

Blockchain Application: DEX (Decentralized Exchange)

Presented By Hyunjin Choo

Contents

- 1 Introduction**
- 2 Background**
- 3 CEX vs DEX**
- 4 Types of DEX**
- 5 Future Works**
- 6 Conclusion**

Contents

1 Introduction

2 Background

3 CEX vs DEX

4 Types of DEX

5 Future Works

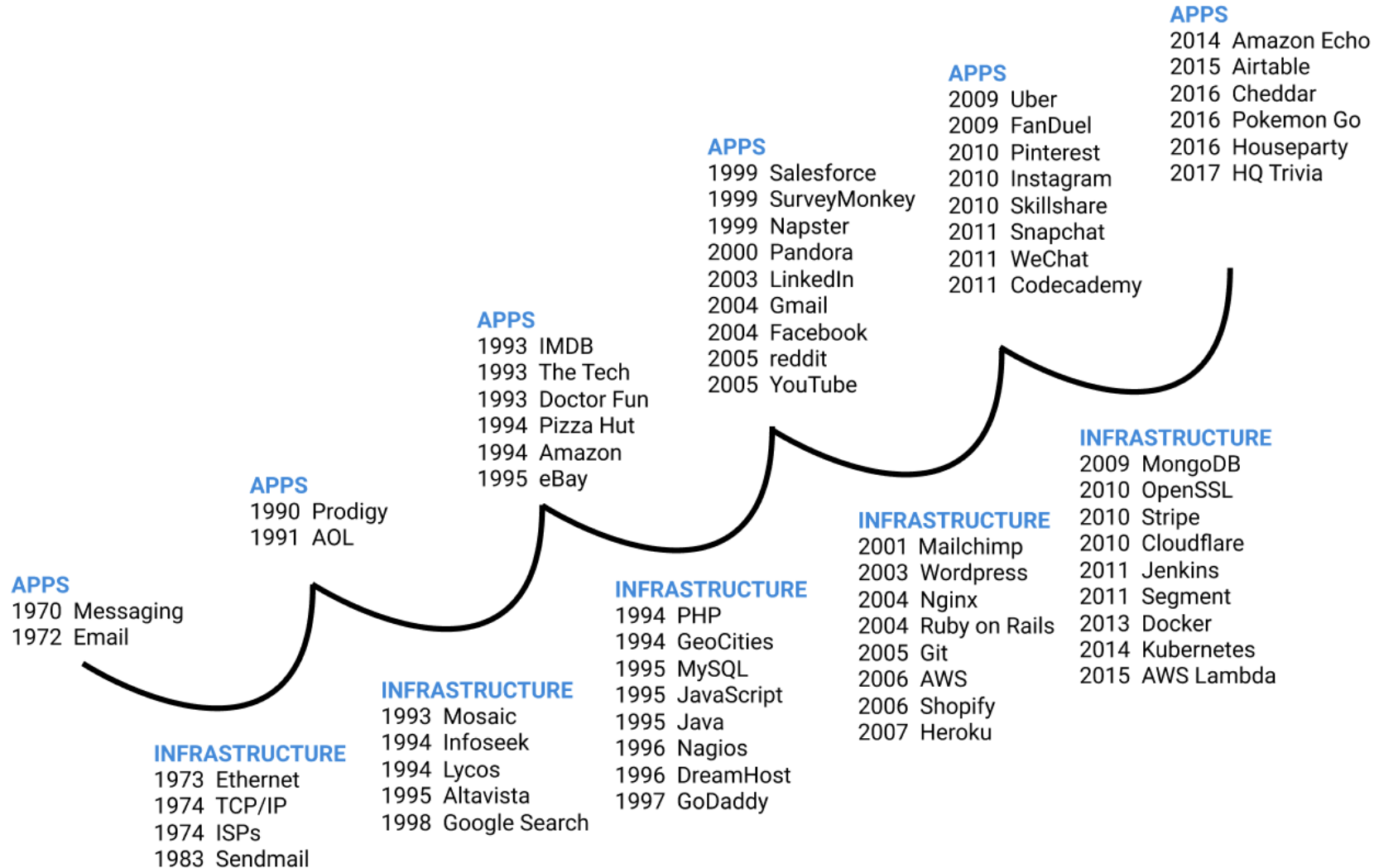
6 Conclusion

The Myth of The Infrastructure Phase

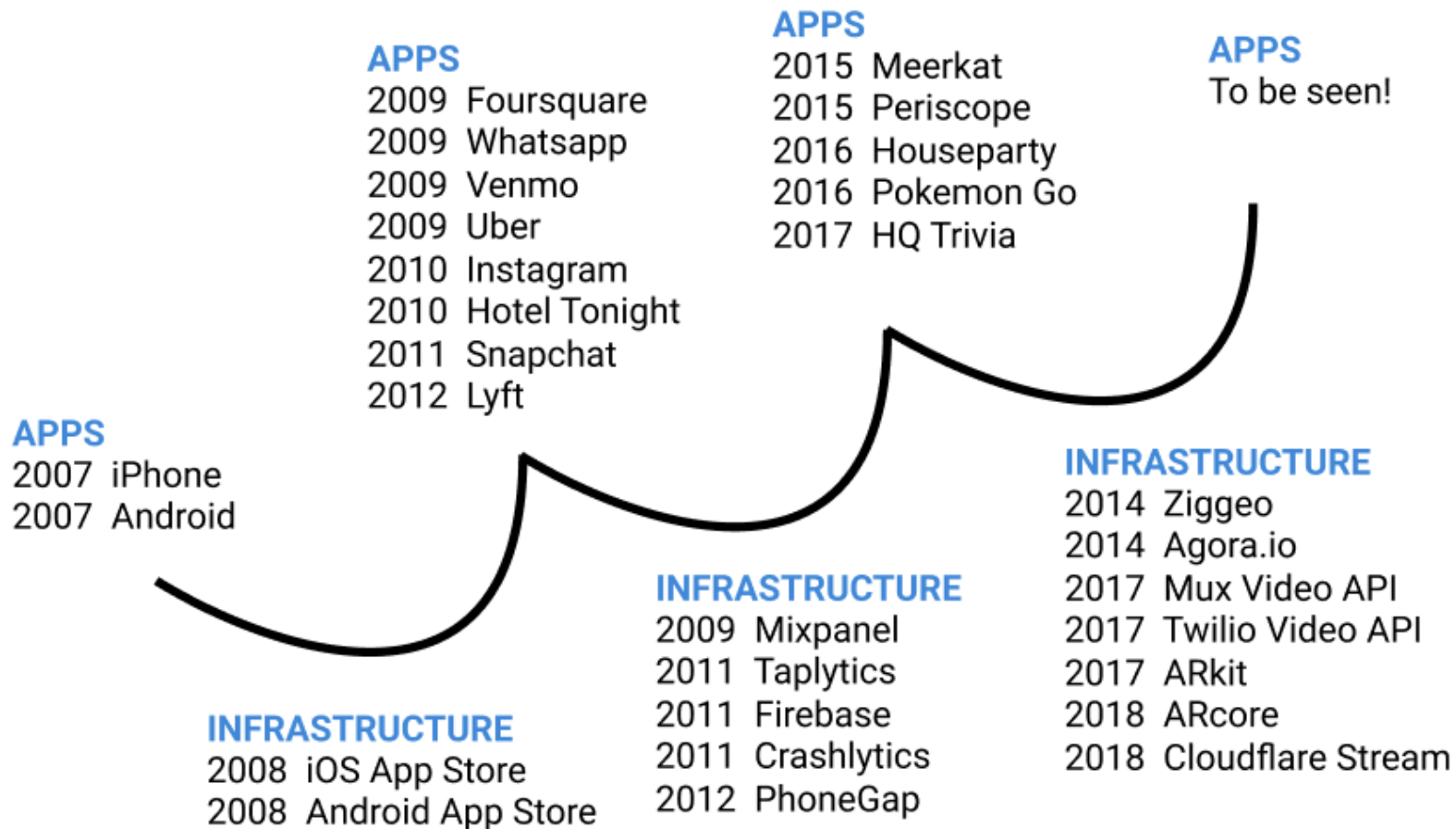
- ❖ OCT 01, 2018 By UNION SQUARE VENTURES
- ❖ Platforms evolve from an iterative cycle of apps → infrastructure → apps → infrastructure



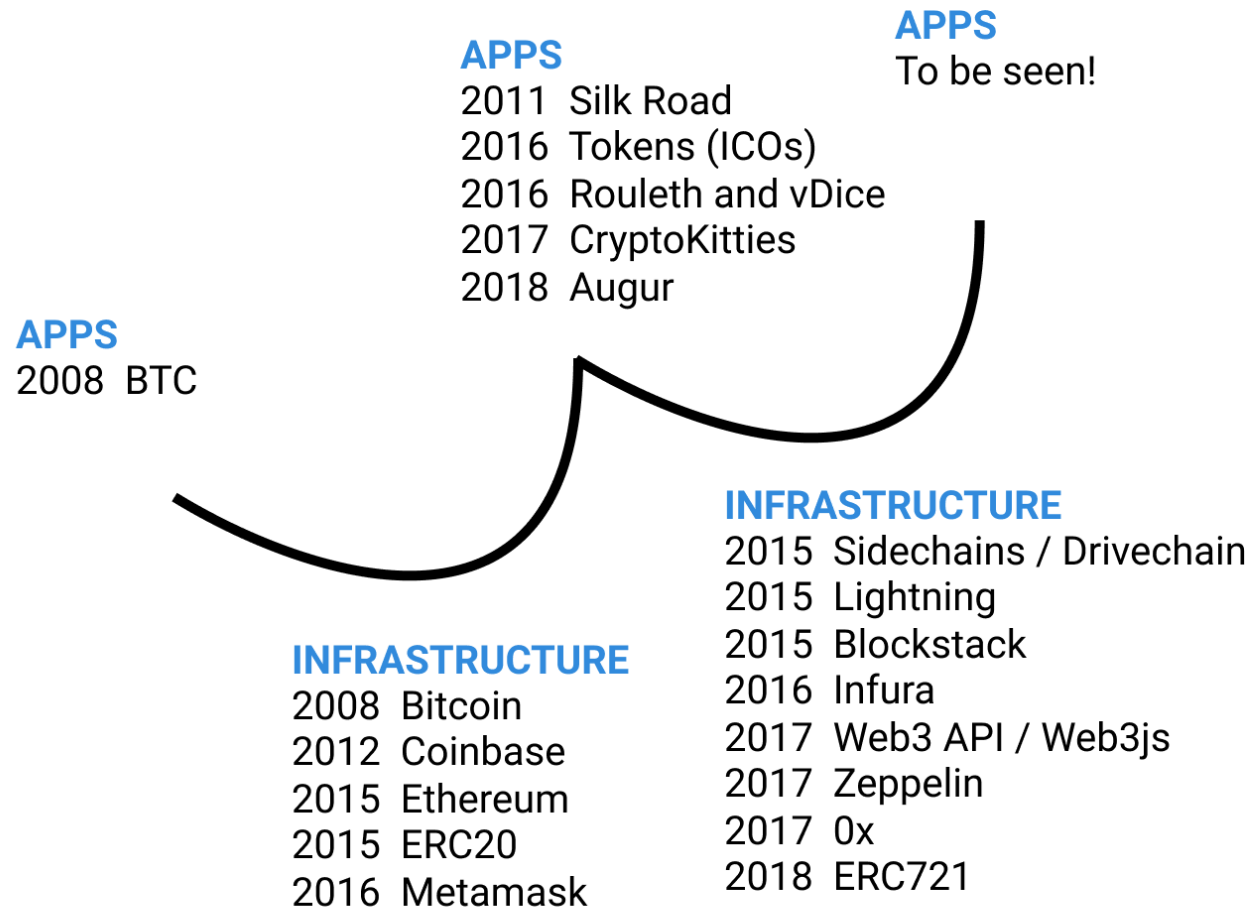
A History of the Internet



A History of the Mobile Apps



Next Big Thing for Web 3.0?



