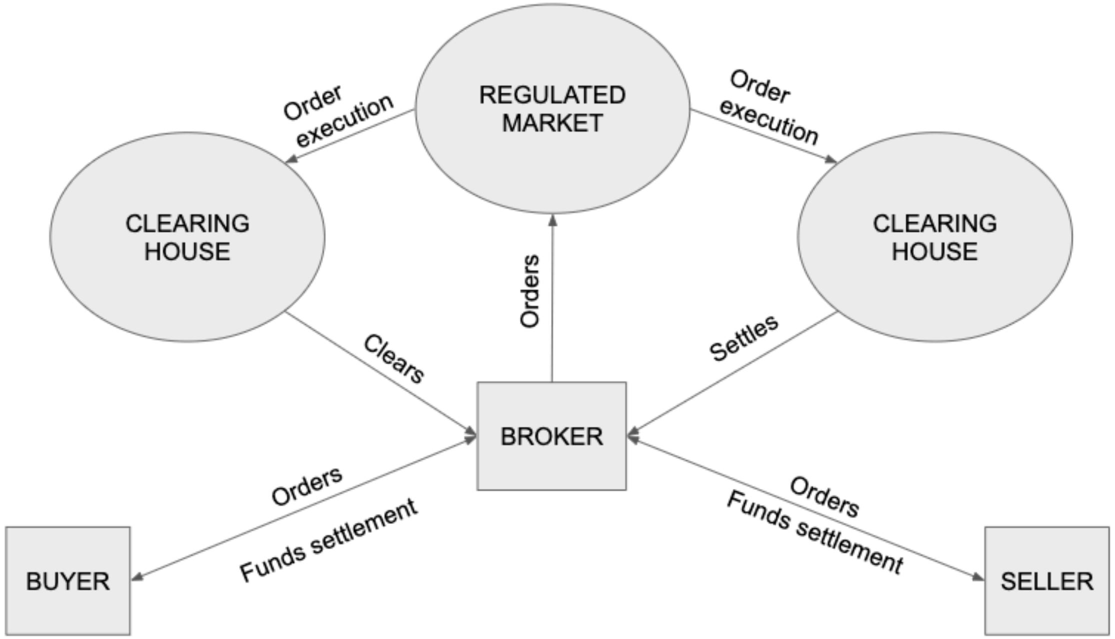
Report any problems through the feedback page.

Netscape Communications, Netscape, Netscape Navigator and the Netscape Communications logo are trademarks of Netscape

