Blockchain DLOC Sem VII

CSDC7022 : Block Chain

Module - 2 : Cryptocurrency (8 Hours)

Instructors : Dr. Nupur Giri & Mrs. Lifna C S

Department of Computer Engineering, VESIT, Mumbai

Topics to be covered

- Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security),
- Cryptocurrency wallets: Hot and cold wallets,
- Cryptocurrency usage,
- Transactions in Blockchain, UTXO
- Where do transaction fees come from?
- How do Wallets work ?
- What is Segregated Witness (SegWit) ?
- Understanding Mining Difficulty
- Mining Pools and its methods
- Nonce Range
- How Miners Pick transactions ?

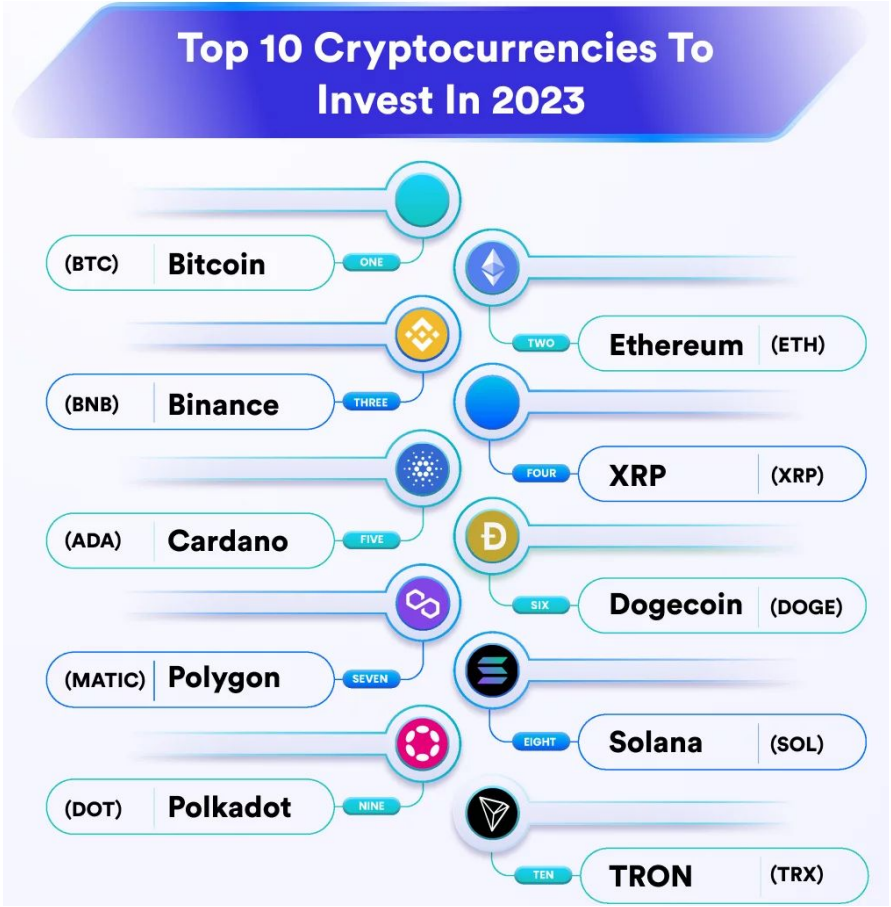
Topics to be covered

- CPUs Vs GPUs Vs ASIC
- Life of a miner
- How do Mempool Works ?
- Double Spending Problem - 51% Attack
- Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".
  - Consensus in Bitcoin
- Consensus Mechanisms :
  - Proof of Work (PoW),
  - Proof of Stake (PoS),
  - Proof of Elapsed Time (PoET),
  - Proof of Burn(PoB),

Cryptocurrency as a Form of Currency

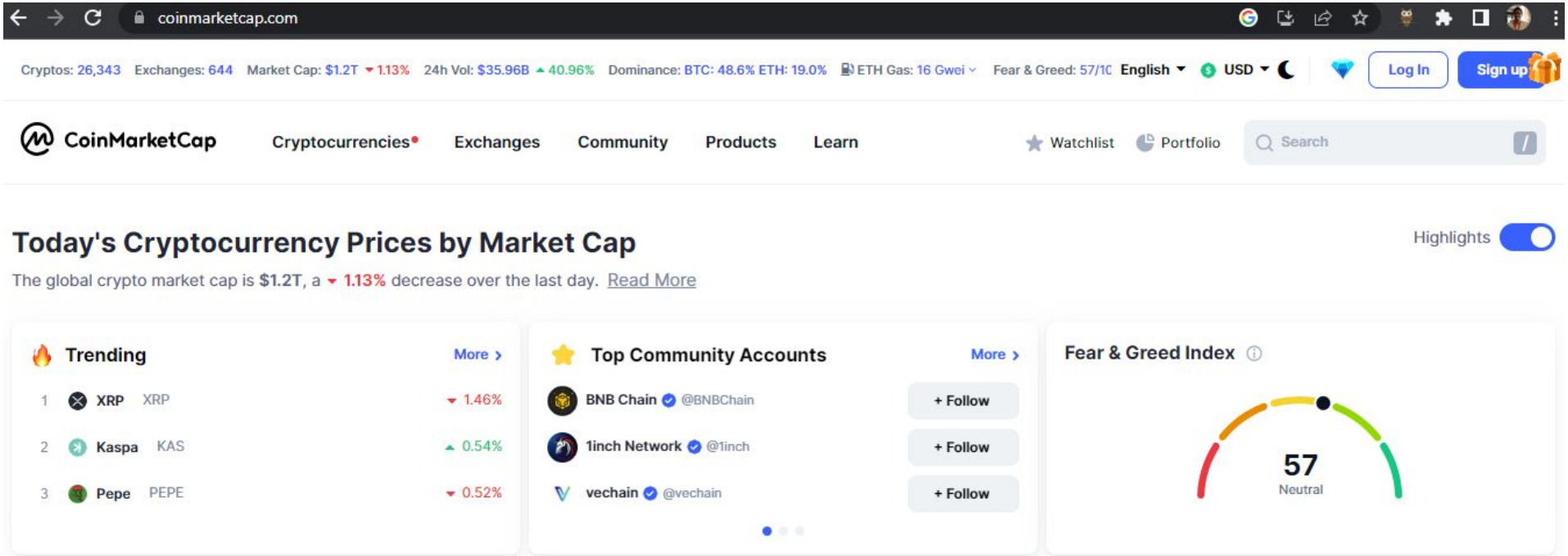
- **Cryptos** - Eg. **Bitcoin, Litecoin, Shiba Inu, and Dogecoin** Monero
- Various companies and even countries around the world accept some of these digital currencies for conducting transactions.
- However, the **high volatility of Bitcoin and other popular cryptocurrencies makes it unsuitable for everyday use by the public.**

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)



Courtesy : Blockchain Council

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)



Courtesy :Coin Market Cap

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)

coinmarketcap.com

#	Name	Price	1h %	24h %	7d %	Market Cap	Volume(24h)	Circulating Supply	Last 7 Days
1	Bitcoin BTC	$30,031.33	0.06%	0.79%	1.81%	$583,582,180,536	$13,915,787,862 463,789 BTC	19,432,443 BTC	
2	Ethereum ETH Buy	$1,902.23	0.18%	1.49%	0.93%	$228,649,199,593	$6,805,217,681 3,580,338 ETH	120,200,810 ETH	
3	Tether USDT	$1.00	0.01%	0.02%	0.03%	$83,764,794,851	$25,119,445,910 25,121,670,369 USDT	83,750,478,228 USDT	
4	XRP XRP	$0.742	0.91%	1.28%	55.55%	$38,988,478,793	$2,488,792,945 3,362,636,583 XRP	52,544,091,958 XRP	
5	BNB BNB Buy	$242.45	0.16%	0.16%	1.84%	$37,785,564,247	$622,141,330 2,566,277 BNB	155,848,474 BNB	
6	USD Coin USDC	$0.9997	0.03%	0.03%	0.07%	$27,061,775,100	$3,257,441,382 3,258,388,639 USDC	27,068,995,625 USDC	
7	Cardano ADA	$0.3063	0.70%	3.54%	4.69%	$10,714,886,745	$306,184,269 999,796,052 ADA	34,981,876,368 ADA	

Courtesy :Coin Market Cap

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)

BitCoin

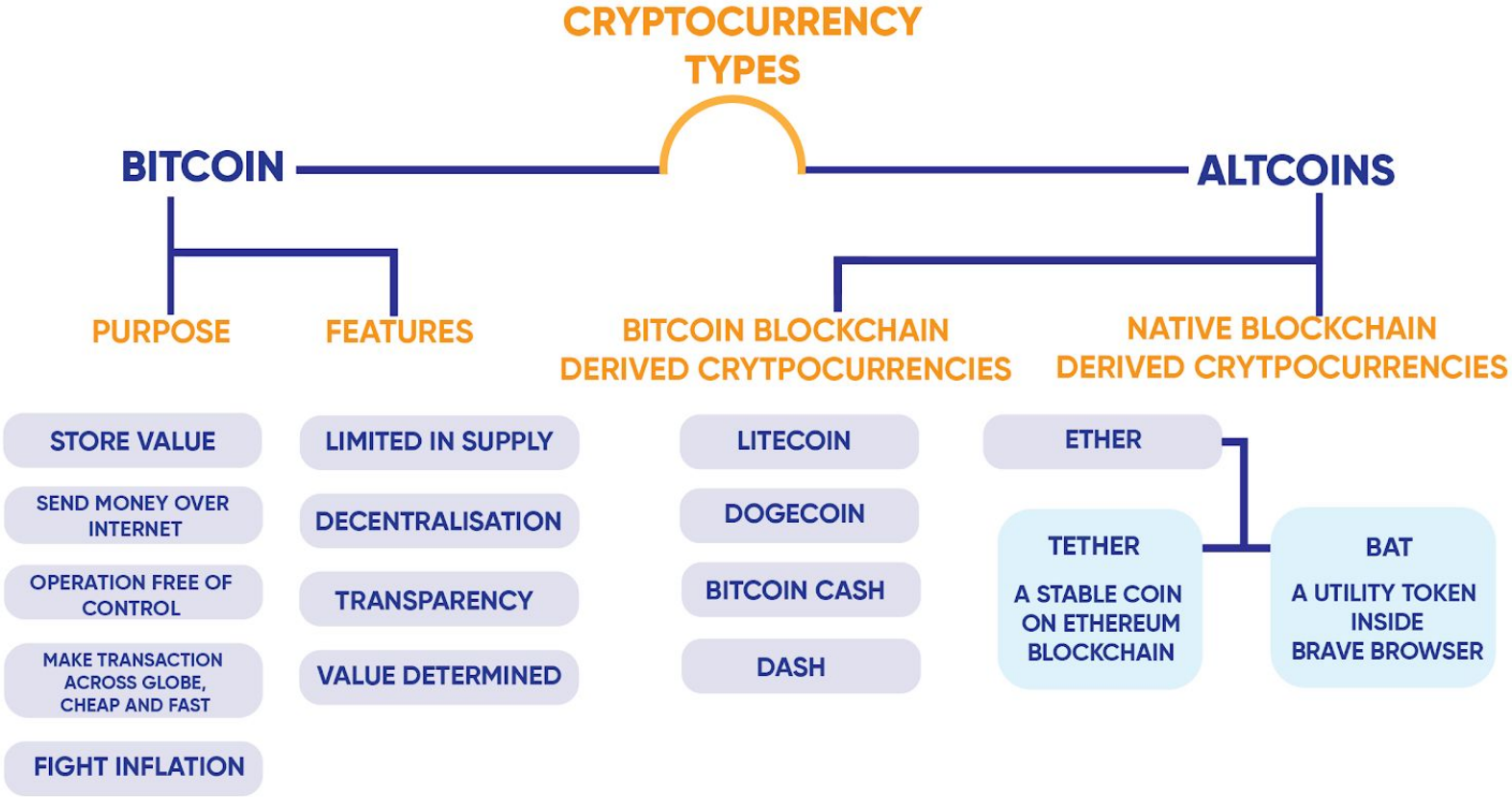
- Launched in **2009**
- **world's largest cryptocurrency** by market capitalization.
- Bitcoin is **created, distributed, traded, and stored using a decentralized ledger system (**Blockchain)
- Bitcoin and its ledger are **secured by proof-of-work (PoW) consensus,**
- Bitcoin can be **purchased via various cryptocurrency exchanges.**
- **first decentralized virtual currency**
- provides **secure global transactions quickly and without third-party manipulations**.
- **created to address the inefficiencies in global financial systems**.
- Bitcoin is **not issued by any government**, and **banks do not manage accounts or validate transactions.**
- It is **based on a cryptographic system** that uses certain codes and numbers to keep information safe and secure.
- **stored in digital wallets that allow users to manage and trade their coins.**
- **currently accepted as a means of payment for products sold or services provided.**
- **offers lower transaction fees compared to traditional online payment mechanisms.**
- However, **the value of Bitcoin has been extremely volatile over the past few years.**

Altcoins or Alternative Coins

- **Describe all cryptocurrencies other than Bitcoin**.
- These coins also **use blockchain technology that allows secure peer-to-peer transactions**.
- Altcoins were built on the success of Bitcoin by **slightly changing the rules to appeal to different types of users**.
- They essentially **solve the inefficiencies of Bitcoin**.
  - **Litecoin** - *address issues related to scalability, higher transaction time & charges, and environmental concerns*
  - **Ether** - *created based on the idea that blockchain tech can be used to create applications that go beyond just enabling a digital currency.*
- There are **more than 10,000 altcoins** in existence today.
- Altcoins come in **several types based on what they were designed for.**

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)



Stablecoins

- **Class of cryptocurrencies backed by reserve assets** (cash or commodity).
- **offer price stability while ensuring all basic features or benefits of cryptocurrencies.**
- Provides **instant processing and security of payments.**
  - **1 Tether (USDT)** is pegged to (or **backed by) 1 US Dollar**, as fiat currencies are pegged to an underlying asset such as gold or foreign exchange reserves, **their valuations remain free from wild movements.**
  - **PAX Gold,** a digital token **backed by physical gold**. (currently, **1 PAXG is nearly 30 grams**)
- The basket is meant to act as a reserve to redeem holders if the cryptocurrency fails or faces problems. Price fluctuations for stablecoins are not meant to exceed a narrow range.

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Utility Tokens

- **Coins → operate as currency,**
- **Tokens** are **programmable assets that work on other cryptos' blockchains**. Utility tokens are those used for a specific purpose or use-case, generally for spending within a particular blockchain ecosystem. These tokens **allow their holders to access a company's product or service.**
  - **Eg - 1 : Basic Attention Token (BAT)** is a utility token of **Brave, a free and open-source web browser**
    - BAT was created to **improve the security and efficiency of digital advertising** through blockchain Tech.
    - It **tracks the time and attention of media consumers on websites using the Brave browser.**
    - BAT aims to **efficiently distribute advertising money between advertisers, publishers, and readers of online marketing content and ads.**
  - **Eg - 2** : Ether is another utility token used to **facilitate transactions under Ethereum's blockchain network**.
- Utility tokens are **used to provide services within a network.**
  - Eg : **used to purchase services, pay network fees, or redeem rewards**.
  - Eg : **Filecoin,** to **buy storage space on a network and secure the information**
- Utility tokens can be **purchased on exchanges and held,** helps to keep blockchain network functioning.

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)

Security/Equity Tokens

- **Tokenized assets offered on stock markets**.
- *Tokenization* is the *transfer of value from an asset to a token*, which is then made available to investors.
- **Any asset can be tokenized,** such as real estate or stocks.
- For this to work, the asset must be secured and held. Otherwise, the tokens are worthless because they wouldn't represent anything.
- **Regulated by the Securities and Exchange Commission** because they are *designed to act as securities*.
    - In ***2021,*** the **Bitcoin wallet firm Exodus** successfully completed a Securities and Exchange Commission-qualified **Reg A+ token** offering, allowing for **$75 million shares of common stock to be converted to tokens on the Algorand blockchain. (**Historic event : *first digital asset security to offer equity in a United States-based issuer.)*
- Current Scenario :
    - A blockchain-based company can **issue a whitepaper, outlining details of its projects, future plans, and issue size.** They can **raise funds via an Initial Coin Offering (ICO).**
    - Similar to an **initial public offering (IPO),** wherein a **firm raises funds by selling its shares to the public.**
    - ***Interested investors can apply to an ICO and receive a new cryptocurrency token*** issued by the company.
    - This token may have ***some utility in using the product or service the company is offering***.
    - It **represent a stake in the company or project.**

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Asset Tokens

- **Cryptocurrency backed by a real asset**.
- **Any asset, agreement, or contract between parties** can be ***settled using crypto***.
  - Eg : **Non-Fungible Tokens or NFT**s.
    - These are t**okens that exist on a blockchain and cannot be replicated**.
    - NFTs can be **used to represent ownership of unique items, including art, images, videos, collectibles, and even real estate.** However, buying an NFT of an image or art does not mean the buyer gets the copyright of the underlying item.
    - Unlike most digital items that **can be endlessly reproduced**, each **NFT has a unique digital signature**

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Meme Coins

- Inspired by **a joke or a silly take on other well-known cryptocurrencies**.
- They typically **gain popularity in a short period of time**, often *hyped online by prominent influencers or investors attempting to exploit short-term gains.*
- Eg: Dogecoin.
  - created by IBM software engineer Billy Markus and Adobe software engineer Jackson Palmer.
  - wanted to create a peer-to-peer digital currency that could reach a broader demographic than Bitcoin

Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Governance Tokens

- **Allow holders certain rights within a blockchain**,
  - such as *voting for changes to protocols* or
  - having *a say in decisions of a decentralized autonomous organization (DAO)*.
- Because they are generally **native to a private blockchain** and used for blockchain purposes,
- they **are utility tokens** but have come to be accepted as a separate type because of their purpose

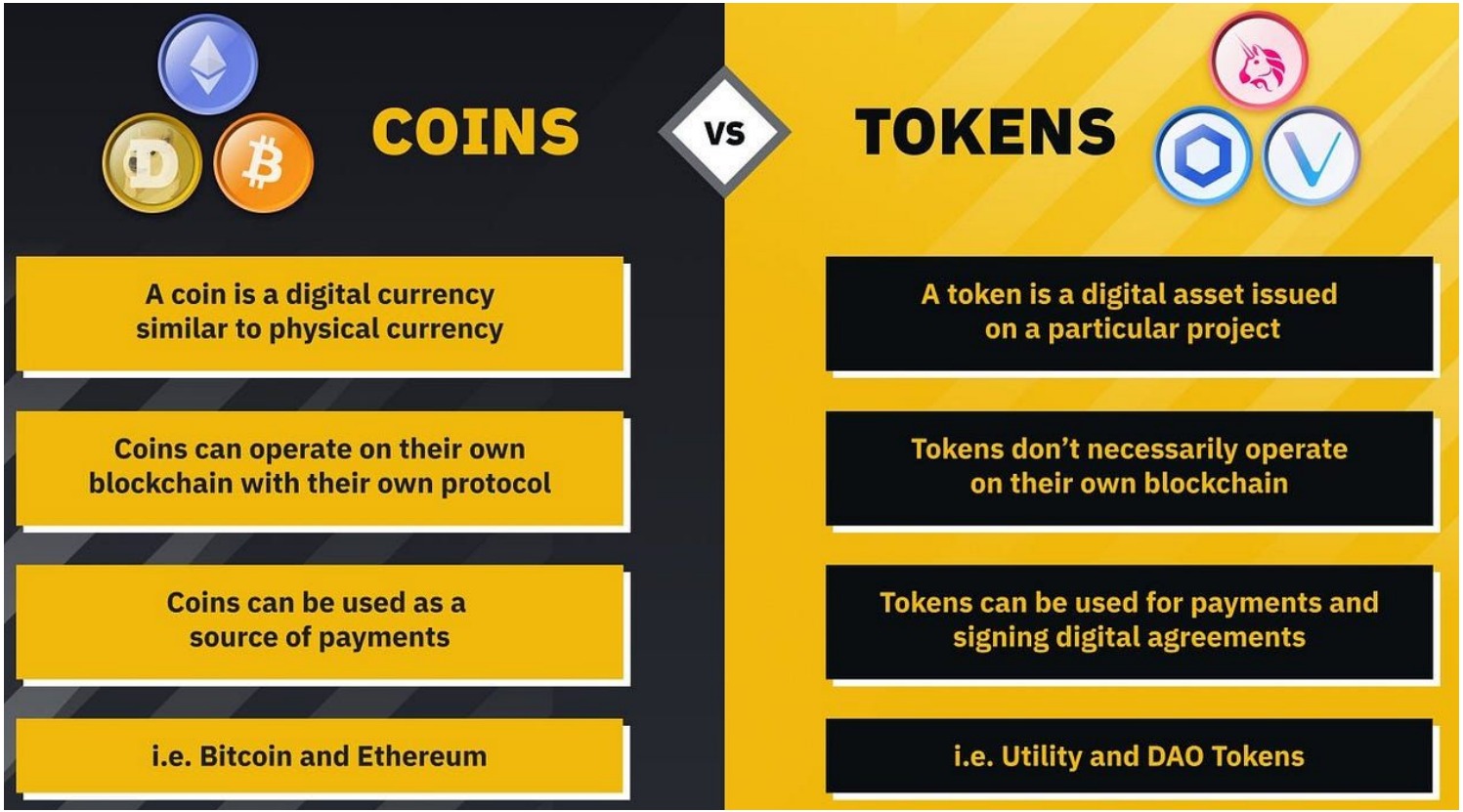
Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Pros and Cons of Altcoins