Blockchain and Exchange

- ❖ The primary goal of public blockchain is to return the control of money to the owners
 - We measure the value of goods and services (medium-of-exchange), or rich and poor (store of value) by the amount of Fiat currencies, which are evolved from the barter and issued and controlled by the government
 - Cryptocurrencies (Coins) such as Bitcoin or Ethereum instead of Fiat currencies are used in the token economy and tokens such as Tether and MakerDAO are issued on the blockchains
- ❖ However, we have to use 3rd service cryptocurrency exchange as a 1st gateway to enter the token economy from the real world
 - Cryptocurrencies became famous for price fluctuation first but not as currencies or assets
 - Cryptocurrency exchanges are for-profit businesses that allow customers to move between different cryptocurrencies and fiat currencies

A History of Theft and Loss

Technology

Bitcoin Price Plunges as Mt. Gox Exchange Halts Activity

Carter Dougherty

February 7, 2014, 8:25 PM GMT

Bitcoin plunged more than 8 percent today after a Tokyo halted withdrawals of the digital currency, citing technic



Bitcoin exchange BitFloor shuttered after virtual heist

Nearly a quarter million dollars worth of the peer-to-peer currency was stolen by accessing unencrypted backup wallet keys.

BY STEVEN MUSIL / SEPTEMBER 4, 2012 8:50 PM PDT



TECH • BITCOIN

Bitcoin Worth \$72M Was Stolen in Bitfinex Exchange Hack in Hong Kong



Bitstamp exchange hacked, \$5M worth of bitcoin stolen

The European bitcoin exchange suspends its service after it was hacked. ZDNet can confirm. Less than 20,000 bitcoins were stolen from an operational wallet.

By David Schindler for ZDNet | January 8, 2015 — 10:43 AM (UTC-05:00) | Topic: Security



Contents

1 Introduction

2 Background

3 CEX vs DEX

4 Types of DEX

5 Future Works

6 Conclusion

Exchange 101 (1)

- ❖ An exchange is an organized market where (especially) tradable securities, commodities, foreign exchange, futures, and options contracts are sold and bought

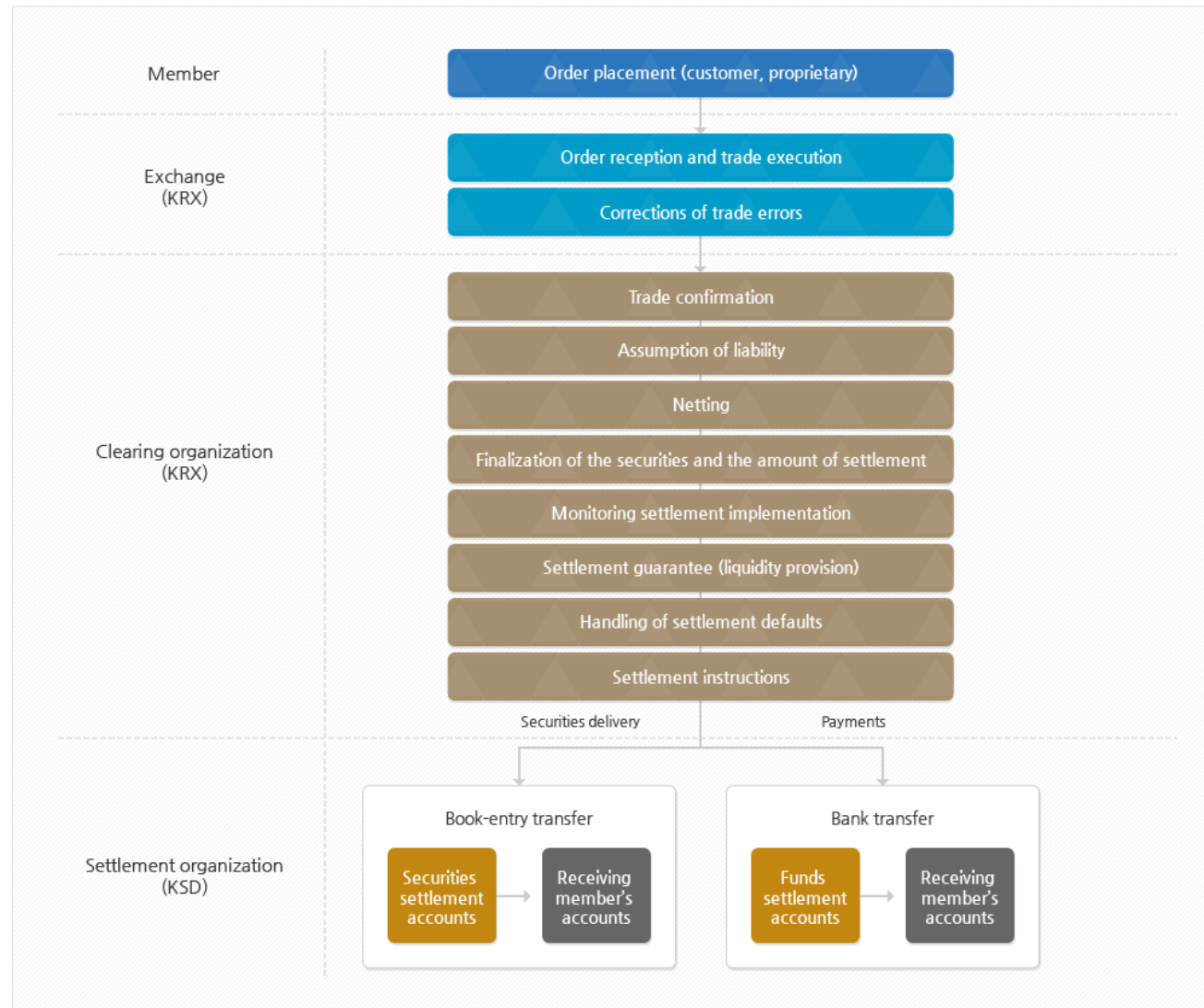


Exchange 101 (2)

- ❖ Purposes for using an exchange
 - Arbitrage: Simultaneous purchase and sale of equivalent assets at prices which guarantee a fixed profit at the time of the transactions
 - Hedging: Simultaneous purchase and sale of two assets in the expectation of a gain from different movements in the price
 - Speculation: Purchase or sale of an asset in the expectation of a gain from changes in the price of that asset

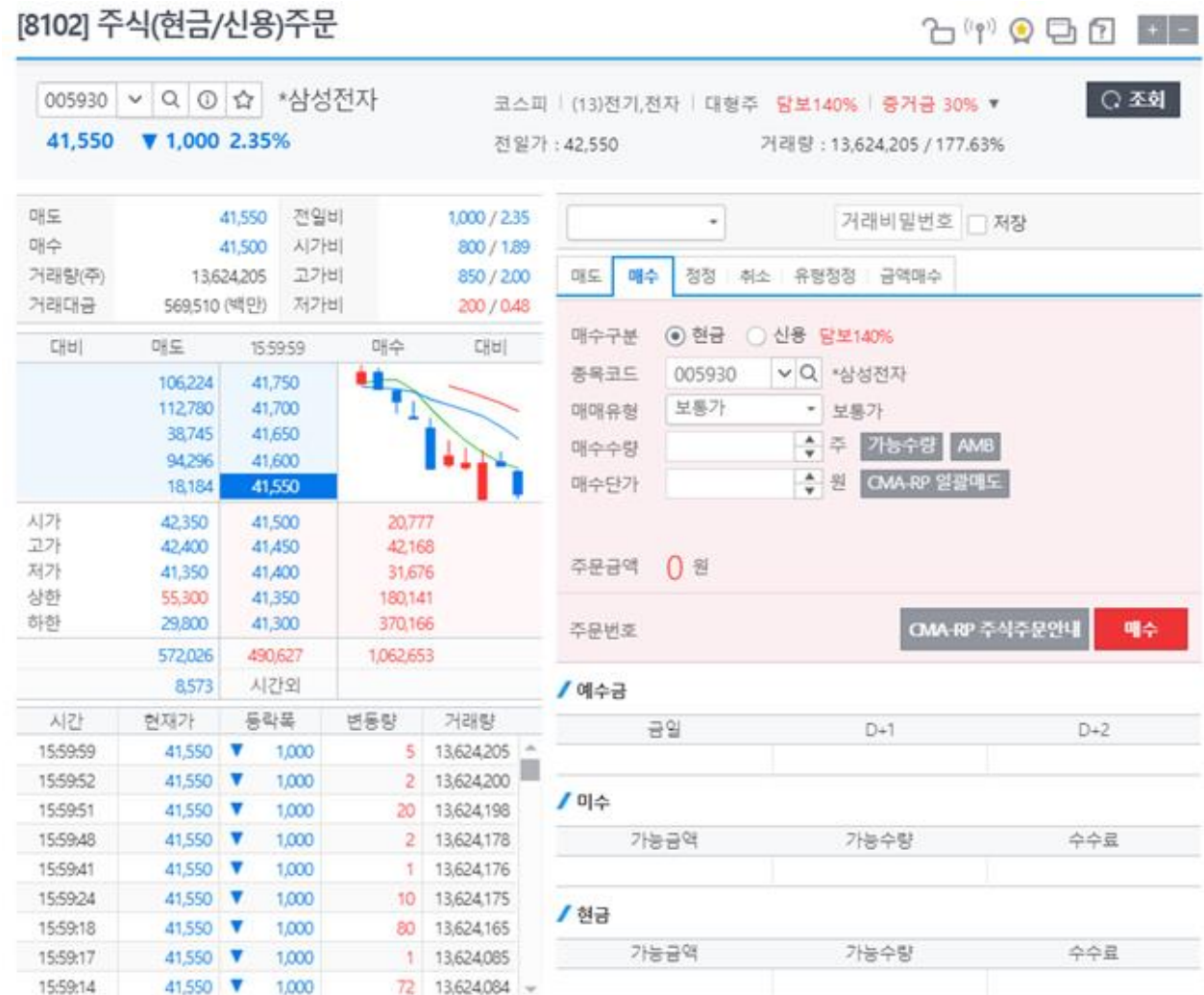
- ❖ Functions of an exchange
 - Ensure fair and orderly trading
 - Efficient dissemination of price information for any securities
 - Give a platform from which to sell securities to the investing public

Trade Stock on KRX (1)



Trade Stock on KRX (2)

- ❖ Open account and deposit fund at securities company
- ❖ Free deposit/withdrawal commission fees
- ❖ Place an order through HTS (PC) or MTS (Mobile)
- ❖ Order is delivered to KRX and matched by KRX
- ❖ Securities transaction tax (Sell): 0.3% → 0.25%
- ❖ Trading fee: 0.01%



