

Blockchain's Core Infrastructure & Support Infrastructure

Martinet Lee



/Outline

- Introduction to Blockchain Industry
- Core infrastructure
 - Node
 - Miner/Staker
- Support infrastructure
 - CEX
 - Wallet
 - API Endpoint
- How to store your funds securely?
- Proof of Solvency



<Blockchain Industry>



/Layer1s

The blockchains themselves:

- Bitcoin
- Ethereum
- Solana
- Polkadot
- Cosmos

Core developers: programming language is typically in Rust or Go. Consensus algorithm, P2P Network, Network security, Compiler, etc.

/Mining & Staking

These companies offer security through investing in hardware or **pooling**/purchasing the blockchain's native token to participate in the protocol. The main value they provide: **securing the protocol(s) they participate in.**

- Bitfury
- Bitmain
- Lido
- Stakewise

/Wallet Software

it is impossible to expect everyone to write their own script to create their own address and sign their own transactions. Someone has to write for them. The main value they provide: Easy UI/UX for users to interact with the blockchain.

- Metamask
- Fireblocks

/Centralized Exchange

People need a place to exchange cryptocurrencies with fiat money. The main value they provide: allow fiat on-ramp and facilitate trading.

- Coinbase
- Binance
- FTX (GG)
- XREX
- Quadriga (GG)

/Hardware Wallet

Storing seedphrases and secrets in a connected device itself is not really secure. A better security is to have a device that is not connected to the internet, store the private keys there and only use that device to sign transactions. The main value they provide: Good UI/UX for secure transaction signing.

- Ledger
- Trezor

/Block Explorers

The general users need a generic interface to browse and maybe interact with a blockchain.

The main value they provide: a generic and transparent information aggregator for lower level details of a blockchain including blocks and txs.

- Etherscan

/Node API providers

To interact with the blockchain, one must send a message to a node. Either users run a node themselves, or they would need to send the message to a node run by others. The main value they provide: **allow others to outsource the node running complexity.**

- Consensys (Infura)
- Alchemy
- Tenderly

/Oracles

Blockchain cannot reference to real life data as it only have access to its own state transitions. An Oracle relies on external party to send the data onto the blockchain so that smart contracts on the blockchain can access it. The main value they provide: **enabling applications on blockchain that need real-life data.**

- Chainlink

/Security

As most of the applications on blockchain are about financial assets, naturally it becomes the target of hackers. The security industry assesses projects to find vulnerabilities so that devs can patch the issues. The main value they provide: **securing assets and call out malicious applications.**

- Quantstamp
- Slowmist
- Consensys Diligence
- Trail of Bits

/GovTech

Tracks malicious activity and illicit funds on-chain. This sector is sometimes contentious in the space as they provide government tools to monitor and invade privacy. The main value they provide: **Monitoring illegal activities and money laundering.**

- Chainanalysis
- Cipherblade

/Intelligence Provider

Watches the data on chain and provide intel on transactions. Compile and publish research with trading or project insights.

- Nansen
- Messari

/Decentralized Application

They mostly fall into two large categories: **Decentralized Finance** and NFT (arts, gaming, IP) space. The main value they provide vastly depends on the applications themselves, but they **mostly allow anyone to access them without any censorship or control with an aggressive transparency.** (Is this good or bad?)

- Defi
- NFT

/Layer2s

Layer2s allow users to transact on them and periodically commits result onto the L1. In this fashion, complex computations can be done on L2s and only commit the aggregated result onto the L1, saving computation cost by thousands. The main value they provide: **making transactions that are secured by the blockchain much cheaper.**

- ZKSync
- Scroll
- Arbitrum
- Optimism
- Boba

<Core Infrastructure>

/Core devs & Node /Miners & Stakers / How does blockchain upgrade?



/What do core developers of a blockchain do?

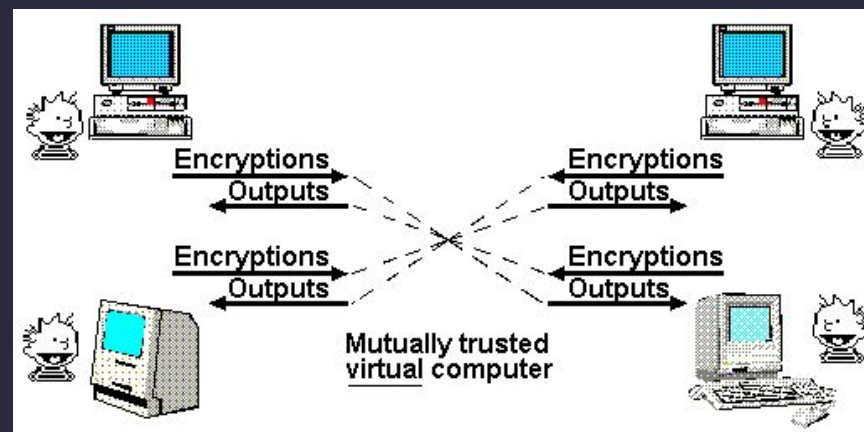
- Protocol design (consensus mechanisms, virtual machine design, etc)
- Incentive design
 - Related to the security of the protocol
- API design
- Initial language design
- Node implementation (first version)
- Updating the protocol/incentive design

/What is a node?

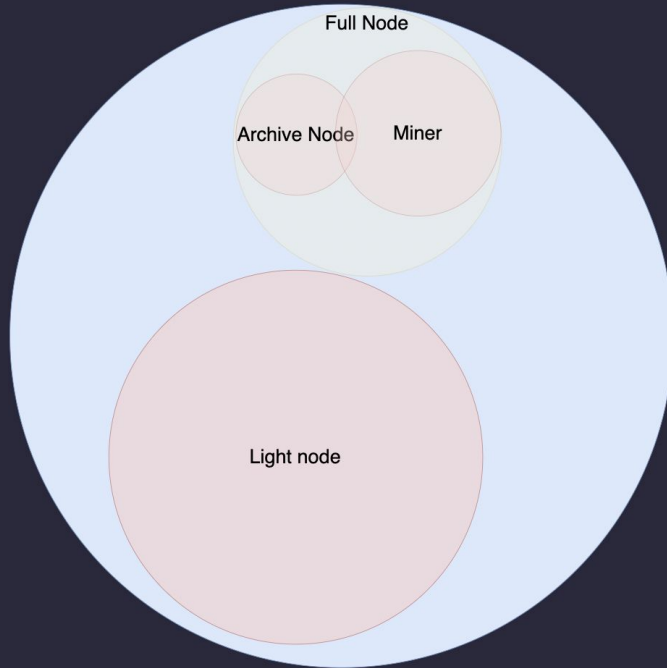
A node is a machine that participates in the blockchain network. They may actively participate in proposing blocks to earn profits or only sending transactions to the network.

- Full node
 - Archive node
- Light node

/What is a node?



/What is a node?



Miner has to be a full node as they need to validate all TXs.

Light client connects to a full node.