- **Pros**
  - Improve upon another cryptocurrency's weaknesses
  - Higher survivability
  - Thousands to choose from
- **Cons**
  - Lower popularity and smaller market cap
  - Less liquid than Bitcoin
  - Difficult to determine use cases
  - Many altcoins are scams or lost developer and community interest

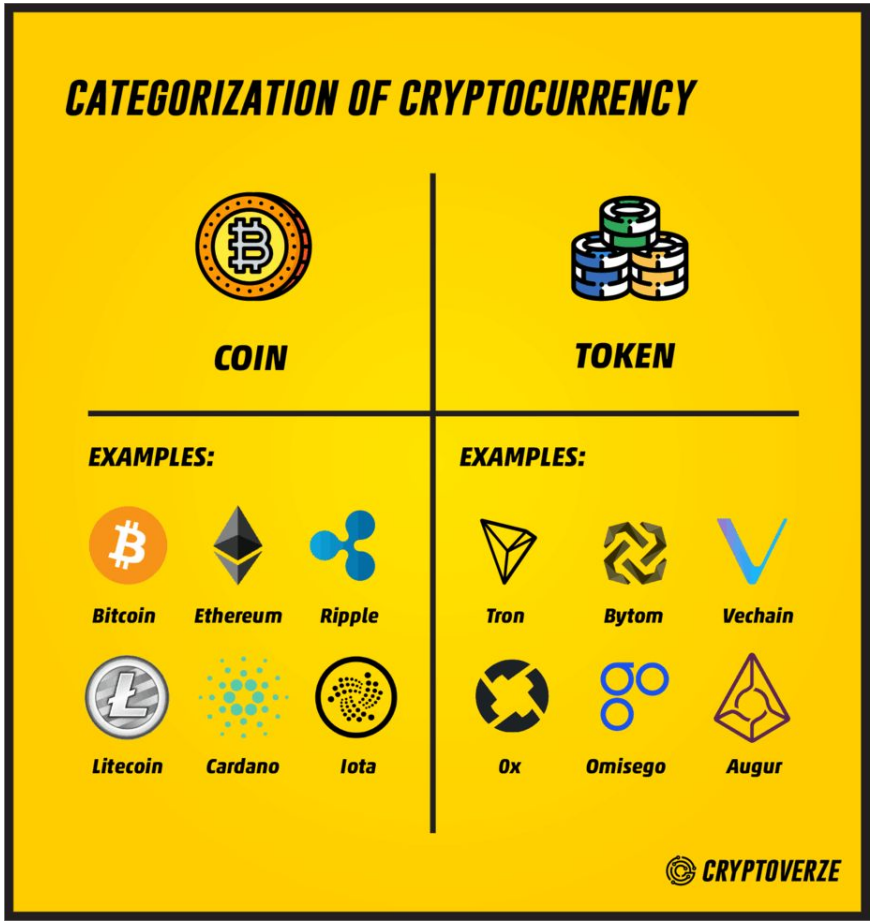
Courtesy : JAKE FRANKENFIELD
Cherian Varghese

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)

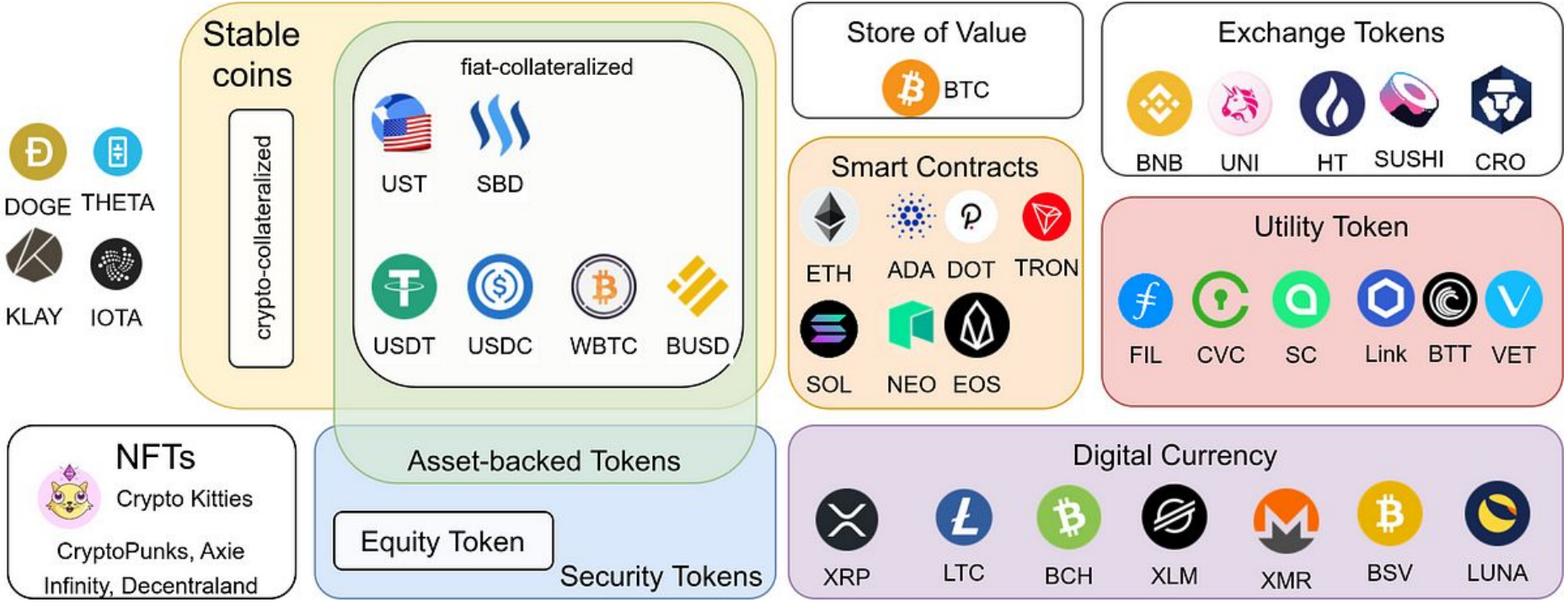


Courtesy : Abhinav Jain

Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)



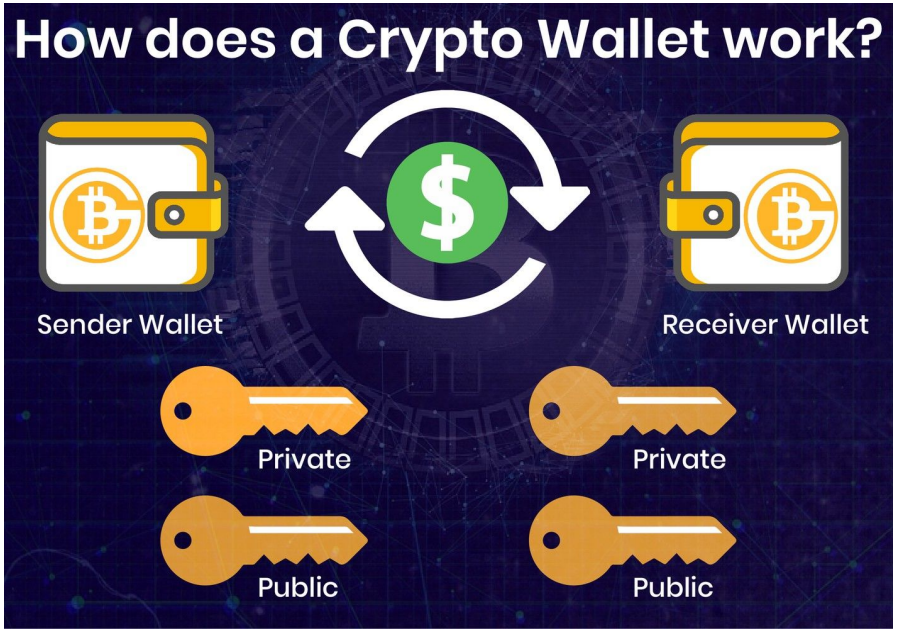
Cryptocurrency: Bitcoin, Altcoin, and Tokens (Utility and Security)



Courtesy : Martin Thoma

Cryptocurrency wallets: Hot and cold wallets

- A cryptocurrency wallet is a **software program that stores your digital money**.
- **store your private keys** - the passwords that give you access to your cryptocurrencies
- Keeps the **crypto safe and accessible.**
- **allow the user to send, receive, and spend cryptocurrencies** like Bitcoin and Ethereum.



Courtesy : Coinbase, Benzinga Blockchain Simplified

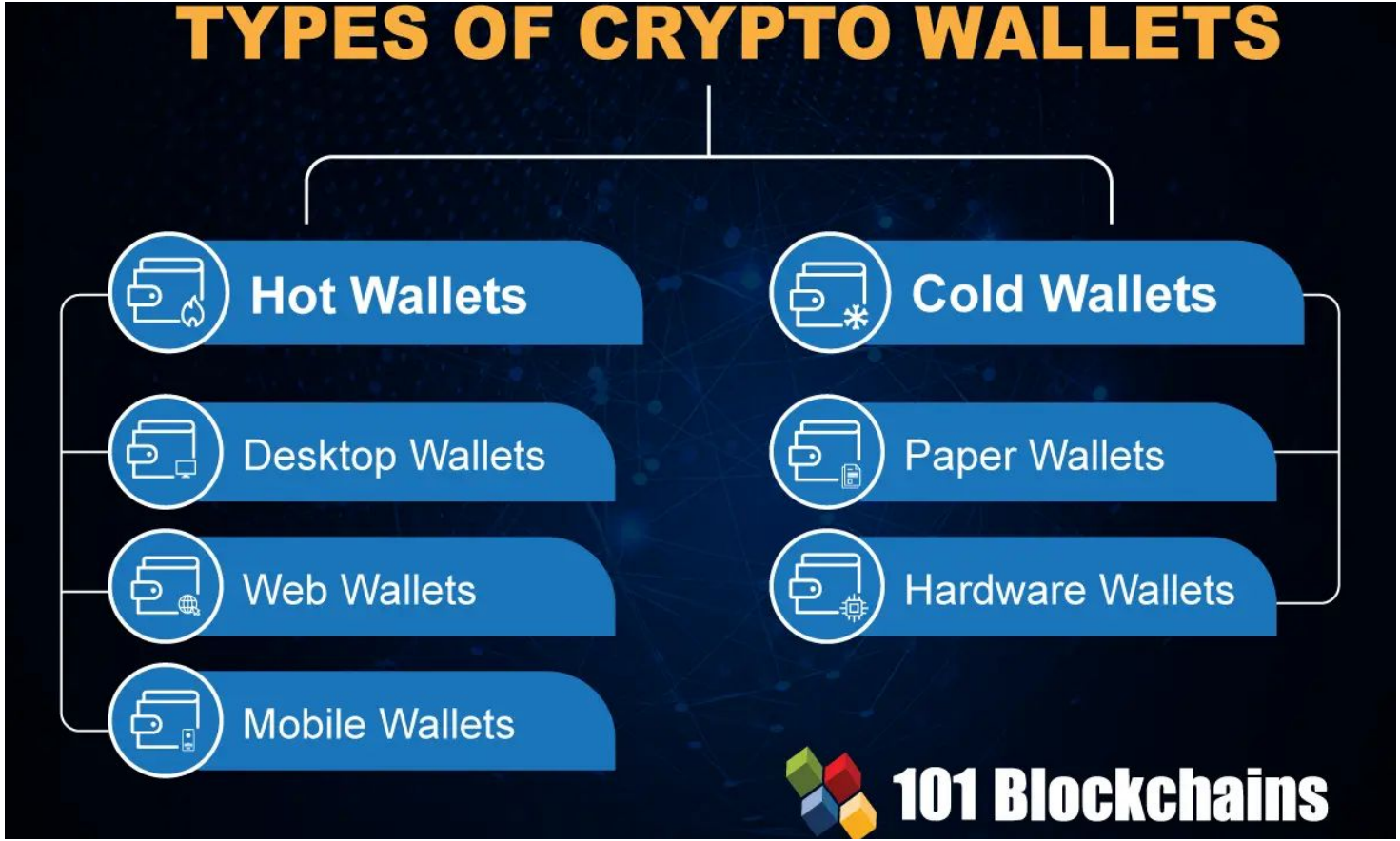
Cryptocurrency wallets: Hot and cold wallets

Why are crypto wallets important?

- Normal wallet - holds actual cash,
- Crypto wallets
  - **don’t store your crypto** instead store **private keys**
    - used to access live holdings on the blockchain
    - prove the ownership of your digital money
    - Allows to perform transactions.
    - Losing private keys ⇒ losing access to your money.
  - That’s why it’s i**mportant to keep the hardware wallet safe, or use a trusted wallet provider like Coinbase.**

Courtesy : Coinbase

Cryptocurrency wallets: Hot and cold wallets



Courtesy : 101 Blockchains

Cryptocurrency wallets: Hot and cold wallets

HOT Wallets - Online Wallets

- also known as a **web wallet,**
- allows you **access to your cryptos via the Internet.**
- The online **wallet provider stores your crypto's private key on their server.**
- The **online wallet service website**
  - **send you the crypto code**,
  - will save your keys and
  - will give you the ability to access your keys.
- Advantages
  - **Enable fast transactions**.
  - May be **able to manage multiple cryptocurrencies.**
  - Conveniently **use on the go and for active trading**.
- Disadvantages:
  - **Risk of online security** such as hacks and scams.
  - **Risk of personal protection** such as computer viruses.
  - A **third-party is storing your cryptos**, not you.

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

HOT Wallets - Mobile Wallets

- **available on cell phone through an app**.
- Just **like Apple Pay / Google Pay / PayTM**, you can use mobile wallets when shopping in physical stores as cryptocurrencies become more acceptable.
- Online wallets offer mobile versions as well.
- Advantages
  - Can be **safer than online wallets.**
  - Conveniently **use on the go.**
  - Offer **additional features such as QR code scanning.**
- Disadvantages:
  - **Risk of losing your crypto assets** if your phone is lost or damaged.
  - **Risk of mobile viruses and malware**.

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

HOT Wallets - Desktop Wallet

- Another choice that can be **safer than online wallets**.
- *One can download your desktop wallet and install it on your computer*.
- **Are safe if the computer is not**, or even better, has never been **connected to the Internet.**
- If a **desktop computer has never been connected to the Internet**, ⇒ a **cold wallet.**
- Advantages of desktop wallets include:
  - A **convenient choice** for those who trade cryptos from their computers.
  - **Private keys are not stored on a third-party server**.
  - **If the computer is not connected to the Internet, it can be extremely safe.**
- Disadvantages of desktop wallets include:
  - **Harder to use your crypto-assets on the go.**
  - **If connected to the Internet, it turns into a less secure hot wallet.**
  - If **you don't backup your computer and it dies, you lose your cryptos**.

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

COLD Wallets - Hardware Wallets

- Arguably be one of the **safest types of cryptocurrency wallets** out there.
- They **store your private keys on a device like a USB drive**.
- You are **still able to make online transactions.**
- **As they are offline most of the time, ⇒ a cold wallet.**
- Advantages of hardware wallets include:
  - One of the **safest crypto wallet options.**
  - **Great for storing large amounts of cryptocurrencies** that you don't want to use on a day-to-day basis.
- Disadvantages of hardware wallets include:
  - **Most expensive type of wallet**.
  - **Not as user-friendly** especially for beginners, but an absolute must for large crypto amounts.

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

COLD Wallets - Paper Wallets

- A **super cold crypto wallet.**
- To use, one **need to print out your private and public keys**.
- **Send funds by transferring the money to wallet's public address**
- **Withdraw or send your currencies by entering your private keys** / **Scan the QR code** on the paper wallet.
- Advantages of paper wallets include:
  - Essentially **hacker-proof**.
  - **Not stored on a computer or mobile**.
  - **Not stored on a third-party server.**
- Disadvantages of paper wallets include:
  - **Not user-friendly** for none-geeks.
  - **Harder to use** for day-to-day transactions.
  - They **can catch fire**.

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

	Hot wallet	Cold wallet
Price	These are usually free, and some pay interest on stored crypto.	These require the purchase of an external device, around $50 to $250.
Better for	Hot wallets are convenient to access and use for trading.	Cold wallets are better suited for long-term storage.
Maximum number of cryptos	Hot wallets can store anywhere from one to tens of thousands of cryptocurrencies.	Cold wallets store anywhere from 1,000 to tens of thousands.
Cybersecurity	Average. Because they are connected to the internet, they could potentially be vulnerable to hacking.	Excellent. They can't be accessed online, but they require security measures to keep them from getting damaged, lost or stolen.
Loss protection	Good. Most have recovery and backup options and can be accessed from multiple devices.	Average. Most have recovery and backup options for a lost password, but not for a lost device.
Ease of transfer to exchanges	Excellent. Hot wallets are easily accessible as the wallet is already internet-connected.	Average. Cold wallets require an extra step to connect online through USB, Wi-Fi or QR code.

Courtesy : NerdWallet

Cryptocurrency wallets: Hot and cold wallets

SUMMARY OF CRYPTOCURRENCY WALLETS

	SOFTWARE	ONLINE	HARDWARE	PAPER
PROS	User-controlled Security For POS coins, allows minting	High convenience, Accessible from any browser without needing to download the Blockchain	Protects user's private keys, which are stored on the device Can be recovered with PIN and seed	Extremely secure. Can't be hacked using digital means Great for long term storage
CONS	Must download entire Blockchain for each type of coin/token	Susceptible to key logging hacks Can't stake POS coins Unknown level of security	Doesn't support all coins/tokens Can't stake POS coins	Inconvenient to use for transactions
EXAMPLES	ELECTRUM, ARMORY	BLOCKCHAIN, MyEtherWallet	Ledger, TREZOR	

INVEST DIVA

Courtesy : Coinbase, Benzinga

Cryptocurrency wallets: Hot and cold wallets

3 Common cryptocurrency wallets

TYPES OF STORAGE	 Hot Wallet	 Cold Wallet	 Custodial Wallet
HOW IT WORKS	Web-based. It is always connected to the internet and crypto network.	Offline. It is not connected to the crypto network or internet.	A third party stores your crypto for you.
WHERE IS THE PRIVATE KEY STORED	Online	Offline	Could be either online or offline.
BENEFITS	Convenience, ease of use.	Highest level of security.	Simplest option, most convenient.
DISADVANTAGES	Vulnerable to online attacks.	Cost of device, inconvenience for day-to-day transactions.	You need to trust the third party.