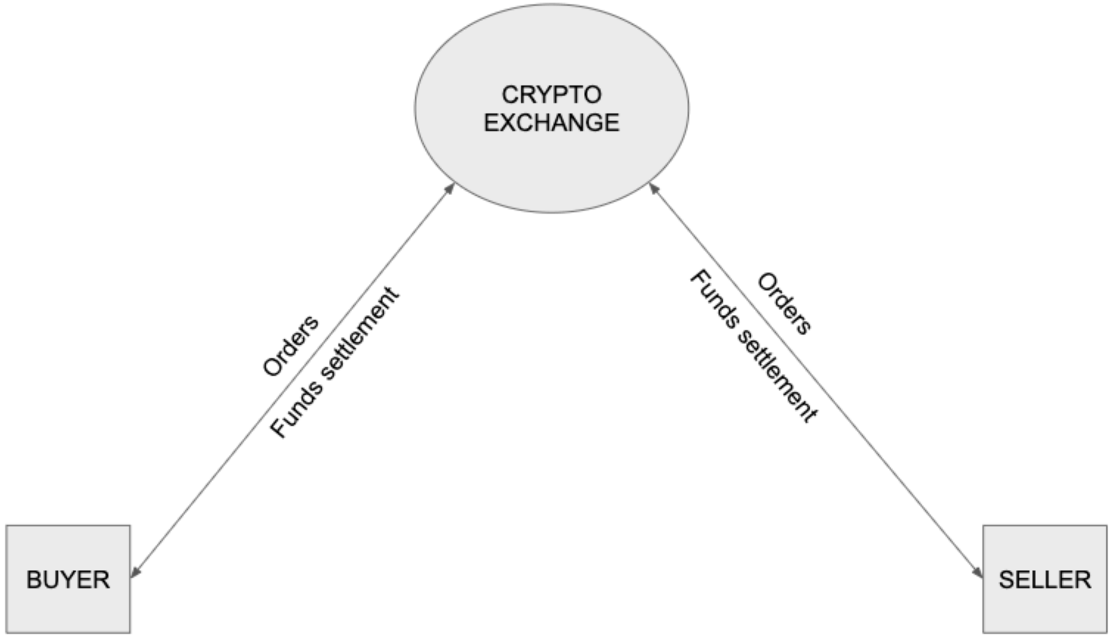
Document: Done

Crypto-exchanges are as necessary as web browsers to navigate among cryptocurrencies.