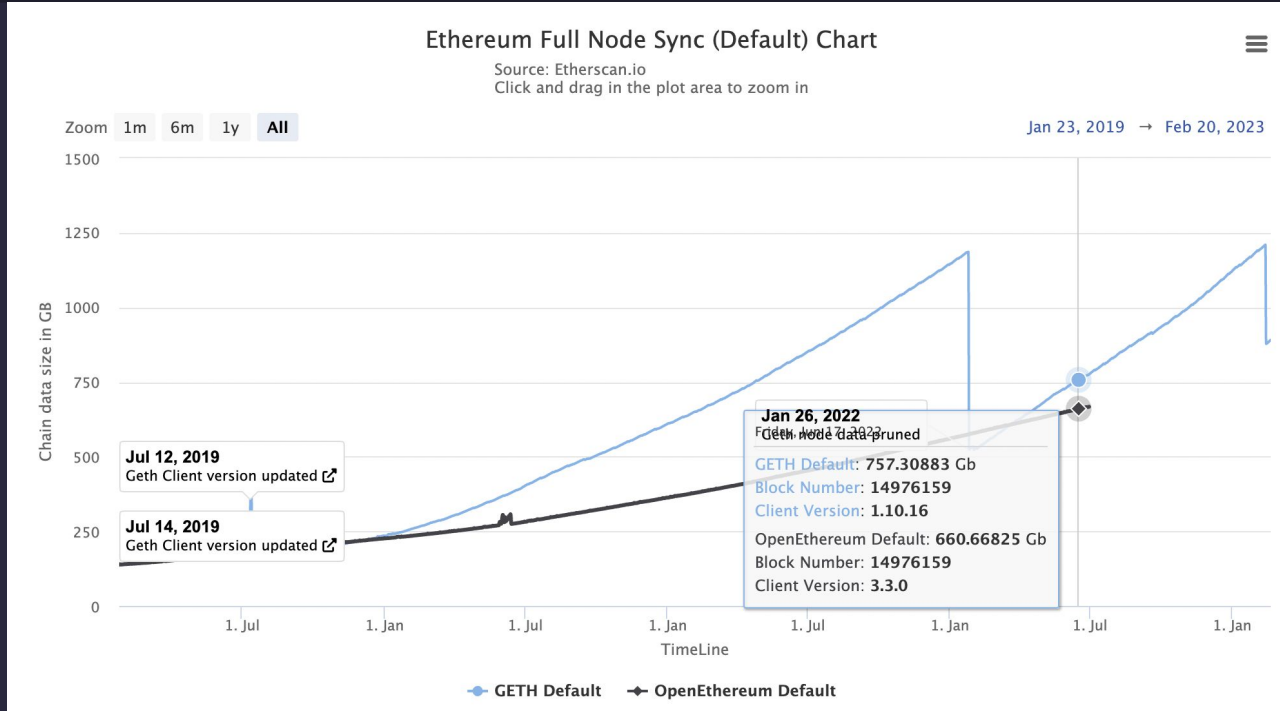
/Full node

- Needs to be online and in sync with the network.
- Stores:
 - Blockheaders and All transactions in block
 - A limited number of block states history
 - Verify blocks that are being propagated, doesn't accept if it is wrong.
 - Broadcasts verified blocks.

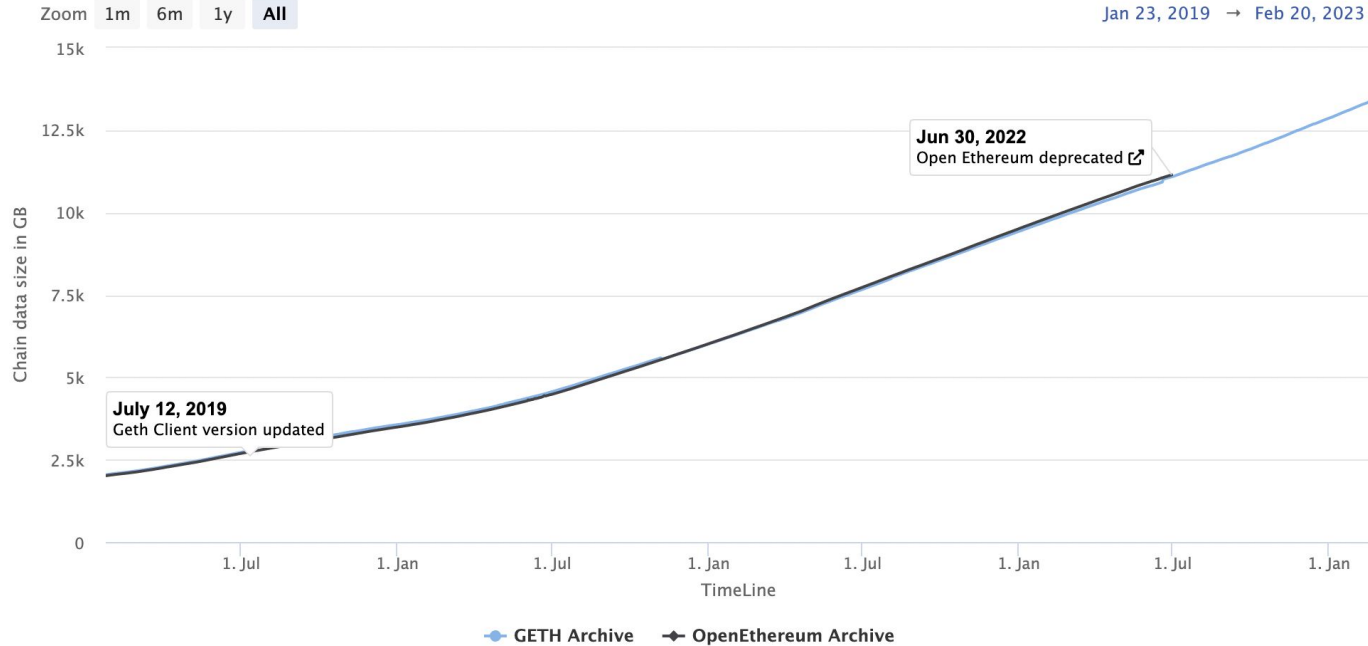
/Light node

- Only downloads Blockheaders.
 - 366 GB v.s. 60 MB (BTC); 360GB v.s. 4.8GB (ETH)
- Relies on full node
 - Tells the full node the addresses that it listens to
 - Full node sends the transactions relevant to the light client (whatever the light node tells it to send) and their merkle proofs

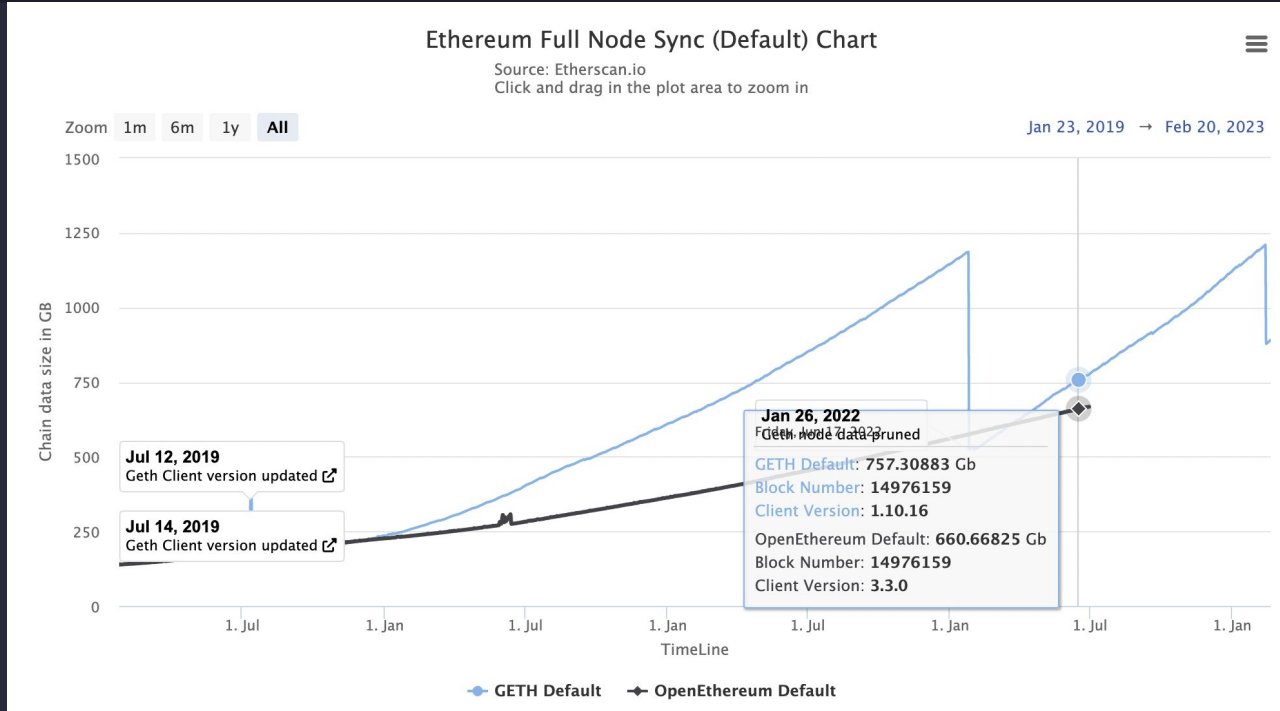
/Hardware requirement for running a node?