Courtesy : DBS Treasures

Cryptocurrency wallets: Custodial Vs Non-Custodial Wallets

Custodial Wallets vs Non-Custodial Wallets

Custodial Wallet	Non-Custodial Wallet
Custodian or Third party has control over funds	Users have control of their funds
Not very secure as keys are with a third party	Extremely secure as users have their private keys
Accounts can be restored in case of lost keys	Funds cannot be recovered in case of lost keys
Transaction fees are comparatively lesser	Users bear the complete transaction fees
Slower withdrawals due to KYC/AML checks	Withdrawals are comparatively faster

Courtesy : Blockchain Simplified

Cryptocurrency wallets: Custodial Vs Non-Custodial Wallets

Courtesy : Blockchain Simplified

Cryptocurrency wallets: Custodial Vs Non-Custodial Wallets

Courtesy : Blockchain Simplified

Cryptocurrency wallets: Hardware Vs Software wallets

	SafePal Hardware wallet	SafePal Software Wallet
Private Key Storage Location	Financial grade EAL5 Chip+ secure element	Users' Cellphone
Wallet Type	Decentralized wallet	Decentralized wallet
Access to internet	No	Yes
Management Tool	SafePal APP	SafePal APP
Import method	Mnemonic phrase	Private Key Mnemonic Phrase Keystore Observation Mode
Passphrase	Supported	Supported
Assets	All of the SafePal supported assets (xx chains and 30,000+ tokens)	All of the SafePal supported assets (xx chains and 30,000+ tokens)

Courtesy : SafePal

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Classification of Wallets based on dependency of the keys

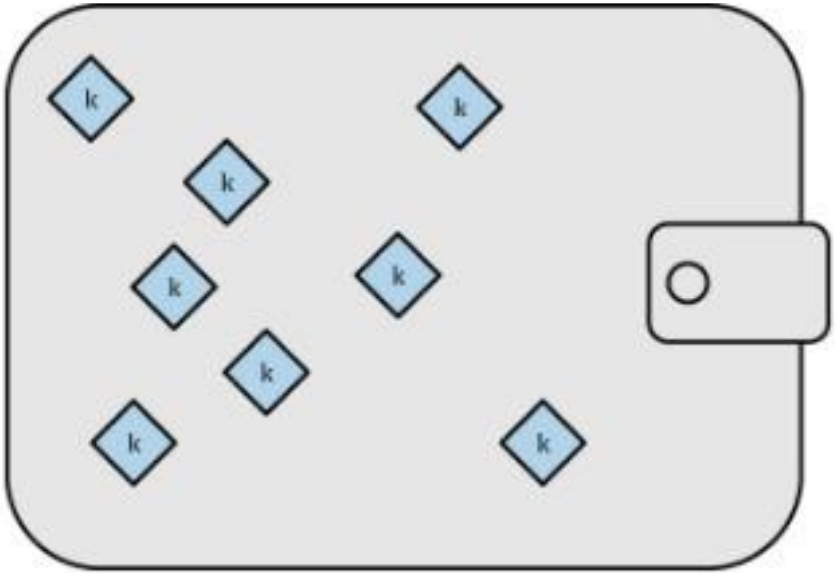
- **Non-deterministic wallet,**
  - each key is independently generated from a random number.
  - also known as a **JBOK "Just a Bunch Of Keys."**
- **Deterministic wallet**,
  - **All the keys are derived from a single master key ⇒ Seed.**
  - **All the keys** in this wallet **are related to each other and can be generated again if one has the original seed.**
  - The **most commonly used derivation method** uses a tree-like structure and is known as a **Hierarchical deterministic or HD wallet.**

Courtesy : Cointelegraph

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Disadvantages of Nondeterministic (Random) Wallets

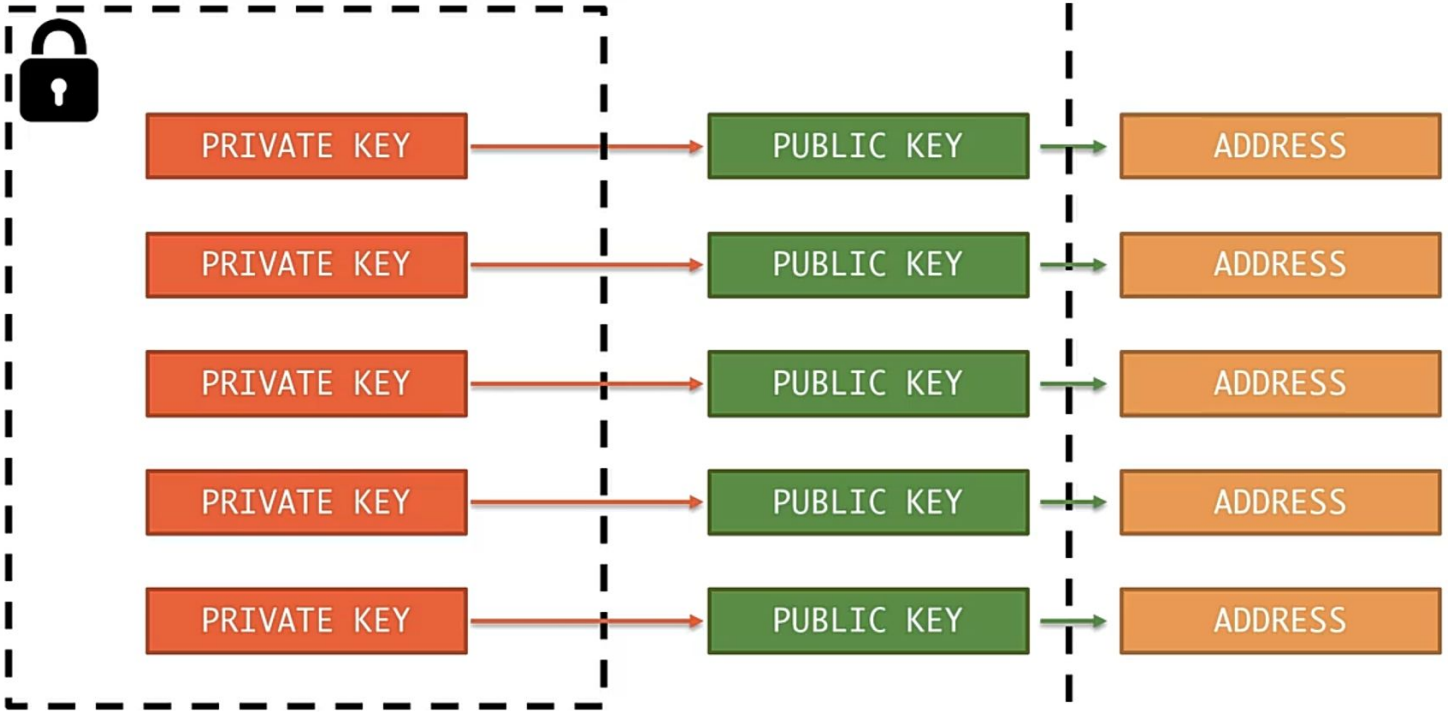
- Random keys generated needs to be backed up frequently.
- Address reuse reduces privacy by associating multiple transactions and addresses with each other.



Courtesy : Cointelegraph

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Non-Deterministic Wallets



Courtesy : Super Data Science

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Deterministic (Seeded) Wallets

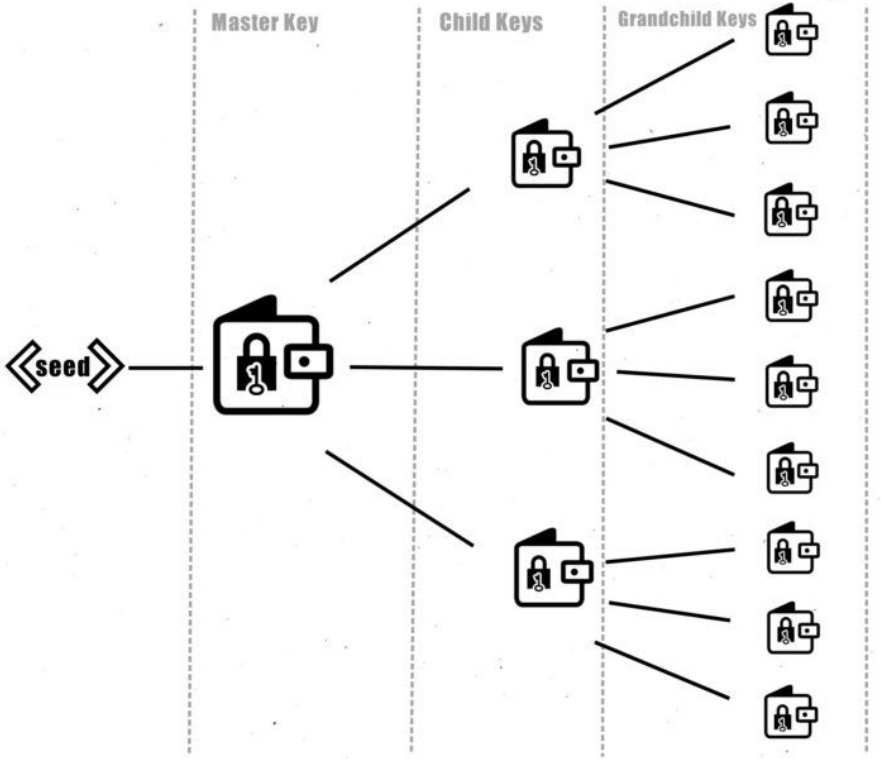
- contain **private keys that are all derived from a seed**, (one-way hash)
- Seed is a **randomly generated number**
  - combined with other data, an index number/ “chain code” to derive the private keys.
  - the seed is sufficient
    - to **recover all the derived keys,**
    - ensures **a single backup at creation time is sufficient.**
- wallet export / import, **allowing for easy migration of all the user’s keys between different wallet implementations.**

Courtesy : Cointelegraph

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Hierarchical Deterministic Wallets (HD Wallets)

- Most advanced form of deterministic wallets
- defined by the **BIP-32** standard.
- contain keys **derived in a tree structure**, to an **infinite depth**
- Tree structure can be used to **express additional organizational meaning**,
- Eg: Branches of keys can also be used in corporate settings, allocating different branches to departments, subsidiaries, specific functions, or accounting categories.



Courtesy : Coingossip

Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Advantages of HD Wallets.

1. **No need to backup all your keys**, whenever you make transactions, **just backup the Seed praise securely.**
2. **Privacy is well guarded** using the hierarchical structure mechanism.
3. **Store multiple unique currencies within the same HD wallet**
4. **n-Number of public addresses can be generated to prevent re-use of addresses**.
5. **Backup of a private key from the hierarchical tree,** still your other addresses will remain safe.
6. **Move millions of dollars across borders without using a hardware wallet or mobile wallet app.**
7. **Users can create a sequence of public keys without having access to the corresponding private keys.** Thus **HD wallets to be used on an insecure server**
8. The **public keys do not need to be preloaded or derived in advance,**

Courtesy : Coingossip

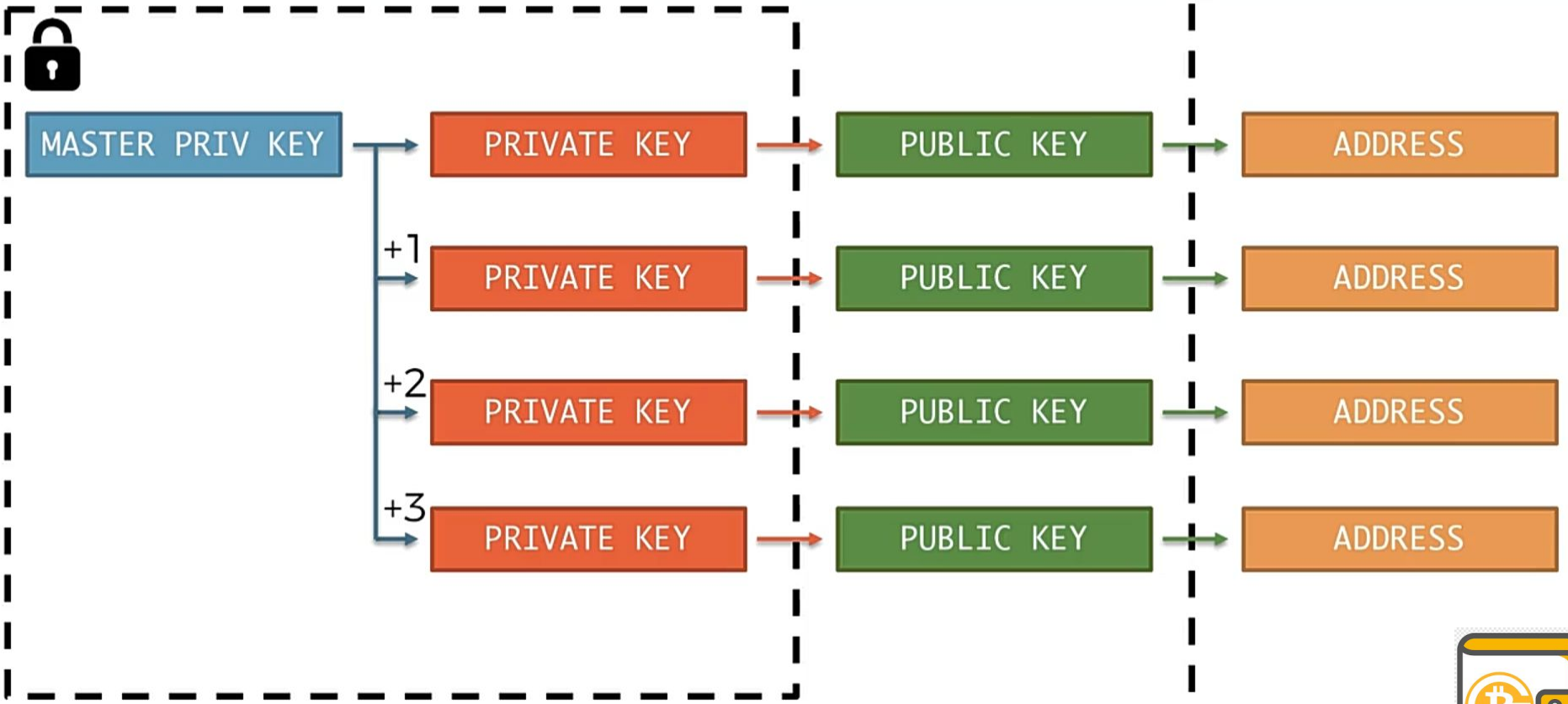
Cryptocurrency wallets: Deterministic Vs Non-deterministic wallets

Disadvantages of HD wallets.

1. **Confuse new users**, as your **receiving address changes every time.**
2. If you chose **hard to memorizable seed praises then, it is difficult to backup all your key pairs** when the wallet is stolen or lost. **Chose memorizable key praise.**
3. you can **securely hand out child keys with no risk to the parent key,** and you **can hand out master public keys with no risk to the master private key**, you **cannot do both at the same time**.

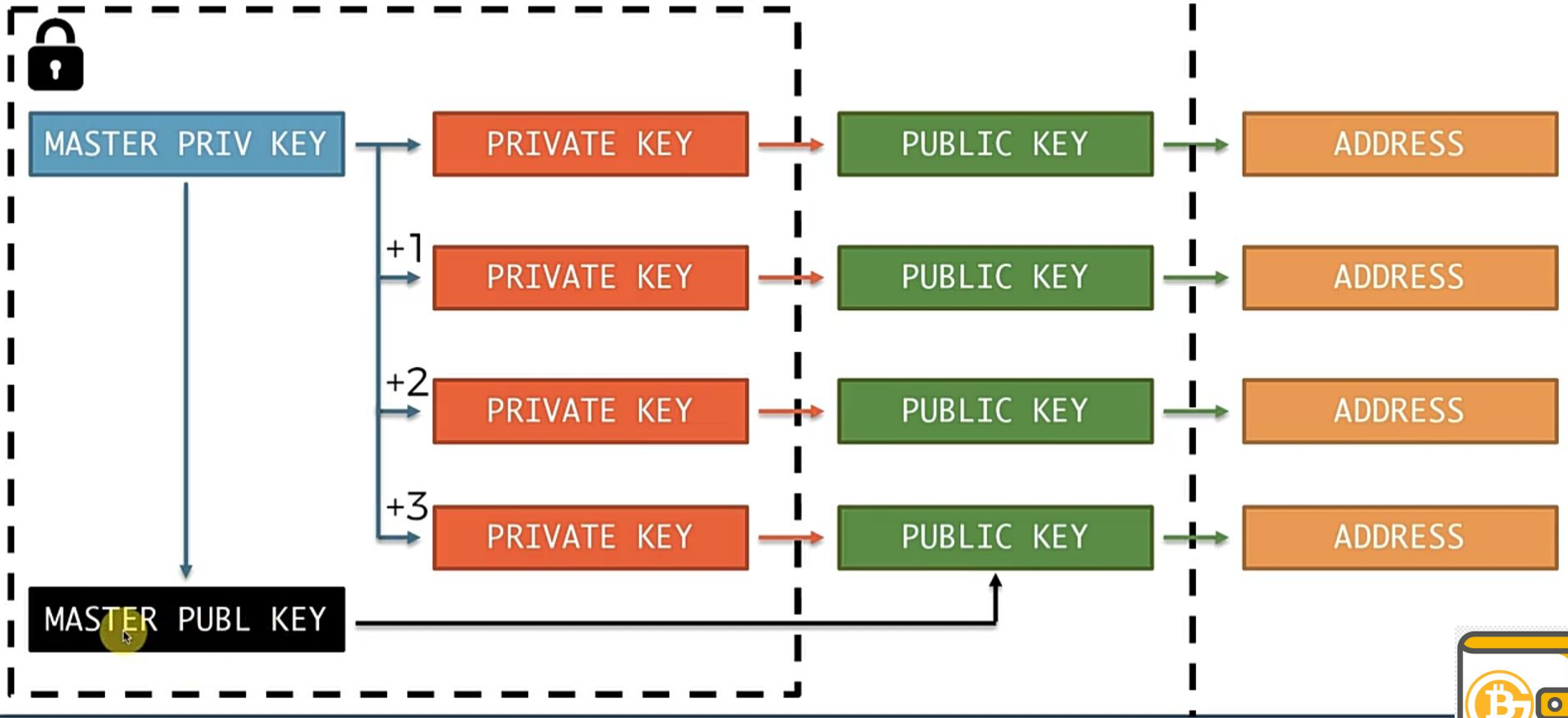
Courtesy : Coingossip

Hierarchical Deterministic (HD) Wallets



Courtesy : Super Data Science

Hierarchical Deterministic (HD) Wallets



Hierarchical Deterministic (HD) Wallets

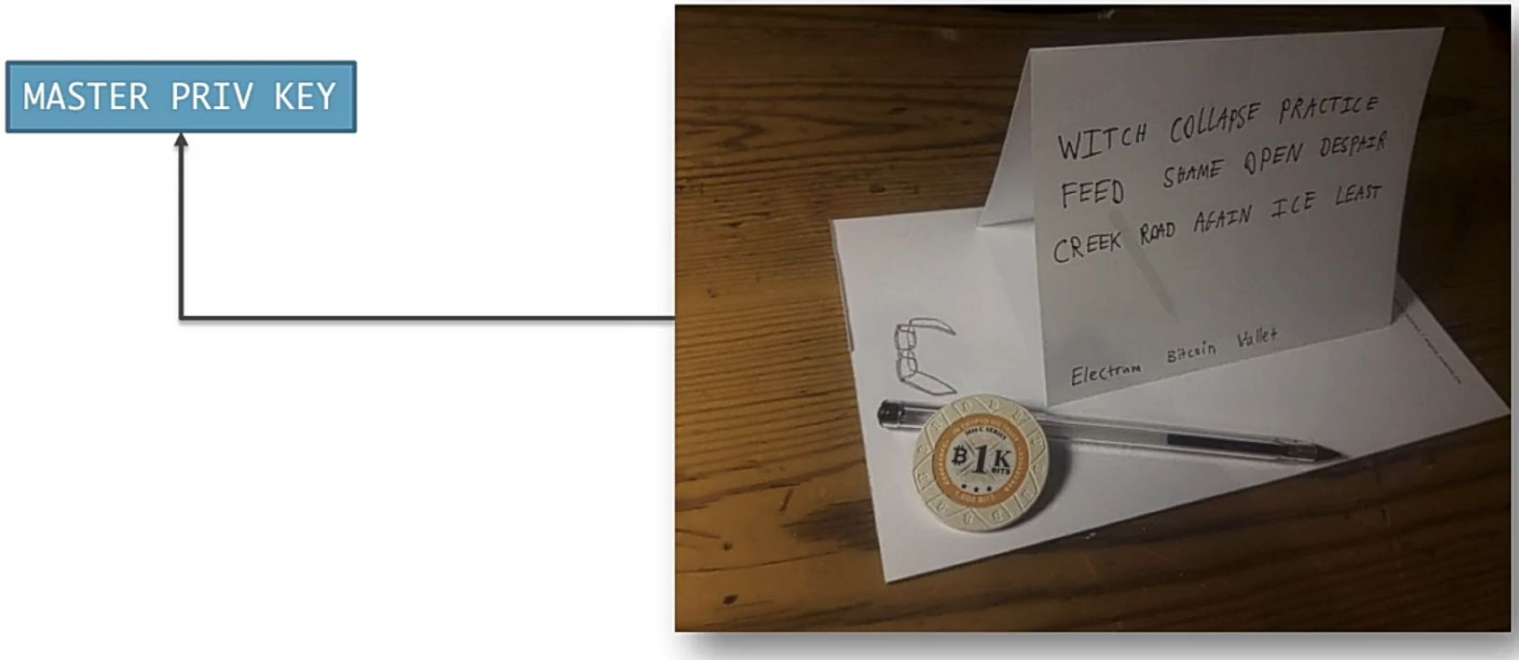


Image source: https://en.bitcoin.it/wiki/

Courtesy : Super Data Science

Cryptocurrency wallets:

Wallet Best Practices

- certain common industry standards have emerged that **make bitcoin wallets broadly interoperable, easy to use, secure, and flexible.**
- These common standards are:
  - **Mnemonic code words**, based on **BIP-39**
  - **HD wallets**, based on **BIP-32**
  - **Multipurpose HD wallet structure**, based on **BIP-43**
  - **Multicurrency and multiaccount wallets**, based on **BIP-44**
- Eg : Breadwallet, Copay, Multibit HD, and Mycelium (software wallets)
- Eg : Hardware : Keepkey, Ledger, and Trezor.