Crypto-exchange workflow
VS/ MTF workflow

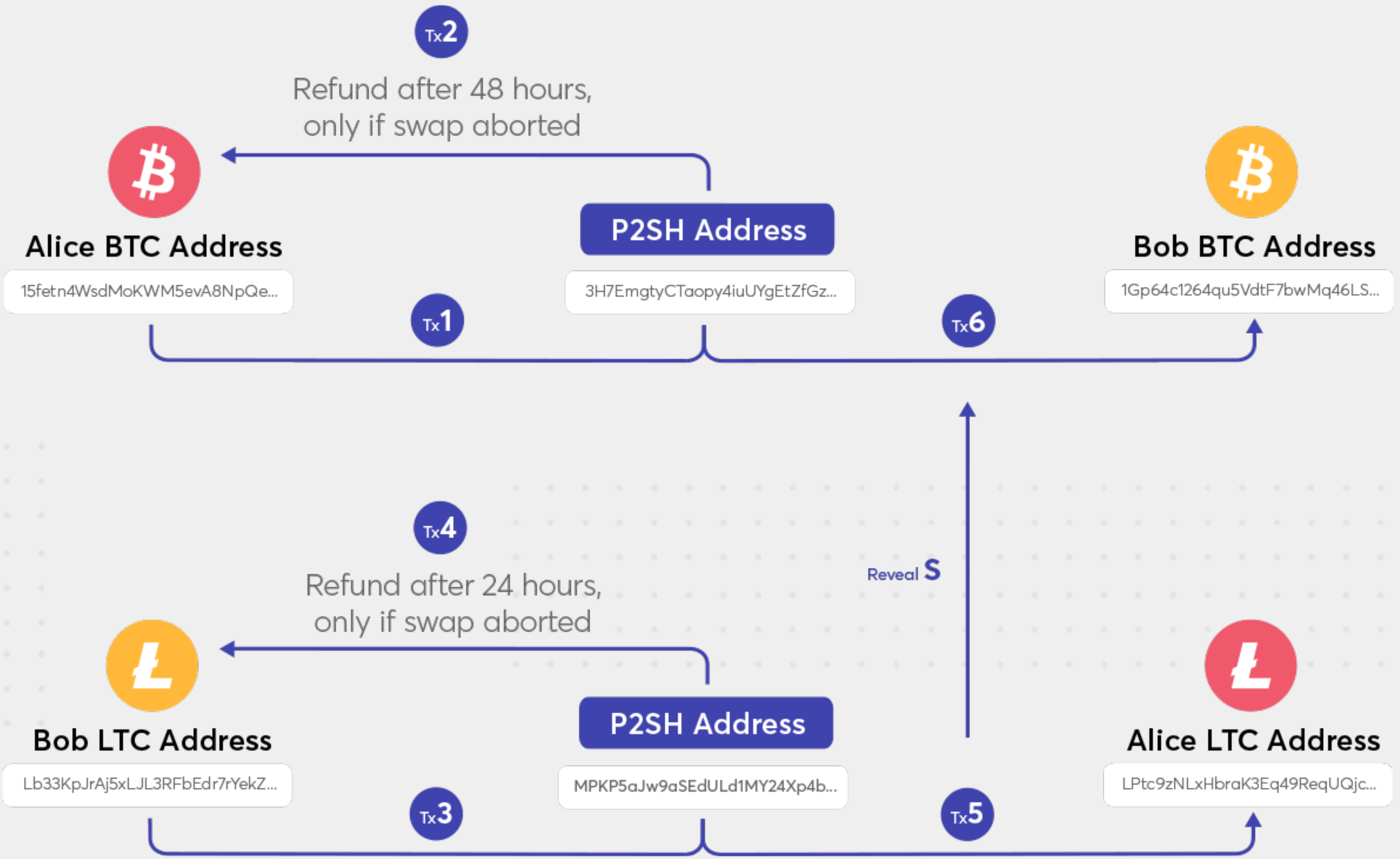


MTF workflow



Crypto-exchange workflow

Atomic Swap Transactions



Tx2

Refund after 48 hours,
only if swap aborted

Alice BTC Address

15fetn4WsdMoKWM5evA8NpQe...

P2SH Address

3H7EmgtyCTaopy4iuUYgEtZfGz...

Bob BTC Address

1Gp64c1264qu5VdtF7bwMq46LS...

Tx1

Tx6

Tx4

Refund after 24 hours,
only if swap aborted

Reveal S

Bob LTC Address

Lb33KpJrAj5xLJL3RFbEdr7rYekZ...

P2SH Address

MPKP5aJw9aSEdULd1MY24Xp4b...

Alice LTC Address

LPtc9zNLxHbraK3Eq49ReqUQjc...