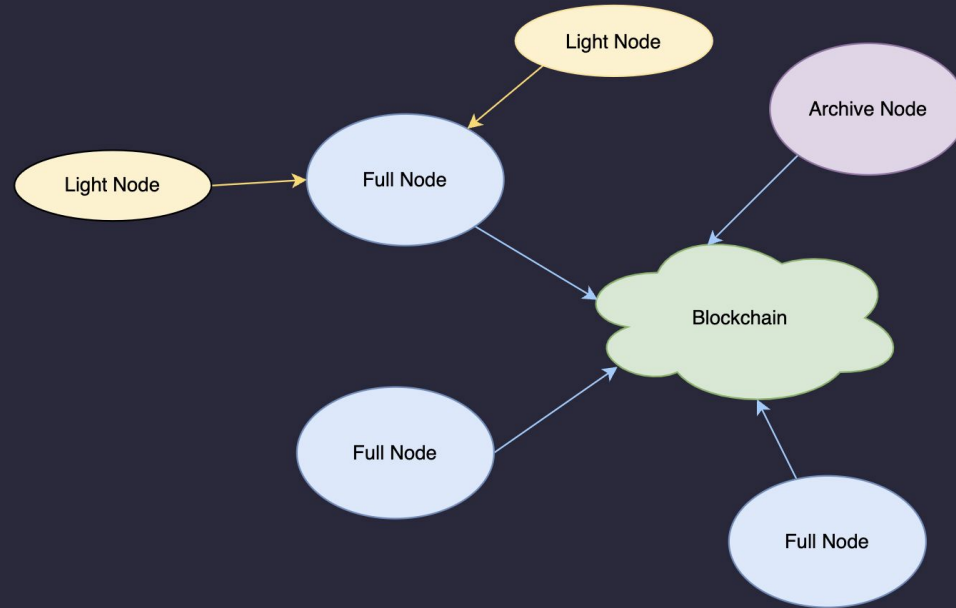
/Hardware requirement for running a node?



/Hardware requirement for running a node?



/Node network roughly looks like ...



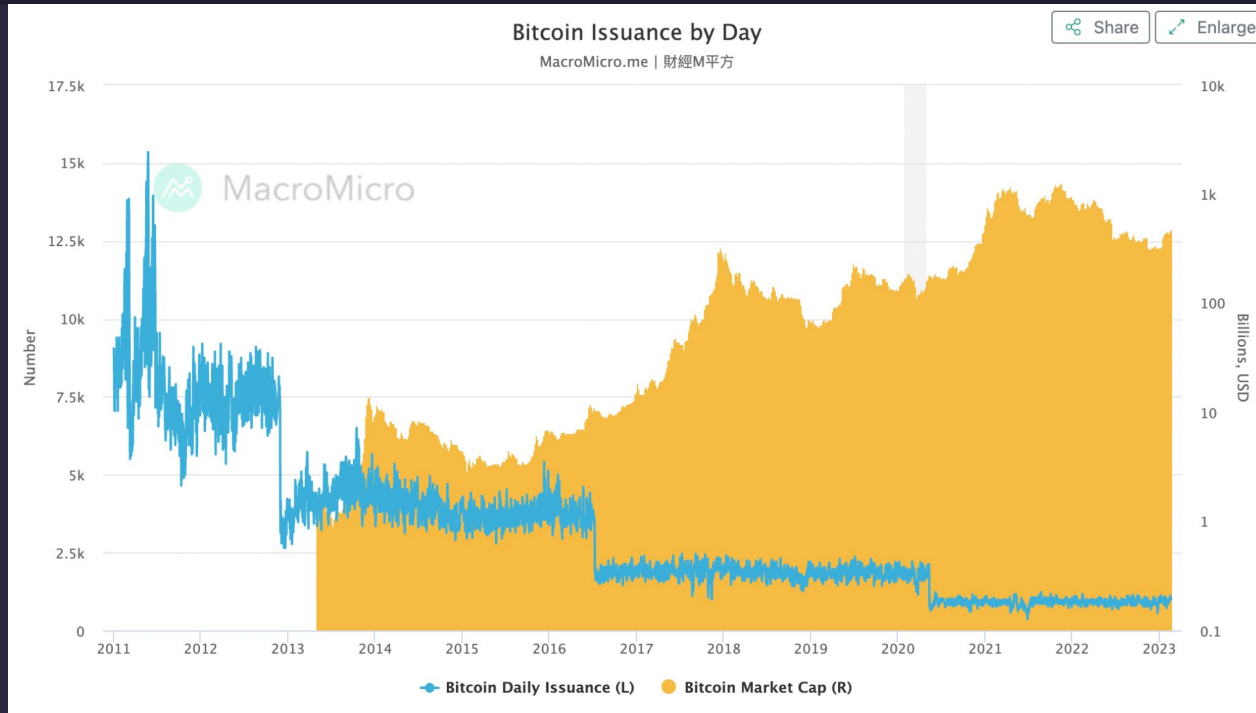
/Discussion

- If there is no archive node, is the network secure?
 - If not, how many archive nodes do we need to secure the network?
 - If yes, what is archive node used for?
- Security Consideration of light client
 - If you only sync with one full node..
 - Is there other consideration?

/Miners & Stakers

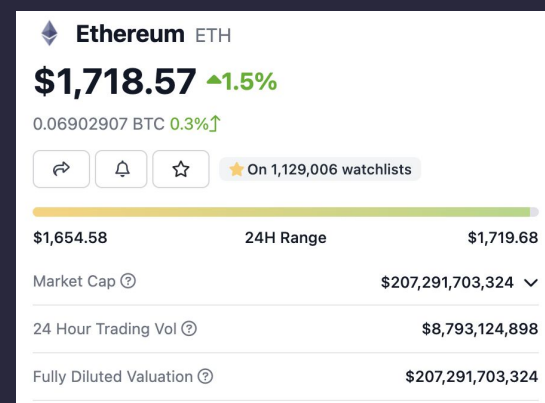
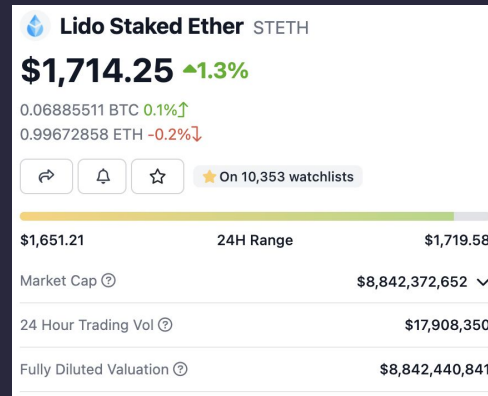
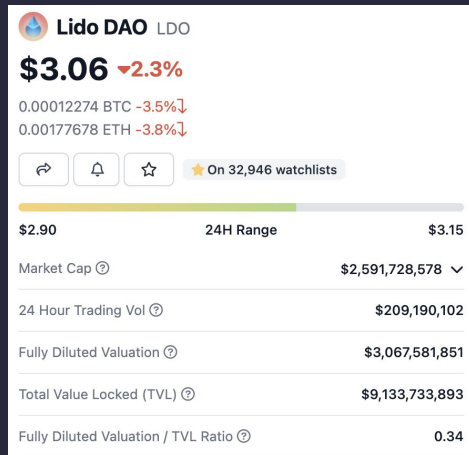
- Organizations that proposes new blocks to obtain rewards from the network.
- **Cost:** Hardware cost & Electricity cost for maintaining the node & (*electricity cost for competing in hashrate if it is PoW*)
- Reward: Block rewards

/Miners & Stakers



/Individuals cannot mine/stake anymore..?

- Pooling! How does pooling work?
 - Pooled mining & pooled staking?

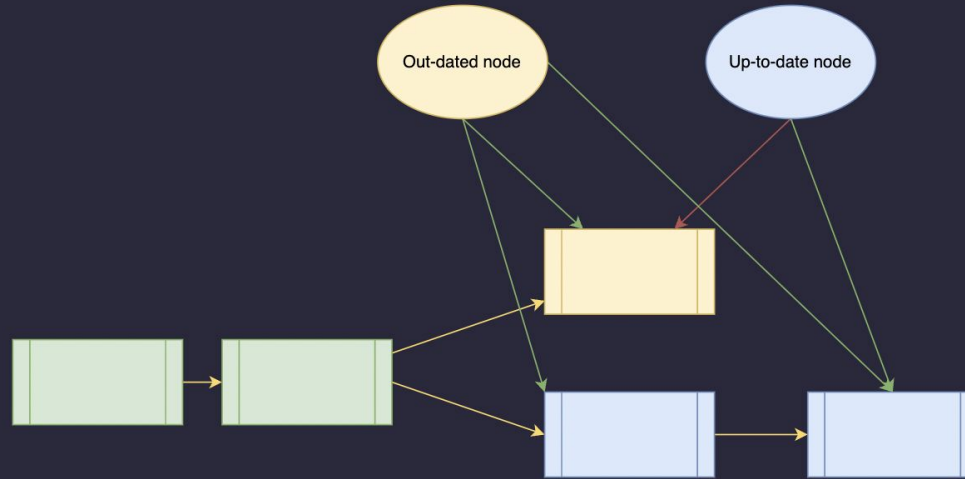


/How does a blockchain upgrade?

- Core devs propose changes and updates the spec.
- Team (may or may not be the core devs) who work on node implementations update accordingly.
- Miners/Stakers will need to update their node implementation accordingly. Sometimes this does not happen.
- **Discussion:**
 - Why would miners/stakers NOT upgrade their node implementation?
 - What happens when a set of miners/stakers does NOT upgrade their node implementation?