Cryptocurrency Usage

Advantages of Cryptocurrency

1. Inflation Protection (Bitcoin having an hard cap - $21 million)
2. Transactional Speed
3. Cost Effective Transactions
4. Decentralization
5. Diversity
6. Accessibility
7. Safe And Secure
8. Transparent
9. Private
10. Currency Exchanges Are Done Effortlessly

Courtesy : Forbes.com

Cryptocurrency Usage

Disadvantages of Cryptocurrency

1. **Cryptocurrency claims to be an anonymous form of transaction**, but they are **actually pseudonymous** which means they leave a digital trail that the Federal Bureau of Investigation can decode.
2. constant risk of a **51% attack**
3. The majority of blockchains work on the proof-of-work consensus mechanism, which requires **high computational power.**
4. The **lack of key policies related to transactions** serves as a major drawback of cryptocurrencies.
    - **No refund or cancellation policy** can be considered the default stance for transactions wrongly made across crypto wallets and each crypto stock exchange or app has its own rules.

Courtesy : Forbes.com

Cryptocurrency Usage

Are Cryptocurrencies Legal In India?

- are **not regulated or issued by any central authority in India.**
- There are **no guidelines laid down for sorting disagreements while dealing with cryptocurrency**.
- Do trade in crypto, **do it at your own risk**.
- **Till 2022, cryptocurrency was unregulated in the country.**
- This changed after the **government set forth a 30% and 1% tax on profits from cryptocurrencies and tax deducted at source** respectively in the **Union Budget of 2022.** This event marked the **Indian government's official regulation of cryptocurrency in the country.**
- While many supported the decision as it marks the very start of the road to getting cryptocurrency recognition, the **Government of India still has to issue an official note for cryptocurrencies to be considered legal in India.**

Courtesy : Forbes.com

Cryptocurrency Usage

Tax on Cryptocurrency in India

- **most confusing investment aspects** in India.
- In the recent **Union Budget 2022, a tax regime for digital or virtual assets** that include cryptocurrency has been introduced.

1. Crypto investors are required to **keep a well-calculated record of losses and gains as a part of their income.**
2. **On the earnings from the transfer of virtual or digital assets,** a **30% tax will be charged.** The tax includes cryptocurrencies, NFTs, etc.
3. **Cost of acquisition along with no deduction will be permitted** while reporting gains from the transfer of virtual or digital assets.
4. A **tax of 1% on tax deducted at source (TDS) on the buyer's payment if it crosses the threshold limit**.
5. If someone **receives cryptocurrency as a gift or it is transferred then it is subjected to tax at the beneficiary's end.**
6. If **investors face any loss from the virtual or digital asset investment, it cannot be recovered against other income.**

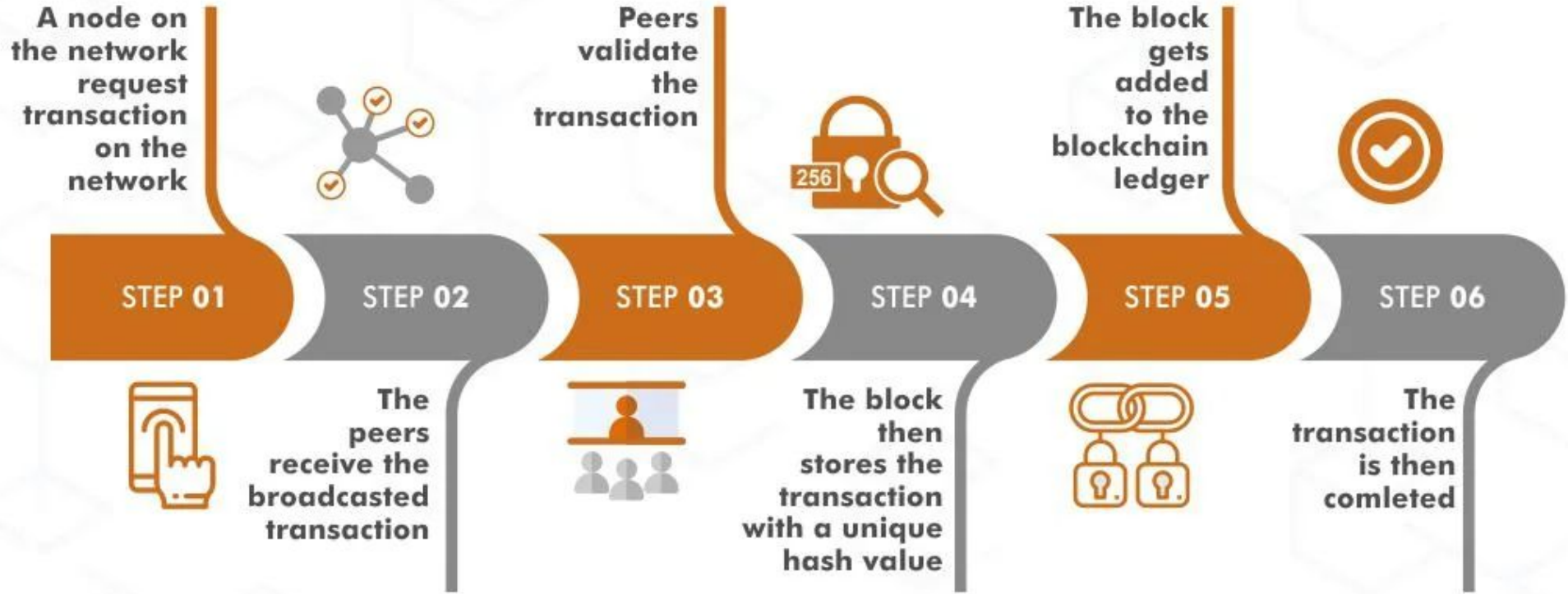
Courtesy : Forbes.com

Transactions in Blockchain

- A transaction is a **transfer of value on the blockchain.**
- A transaction is **when one person gives a designated amount of cryptocurrency they own to another person.**
- To perform transactions on the blockchain, you need a crypto wallet.
- **Each wallet is protected by a special cryptographic method** that uses a **unique pair of distinct but connected keys: a private and a public key.**
  - A **public key / blockchain address**, is a **series of letters and numbers that a user must share in order to receive funds.**
  - **Private key** must be **kept secret,** much like your bank card pin number, as it **authorizes the spending of any funds received by the associated public key.**
- **With their wallet, a user** (whoever has the private key) **can authorize or sign transactions** and thereby transfer value to a new owner.
- The transaction is then broadcast to the network to be included in the blockchain.

Courtesy : Ledger.com

Transactions in Blockchain - Life Cycle



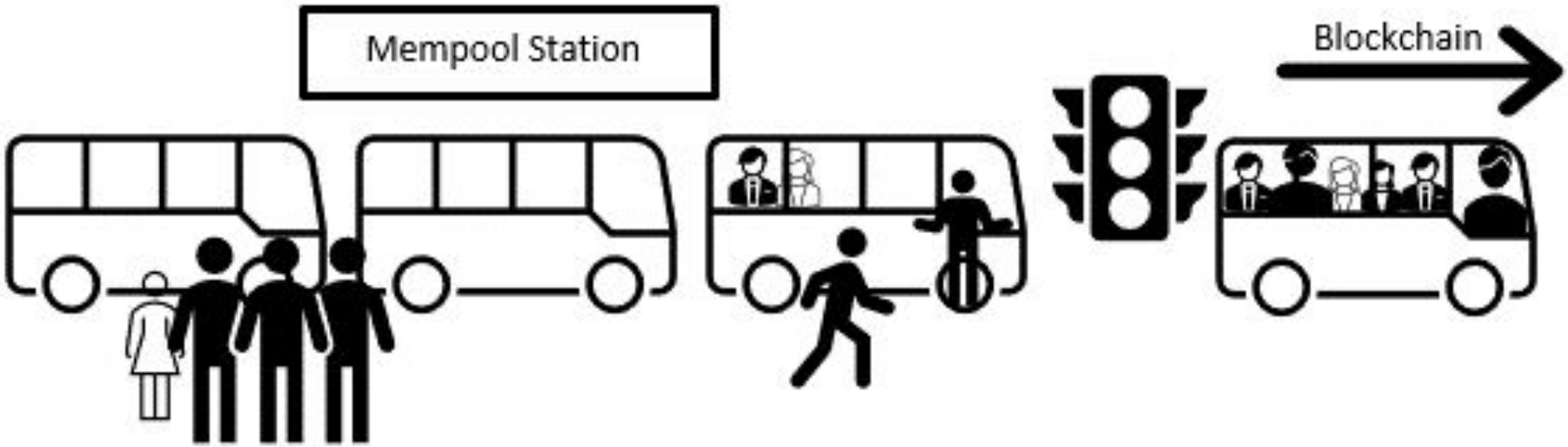
Courtesy : CBCAmerica

Transactions in Blockchain - Life Cycle

1. Someone requests a transaction. The transaction could involve cryptocurrency, contracts, records, or other information.
2. **Transaction is broadcast to all P2P** participation computers in the specific blockchain network. These are called **Nodes**. All transactions are published to the **Mempool** or memory pool, where they are considered 'pending'. **Gas fees** are paid by users as part of the transaction to compensate for the computing energy required to process and validate transactions on the blockchain.
3. **Miners** verify the transaction. Every computer in the network checks the transaction against some validation rules that are set by the creators of the specific blockchain network.
4. **Validated transactions** are stored into a block and are sealed with a lock referred to as the **Hash**.
5. **New block is added to the existing Blockchain**. This block becomes part of the blockchain when other computers in the network validate if the lock on the block is correct.
6. The transaction is complete. Now the transaction is part of the blockchain and cannot be altered in any way.

Courtesy : Ledger.com

Transactions in Blockchain - The Bus Station Analogy

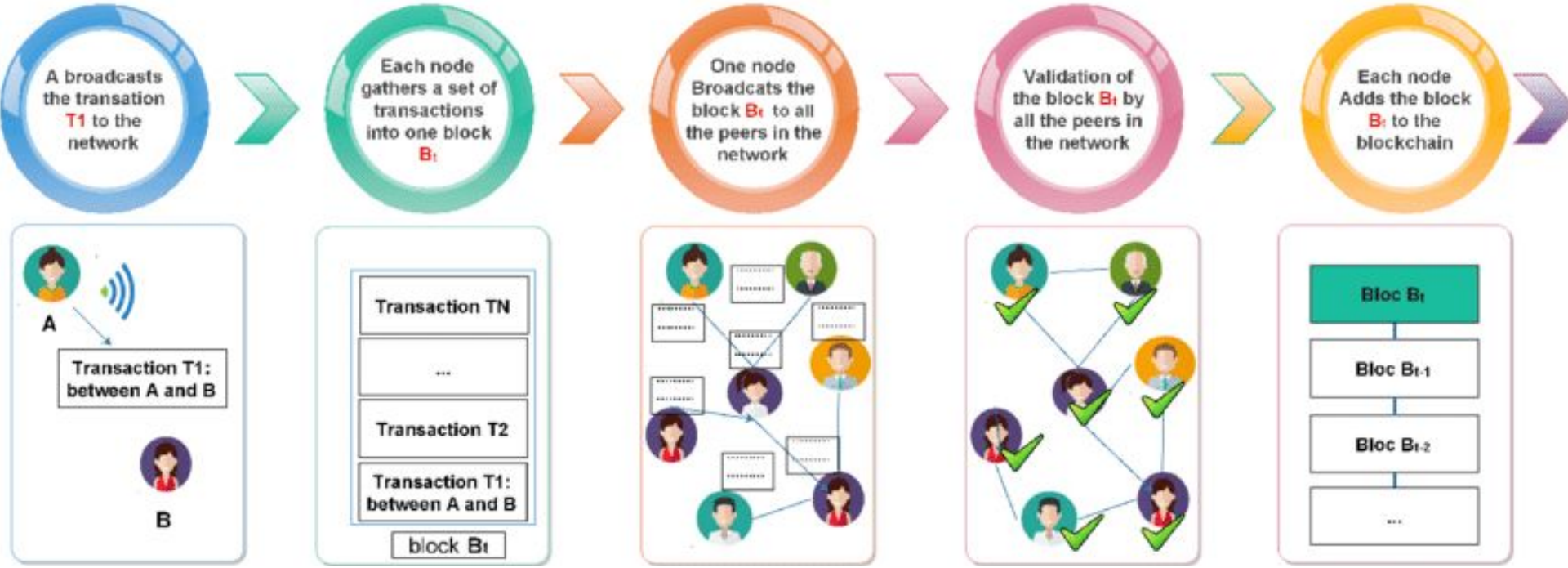


Courtesy : TxStreet

Transactions in Blockchain - Live Demo

Courtesy : TxStreet

Transactions in Blockchain - Example



Courtesy : Research Gate

Transactions in Blockchain - Example

- Alice wants to send two coins to Bob.
- Each transaction has **three main parts**:
  - **The input:** Alice's private coin address, she wants to spend.
  - **The output:** Bob's public key or coin address.
  - **Amounts:** the amount of coins Alice wants to spend.

1. **Alice signs a message with the transaction details using her private key.** The message contains the input, output, and amount to be sent.
2. The **transaction is then broadcast to the network** saying the amount of coins in her account should go down by two. The amount in Bob's account should increase by two.
3. **Each computer in the network will receive the message** and apply the requested transaction to its copy of the ledger, updating the account balances.
4. **Add the transactions into the MemPool.**
5. **Miner** select few transactions from MemPool and tries to **solve Cryptographic Puzzle.**
6. On solving the Puzzle, the **Block is broadcasted to the network for validation**.
7. After adding Block into the Blockchain, **Transactions added in the Block are later removed from MemPool**

Courtesy : Research Gate

Transactions in Blockchain

UTXO - Unspent transaction output

- The fundamental building block of a bitcoin transaction
- Transaction outputs are **indivisible chunks of bitcoin currency,** recorded on the blockchain, and recognized as valid by the entire network.
- Bitcoin full nodes track all available and spendable outputs
- **UTXO set** - The collection of all UTXO
  - set grows as new UTXO is created
  - shrinks when UTXO is consumed.
- Every transaction represents a change (state transition) in the UTXO set.
- Eg:User receiving 1 BTC → wallet detected a UTXO that can be spent by any key in the wallet
- **Users Bitcoin balance = Sum of all UTXO** in the users wallet can detect in the network.
  1. scanning the Blockchain
  2. aggregating the **value of UTXO that wallet can spent using the keys** it stores.

Transactions in Blockchain

UTXO - Unspent transaction output

- Have an arbitrary value denominated as a multiple of satoshis
- 1 BTC can be divided into 8 decimal places of satoshi.
- Can only be consumed in its entirety by a transaction.

Wallet Strategies to satisfy a purchase amount (done by the user wallet automatically)

- Combine several smaller units
- Finding exact change
- Using a single UTXO larger than the transaction value.

Coinbase

- Special type of transaction appears as the 1st transaction in each block.
- Placed / created by the miner as a reward for mining (**Bitcoin Money Supply is created)**
- Does not consume UTXO

Transactions in Blockchain

UTXO - Unspent transaction output

- Every bitcoin transaction creates outputs, which are recorded on the bitcoin ledger.
- **Transaction outputs consist of two parts:**
  1. An **amount of bitcoin**, denominated in satoshis, the smallest bitcoin unit
  2. A **cryptographic puzzle** that determines the conditions required to spend the output
     - **locking script / witness script / scriptPubKey / P2PKH (Pay to Public Key Hash)**

Transaction Serialization

- Process of converting the internal representation of a data structure such that it can be transmitted one byte at a time

Transaction Deserialization / Parsing

- Process of converting byte stream representation of a transaction to internal representation of a data structure

Transactions in Blockchain

Transaction inputs

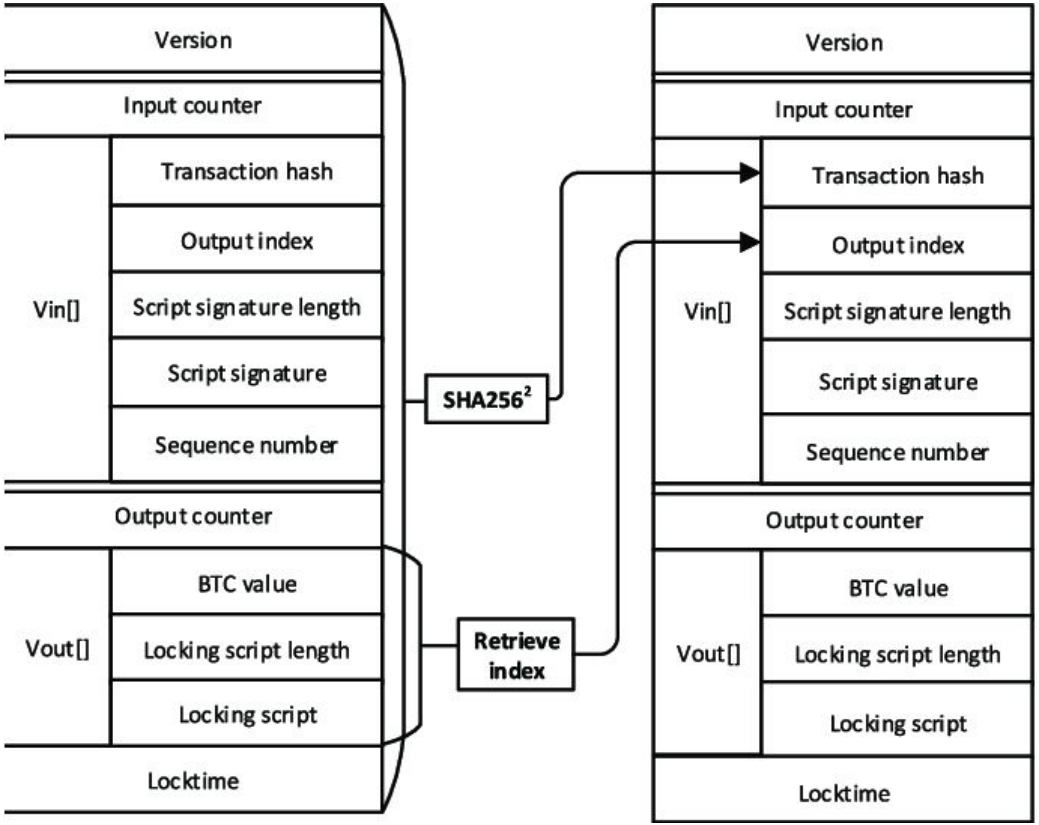
- identify (by reference) which UTXO will be consumed
- provide proof of ownership through an **unlocking script / Digital Signature**