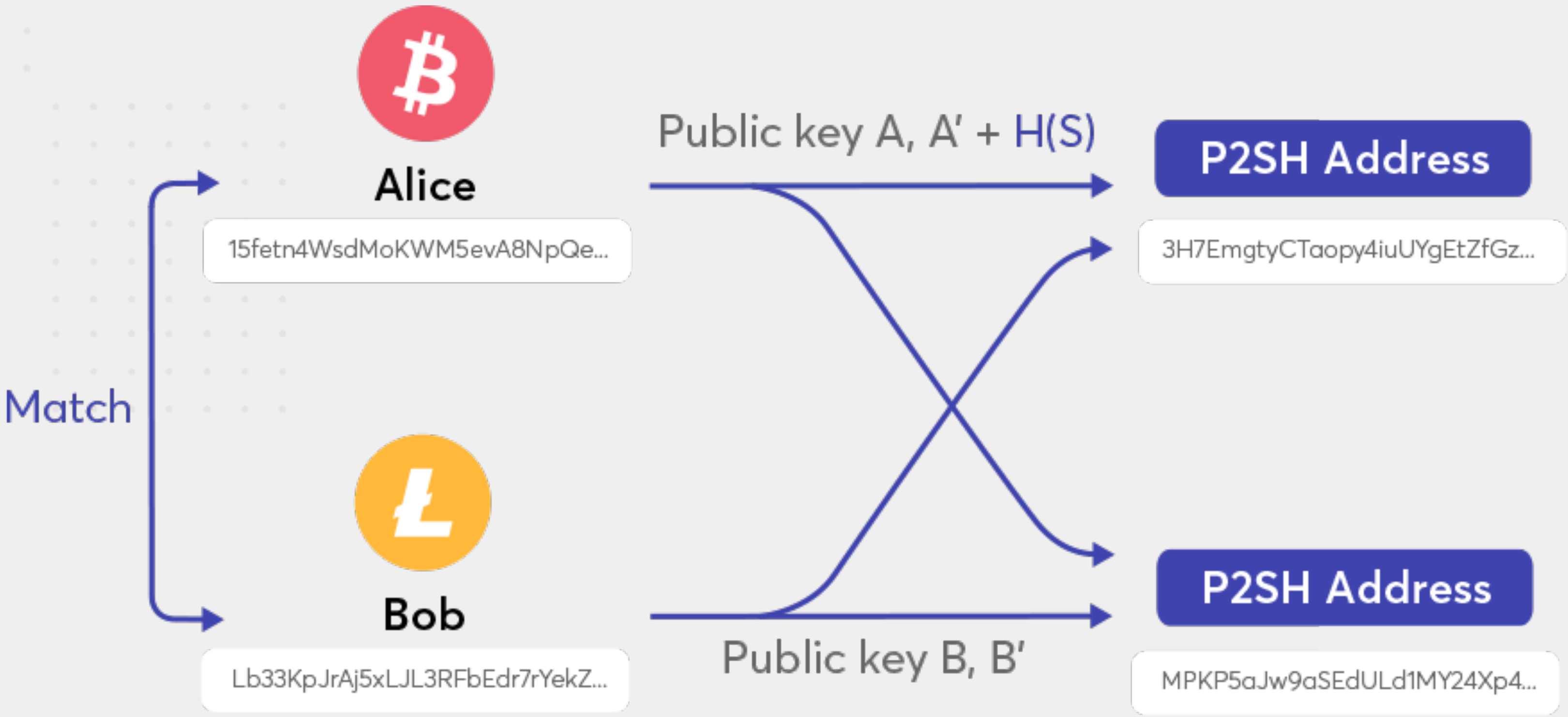
Tx3

Tx5

▶ PHASE 0

Alice and Bob are **matched**

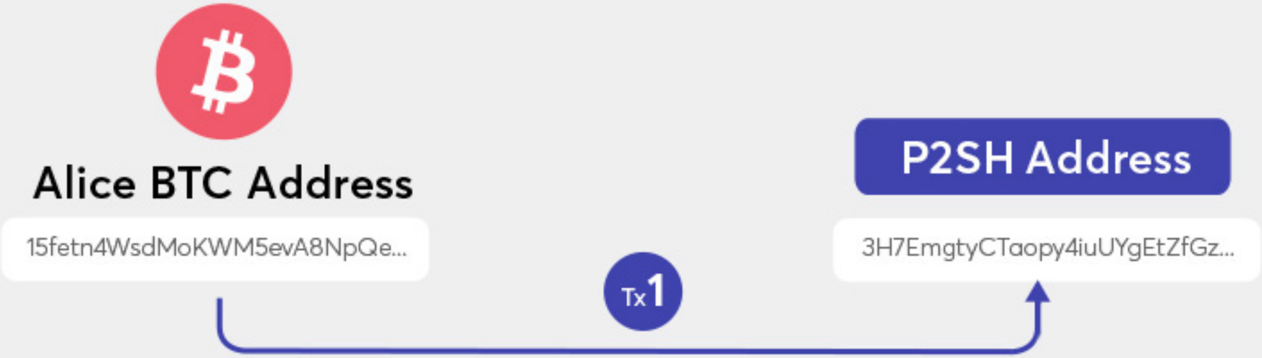
Alice creates a bid offer with a public key and the hash of her secret S.


Alice
15fetn4WsdMoKWM5evA8NpQe...
Match
Bob
Lb33KpJrAj5xLJL3RFbEdr7rYekZ...
Public key A, A′ + H(S)
Public key B, B′
P2SH Address
3H7EmgtyCTaopy4iuUYgEtZfGz...
P2SH Address
MPKP5aJw9aSEdULd1MY24Xp4...

PHASE 1.1

Alice **bails in**

Alice constructs TX1 to bail in x BTC but does not broadcast it yet.