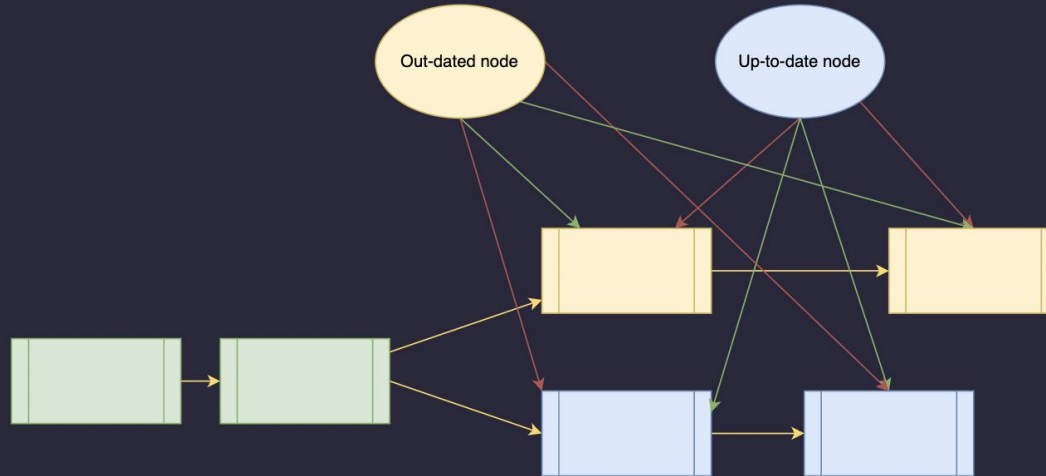
/Forks: Soft fork

- Upgrades that are backward compatible – soft fork.
- **Discussion:** What happens when there is a soft fork?



/Forks: Hard fork

- Upgrades that are breaking changes – hard fork.
- **Discussion:** What happens when there is a hard fork?



/Example: Upgrading Ethereum from PoW to PoS

- What is PoS?
- Updating the Protocol design + Incentive design



<Support Infrastructure>

**/Wallet /Centralized Exchanges /Block Explorers
/API endpoint providers**



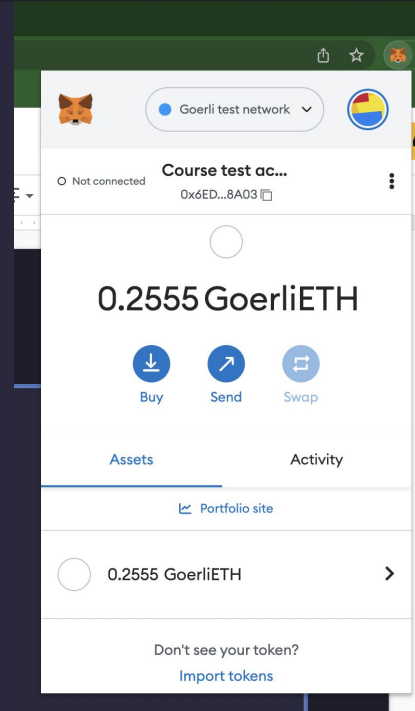
/Wallet

Wallet is a piece of software that assists users with:

- Generating address by generating public key and private key.
- Managing and store private keys.
- Signing transactions - providing them with a better interface than command line.

/Wallet Classification

- Browser extension
- Desktop app
- Mobile phone
- (Not your wallet)
 - Custodial wallet



/Mnemonic

- A series of words that is used to derive private keys and addresses. BIP-39 describes the specification of how Bitcoin wallets implements the mnemonic.
- Whoever gets your private key gets your funds. Do not show people your mnemonic!
- Do NOT use the mnemonic shown in the right

Your Seed Phrase

Your Seed Phrase is used to generate and recover your account.

1. issue

2. flame

3. sample

4. lyrics

5. find

6. vault

7. announce

8. banner

9. cute

10. damage

11. civil

12. goat

Please save these 12 words on a piece of paper. The order is important. This seed will allow you to recover your account.



I understand that if I lose my seed phrase that I will not be able to recover my account.

Accept

/Paper Wallet



A Bloomberg TV Host Gifted Bitcoin On Air And It Immediately Got Stolen

Sam Ro Dec 23, 2013, 8:29 PM



"milkywaymasta" used this image to digitally mug Bloomberg's Adam Johnson. Bloomberg TV

/Very Important Note about wallets

- Not your key, not your money
- UX perspective – you may lose your key. Key lost is
 - Discussion: What are some possible mitigations?

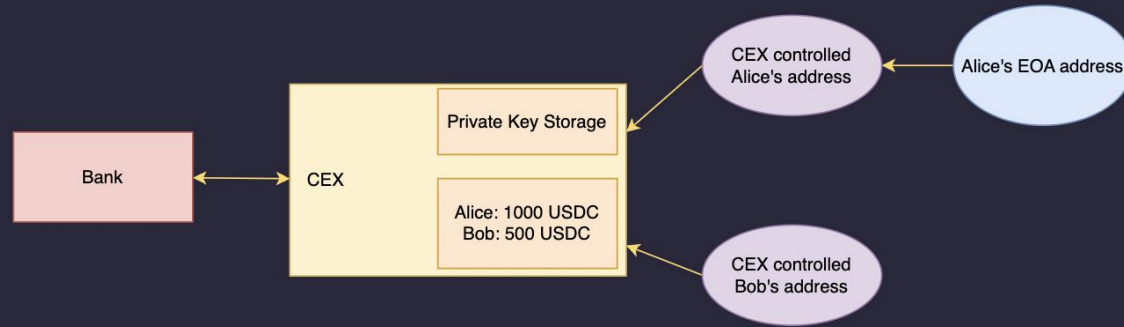
/Centralized Exchange (CEX)

A centralized exchange is like a traditional bank where they store the information of your money in a centralized manner.

There is no significant difference between a cryptocurrency centralized exchange and a stock exchange or a bank.

/How does a basic CEX work?

- Database as ledger
- Generate unique address for people to deposit
- Detect transfer events
- Key management on their side, users don't hold the key.



/CEX is web2 or web3?

- **Discussion:** How to misbehave as a CEX?
 - Quadriga
 - FTX

/We want our CEX to be solvent

Traditionally, you bring in an auditor and check that your assets are greater than liability. The auditor put down their signature and put their reputation & license at risk.

/Proof of Solvency for CEX

Proving solvency consists of 3 parts:

1. Claiming that assets are greater than liability.
2. Proof of Asset - Proving that I own the asset I claimed to own in part 1.
3. Proof of Liabilities - Proving that the liability I claimed in part 1 is indeed my liability.

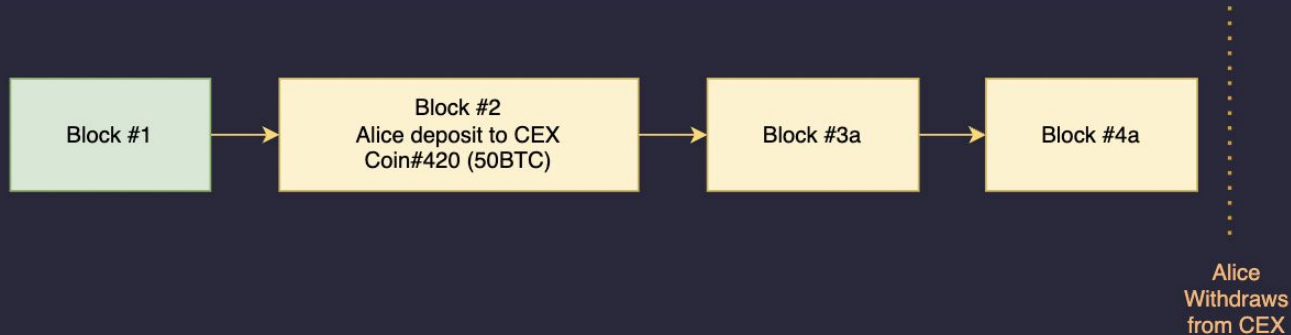
There are cryptographic tools to assist us on this matter!

We will explore this later if we have time!