Transaction input contains four elements:

1. A transaction ID, referencing the transaction that contains the UTXO being spent
2. An **output index** (vout), identifying which UTXO from that transaction is referenced (first one is zero)
3. A **scriptSig,** which satisfies the conditions placed on the UTXO, unlocking it for spending
4. A sequence number

Note : Once a transaction is broadcasted, *every validating node needs to retrieve the UTXO reference in the transaction inputs in order to validate the transaction.*

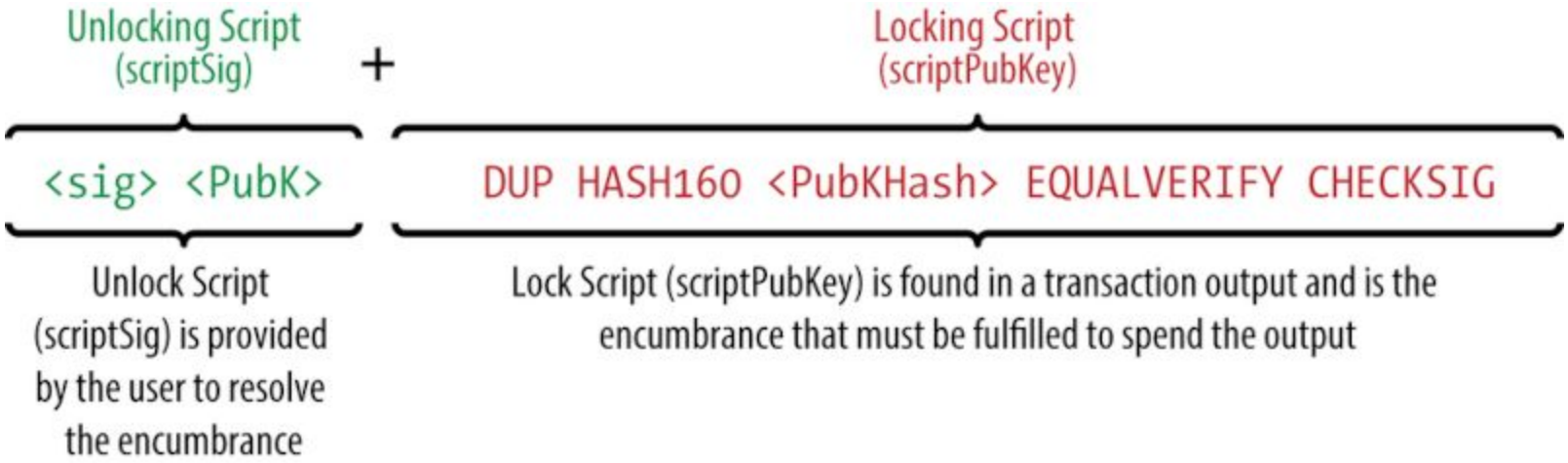
Transactions in Blockchain - Structure



Courtesy : Research Gate
Oreilly

Transactions in Blockchain

Validation - The unlocking script is first copied, then the UTXO that references the input is retrieved, this UTXO consists of a locking script. Both scripts are executed in a sequence. We say the input is valid if the unlocking script satisfies the locking script conditions. Note that a transaction can have multiple inputs, in this case, all inputs are validated independently, this is part of the overall validation of a transaction. Valid transactions satisfying the output conditions are considered 'spent' and removed from the UTXO set



Transactions in Blockchain

Transaction Fees

- Incentives given to the miner for mining blocks
- Disincentive against abuse of the system by imposing a small cost on every transaction
- Encourages processing priority
- ***Calculated*** :
  - **Initially,** based on the siae of the transaction in KB (not on the value of the transaction)
  - **Now**, based on network capacity & transaction volume.
- **MinRelayTxFee** (Bitcoin) : Default : **0.00001 BTC**
- If **TxFee < MinRelayFee**

  ⇒ Transaction is free

  ⇒ Relayed only if there is space in mempool / Dropped
- Transaction can have different levels of Priority based on TxFees
  - High ⇒ user pays high TxFees
  - Medium or Low ⇒ user pays low TxFees

Transactions in Blockchain

Adding Transaction Fees to Transactions

- No field in Fees in the Transaction Structure
- TxFees = Excess amount that remains after all outputs have been deducted from all inputs
  - **TxFees = Sum(Inputs) - Sum(Outputs)**
- Ideal TxFees to ensure that transactions get confirmed and verified
  - **TxFees = size of Transaction * per KB fees**

Scenario - 1 : Alice has 0.2 BTC

- 0.015 BTC ⇒ UTXO to Bob
- 0.001 BTC ⇒ UTXO to Miner (as TxFees)
- 0.184 BTC ⇒ UTXO back to Alice

Scenario - 2 : Eugenia raising funds for Children's Charity (purpose purchase school books)

- collected 50 BTC as thousands of UTXO as TxInputs
- Pay the purchaser as one UTXO
- Pay higher TxFees as there are many small TxInputs so that transaction is processed promptly.

Transaction in a Live Block

Bitcoin Block 800,041

Mined on July 24, 2023 03:17:23 • All Blocks

Unknown

Coinbase Message • ▓,H>d/Foundry USA Pool #dropgold/IRq ▓▓▓▓▓▓▓▓▓

A total of 234.86 BTC ($6,978,185) were sent in the block with the average transaction being 0.0394 BTC ($1,170.67). Unknown earned a total reward of 6.25 BTC $185,703. The reward consisted of a base reward of 6.25 BTC $185,703 with an additional 0.0696 BTC ($2,067.99) reward paid as fees of the 5,967 transactions which were included in the block.

Details

Hash	00000-6bb64	Depth	1
Capacity	191.28%	Size	2,005,719
Distance	13m 21s	Version	0×20800000
BTC	234.8568	Merkle Root	79-6a
Value	$6,978,185	Difficulty	53,911,173,001,054.59
Value Today	$6,858,763	Nonce	1,134,080,607
Average Value	0.0393592782 BTC	Bits	386,218,132
Median Value	0.00000330 BTC	Weight	3,992,856 WU
Input Value	234.93 BTC	Minted	6.25 BTC
Output Value	241.18 BTC	Reward	6.31961394 BTC
Transactions	5,967	Mined on	24 Jul 2023, 15:17:23
Witness Tx's	5,915	Height	800,041
Inputs	6,274	Confirmations	1

Coinbase Txn

Last | First | ↗ Value | ↘ Value | ↗ Fee | ↘ Fee

Coinbase

0	ID: ac16-528a 7/24/2023, 15:17:23	From Block Reward To 2 Outputs	6.31961394 BTC • $187,771 Fee 0 Sats • $0.00
1	ID: 7528-6e68 7/24/2023, 15:16:15	From bc1q-pemf To 2 Outputs	5.83754433 BTC • $173,448 Fee 36.0K Sats • $10.70
2	ID: f2e7-89d2 7/24/2023, 15:17:18	From bc1q-pemf To 3 Outputs	9.05621531 BTC • $269,082 Fee 44.5K Sats • $13.22
3	ID: 13e5-a4fa 7/24/2023, 15:17:04	From bc1q-pemf To 3 Outputs	5.82139949 BTC • $172,968 Fee 44.5K Sats • $13.22
4	ID: 6480-13dd 7/24/2023, 15:17:10	From 12oz-cNEA To 1MU3-m7aM	0.04040926 BTC • $1,200.66 Fee 25.8K Sats • $7.66
5	ID: d69d-48fe 7/24/2023, 15:17:23	From bc1q-n6eg To bc1q-6ctp	0.00826518 BTC • $245.58 Fee 12.9K Sats • $3.83
6	ID: dd90-ae7f 7/24/2023, 15:17:18	From bc1q-2pzk To bc1q-yqaj	0.00630000 BTC • $187.19 Fee 10.0K Sats • $2.97
7	ID: e519-7c53 7/24/2023, 15:16:26	From bc1q-6e3z To 2 Outputs	4.09893700 BTC • $121,789 Fee 12.1K Sats • $3.60

Courtesy : Blockchain.com

Transactions and UTXOs

Mark	->	Me	0.1 BTC
Hadelin	->	Me	0.3 BTC
~~Helen~~	~~->~~	~~Me~~	~~0.6 BTC~~
Susan	->	Me	0.7 BTC

UTXOs

I want to Buy a bicycle for 0.5 BTC

TRANSACTION:

Input:
0.6 BTC from Helen

Output:
0.5 BTC to the bike shop,
0.1 BTC back to myself

UTXO
For the bike shop

UTXO
For me

Transactions and UTXOs

Mark	->	Me	0.1 BTC
~~Hadelin~~	~~>~~	~~Me~~	~~0.3 BTC~~
~~Susan~~	~~>~~	~~Me~~	~~0.7 BTC~~
~~Me~~	~~>~~	~~Me~~	~~0.1 BTC~~

} UTXOs

I want to Buy a 2nd bicycle for 1.1 BTC

TRANSACTION:

Input:
0.3 BTC from Hadelin,
0.7 BTC from Susan,
0.1 BTC from Me

}

Output:
1.1 BTC to the bike shop,

UTXO
For the bike shop

Where do transaction fees come from?

Mark	->	Me	0.1 BTC
Sarah	->	Me	0.1 BTC
~~Hadelin~~	~~->~~	~~Me~~	~~0.4 BTC~~
~~Ebay~~	~~->~~	~~Me~~	~~0.3 BTC~~
~~Hadelin~~	~~->~~	~~Me~~	~~0.3 BTC~~

} UTXOs

I want to Buy a 3rd bicycle for 0.9 BTC and an apple for 0.02 BTC

TRANSACTION:

Input:
- 0.4 BTC from Hadelin,
- 0.3 BTC from Ebay
- 0.3 BTC from Hadelin

Output:
- 0.9 BTC to the bike shop, ← UTXO for the bike shop
- 0.02 BTC to the fruit shop, ← UTXO for the bike shop
- 0.06 BTC to myself ← UTXO for me

Fees: 0.02 BTC ← UTXO for the miner

Courtesy : Super Data Science

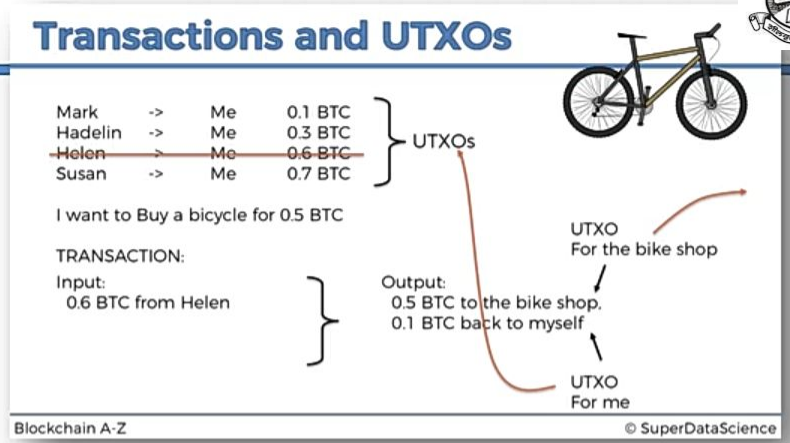
Where do transaction fees come from?

Mark	->	Me	0.1 BTC
Sarah	->	Me	0.1 BTC
Me	->	Me	0.0.6 BTC

} UTXOs

How Wallets Work

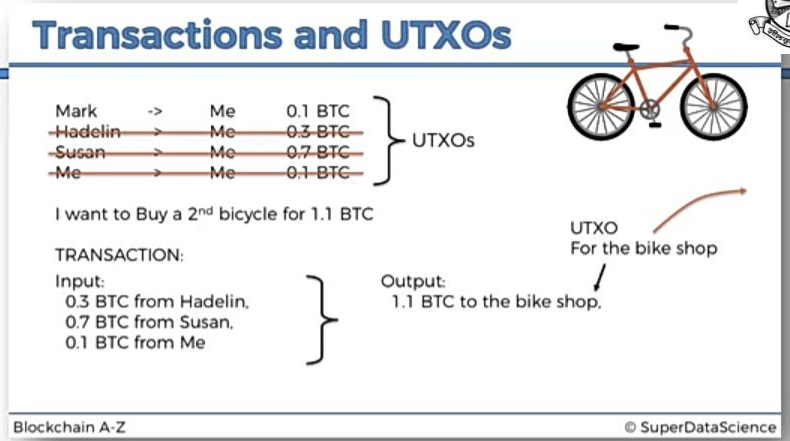
504	Me	->	Bike Shop	0.9 BTC
	Me	->	Fruit Shop	0.02 BTC
	Me	->	Me	0.06 BTC
503	Sarah	->	Me	0.1 BTC
	Hadelin	->	Me	0.4 BTC
	Ebay	->	Me	0.3 BTC
	Hadelin	->	Me	0.3 BTC
502	Me	->	Bike Shop	1.1 BTC
	Me	->	Bike Shop	0.5 BTC
	Me	->	Me	0.1 BTC
501	Mark	->	Me	0.1 BTC
	Hadelin	->	Me	0.3 BTC
	Helen	->	Me	0.6 BTC
	Susan	->	Me	0.7 BTC



Courtesy : Super Data Science

How Wallets Work

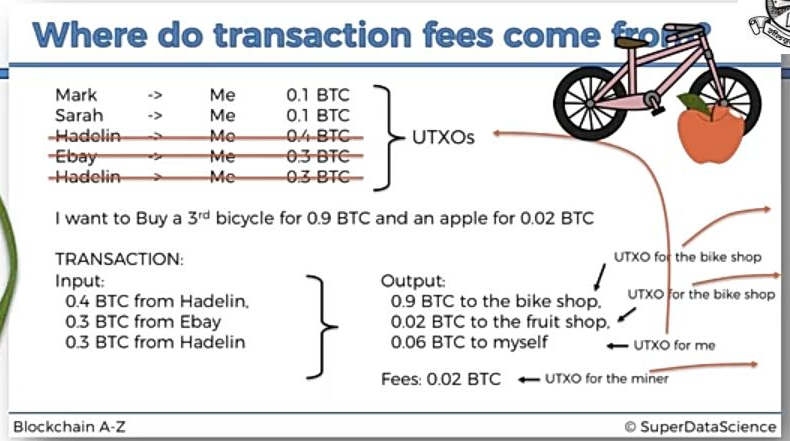
504	Me	->	Bike Shop	0.9 BTC
	Me	->	Fruit Shop	0.02 BTC
	Me	->	Me	0.06 BTC
503	Sarah	->	Me	0.1 BTC
	Hadelin	->	Me	0.4 BTC
	Ebay	->	Me	0.3 BTC
	Hadelin	->	Me	0.3 BTC
502	Me	->	Bike Shop	1.1 BTC
	Me	->	Bike Shop	0.5 BTC
	Me	->	Me	0.1 BTC
501	Mark	->	Me	0.1 BTC
	Hadelin	->	Me	0.3 BTC
	Helen	->	Me	0.6 BTC
	Susan	->	Me	0.7 BTC



Courtesy : Super Data Science

How Wallets Work

504	Me	->	Bike Shop	0.9 BTC
	Me	->	Fruit Shop	0.02 BTC
	Me	->	Me	0.06 BTC
503	Sarah	->	Me	0.1 BTC
	Hadelin	->	Me	0.4 BTC
	Ebay	->	Me	0.3 BTC
	Hadelin	->	Me	0.3 BTC
502	Me	->	Bike Shop	1.1 BTC
	Me	->	Bike Shop	0.5 BTC
	Me	->	Me	0.1 BTC
501	Mark	->	Me	0.1 BTC
	Hadelin	->	Me	0.3 BTC
	Helen	->	Me	0.6 BTC
	Susan	->	Me	0.7 BTC



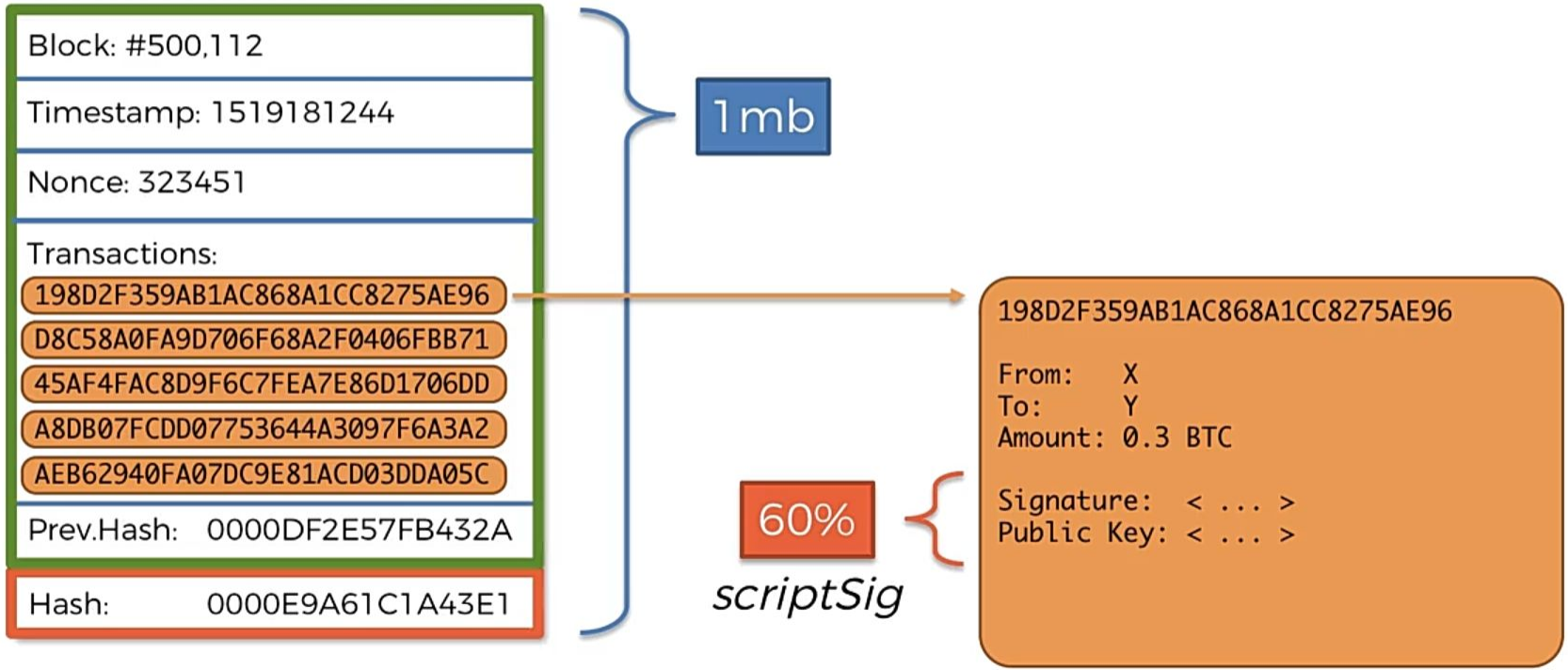
Courtesy : Super Data Science

How Wallets Work

504	Me	->	Bike Shop	0.9 BTC
	Me	->	Fruit Shop	0.02 BTC
	Me	->	Me	0.06 BTC UTXO
503	Sarah	->	Me	0.1 BTC UTXO
	Hadelin	->	Me	0.4 BTC
	Ebay	->	Me	0.3 BTC
	Hadelin	->	Me	0.3 BTC
502	Me	->	Bike Shop	1.1 BTC
	Me	->	Bike Shop	0.5 BTC
	Me	->	Me	0.1 BTC
501	Mark	->	Me	0.1 BTC UTXO
	Hadelin	->	Me	0.3 BTC
	Helen	->	Me	0.6 BTC
	Susan	->	Me	0.7 BTC