Contents

1 Introduction

2 Background

3 CEX vs DEX

4 Types of DEX

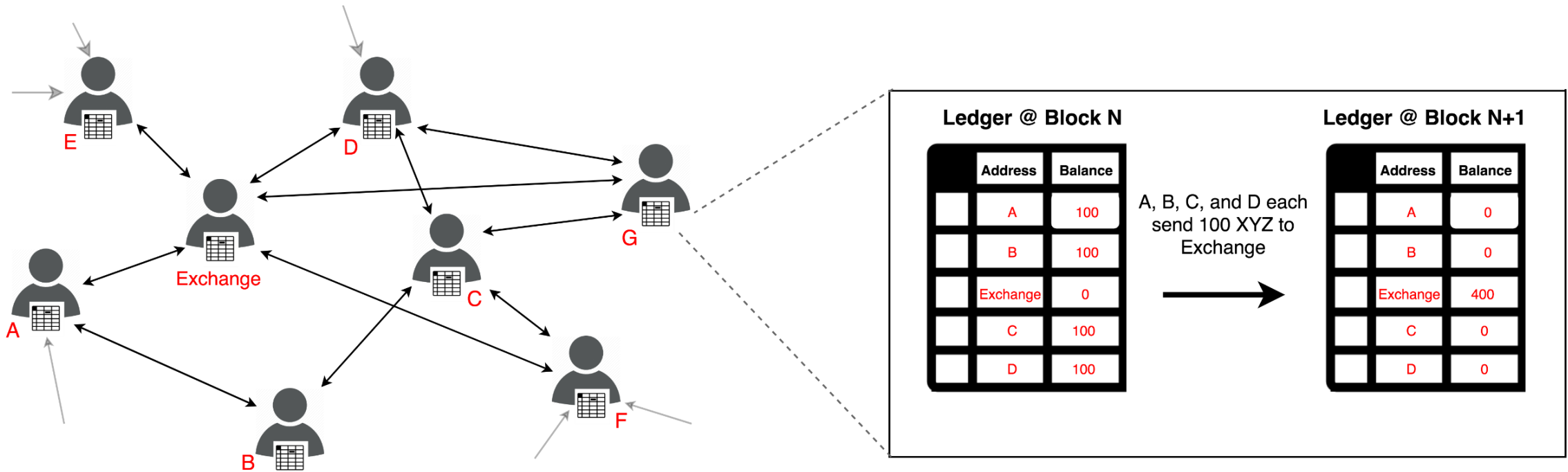
5 Future Works

6 Conclusion

Cryptocurrency Exchange

- ❖ Most exchanges are centralized that the customers have to trust
 - Undermine the nature of the blockchains on which they operate
 - Generate millions of dollars through trading fees and ICO listing fees that can reach \$2.6M per token
- ❖ As of 5/26
- ❖ Trading volume
 - Binance: \$1.6B/day
 - IDEX: \$1.6M/day – #1 DEX but #130 among the all exchanges
- ❖ Market cap of Cryptocurrencies
 - #35 Waves (\$265M) / #41 Aurora (\$200M) / #42 0x (\$190M)

Centralized Exchange (CEX)



Trade on CEX

- ❖ Custody customer funds
 - Deposits fund (either fiat or cryptocurrency) into a pooled wallet, controlled by the exchange
 - The exchange credits a “trading balance”, simply an entry within a centralized database that the exchange updates
- ❖ “Hot” wallet
 - Connected to a network
 - Quick but vulnerable to hacking
- ❖ “Cold” storage
 - Maintained offline, and thus remote from external hackers
 - However, most funds remain in hot wallets
 - An insider such as rogue employee can misappropriate funds with the access to the wallet keys
- ❖ Utilize the exchange’s order book and liquidity pool to trade the assets
 - No control of the private key, thus no control of the fund unless withdrawal
 - Commission fee, limited quantity, and time delay on withdrawal

Trade on CEX (Bithumb) (1)

- ❖ Simple Sign-up and Log in
- ❖ Level verification (KYC / AML)
- ❖ Charge KRW to Virtual Account
- ❖ Deposit/withdraw cryptocurrency

The screenshot displays the 'Verification center' page on the Bithumb website. On the left is a sidebar menu with options: Account management, My Page, Management, Verification center (highlighted), Alert Settings, access information, OTP verification, Transaction management, API management, Online remittance API, and Bithumb Cash Setting. The main content area shows four verification levels in a horizontal sequence, numbered 1 to 4 at the bottom:

- LEVEL 1 Member sign-up**: Requires verifying email or mobile number. Includes 'SMS authentication' and 'E-mail verification' checkboxes.
- LEVEL 2 verification**: Requires completing personal identification (cell phone authentication or ID card submission). Includes 'ID confirmation with cell phone' and 'send ID (passport)' checkboxes.
- LEVEL 3 Written Consent**: Requires clicking a button to fill out a pledge for level 3 verification. Includes a 'prepare for the written pledge' button.
- LEVEL 4 Verify Residence**: Requires clicking a button to submit proof of residence for level 4 verification. Includes a 'submit proof of residence' button.

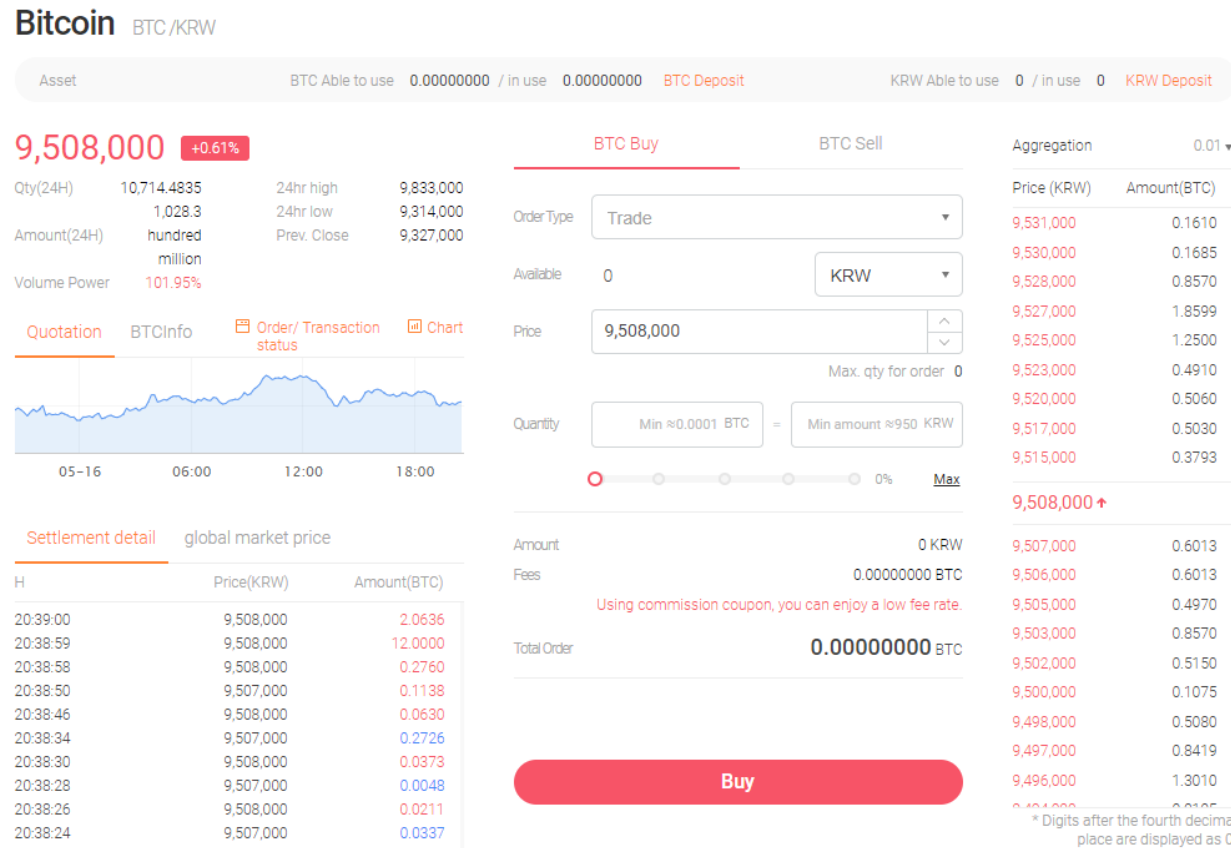
A link 'How to verify Corporate Account (PDF)' is located above the Level 4 section.

The screenshot shows the 'LOGIN' page on the Bithumb website. An orange diagonal banner with the text 'PC' is in the top right corner. The page includes the following elements:

- LOGIN** header.
- Check if the website you are logging in is as below.
- URL field: <https://www.bithumb.com>
- Email field: bithumb@bithumb.com
- Password field: Password
- General sign-up account and Easy Sign-up account are separate, so balance and customer informations are not shared.
- Log in button (orange).
- Member sign-up link.
- Has cell phone number been changed? link.

Trade on CEX (Bithumb) (2)

- ❖ Trading Fee: 0.25% (0.1% for Binance)
- ❖ Free for Deposit / 1,000 KRW / 0.001 Bitcoin (0.0005 for Binance) / 0.01 Ethereum for Withdrawal



Pros of CEX

- ❖ Easy to use
 - Existing and known process
 - Only challenge is an account set up
- ❖ Advanced tools
 - Advanced trading functionalities such as margin trading and different order types (stop losses or limit orders)
- ❖ High performance trading capabilities
 - Real-time trading
 - High liquidity
- ❖ Fiat currency trading
 - Deposit fund directly from the bank account to purchase cryptocurrency

Cons of CEX (1)

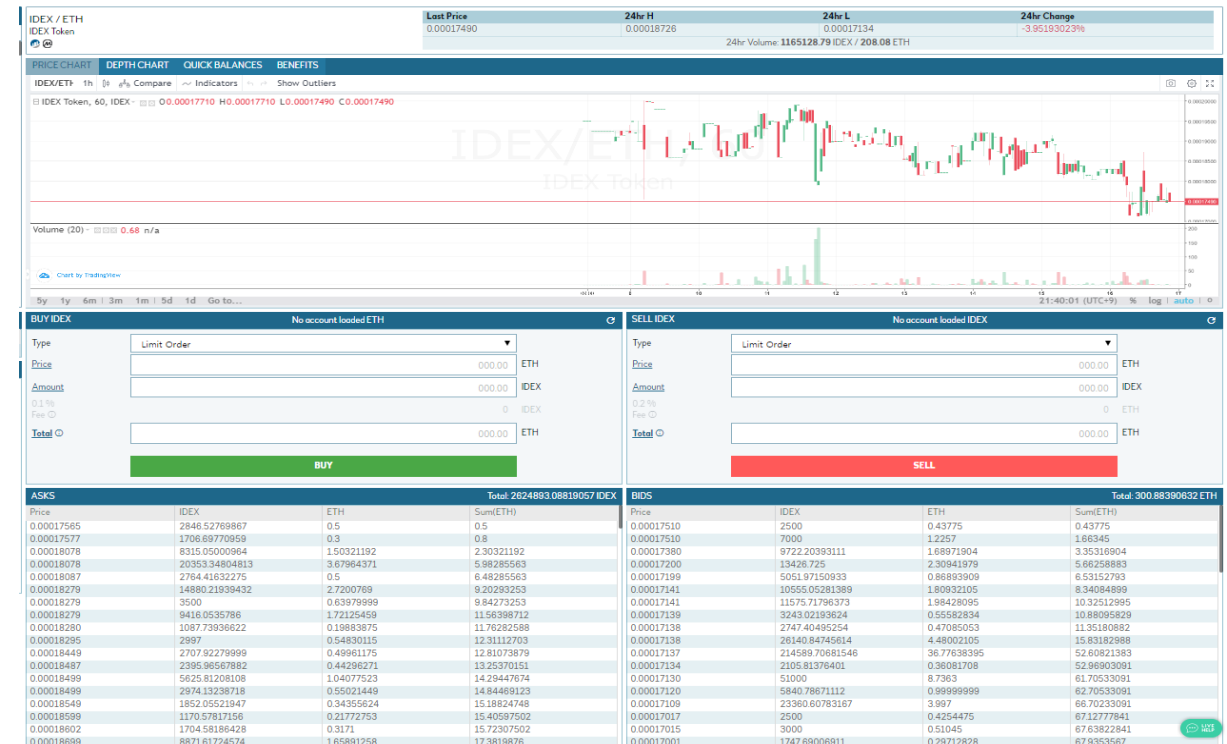
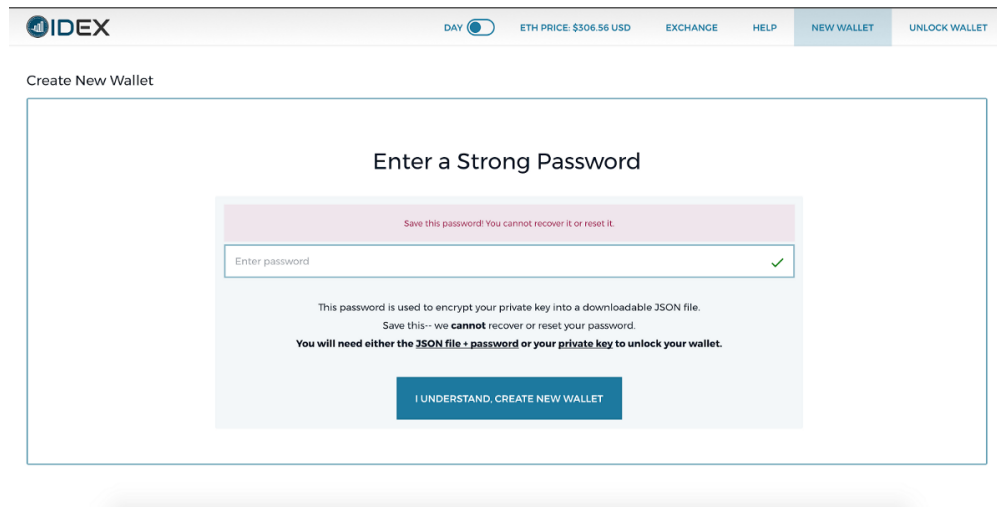
- ❖ Central points of failure – Custody risk
 - Since transactions are irreversible and CEXs have a large amount of assets (Binance's Bitcoin deposit \$3B) with their private keys are kept all together, perfect targets for a hacker
 - Mt.Gox lost 650,000 BTC (\$350M) in 2011 and Binance lost 7,000 BTC (\$50M) recently
 - No insurance and no authority to track and investigate
 - Systemic risks such as consensus or governance
- ❖ Off-chain record
 - Not all transactions are recorded on the blockchain, so do the exchanges really own cryptocurrencies claimed in the database?
 - HitBTC (#12): "Withdrawals are temporarily disabled on your account" message
- ❖ Mismanagement
 - Front running, a process whereby an exchange inserts its own order in anticipation of the price movement, which is illegal and policed in regulated markets
 - Cross trading, buy and sell orders for the same asset, is more than 60% by BTI (Blockchain Transparency Institute)
 - Some exchanges abuse customer funds