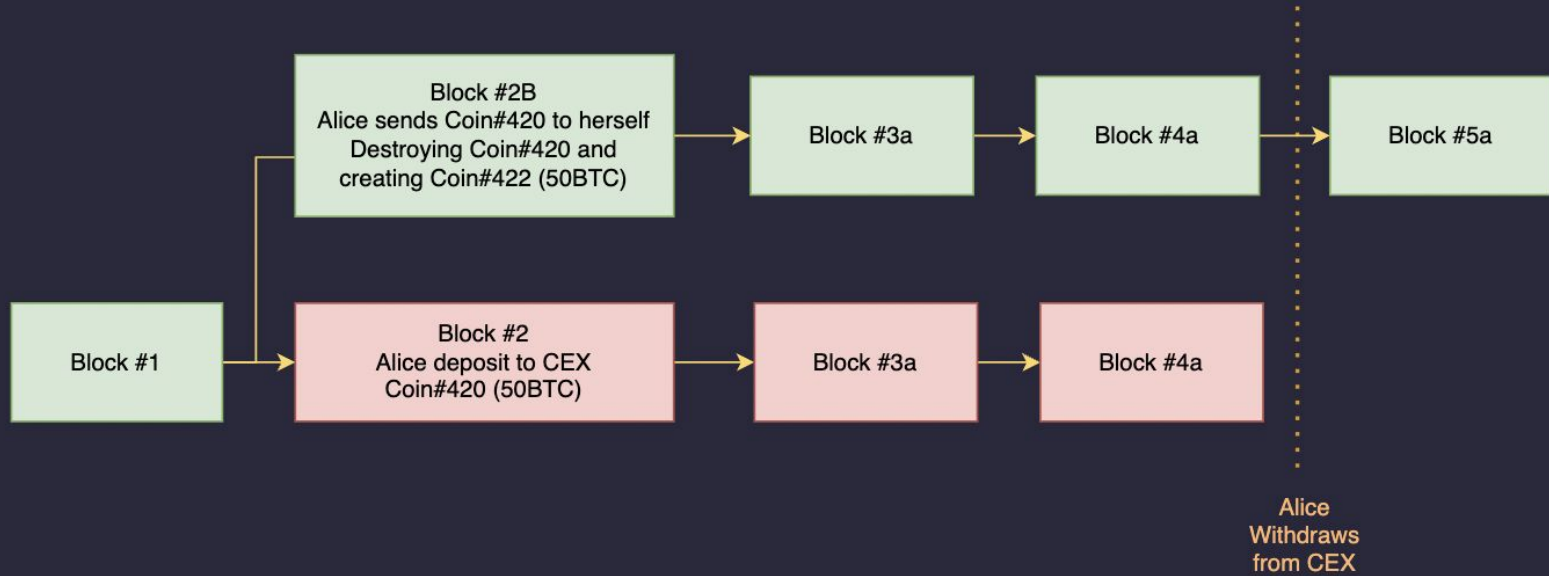
/Double Spending attack on CEX (1)



/Double Spending attack on CEX (2)



/Double Spending attack on CEX (3)



/Examples of Double Spending attack on CEX



HELEN PARTZ

SEP 04, 2018

Bittrex to Delist Bitcoin Gold by Mid-September, Following \$18 Million Hack of BTG in May

Bittrex will delist Bitcoin Gold by September 14, following an \$18 million double-spending hack of BTG in May.




JACK MARTIN

JAN 27, 2020

Bitcoin Gold Blockchain Hit by 51% Attack Leading to \$70K Double Spend

The Bitcoin Gold blockchain suffered a second 51% attack in two years, leading to \$70,000 worth of BTG being double spent.

/Rent Hashing power: NiceHash

 Mining ▾ Hash Power Buying ▾ EasyMining Help Blog Log in GET STARTED			
ALGORITHM	MIN. PRICE	AVG. PRICE	
Scrypt	0.00001024 BTC/TH/day	0.1087 BTC/TH/day	MARKETPLACE
SHA256AsicBoost	0.00000000031232 BTC/EH/day	3.4449 BTC/EH/day	MARKETPLACE
SHA256	0.000000000322 BTC/EH/day	4.5391 BTC/EH/day	MARKETPLACE
X11	0.000000567 BTC/PH/day	0.5725 BTC/PH/day	MARKETPLACE
X13	0.00000019 BTC/TH/day	0.0035 BTC/TH/day	MARKETPLACE
Keccak	0.0000006443 BTC/PH/day	0.7980 BTC/PH/day	MARKETPLACE
NeoScrypt	0.0002 BTC/GH/day	0.0042 BTC/GH/day	MARKETPLACE
Qubit	0.00000007 BTC/TH/day	0.0012 BTC/TH/day	MARKETPLACE

/PoW 51% attack cost

Name	Symbol	Market Cap	Algorithm	Hash Rate	1h Attack Cost	NiceHash-able
Bitcoin	BTC	\$479.24 B	SHA-256	292,989 PH/s	\$1,739,988	0%
Litecoin	LTC	\$6.92 B	Scrypt	678 TH/s	\$77,094	8%
EthereumClassic	ETC	\$3.22 B	Etchash	126 TH/s	\$29,134	3%
BitcoinCash	BCH	\$2.77 B	SHA-256	1,853 PH/s	\$11,005	9%
BitcoinSV	BSV	\$840.56 M	SHA-256	648 PH/s	\$3,850	27%
Zcash	ZEC	\$812.84 M	Equihash	9 GH/s	\$5,845	12%
Dash	DASH	\$795.30 M	X11	3 PH/s	\$1,752	5%

source: <https://www.crypto51.app/>

/How to prevent this attack as a CEX?

You run a CEX, and you want to prevent the double spending attack. What are the mitigation strategies?

/Block Explorers (recap)

The general users need a generic interface to browse and maybe interact with a blockchain.

The main value they provide: a generic and transparent information aggregator for lower level details of a blockchain including blocks and txs.

- Etherscan

/Block Explorers

cc1045821cbcd5776d5bd8937389ac4f3bba7bc0fe773386d463727b4dfd1312

DETAILS +

#0 735dc6c81b13c36ab267b3956a2d03a3684f423e70107cee11f819a0a00 0.01214166 BTC
17e5e:0



#0 bc1q7cguku9cj9g9eyk7cnml5han5rfwf7p7gzt9vs 0.01180566 BTC

1 CONFIRMATION 0.01180566 BTC

50749b935c45c33aa7697121e9ecd4c14823cb7333f2cecd3ce31af1b3bd8752

DETAILS +

#0 81d71878fb49c7b539a68672465df8320d34b71a7ff2c73f67826db0e40 2.03440908 BTC
31a27:1




#0 3DjPZ66Q3mc5qphvSQGBvggaJJ26ZykwAW 0.05053614 BTC

#1 bc1qw2w4884nnmzje5nemapq3x6qzrp2z8jr5q0n5y 1.98344694 BTC

1 CONFIRMATION 2.03398308 BTC

/Block Explorers

ETH Price: \$1,707.01 (+1.31%) Gas: 35 Gwei


 Home Blockchain Tokens


The Ethereum Blockchain Explorer


All Filters


Search by Address / Txn Hash / Block / Token / Domain Name


Featured: Bridging tokens between Ethereum, Layer 2 and other chains? Browse through the Blockscan [bridges list](#).


 **ETHER PRICE**
\$1,707.01 @ 0.06865 BTC (+1.31%)

 **TRANSACTIONS**
1,879.83 M (12.6 TPS)



 **MED GAS PRICE**
35 Gwei (\$1.25)

 **MARKET CAP**
\$205,680,252,411.00



 **LAST FINALIZED BLOCK**
16671900

 **LAST SAFE BLOCK**
16671931

Latest Blocks

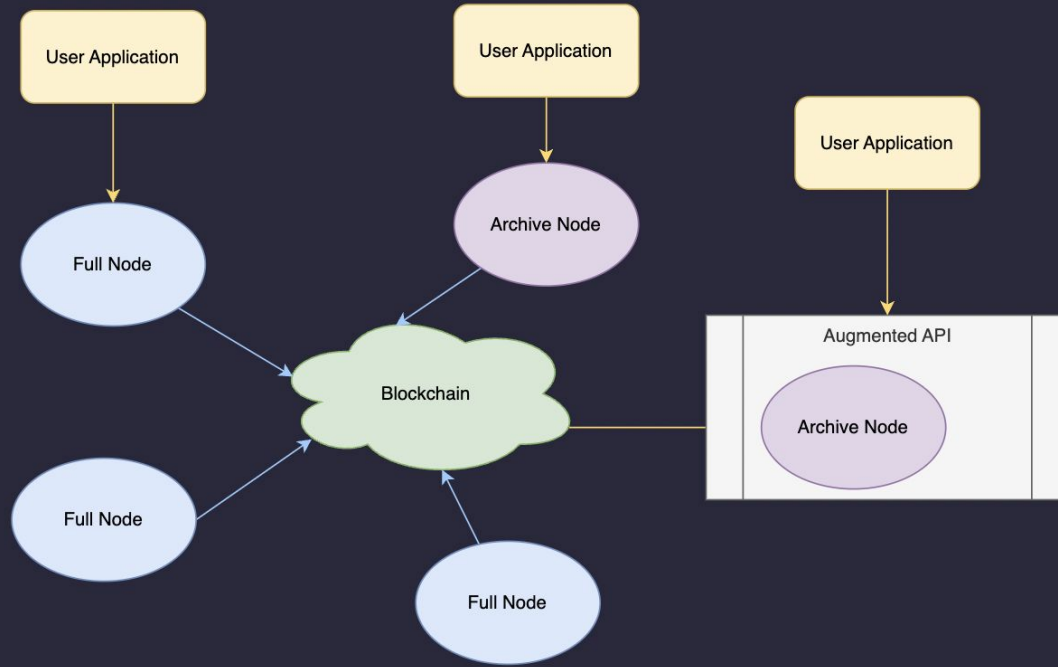
 16671977 14 secs ago	Fee Recipient 0x40638C...4640DD40 134 txns in 12 secs	0.02545 Eth
 16671976 26 secs ago	Fee Recipient Eden Network: Bui... 133 txns in 12 secs	0.03697 Eth