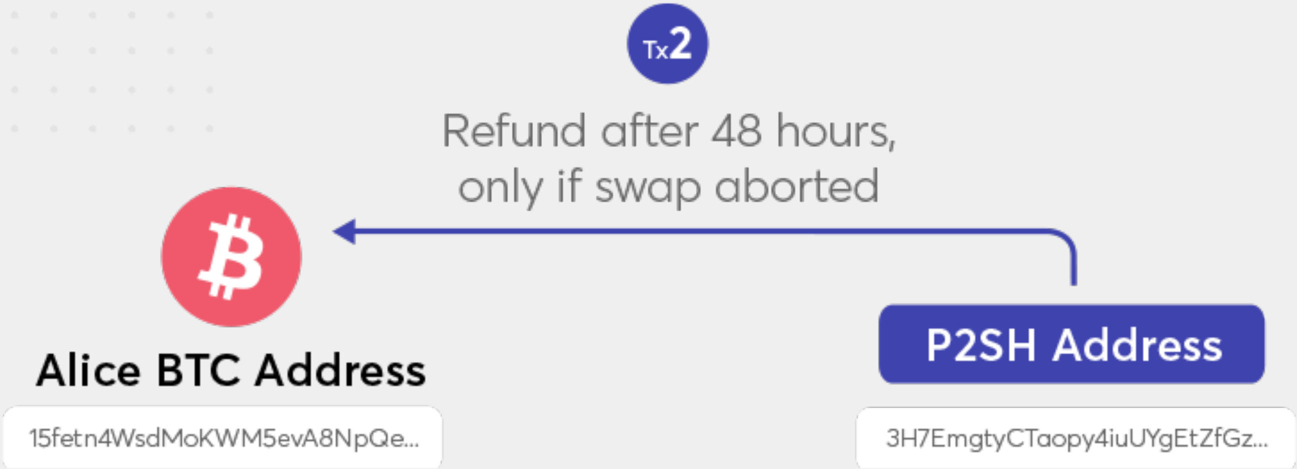
```
IF
// Ordinary claim for B
HASH160 <H(S)> EQUALVERIFY
2 <pubkeyA> <pubkeyB>
ELSE
// Refund for A
2 <pubkeyA’> <pubkeyB’>
ENDIF
2 CHECKMULTISIG
```

▶ PHASE 1.2

Alice **bails in**

Alice creates her timelocked Bitcoin refund TX2 and sends it to Bob for signature.

When Alice receives <sigB2’>, Tx1 is safe for her to broadcast.



15fetn4WsdMoKWM5evA8NpQe...

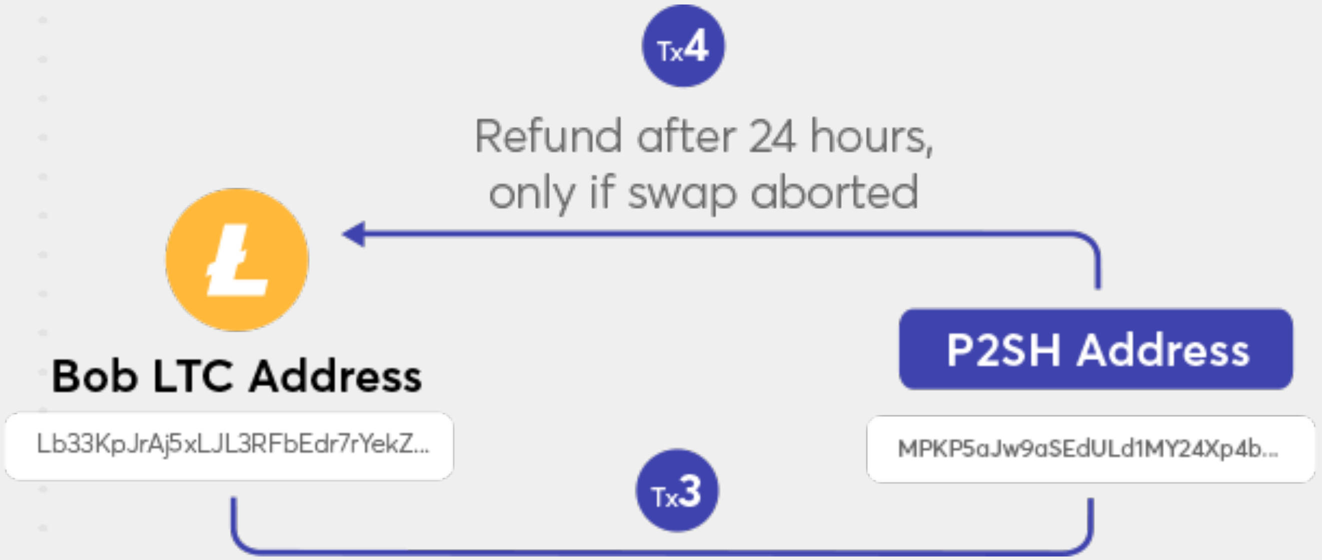
3H7EmgtyCTaopy4iuUYgEtZfGz...