Courtesy : Super Data Science

What is Segregated Witness? (SegWit)



Courtesy : Super Data Science

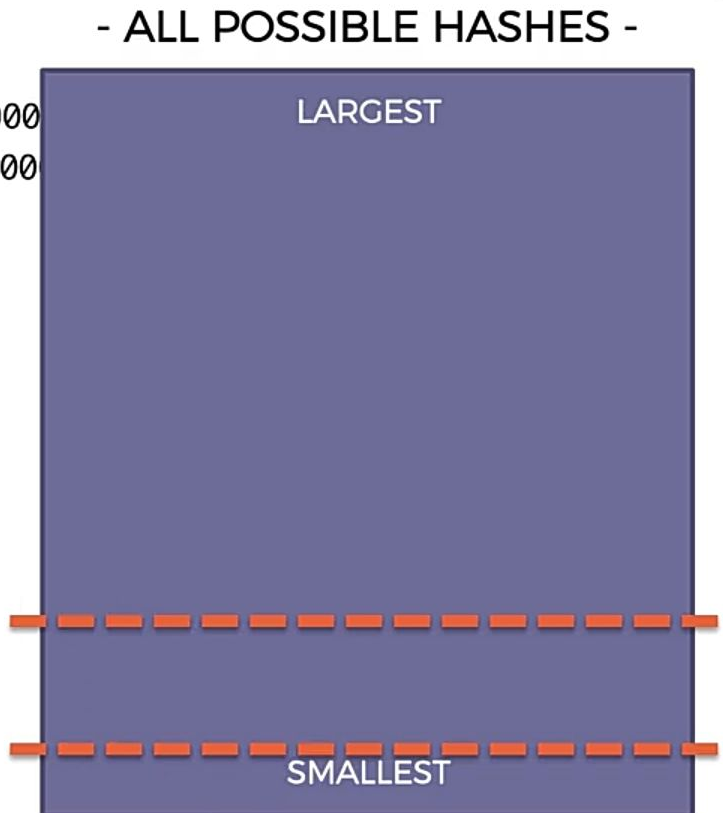
Understanding Mining Difficulty

Difficulty = current target / max target

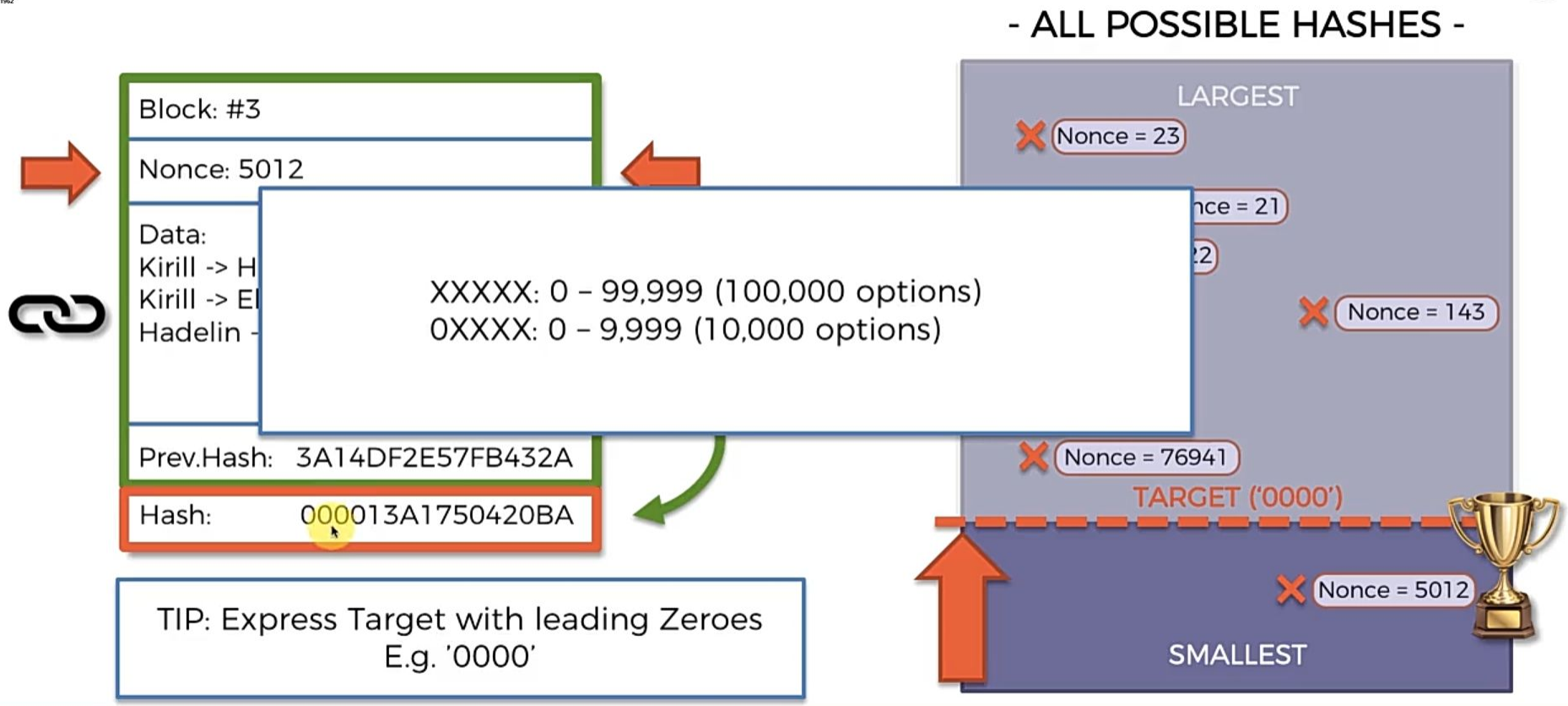
Curr target = `0000000000000000005d97dc0000000000000000000`

Max target = `00000000FFFF0000000000000000000000000000000`

Difficulty is adjusted every 2016 blocks (2 weeks)



Understanding Mining Difficulty



Understanding Mining Difficulty

Difficulty = current target / max target

Curr target = 0000000000000000005d97dc0000000000000000000000000000000000000000

Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

Difficulty is adjusted every 2016 blocks (2 weeks)

Current target = 0000000000000000005d97dc0000000000000000000000000000000000000000

18 zeros

Let's do some estimations:

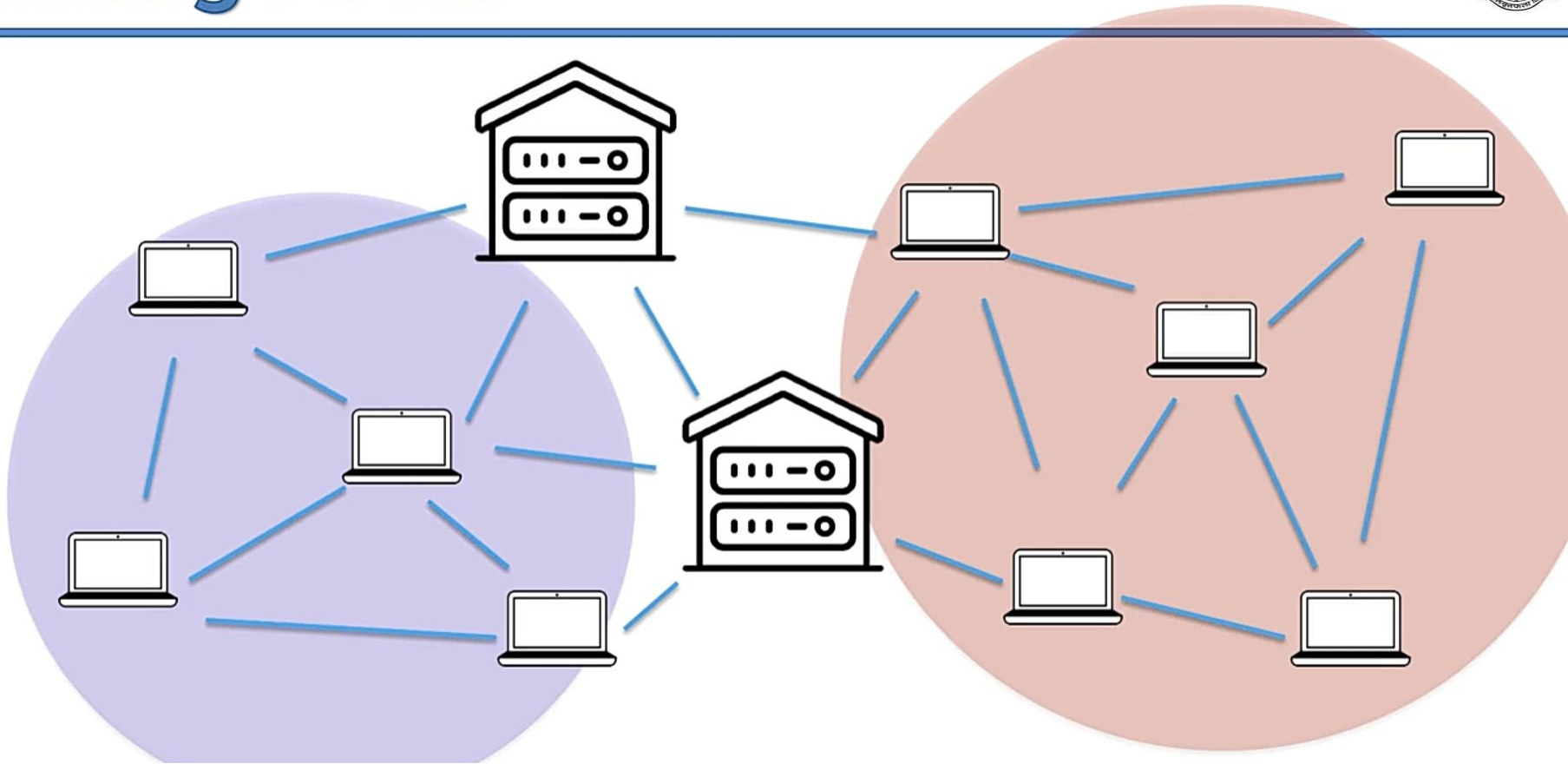
Probability:

Total possible 64-digit hexadecimal numbers: $16 \times 16 \times \ldots \times 16 = 16^{64} \approx 1.1579 \times 10^{77} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

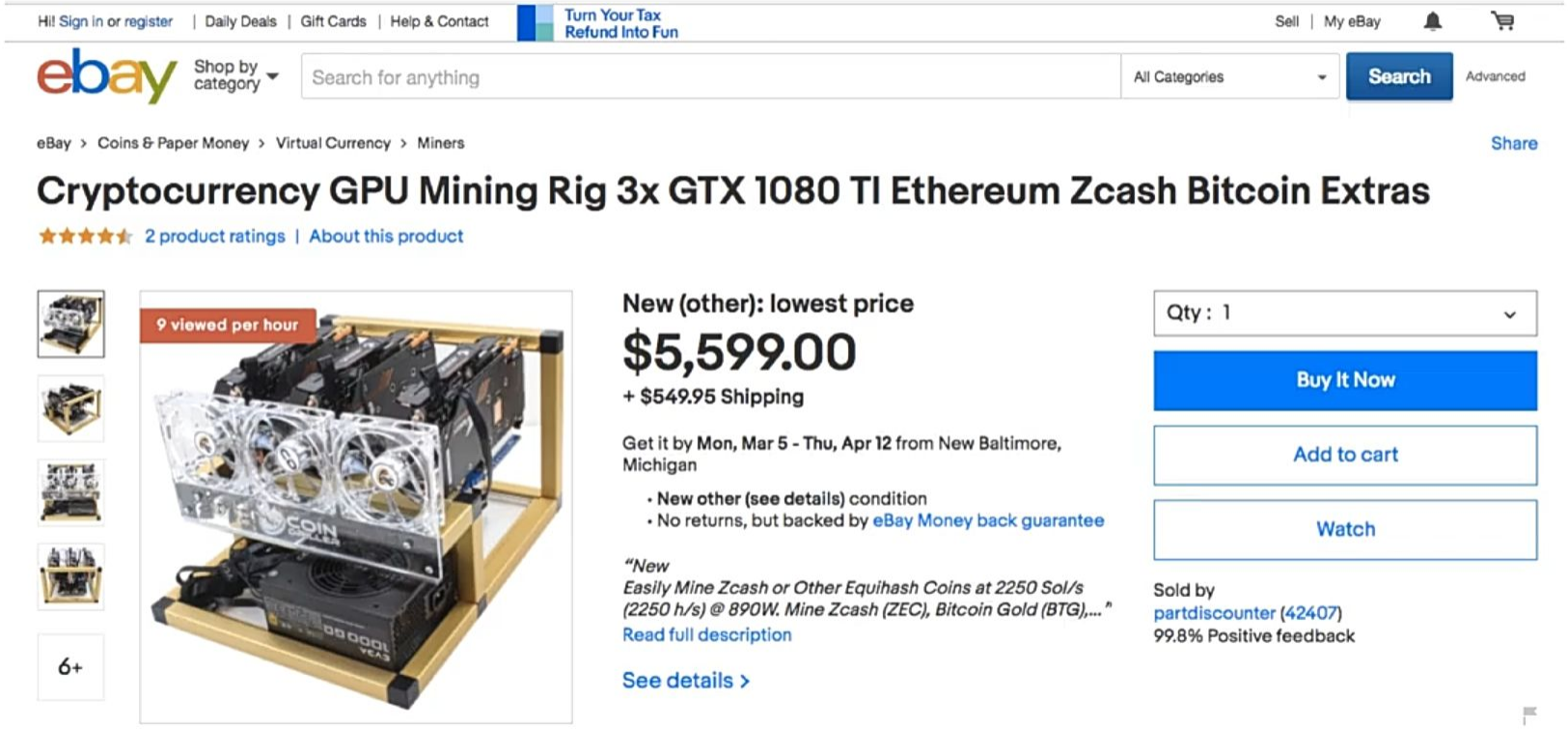
Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Mining Pools



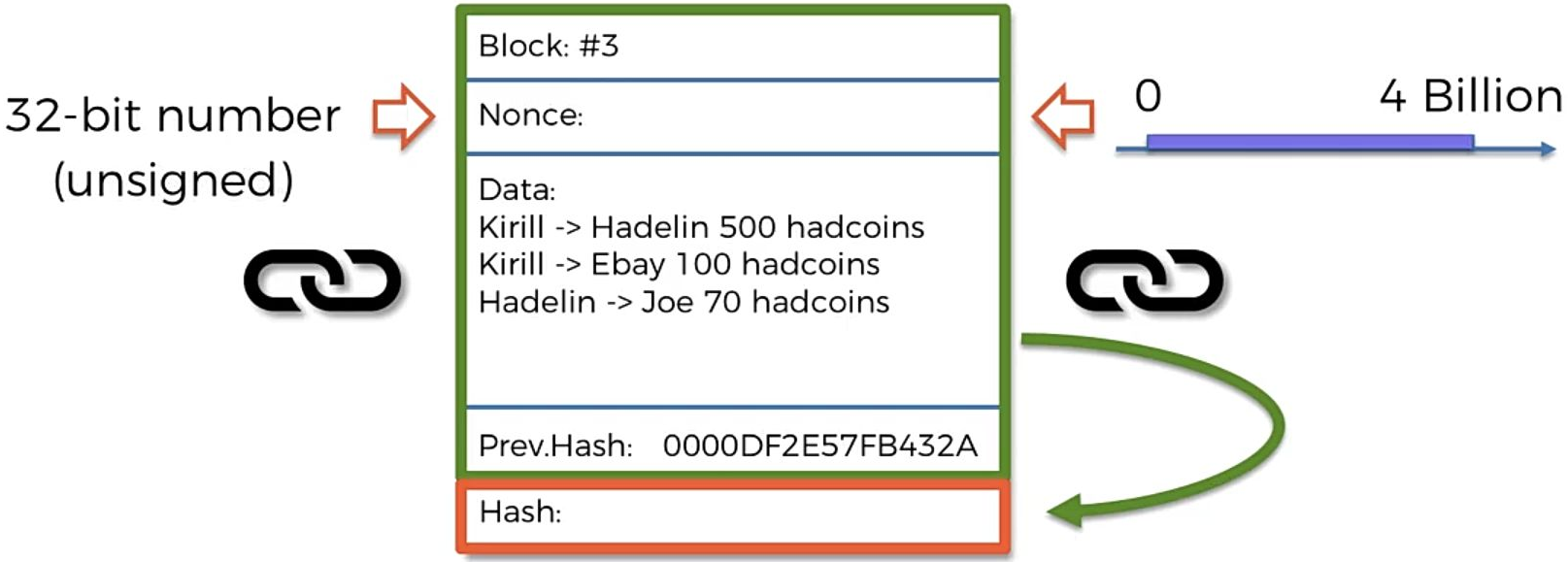
Courtesy : Super Data Science

Mining Pools



Courtesy : Super Data Science

Nonce Range


32-bit number
(unsigned)
Block: #3
Nonce:
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 0000DF2E57FB432A
Hash:
0
4 Billion

Nonce Range

Let's do some estimations:

Difficulty:

Total possible 64-digit hexadecimal numbers: 16 x 16 x …. x 16 = $16^{64} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): 16 x 16 x … x 16 = $16^{64-18} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Nonce:

The Nonce is a 32-bit number, the Max Nonce = $2^{32} = 4{,}294{,}967{,}296 = 4 \times 10^{9}$

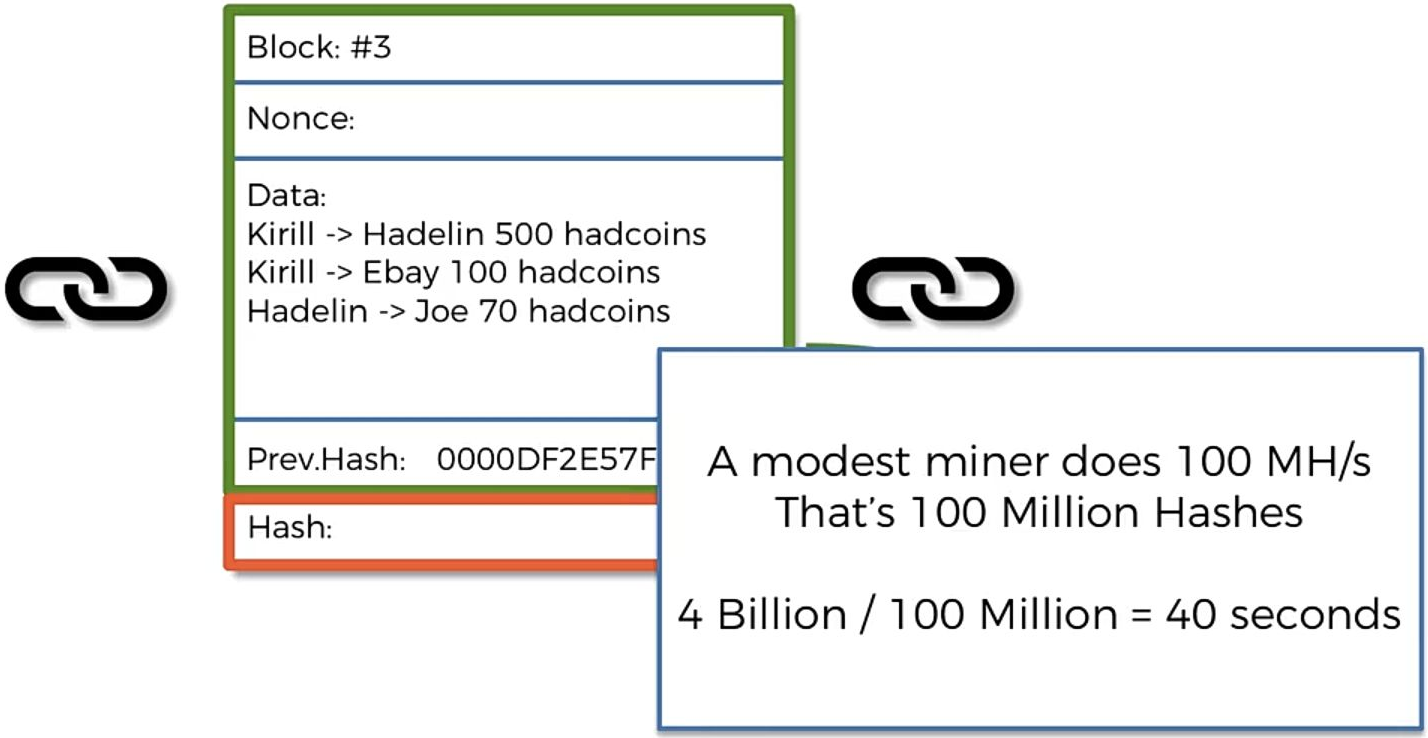
Assuming no collisions, this means 4×10^{9} different hashes