Latest Transactions

 0x55b48f58b3d41... 14 secs ago
 0xe108bfb104c4... 14 secs ago

/API endpoint Providers

- Infura
- Tenderly
- Alchemy
- Quicknode



/API endpoint Providers

- FullNode
 - If you need to send transactions
 - If you only need to simulate within recent blocks
- Archive Node
 - IF you need blockchain state before 256 blocks
- Enhanced API
 - Based on the needs of your application

/Can API endpoint Providers misbehave?

- How can they attack users?

/Can API endpoint Providers misbehave?

- How can they attack users?
 - Censorship: not sending transactions
 - Privacy violation: Collect information of users
- Why are we still using them if there are these attack vectors?

/Ramp up and Scale up

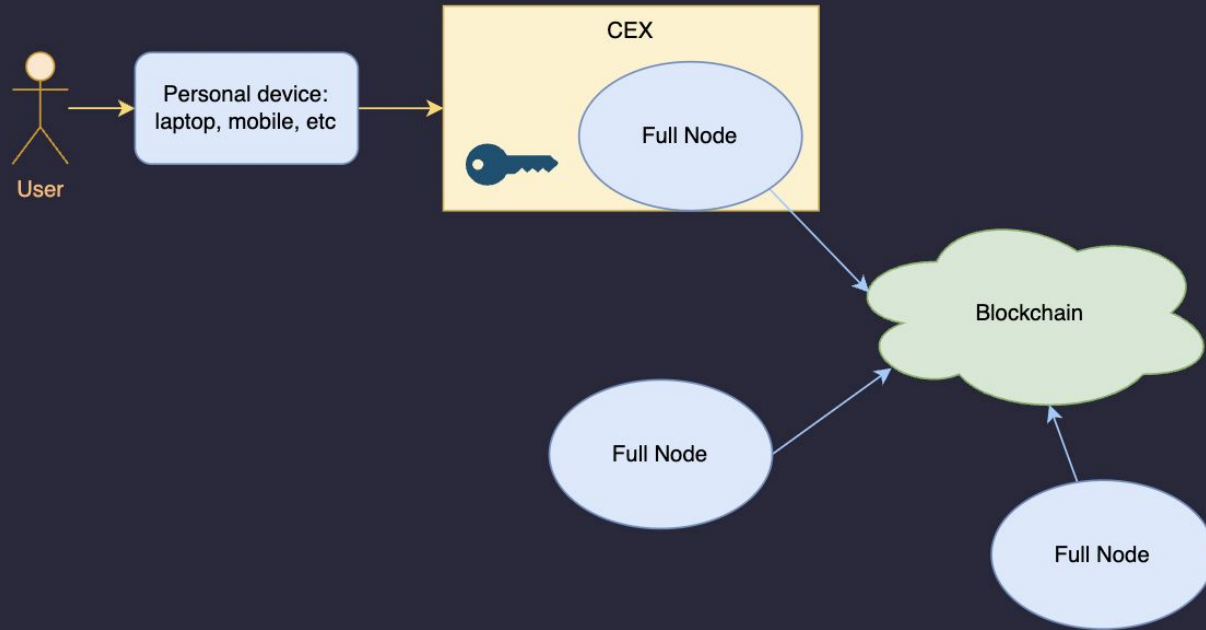
- Ethereum has the most active developer activity
 - A lot of convenient tools -- which means that privacy / decentralization is compromised. But remember, it is “Permissionless” and there are measure to take to counter it.
- For Beginners:
 - Privacy perhaps is not the main concern yet.
(IMPORTANT: it WILL BE)
 - Typical / simplest route (but DOXX):
 - Buy Ether on Centralized exchange
 - Transfer Ether to your Metamask Wallet (there are others too)
 - Interact with the blockchain

/Hardware Wallet

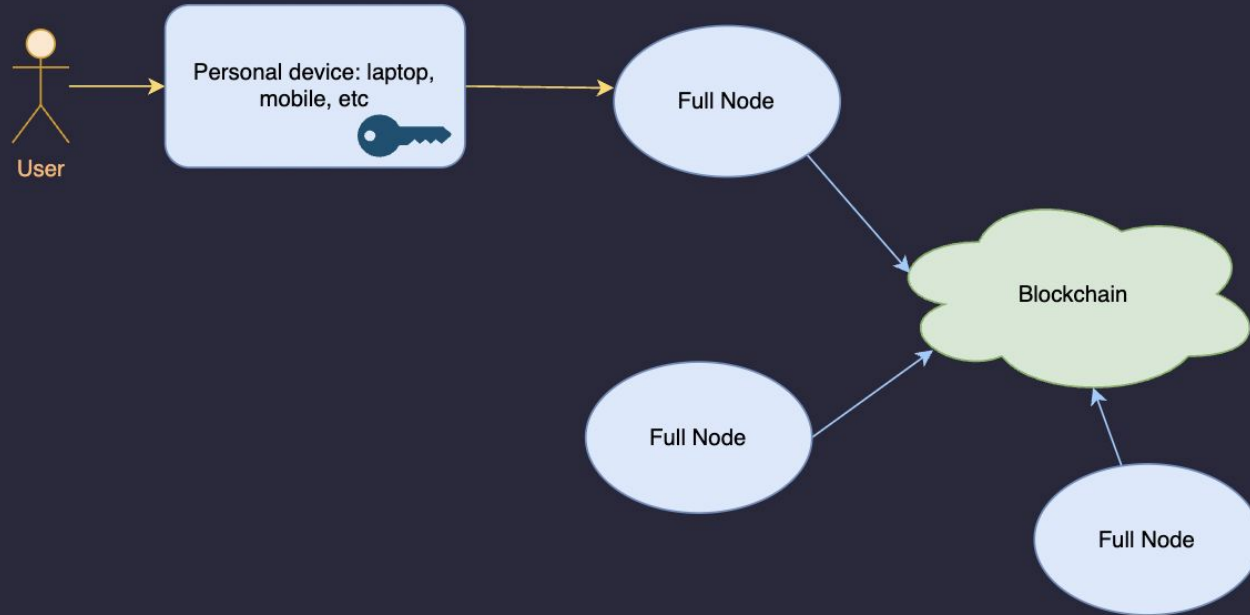
- Store the private key on a hardware that is not connected to the internet. Connects to laptop with USB or bluetooth.
- **Initialize:** input 12 or 24 words of mnemonic. Configure PIN.
- **Usage:** everytime a transaction needs to be signed, the transaction is sent to the device and can only be signed when it is unlocked by PIN.