Cons of CEX (2)

- ❖ Censorship
 - Can prevent users from withdrawing/depositing funds or directly banning for using the platform
 - Governments can ban CEXs (China banned exchanges in 2017) because CEXs are easier to target
- ❖ Higher fees
 - Leverages the power imbalance between exchanges and users/projects to charge high fees
 - Trading fees on Coinbase is 1.49% and listing fees on Binance is \$2.6M
- ❖ Know Your Customer (KYC) rules
 - Follow KYC for verifying users, which are a no-go for privacy-conscious investors
 - Prevent some people in developing countries that do not have official identity documents from accessing exchanges
- ❖ Server downtime
 - Hosting is centralized

Trade on DEX

- ❖ Create a new Ethereum wallet and deposit ETH
- ❖ Trades occur directly between users (peer-to-peer) through an automated process
- ❖ IDEX charges 0.2% for the market taker and 0.1% for the market maker
- ❖ Users also pay gas fees to put their transactions on blockchain



Pros of DEX

- ❖ No central points of failure
 - Trades through decentralized peer-to-peer networks (No single third-party service)
- ❖ Uncensorable
 - Full control over private keys and how funds are used, secured, and transferred
 - Cannot be pressured by regulators and governments to shut down or censor specific trades
- ❖ Lower fees
 - Less operation cost
 - Trades through smart contract execution, and traders only pay transaction fees for miners
- ❖ No KYC
 - Difficult to require KYC because DEXs are not single entities
 - Anonymity and privacy are maintained
 - Anyone can participate conveniently (Owning a wallet is the registration)
- ❖ Less server downtime
 - Hosting is distributed throughout the nodes involved

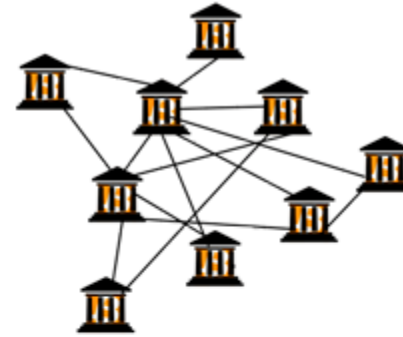
Cons of DEX

- ❖ Not easy to use
 - Complex terminology and a new trading flow
 - Unfriendly for users and need optimization and refinement
- ❖ Limited features
 - Rarely have trading functionalities such as margin trading and different order types (stop losses or limit orders)
- ❖ Low performance trading capabilities
 - On-chain trading is not real-time as all transactions have to be processed by miners
 - Lack of liquidity
- ❖ No fiat currency trading
 - Fiat currencies require a trusted central party to record account balances
- ❖ Smart contract security
 - Vulnerabilities including underflows, overflows, and reentrancy attacks
 - Auditing is needed to validate the security of the contract code and find any vulnerabilities

CEX vs DEX (1)



CENTRALIZED



DECENTRALIZED

EASY TO USE

NOT EASY TO USE

ADVANCED TOOLS

BASIC FEATURES

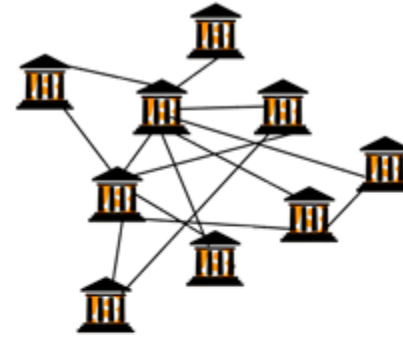
LIQUIDITY

LOW LIQUIDITY

CEX vs DEX (2)



CENTRALIZED



DECENTRALIZED

EXCHANGE CONTROLS FUNDS

USER CONTROLS FUNDS

NOT ANONYMOUS

ANONYMOUS

HACKS & SERVER DOWNTIME

NO HACKS & SERVER DOWNTIME

Contents

1 Introduction

2 Background

3 CEX vs DEX

4 Types of DEX

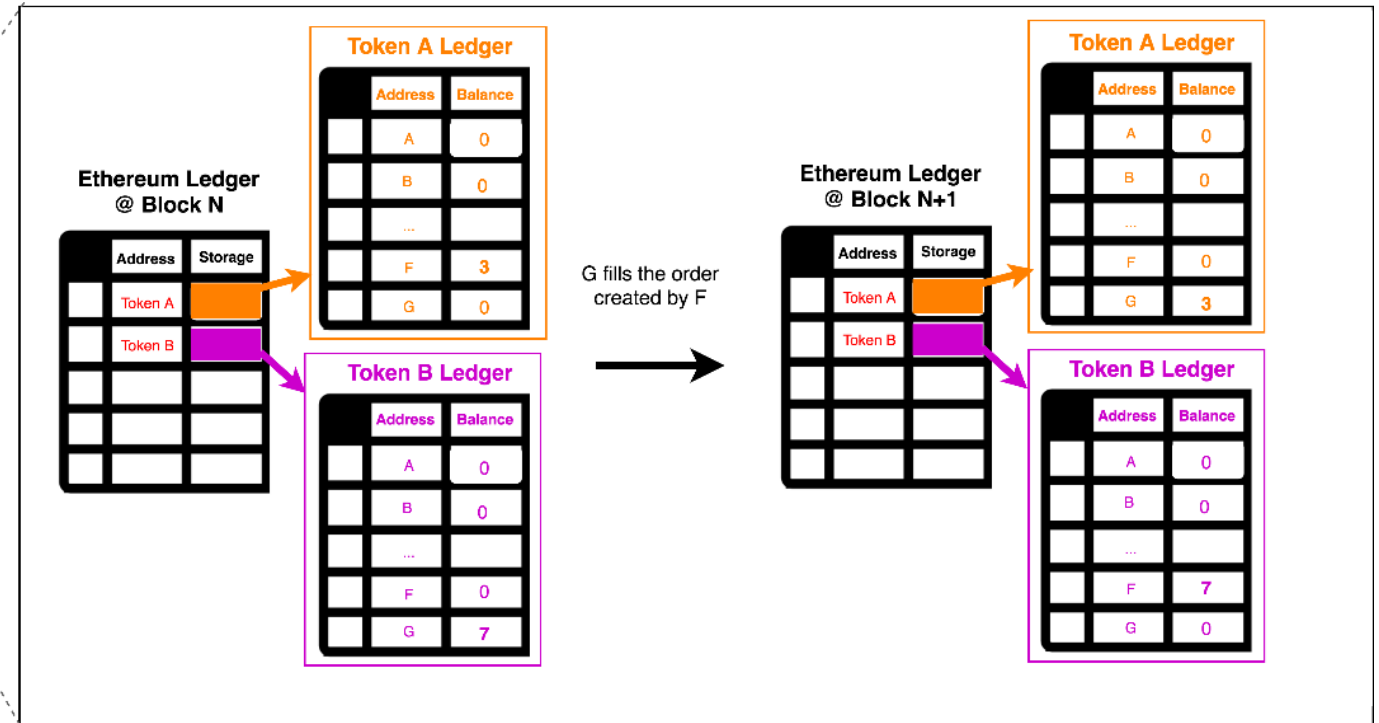
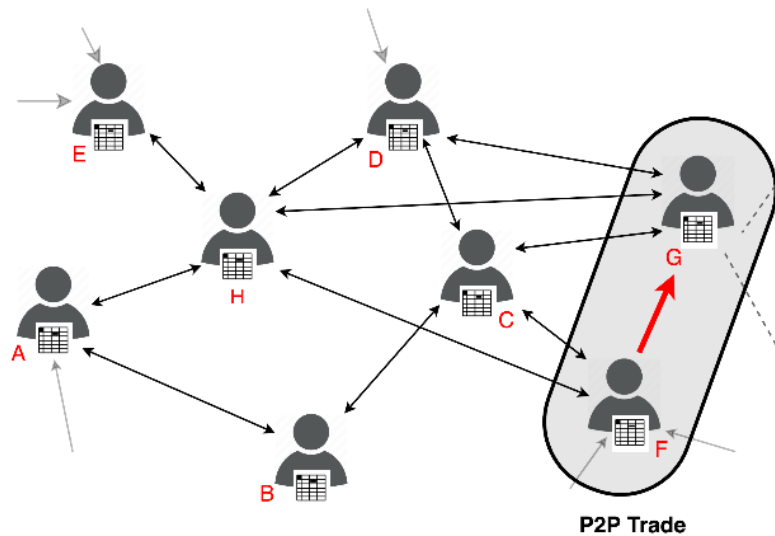
5 Future Works