Probability that ONE of them will be valid: $4 \times 10^{9} \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0.0000000001\%$

Conclusion: One Nonce Range is not enough

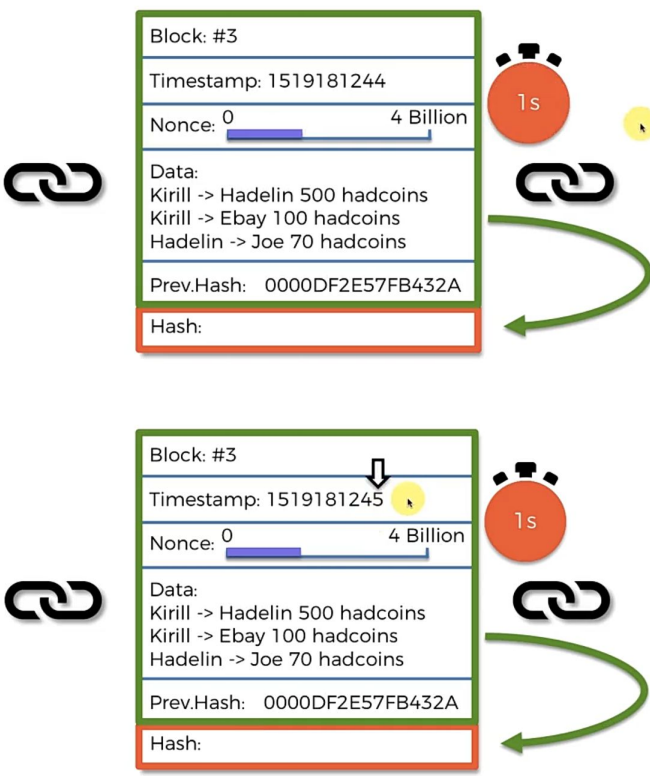
Courtesy : Super Data Science

Nonce Range



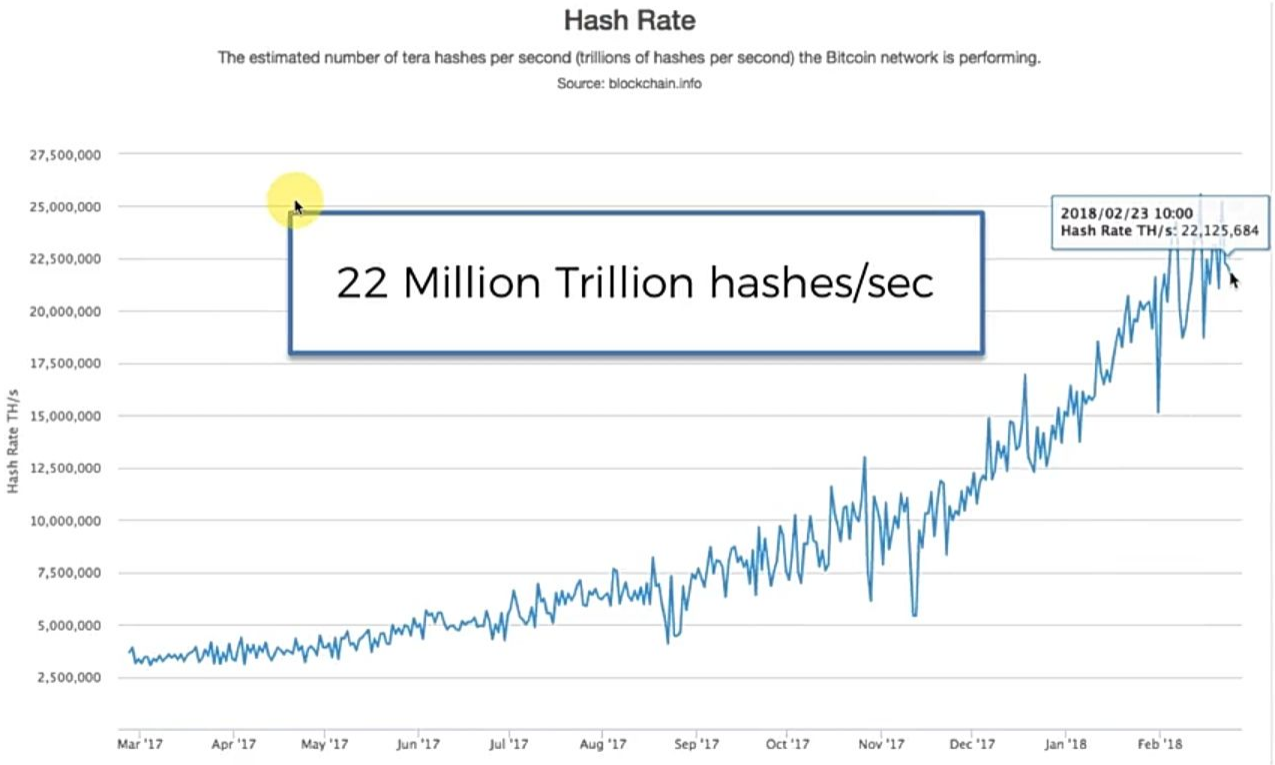
Courtesy : Super Data Science

Nonce Range



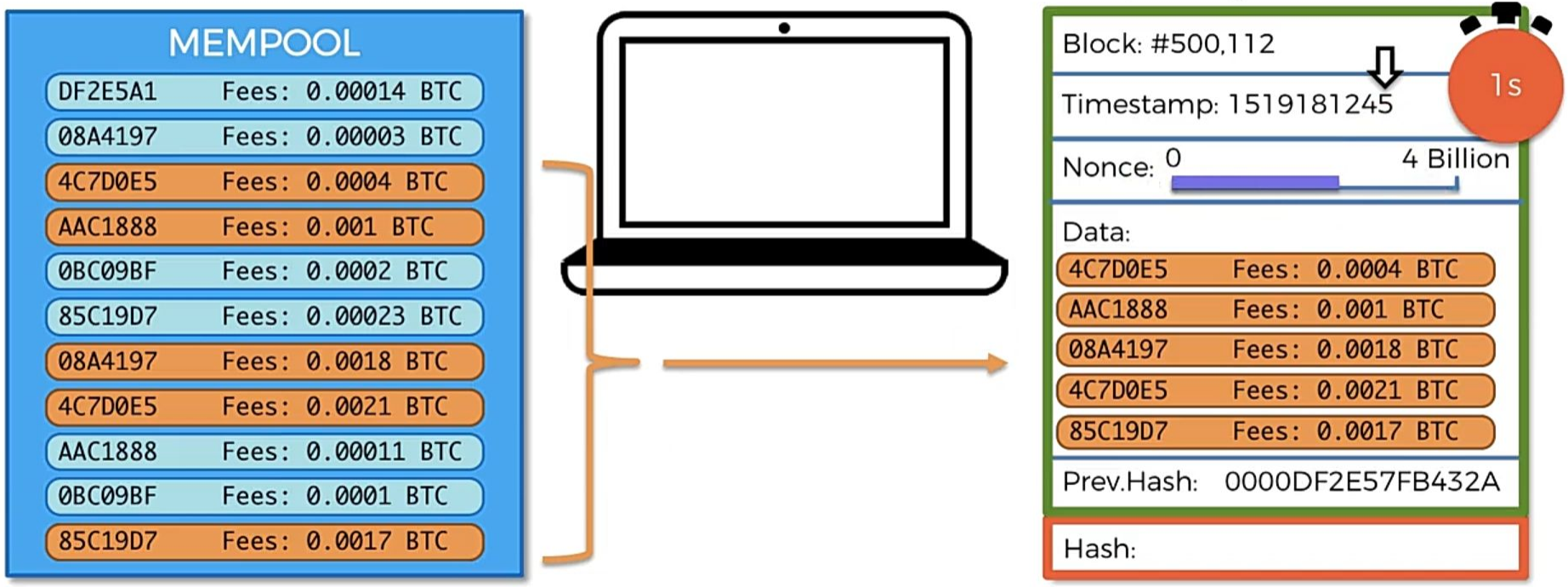
Courtesy : Super Data Science

Nonce Range



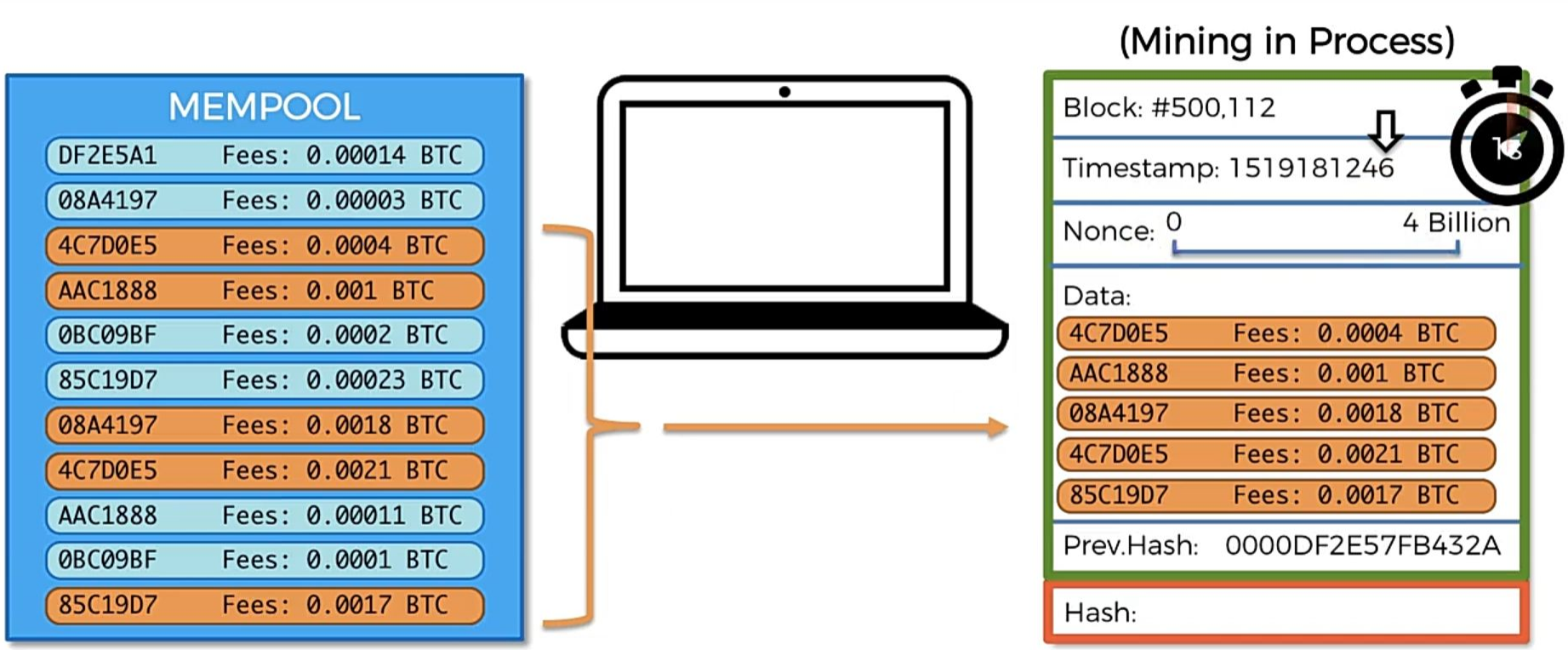
Courtesy : Super Data Science

How Miners Pick Transactions



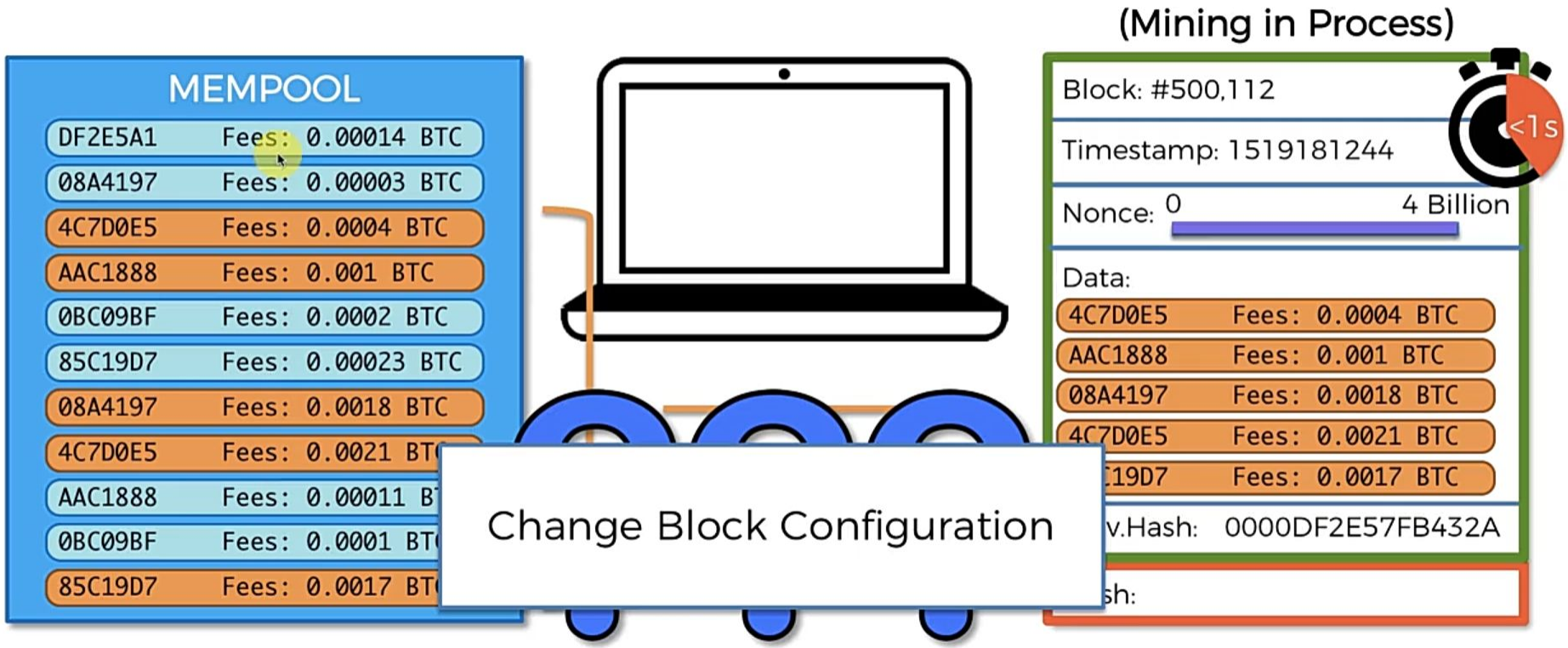
Courtesy : Super Data Science

How Miners Pick Transactions



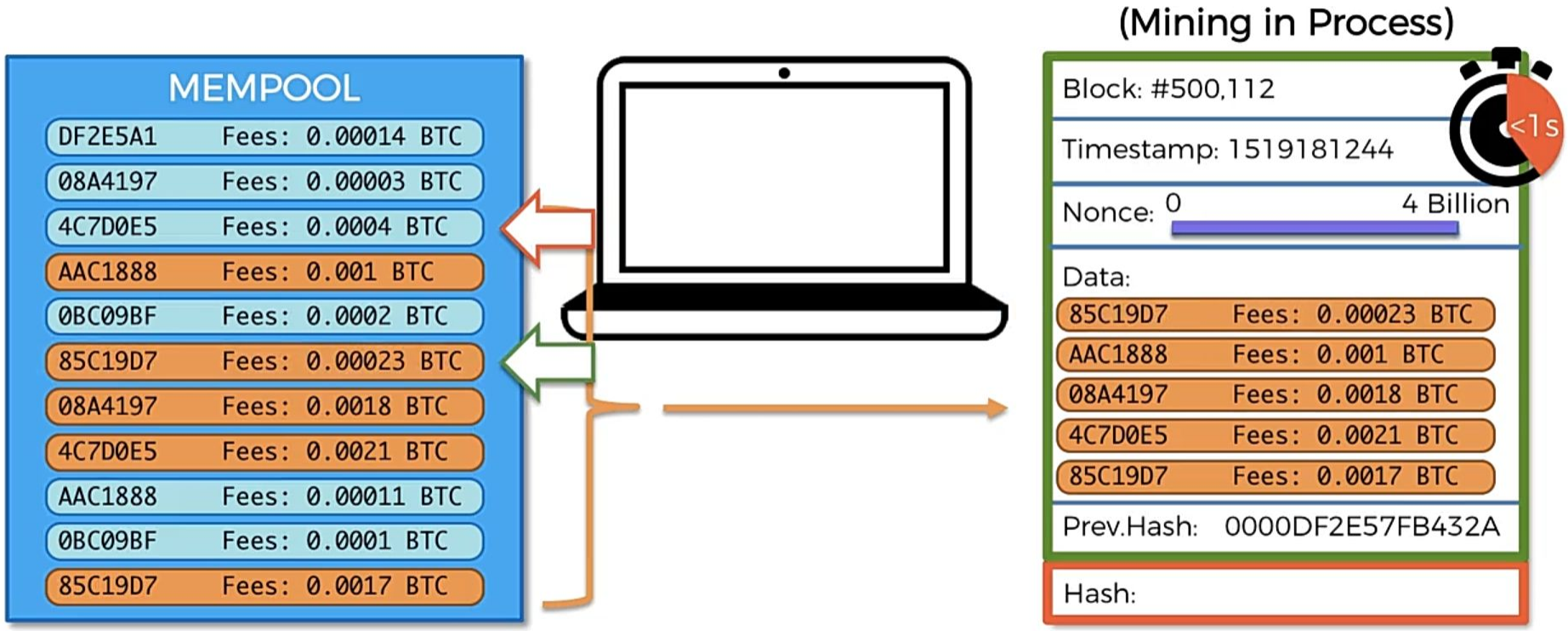
Courtesy : Super Data Science

How Miners Pick Transactions



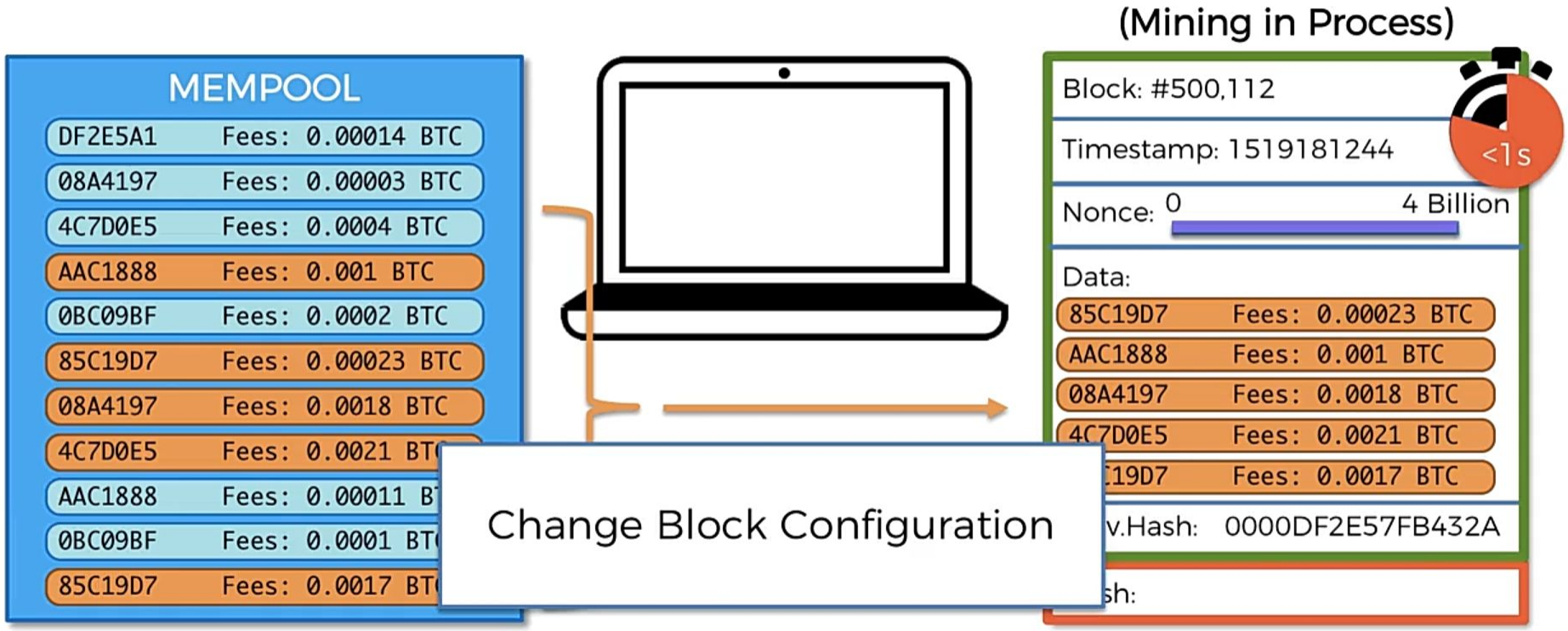
Courtesy : Super Data Science

How Miners Pick Transactions



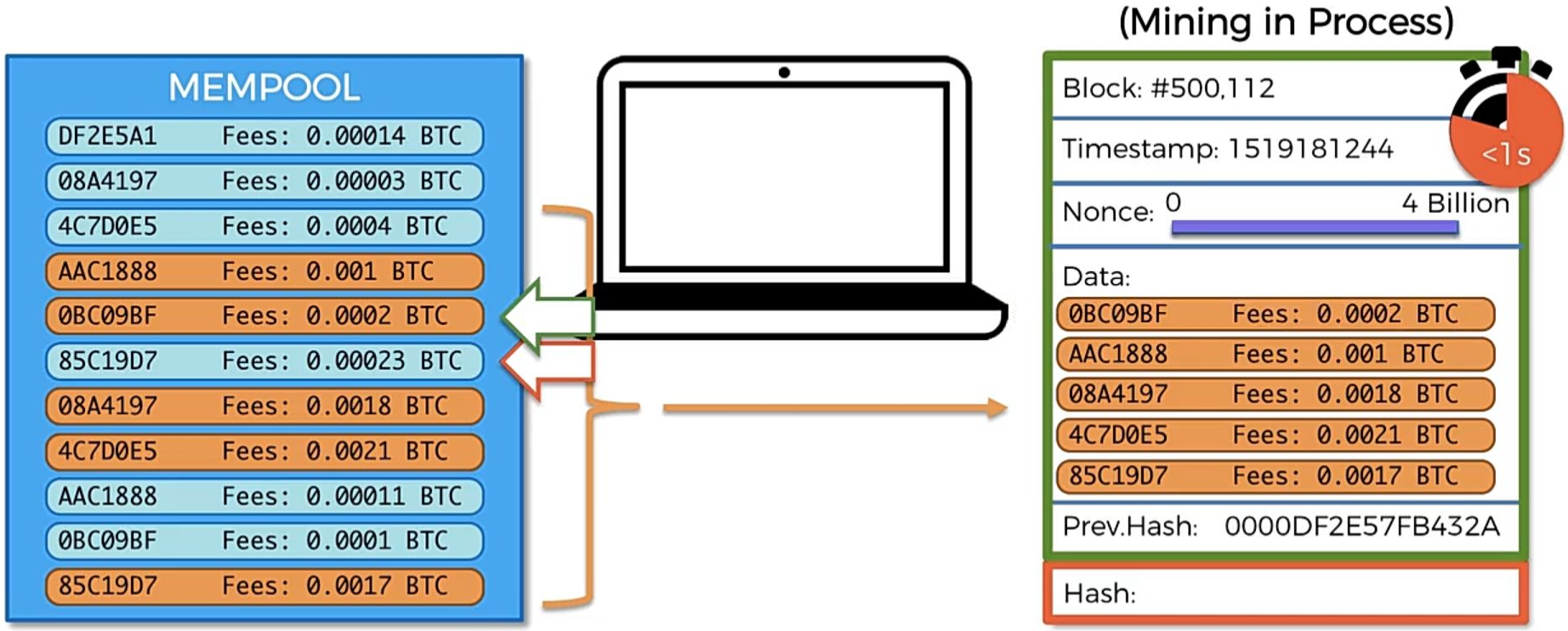
Courtesy : Super Data Science

How Miners Pick Transactions



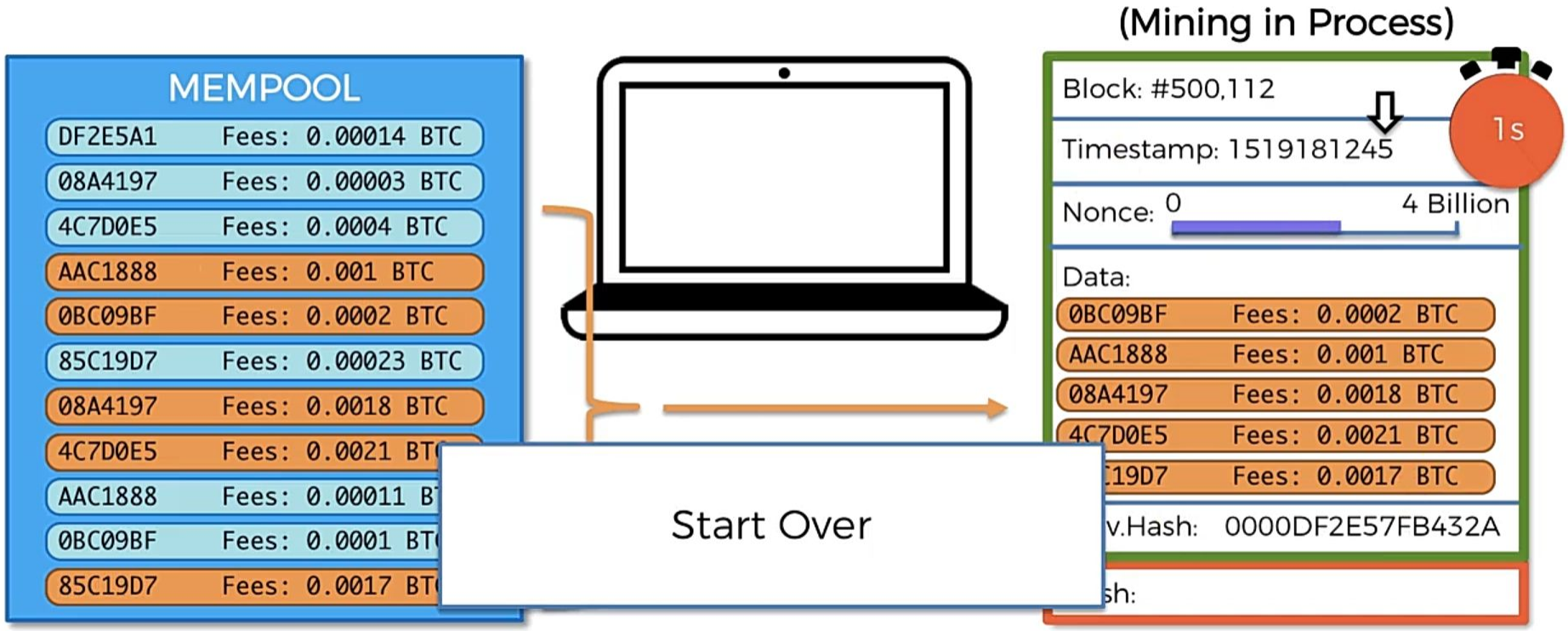
Courtesy : Super Data Science

How Miners Pick Transactions



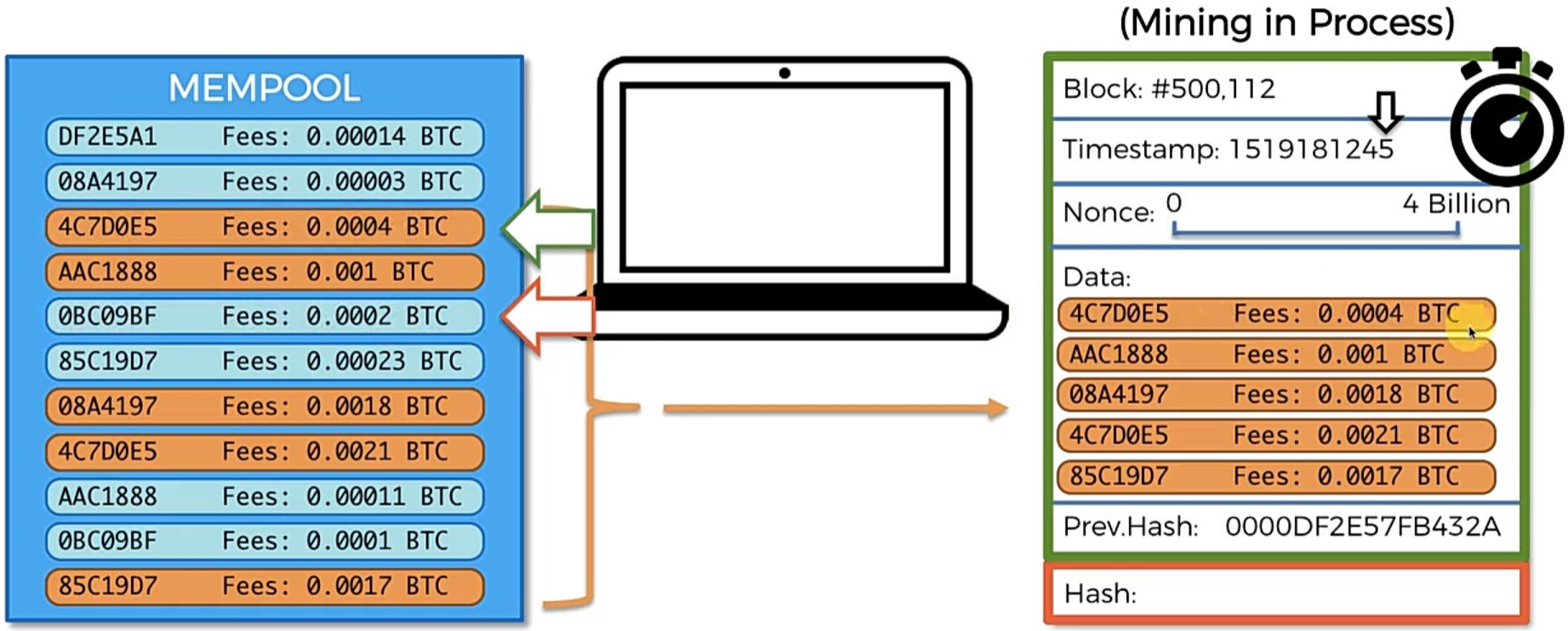
Courtesy : Super Data Science

How Miners Pick Transactions



Courtesy : Super Data Science

How Miners Pick Transactions



Courtesy : Super Data Science

CPUs vs GPUs vs ASICs

CPU = Central Processing Unit	General	< 10 MH/s
GPU = Graphics Processing Unit	Specialized	< 1 GH/s
ASIC = Application-Specific Integrated Circuit	Totally Specialized	> 1,000 GH/s

Cloud Mining

Courtesy : Super Data Science

Life of a Miner

ASIC (Application-specific integrated circuits) Miners

- most **effective and powerful mining hardware**
- Manufacturers build these machines with the sole purpose of mining a specific crypto algorithm
- As mining is an intensive and competitive process, it pushes these machines to their **maximum capabilities**.
- The average lifespan of a well-maintained machine : **3 to 5 years**.
- If kept in harsh or poor conditions, they can deteriorate in **a few months**.