<sigB2’> <sigA2’> FALSE

▶ PHASE 2

Bob **bails in**

Bob creates Litecoin transaction TX3 and his refund TX4.

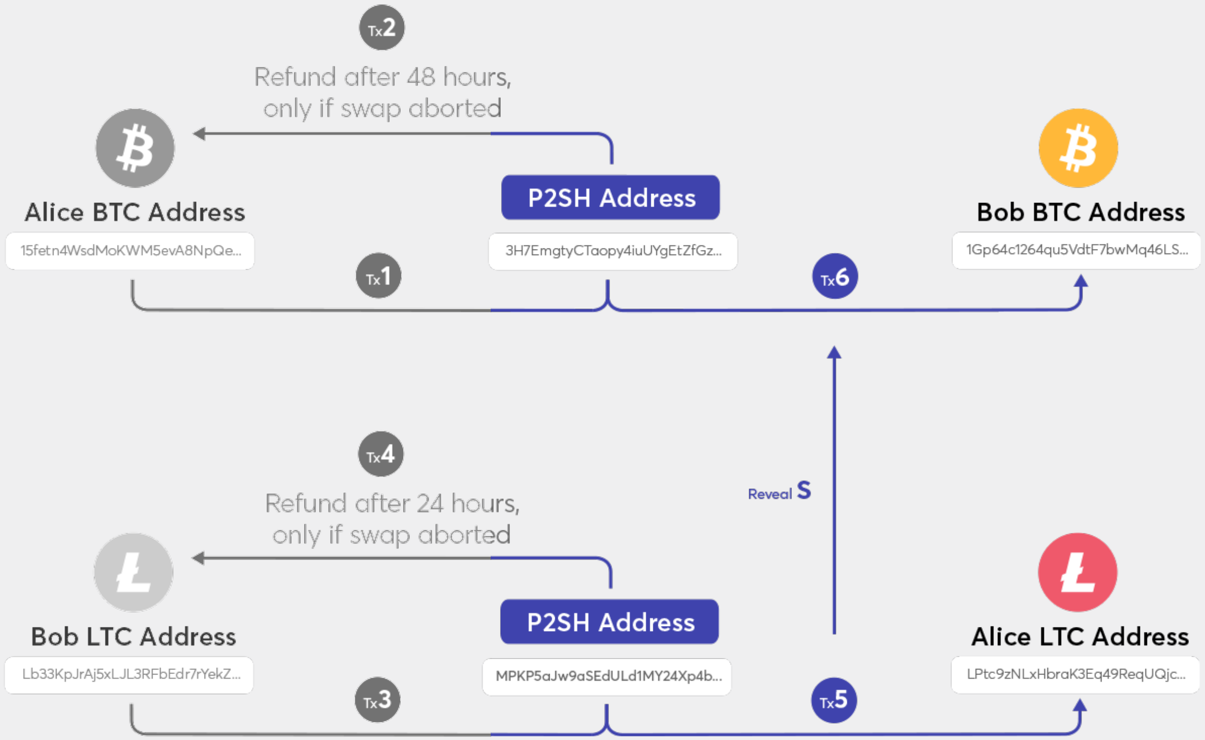


<sigB4’> <sigA4’> FALSE

▶ PHASE 3.1

Alice reveals S and **triggers both transactions**

Alice sends <sigA6>. Bob responds with <sigB5> .