6 Conclusion

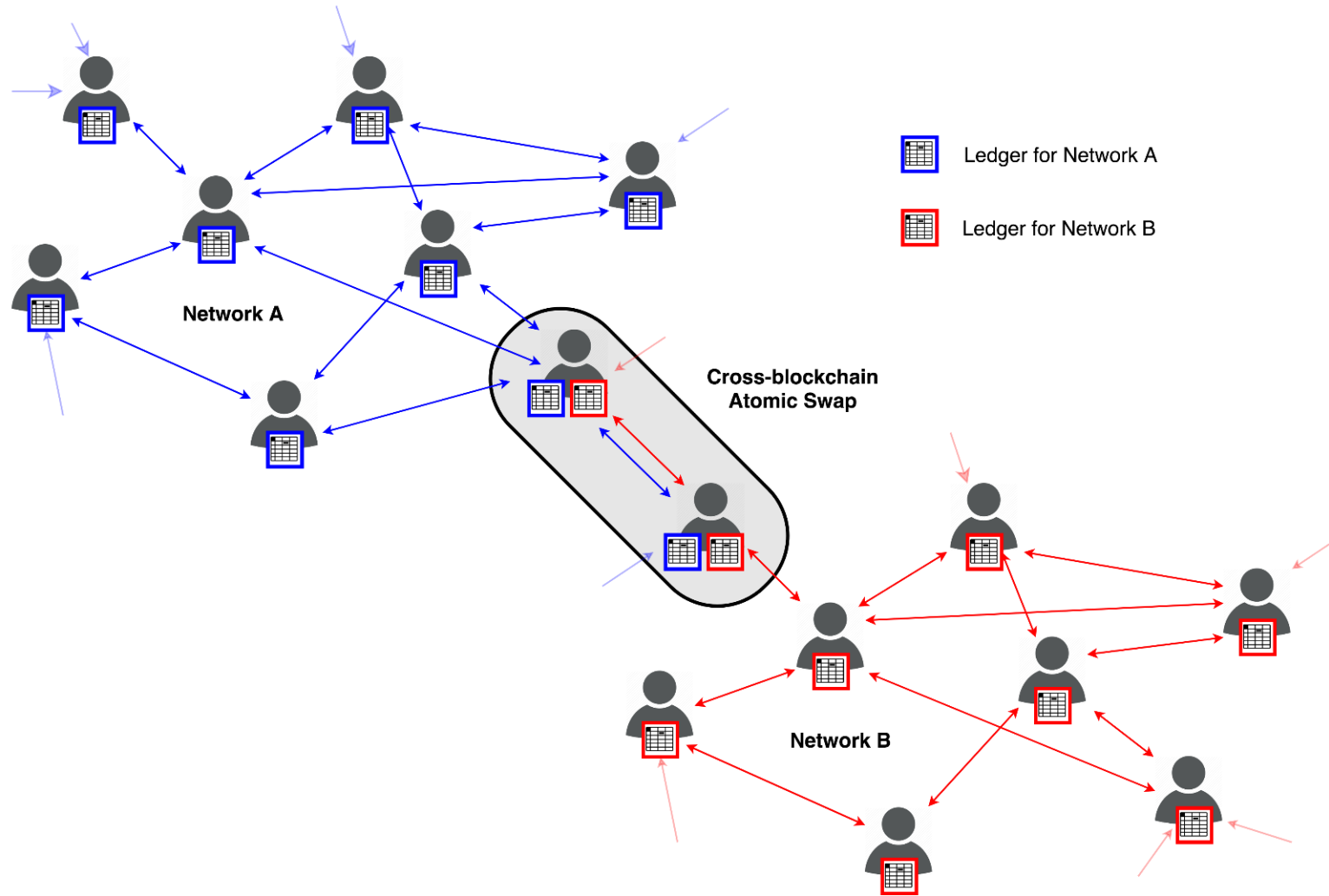
Types of DEX by Currencies

- ❖ Two fundamental exchange models by transaction currencies: currency-centric and currency-neutral
- ❖ Currency-centric exchanges
 - Built on top of singular platform such as Ethereum
 - Limited only to the platform currency it is built on such as ERC20 tokens
- ❖ Currency-neutral exchanges
 - Architected to connect different cryptocurrencies

Currency-centric exchange



Currency-neutral exchange



Types of DEX by Core Functions

- ❖ Four core functions of exchange are capital deposits, order books, order matching, and settlement
 - Each of these functions must be decentralized to create a fully decentralized exchange
 - Trade-offs between being “more decentralized” and “simplicity/functionality”
- ❖ Types of DEX by core functions
 - Off-chain order book and order matching with on-chain settlement
 - By smart contract – Deposit/Withdraw Models / IDEX
 - By relayers/miners – 0x Relayers / EtherDelta
 - On-chain order book, order matching, and settlement by miners – OasisDEX
 - Simplified DEX's – Bancor / Kyber

Deposit/Withdraw Models – IDEX

- ❖ Off-chain order book and order matching with on-chain settlement by smart contract
- ❖ Deposit/withdraw funds into a smart contract
 - Smart contract holds funds and allows trade
 - Withdraw funds when trading is done
- ❖ Not fully decentralized, as IDEX is the only authority that submit trades
 - A single point of custodianship (Smart contract)
 - One of IDEX smart contracts hold over \$12M
- ❖ Process is straightforward and familiar
 - Deposit, trade, and withdraw
 - Provides the speed and UX of CEX, forming a hybrid model

0x Relayers – DDEX, Radar Relay, and Paradex

- ❖ Off-chain order book and order matching with on-chain settlement by relayers
 - DEXs, as relayers, host and maintain order books and “relay” an order to a 0x smart contract to be executed trustlessly on the blockchain
 - Programmable smart contracts allow to set managing fees for the transaction
- ❖ More decentralized process
 - Anyone can be a relayer by maintaining an order book
 - Once a token has permission for trading, deposit/withdraw is not required
 - Full control of funds until the trade is actually made
- ❖ Liquidity sharing between relayers even across the exchanges
 - Collaborate to create more competitive order books (thinner spreads, greater depth, etc.)
 - Trading permissions are shared as well
- ❖ ETH itself cannot be traded “decentrally”, WETH (or wrapped ethereum) is traded
 - Wrap ETH to trade and unwrap WETH to revert back to ETH
 - Use alternate base pairs – stablecoins like DAI, which don’t need to be wrapped
 - Wrapping, unwrapping, and token allowances all require transactions on the blockchain

Trade on 0x Relayers

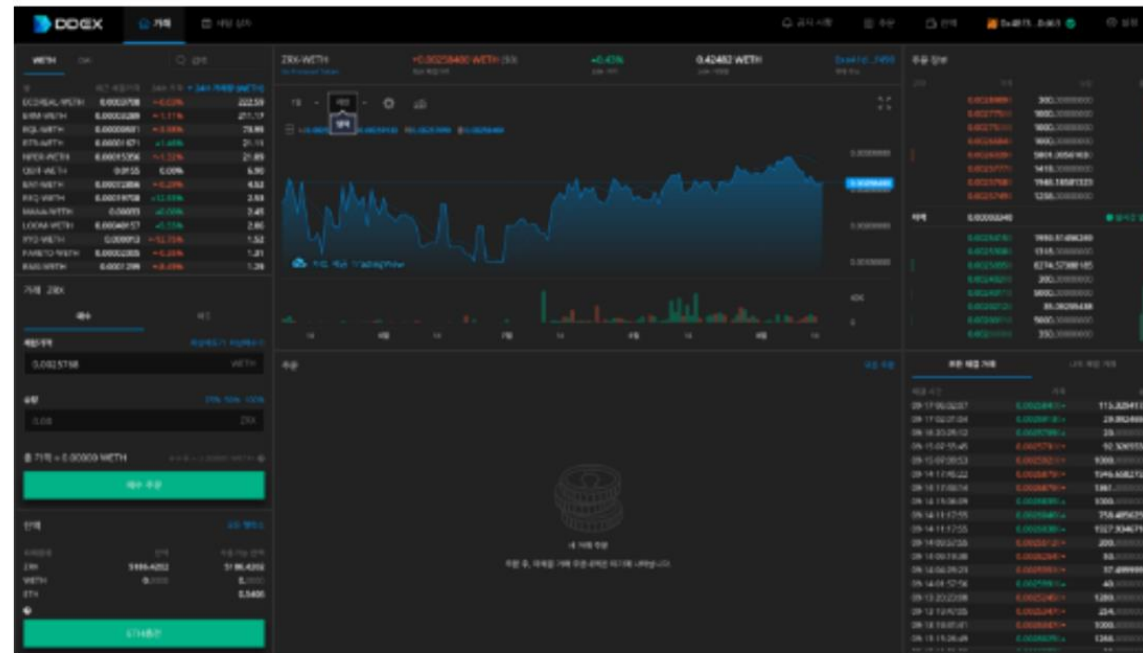
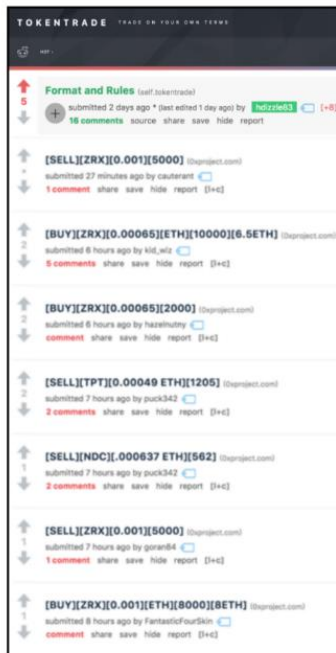
- ❖ “Maker” generates an “order,” which defines the terms of a trade
 - The order is cryptographically signed by the maker, providing verifiable proof of its authenticity

```
{
  "order": {
    "maker": "0xaa40e9f4dadabef71c6864b04e4fbc4c01563601",
    "taker": "0x0000000000000000000000000000000000000000",
    "makerFee": "0",
    "takerFee": "0",
    "makerTokenAmount": "1000000000000000000000000",
    "takerTokenAmount": "1000000000000000000000000",
    "makerTokenAddress": "0xd0a1e359811322d97991e03f863a0c30c2cf029c",
    "takerTokenAddress": "0x6ff6c0ff1d68b964901f986d4c9fa3ac68346570",
    "expirationUnixTimestampSec": "1546329600",
    "feeRecipient": "0x0000000000000000000000000000000000000000",
    "Salt": "79191593431936512524324195543585235073888075871061193308019521801915927235481",
  }
}
```

- ❖ Find someone to act as their counterparty ("Taker")
 - The maker can specify the taker or broadcast it to a large number of people
 - Once the maker finds a taker, the taker injects the order into a corresponding smart contract, which verifies the signature and proceeds the trades

Trade on 0x Relayers

- ❖ “Relayers” help makers and takers to find each other by establishing online meeting places to share and aggregate orders
 - While relayers can charge a fee, never custody users' funds and the blockchain takes care of all of processes
 - The first relayer was the internet message board shown in Figure (left)
 - Relayers provide highly refined web applications recently, DDEX in Figure (right)
 - Some relayers may host a centralized order-book or store other exchange-related data on private servers



EtherDelta


- ❖ Off-chain order book and order matching with on-chain settlement by miners
 - Cancellation orders are mined on-chain, and waiting for the next mined block means that real-time trading becomes impossible
 - No speed benefits of off-chain order processing, and very slow functionality
- ❖ Order book matching is centralized
 - Orders can be censored
 - Security benefit of controlling own funds remains
- ❖ SEC charges EtherDelta founder over 'Unregistered Securities Exchange'

OasisDEX

- ❖ On-chain order book, order matching, and settlement by miners
 - Built by MakerDAO
 - Being completely on-chain, all orders interact directly through the blockchain
 - Fully decentralized, but expensive and slow
- ❖ Changed to Eth2Dai
 - Only supports exchange of ETH and DAI tokens

Comparison between DEXs

Decentralized



	Deposit/Withdraw Models – IDEX	0x Relayers / EtherDelta	OasisDEX
Order books	Off-chain	Off-chain	On-chain
Order matching	Off-chain	Off-chain	On-chain
By	Smart contract	Relayer / Miner	Miner
Speed	Real-time	Slow	Slowest
Automatic matching Fill many orders at once	Yes	No	No
Gas to limit orders	No	No	Yes
Gas to cancel orders	No	Yes	Yes
Gas per trade	High	Medium	Medium
Race conditions	No	Yes	Yes
Scaling	Moderate	No	No

Simplified DEX's – Bancor

- ❖ A market order, the simplest type, abstracts order books completely away from users
 - Restrictive in the way that a user can specify an order
- ❖ Simple and convenient
- ❖ Low order flexibility and a price range rather than a exact price is given
 - Price discovery is a major challenge
 - Completely algorithmic and abstracts into simple algorithmic trading
 - Simplified process, but opens up opportunities for potential arbitrage