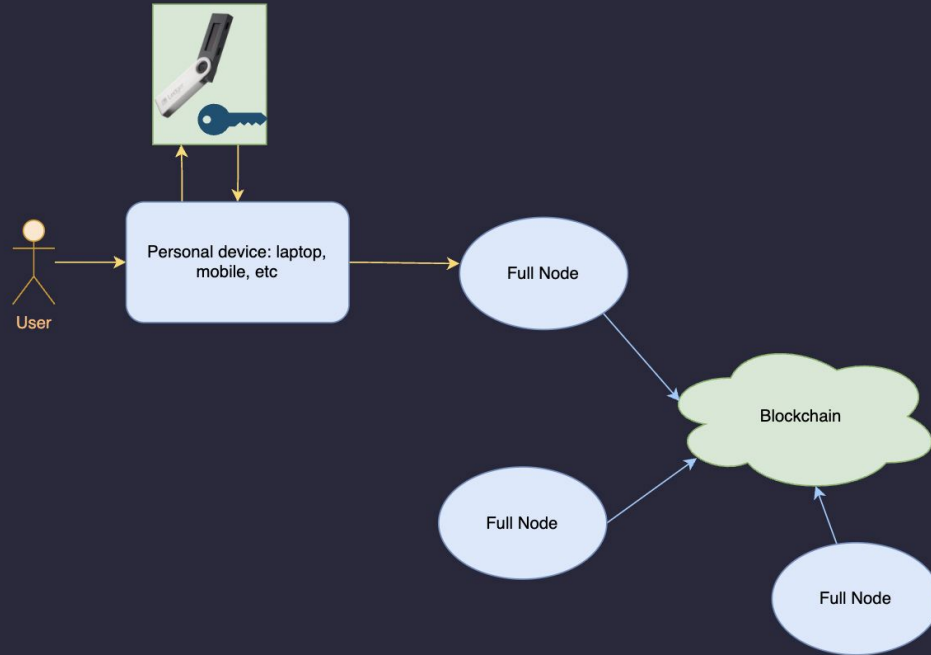
/Private key storage: CEX Users



/Private key storage: Metamask, API endpoint users



/Private key storage: Hardware Wallet



/How to store your funds securely?

- Have only the least amount on CEXs
 - Not your key, not your money!
- Cold wallet / Hot wallet
- Backup your mnemonics, divide them into pieces, and lock them away
- Enterprise level funds - secret sharing mechanism to divide the key to multiple parties.
- Have proper security hygiene.

/Basic Security Hygiene

- Do not download random things from the internet.
- Staying vigilant of phishing email.
- How do you store your password? How secure is your password?
 - Who here uses a Password Manager?



<Proof of Solvency>



/Main Problem statement

You use an exchange, how do you know the exchange has enough funds to allow everyone to withdraw their money out?

Sub problem statements:

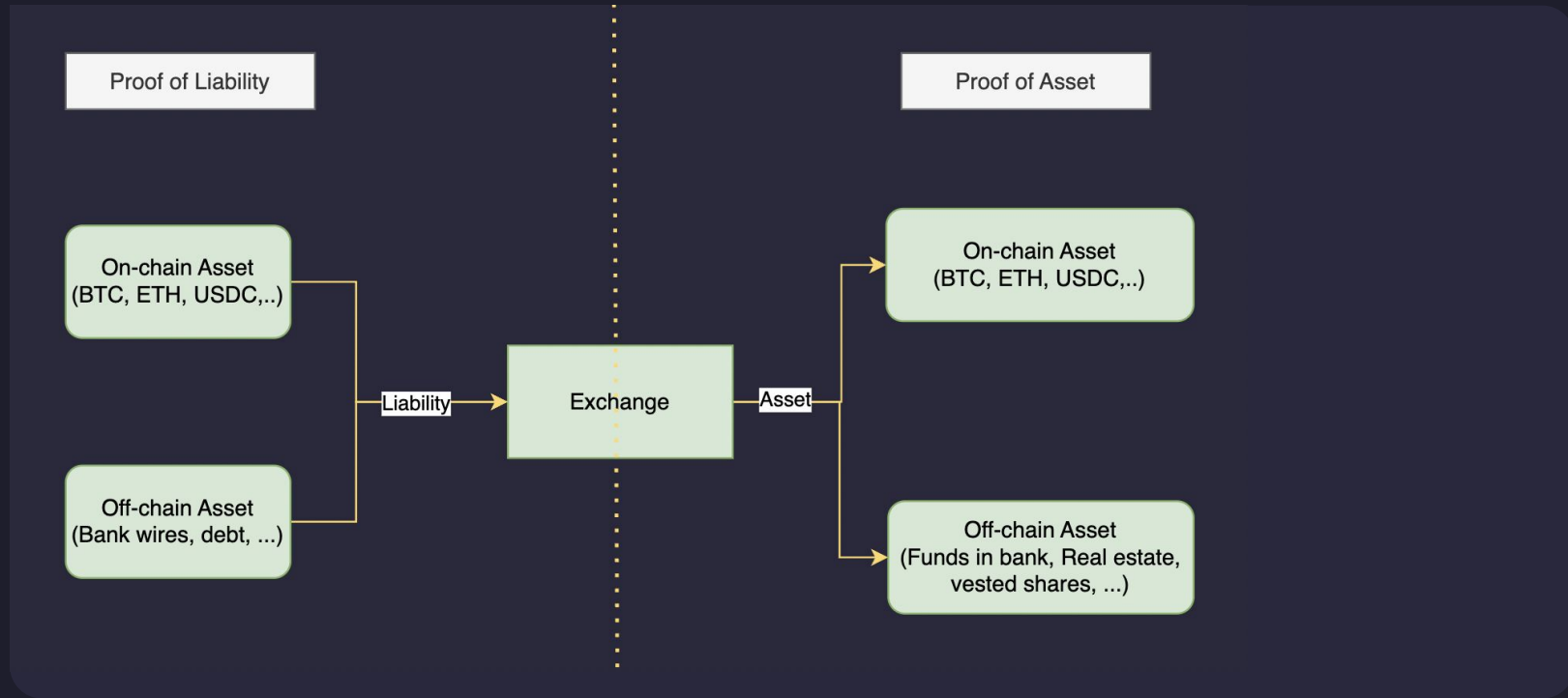
- You also want to retain your privacy
- Exchange also want to retain their secret

/Proof of Solvency for CEX (recap)

Proving solvency consists of 3 parts:

1. Claiming that assets are greater than liability.
2. Proof of Asset - Proving that I own the asset I claimed to own in part 1.
3. Proof of Liabilities - Proving that the liability I claimed in part 1 is indeed my liability.

/Proof of Solvency



/Problem statement of “Proof of Asset”

The exchange says they have **XXX** amount of asset in total. How do we verify it?

Exchange hold on-chain asset and off-chain asset.

/Naive solution: send TXs to prove that you own addresses

Skepticism towards Mt.Gox (2011):

- 420k Bitcoin is moved in a single transaction to prove that they hold the assets

Confidential information (like the size of Mt. Gox's business) was exposed. Only handles the on-chain part.

Signing message with private key also achieves the same thing without the transaction fee.

/A scheme that protects exchange privacy

Setup: Get a set of public keys, mixed with all the public keys that is controlled by the exchange.

Method:

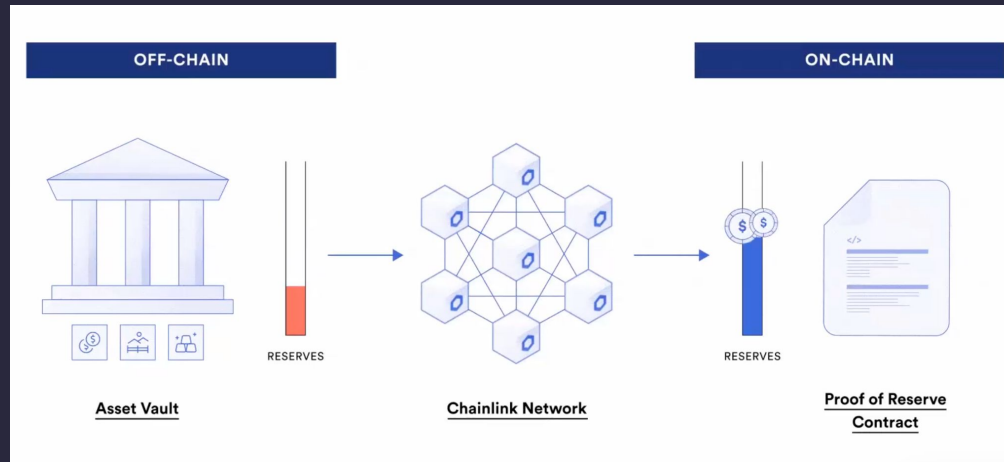
- Prove that the exchange control a subset of the public keys which sums up greater than **XXX**.
- Use **Homomorphic addition** to blind the balance.
- Use **ZKP** to prove that exchange indeed knows the secret keys without revealing which public keys are in its control.

/Exchanges attacking the scheme

- Transferring assets between exchanges to help each other pass proof of assets, short term loans.
- **Solutions:**
 - a. All exchanges do proof of asset at the same time.
 - b. Announce auditing something in the past.
- Note that this only covers on-chain asset.

/Proof of Asset for off-chain assets

- Financial Auditor
- Chainlink Oracle



/Proof of Asset - continuous monitoring

- Assets change all the time. Timestamp is extremely important.
- Key can be lost.
- Assets can change all the time.
- Proof of assets needs to be done like a heartbeat.