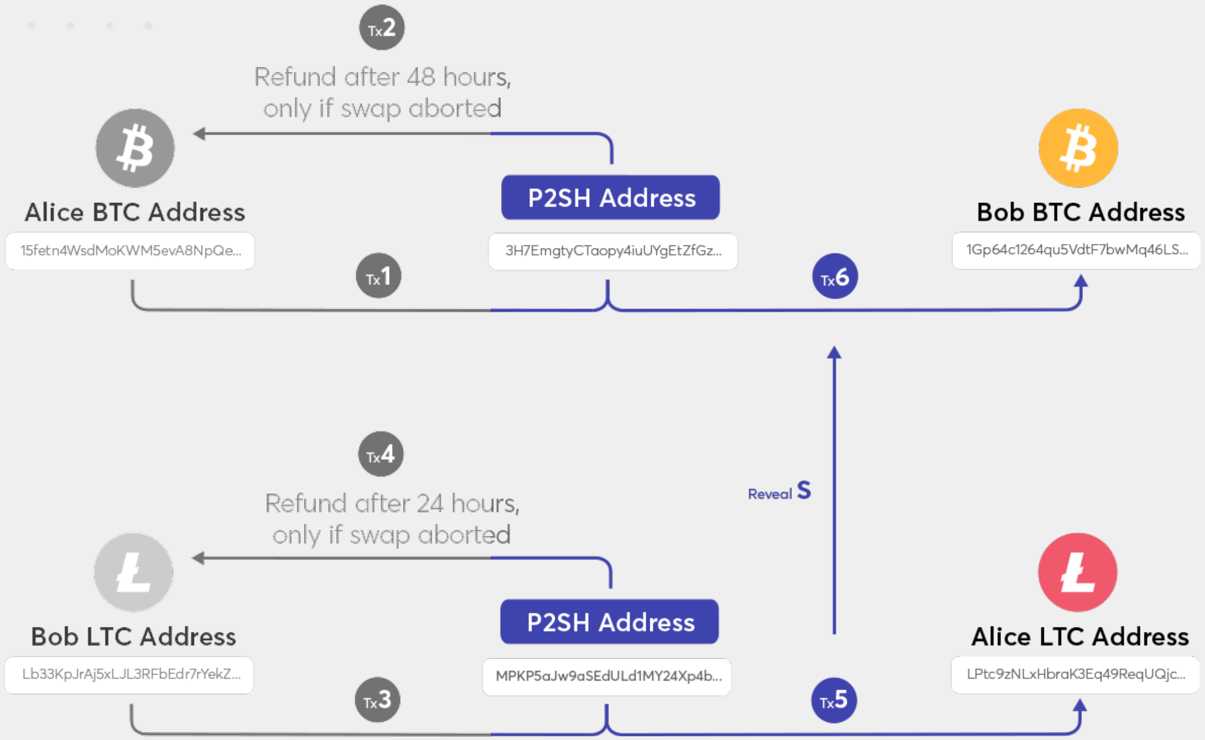


<sigA5><sigB5> <S> TRUE

PHASE 3.2

Bob **collects his bitcoins** with TX6

Bob learns S when Alice broadcasts Tx5.



<sigA6><sigB6> <S> TRUE

Thank you

Pierre Noizat
Chief Executive Officer & Founder

pierre.noizat@blockchain.io

blockchain.io
by paymium