Simplified DEX's – Kyber

- ❖ Matches orders by using smart contracts and reserves
 - All reserve transactions are managed by smart contracts instead of off-chain matchmakers
- ❖ Reserves provide liquidity, and a singular reserve is held by Kyber
- ❖ Additional reserves can be public or private
 - Private reserves are private coin holders who choose to act as a source of crypto for the exchange and set their own rates
 - Public reserves can receive contributions from the public, and the public benefits by sharing in the profits



Contents

- 1 Introduction
- 2 Background
- 3 CEX vs DEX
- 4 Types of DEX
- 5 Future Works**
- 6 Conclusion

Front running

- ❖ Outbid an order placed on an exchange
 - Most DEXs are running on Ethereum, a public Blockchain that anyone can check the memory pool to see an order
- ❖ Once a front-runner identifies that an order has been placed on a DEX
 - Simply jump in front of it by placing the same order except with more gas
 - The first order that was placed is never realized as the order is now gone from the book



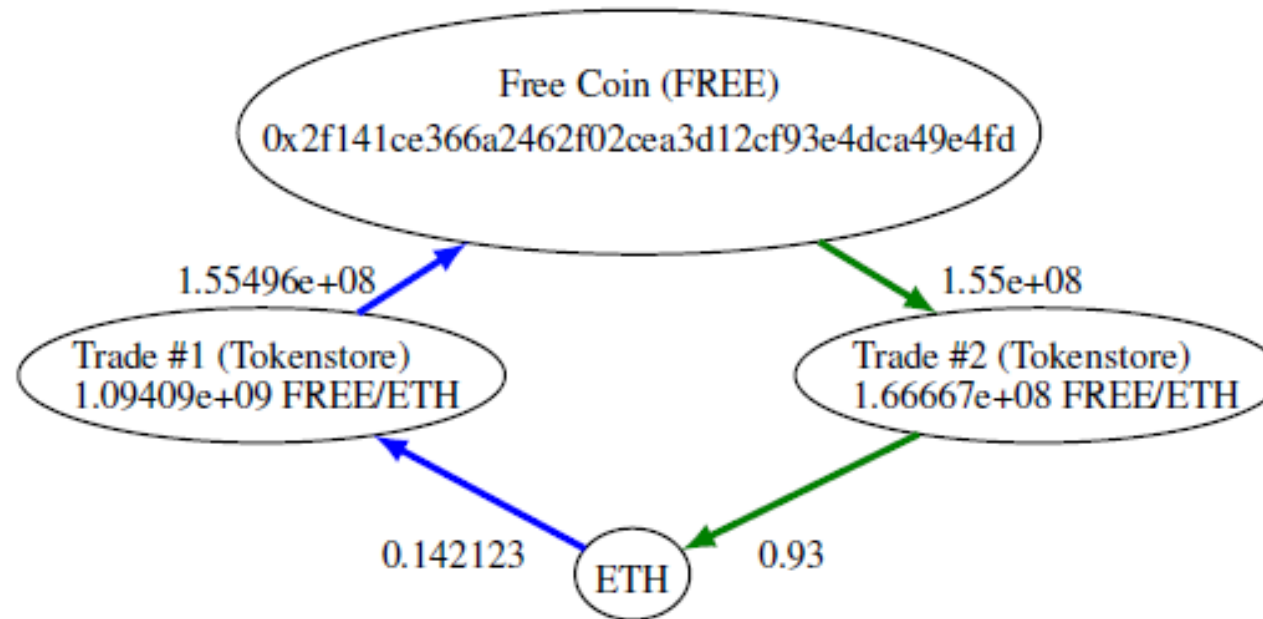
-  TX8 Your TX with low gas
-  TX7 Someone with **higher** gas cutting in front of you

Flash Boys 2.0

- ❖ Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges by Philip Daian, Ari Juels (Cornell Tech), and 6 other people
- ❖ Frontrunning is illegal In regulated markets
 - Generally exploits information asymmetries, can be arisen for actors in advantageous positions in decentralized systems
- ❖ Arbitrage bots have arisen to exploit price abnormality
 - Exhibit similar behaviors — frontrunning, aggressive latency optimization
 - Common on Wall Street, as revealed in Flash Boys
 - DEX bots frontrun user orders and cancellations directly
 - In the event of a typo or market structure weakness

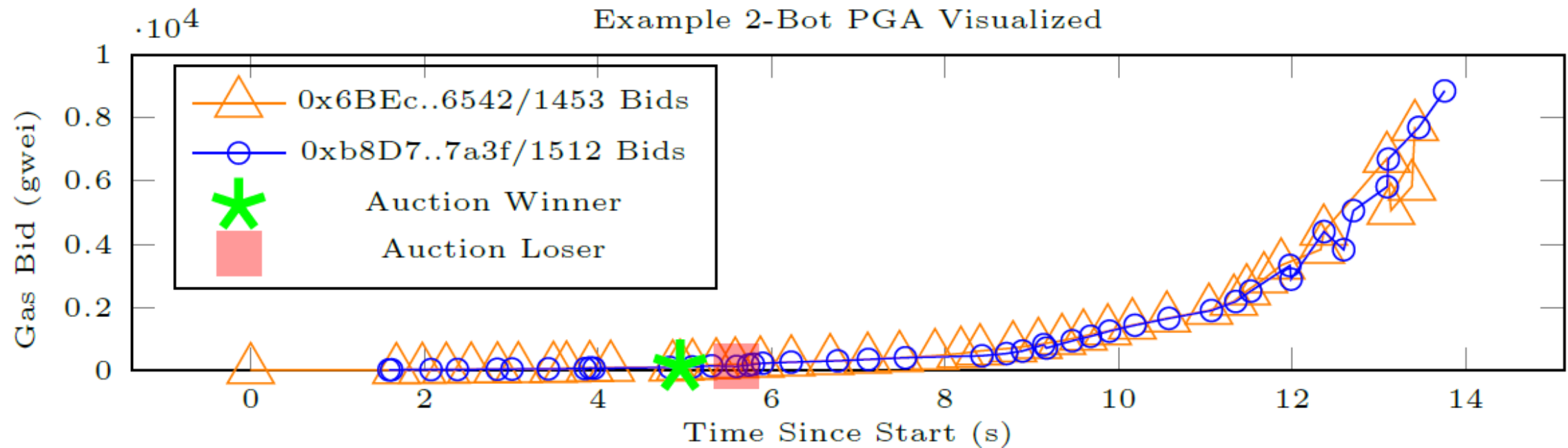
Smart-Contract-Enabled Trade Atomicity

- ❖ Compose single transactions that execute multiple trades across multiple exchanges atomically, with an all-or-nothing failure model
- ❖ $0.93 \text{ ETH} - 0.14123 \text{ ETH} - 0.01518 \text{ ETH (cost)} = 0.77 \text{ ETH (\$267)}$



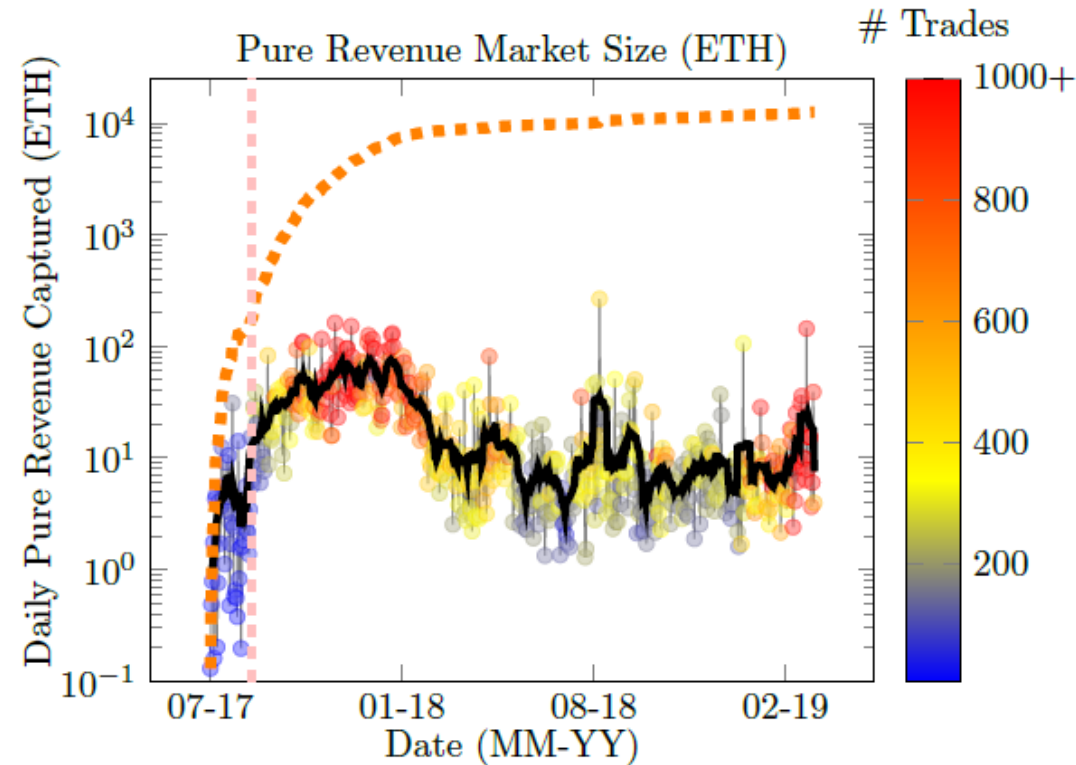
Priority Gas Auction (PGA)

- ❖ Interaction of issuing repeated gas bids



Pure Revenue Arbitrage

- ❖ Active during initial market development 1,000 daily trades / 10-100 ETH daily revenue
- ❖ Matured market with 1-10 ETH daily revenue
- ❖ Recently, the average size decreased but more frequent opportunities