/Proof of Asset - limitation

- Liquidity is not captured in the notion. Consider Off-chain assets such as Real estate or Vested shares.
- “Fractional reserve in terms of liquidity, but in total it is solvent because the assets surpass the liabilities”

/Proof of Liability

The exchange says they owe everyone **XXX amount in total**. How do we verify it?

From user's PoV, regardless of the method (on-chain or off-chain assets) that I have transferred to the exchange, I see a balance on the exchange.

That is **“what the exchange owes me”**.

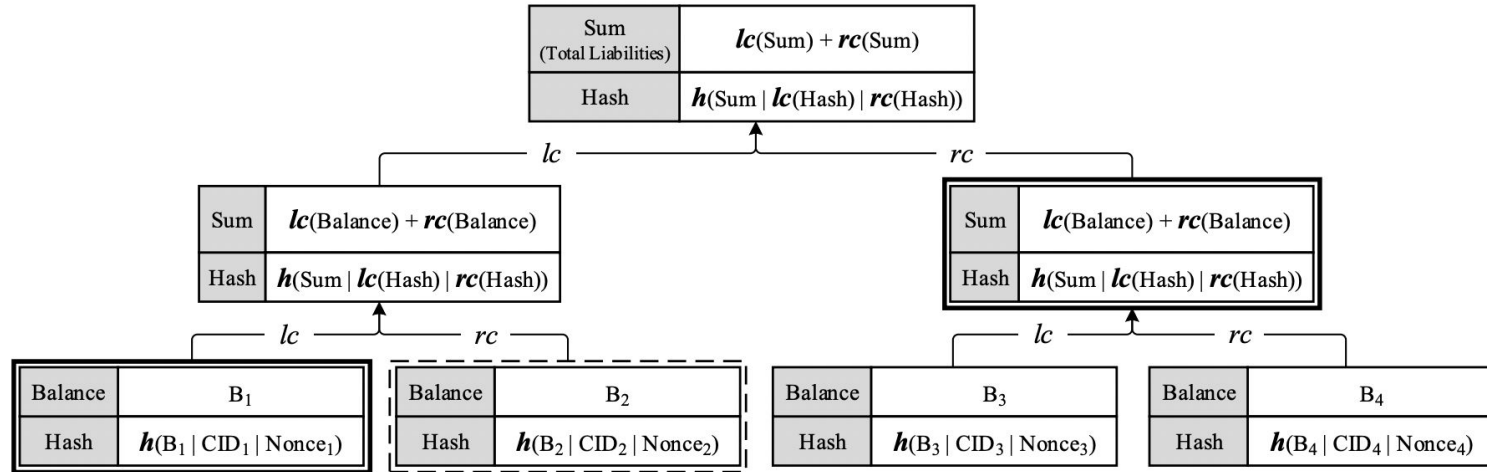
/Proof of Liability - Naive solution

Publish an excel sheet of everyone's "unique identifier" and "balance" Everyone can check if they are being included in the excel sheet.

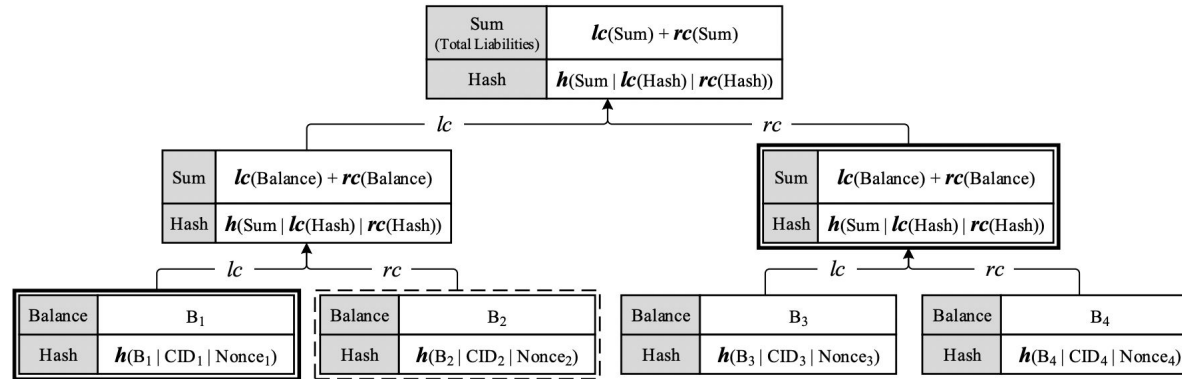
Downside:

- Everyone's balance is revealed to everyone
- Exchange's business size is revealed

/Proof of Liability - Maxwell's modified Merkle Tree



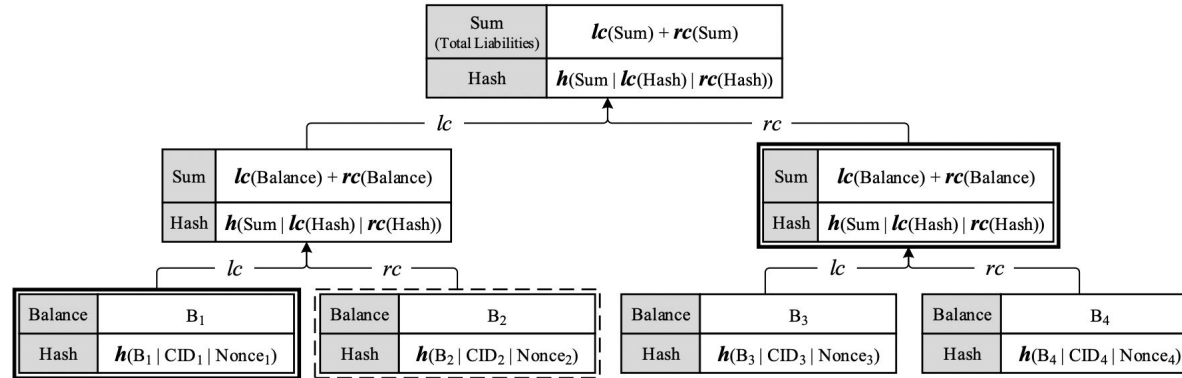
/Proof of Liability - Maxwell's modified Merkle Tree



Downside:

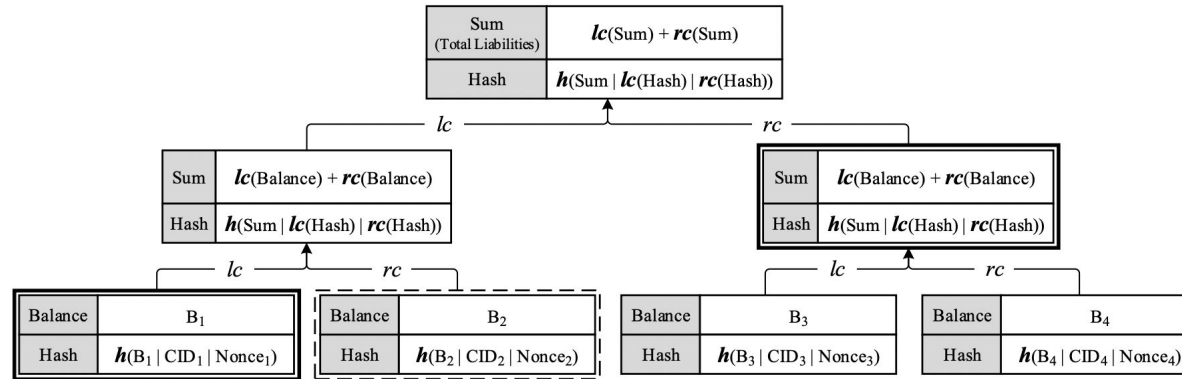
- Neighbor's balance is revealed
- Exchange's balance is revealed

/Proof of Liability - Advancing the idea



Idea: use Homomorphic Encryption to blind balances

/Proof of Liability - Advancing the idea



Problem: Exchange can insert “Negative” balance.

Solution: ZK proof to prove that all balances are in reasonable range.

/Proof of Liability - People need to check the Tree

2% to 5% of total users are needed to make it hard for exchange to cheat.

If people don't check the tree, this is useless.

If the exchange don't provide tooling for people to check the tree, this is useless in practice.

/Proof of Liability - Problems encountered

- **Different Merkle Root can be served to different users**
 - Web2 attack. The proof will be valid, but it is not correct.
 - Solution: root needs to be published to a public bulletin board. Twitter, reddit, blockchain.
- **Privacy for exchange - Merkle tree roughly reveals the size of exchange users**
 - Solution: Use a sparse merkle tree
- **Users with same balance can be assigned to the same node**



/THAT'S A WRAP! (mic drop)



CREDITS: This presentation template was created by **Slidesgo**, and includes icons by **Flaticon**, and infographics & images by **Freepik**