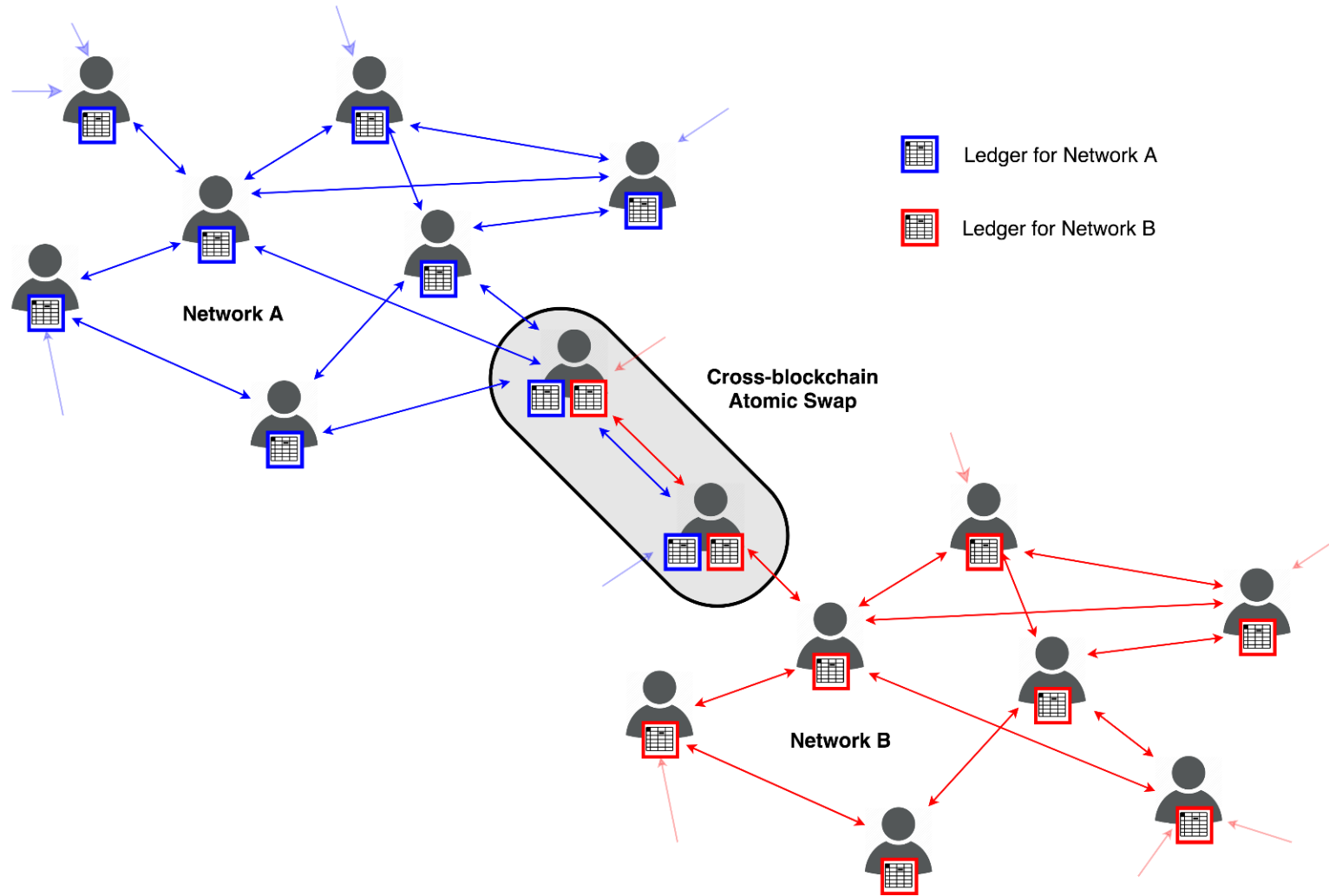
Exploiting MEV

- ❖ Miner-Extractable Value (MEV) is that the miners can extract from manipulation of transactions
 - Order optimization (OO) fees, one case of a MEV
 - By reordering transactions and potentially inserting their own
- ❖ Undercutting attacks
 - When transaction fees exceed the block reward, fork a high-fee block
 - Present threat in Ethereum as success of smart contracts attract OO fees
 - Miners can even “steal” arbitrage opportunities
- ❖ Time-bandit attacks
 - When stealable value exceeds the block rewards, rewind blockchain and use the MEV to subsidize a profitable 51% attack that mines a fork
 - “Rental attacks” are feasible using cloud resources, particularly for systems such as Ethereum that rely heavily on GPUs

Cross-Chain Solution

- ❖ Popular trading pairs are tokens paired with USDT (BTC/USDT, ETH/USDT, ...)
 - Most DEXs trade only Ethereum and Ethereum-based tokens – both the fiat currency and BTC are missing
 - This is a huge reason why DEX's have not seen much adoption currently
- ❖ Most DEXs are built using Ethereum smart contracts to facilitate trades, running on the Ethereum blockchain
 - Transacting tokens on other blockchains (such as Bitcoin) necessitates some "cross-chain" solution, requiring more depth than a simple smart contract
 - CEXs can do this easily because they do not involve any movement on every trade unless withdrawal

Atomic Cross-Chain Swaps (ACCS)



What is ACCS?

- ❖ ACCS is the exchange of one cryptocurrency for another cryptocurrency trustlessly
 - For example, if Alice owns 5 BTCs but instead wants 100 ETHs, she has to go through an exchange
 - However, with ACCS, if Bob owns 100 ETHs but instead wants 5 BTCs, then Bob and Alice could make a trade
- ❖ Utilizes hashed timelock contracts (HTLCs) to ensure that both fulfill the requirements of the trade trustlessly
 - Require the recipient to acknowledge receiving payment prior to a deadline by generating a cryptographic proof of payment
 - If not, the recipient loses the right to the claim the payment, therefore returning the funds back to the sender

Hashed Timelock Contracts (HTLCs)

Ethereum Network



Bitcoin Network



① Creates a secret s
and $h=H(s)$

Hashed Timelock Contracts (HTLCs)

Ethereum Network



Bitcoin Network

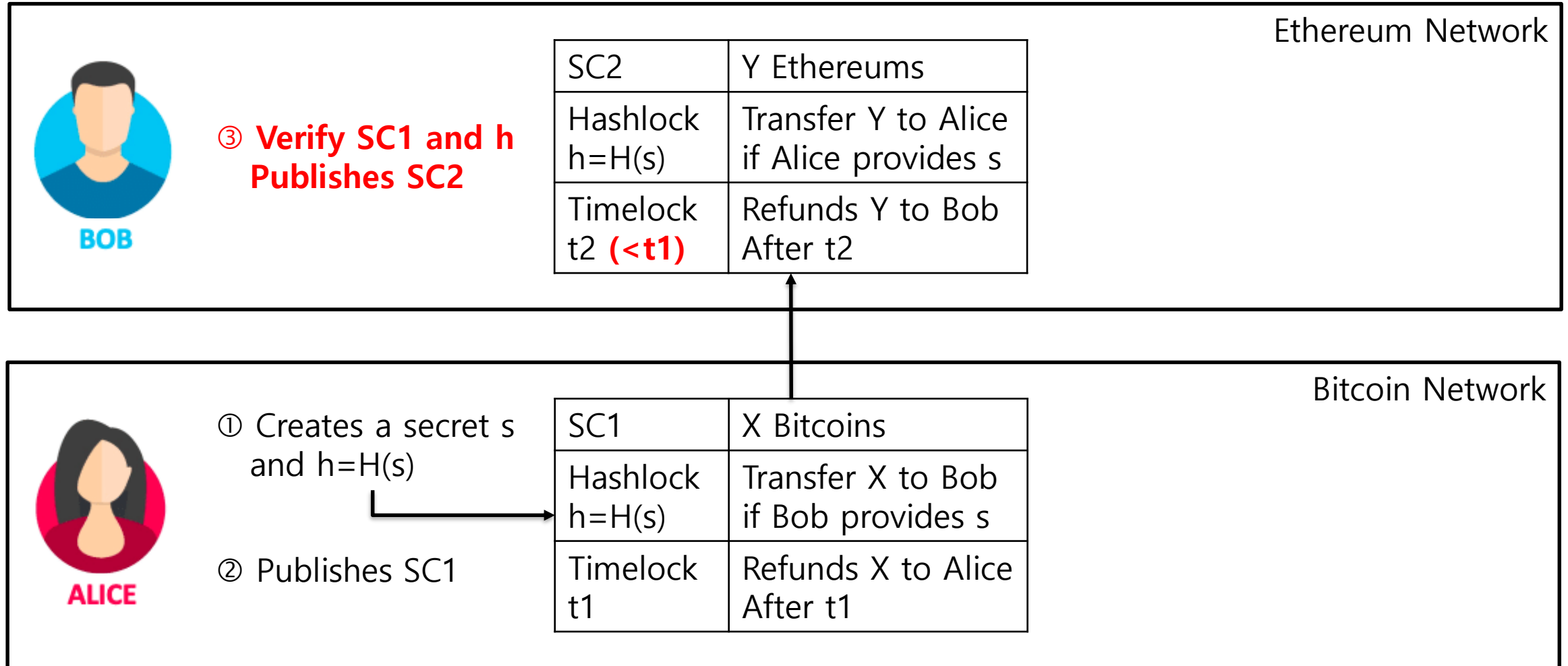


① Creates a secret s
and $h=H(s)$

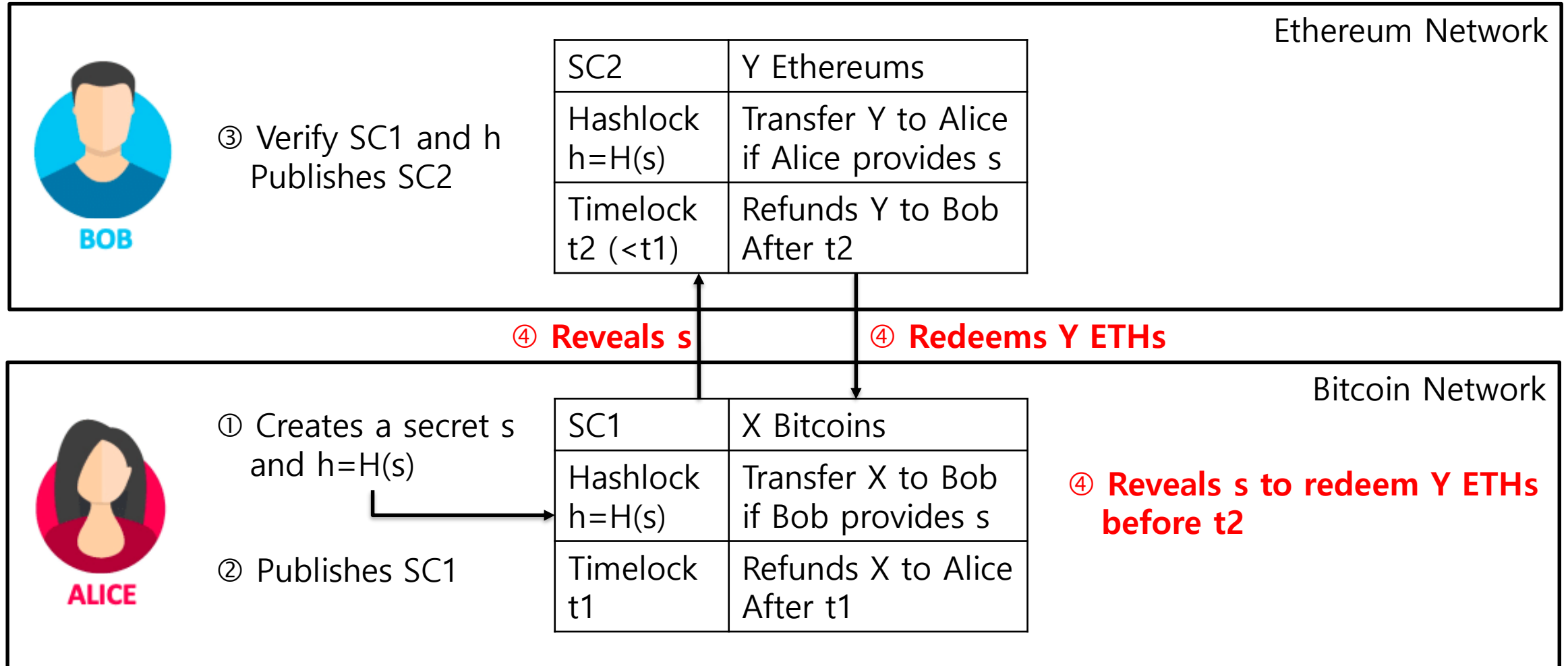
② **Publishes SC1**

SC1	X Bitcoins
Hashlock $h=H(s)$	Transfer X to Bob if Bob provides s
Timelock $t1$	Refunds X to Alice After $t1$

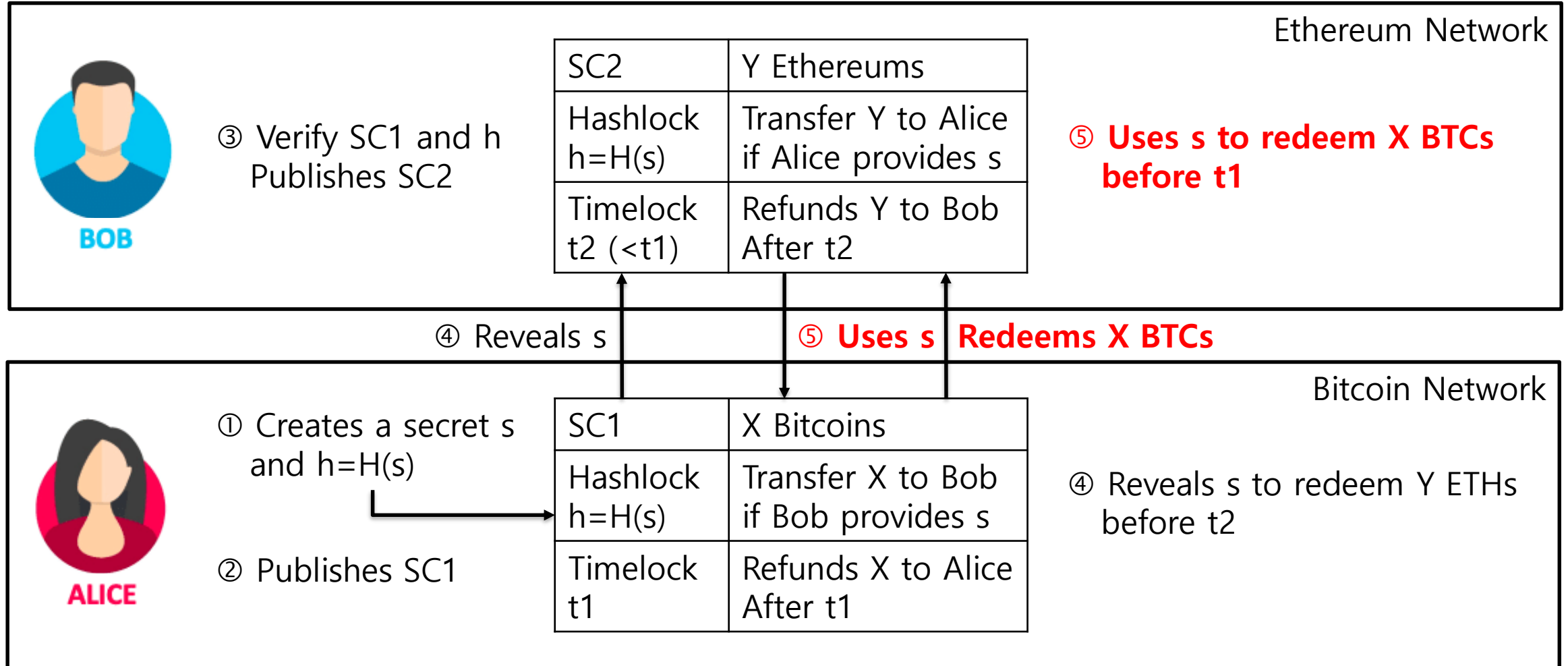
Hashed Timelock Contracts (HTLCs)



Hashed Timelock Contracts (HTLCs)



Hashed Timelock Contracts (HTLCs)



Where We Are Now

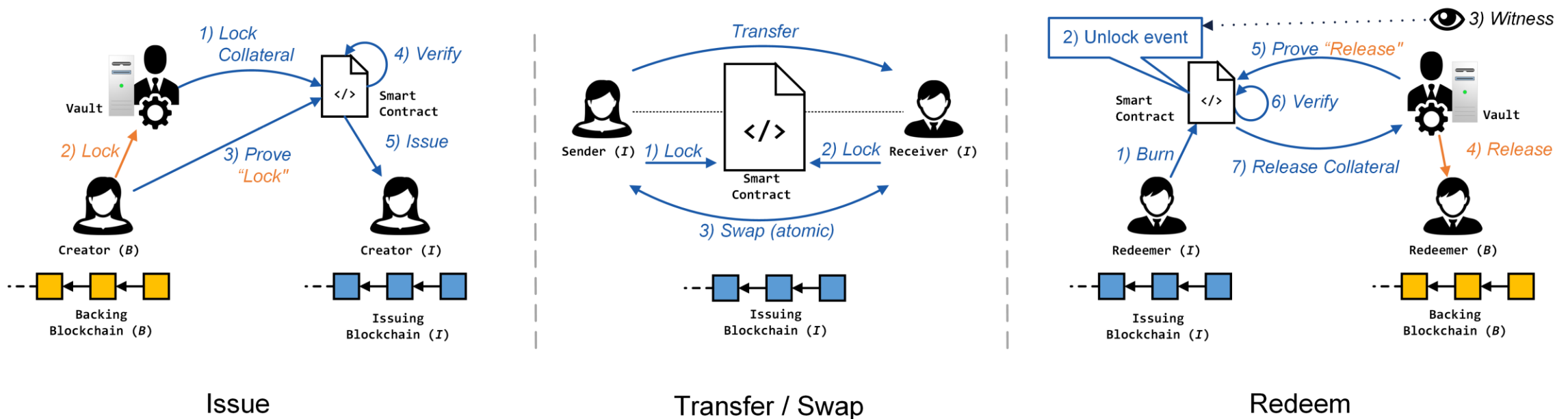
- ❖ Only mechanism to do cross-chain exchange trustlessly
- ❖ The first on-chain atomic swap occurred between Decred and Litecoin in 2017
- ❖ Off-chain atomic swaps to be made off the blockchain, or on layer 2 of a blockchain
 - The first occurred between Bitcoin and Litecoin using the Lightning Network and brought public attention
- ❖ Komodo launched BarterDEX in March 2018 and successfully completed an atomic swap without downloading the entire blockchain

Challenges of ACCS

- ❖ Interactivity – should be online and actively monitor blockchains
 - Violation penalizes for a failure that even happens out of control
- ❖ Synchronizing clocks between blockchains and rely on pre-established communication channels
 - Linked through payment channels such as lightning network
- ❖ Long waiting periods between transfers and four transactions for every swap
 - Expensive, slow, and inefficient
- ❖ Sequential publishing of smart contracts
 - Latency increases with the number of participants increases
- ❖ Same hash function such as SHA-256 for blockchains

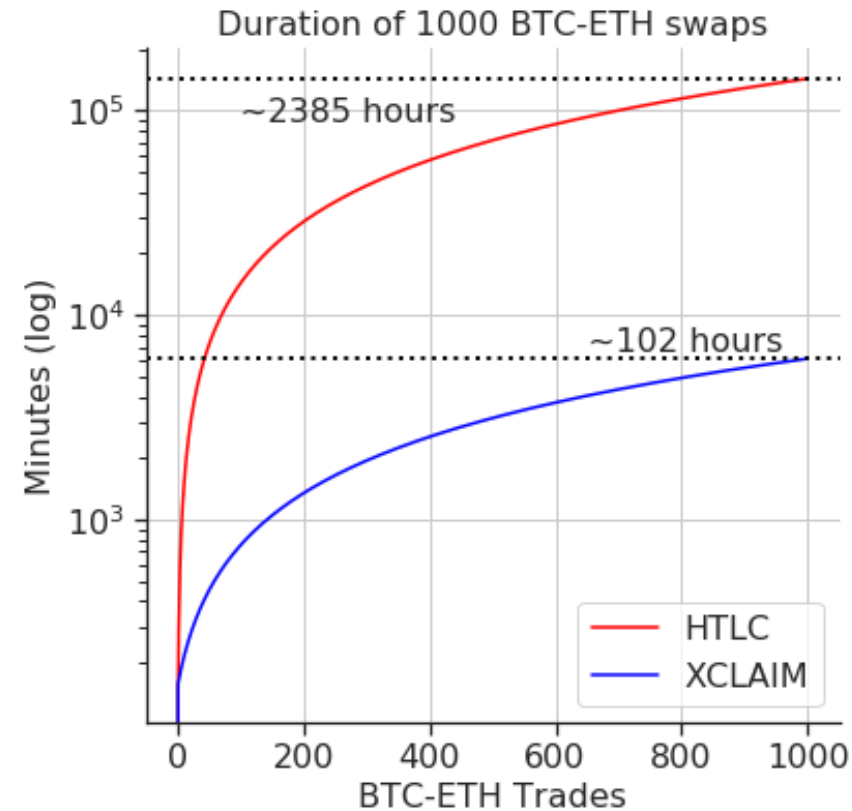
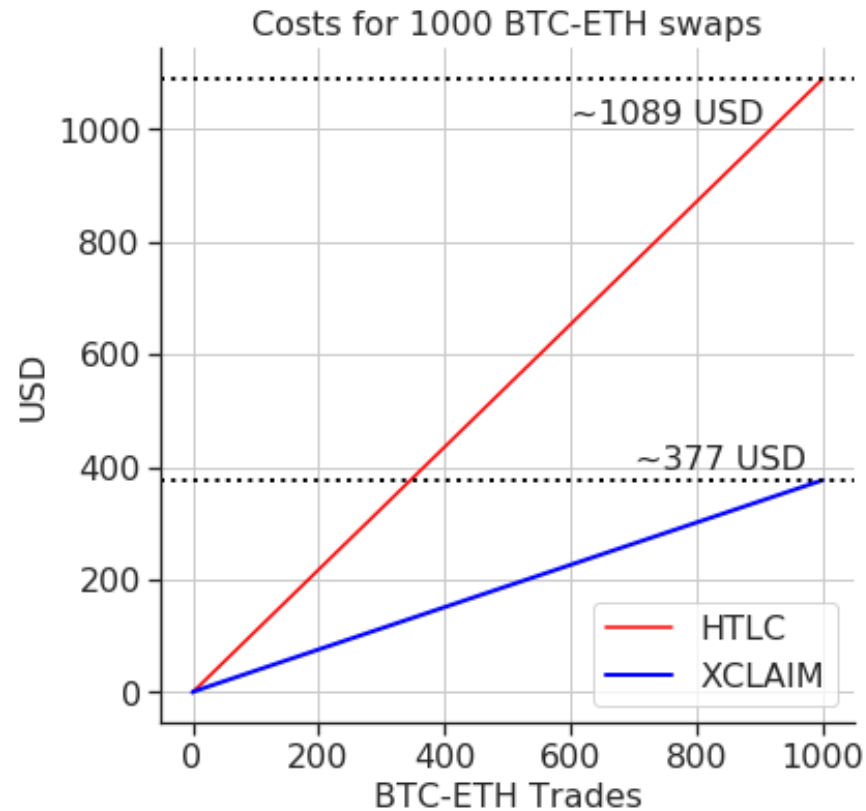
XCLAIM

- ❖ XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets By Alexei Zamyatin and 5 other people, IEEE S&P 2019
- ❖ Framework for cross-chain exchanges using cryptocurrency-backed assets (CbAs), which are 1:1 backed without TTP



XCLAIM vs HTLC AACS

❖ XCLAIM is cheaper and faster than HTLC Atomic Swaps



Remaining Hurdles

- ❖ Regulations are still a grey area for DEX
 - No account creation or KYC process blurs the lines of targeting users and regulatory compliance
 - SEC charges EtherDelta founder over 'Unregistered Securities Exchange'
 - If there is a major loss of some sort, regulators (or civil suits) will target all related parties
- ❖ Programmable smart contracts can help
 - Compliance rules can be directly encoded into smart contracts
 - E.g., Company named "Harbor" can issue Ethereum tokens that automatically enforce regulatory requirements and 0x smart contracts can be extended to support compliant p2p trading
 - To inspect trading activity is possible for regulators and market participants since the blockchain is transparent
- ❖ CEXs can solve their problems so that DEXs becomes less attractive
 - KuCoin (CEX) traders can now self-custody via a "layer two" blockchain protocol trade
 - Managing own keys can be risky for institutional investors

Contents

- 1 Introduction
- 2 Background
- 3 CEX vs DEX
- 4 Types of DEX
- 5 Future Works
- 6 Conclusion**

Conclusion

- ❖ Cryptocurrency exchanges are gateways from the real world to enter the token economy
 - Capital inflows are essential but cryptocurrencies are not functioning well as currencies
 - However, since most exchanges are centralized, there have been many serious problems
- ❖ Blockchain trilemma again
 - Trade in a decentralized way, with good performance and fiat/cross-chain exchange, and securely is impossible now
- ❖ Regulations are still remaining as huge hurdles
 - Money laundering is also possible
- ❖ “Next big thing” should be appeared for blockchain to be the 2nd Internet!

Thank you