Courtesy : Medium, YouTube

Life of a Miner

Common causes for ASIC damage and deterioration are:

1. **Little or no airflow**:
   - ASIC miners release a considerable amount of heat,
   - crucial to keep and run them in a well-ventilated location that keeps air moving and refreshing to avoid overheating.
2. **Humid, damp, or moist environments**:
   - internal components are damaged by humidity, which can cause rust and corrosion.
3. **Extreme temperatures**:
   - can shorten your hardware's lifespan by chipping away its internal components.
   - Cold tends to be less critical, as ASICs release heat that can counter-balance it.
   - Quick swings from below-zero to warm temperatures can cause condensation, provoking irreversible damage.

Courtesy : Medium, YouTube

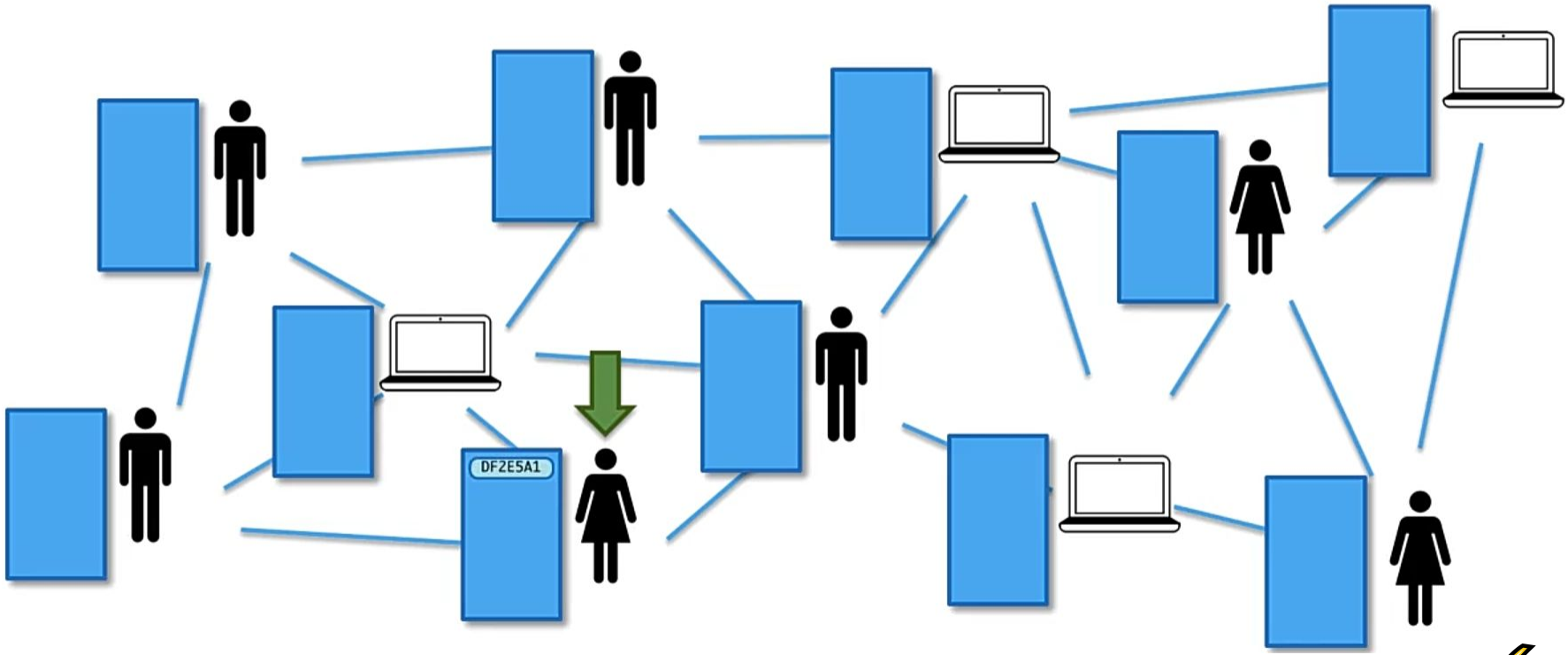
Life of a Miner

Best practices for preserving ASIC miners

1. **Choosing a suitable location**
   - it must be a **dry** room with good, constant **airflow**, so **wide and open spaces** should be the first choice.
   - consider **installing additional fans** to keep the air moving, maintain the room dry, and avoid condensation.
2. **Mitigating the heat**
   - specialized and advanced cooling systems that reduce temperature,
   - innovative ways to **repurpose the heat produced by ASIC machines**, like heating pools or hot tubs, dehydrating fruit, or redirecting it to greenhouses for growing crops.
     - reduce or even eliminate the damage high temperatures have on miners,
     - enable **increased profitability** either by **reducing costs or adding another source of income**.
     - primary priority is **treating the excess heat** to preserve your miners.
3. **Regular maintenance and cleaning**
   - It is essential to **perform regular maintenance and clean the mining hardware**.
   - Removing accumulated dust not only prolongs lifespan, but also keeps performance high.

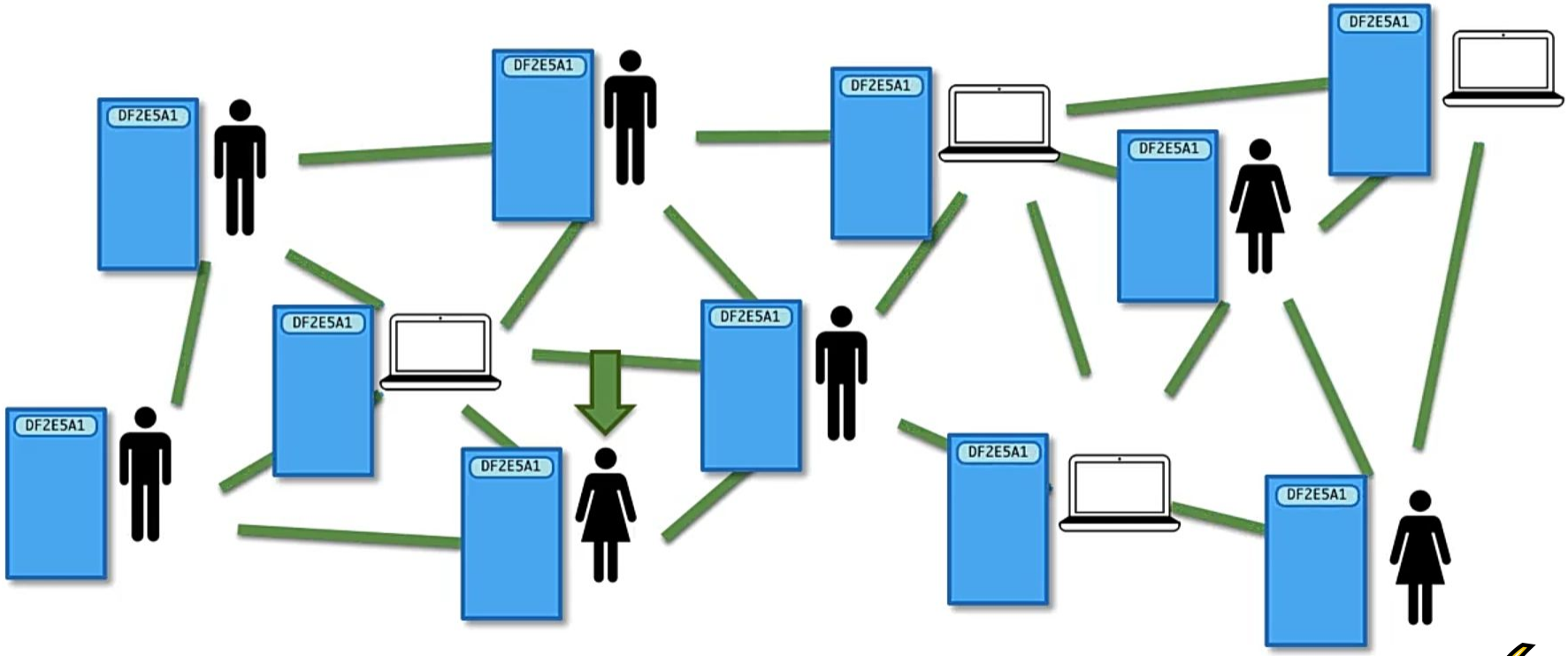
Courtesy : Medium, YouTube

How do Mempools work?



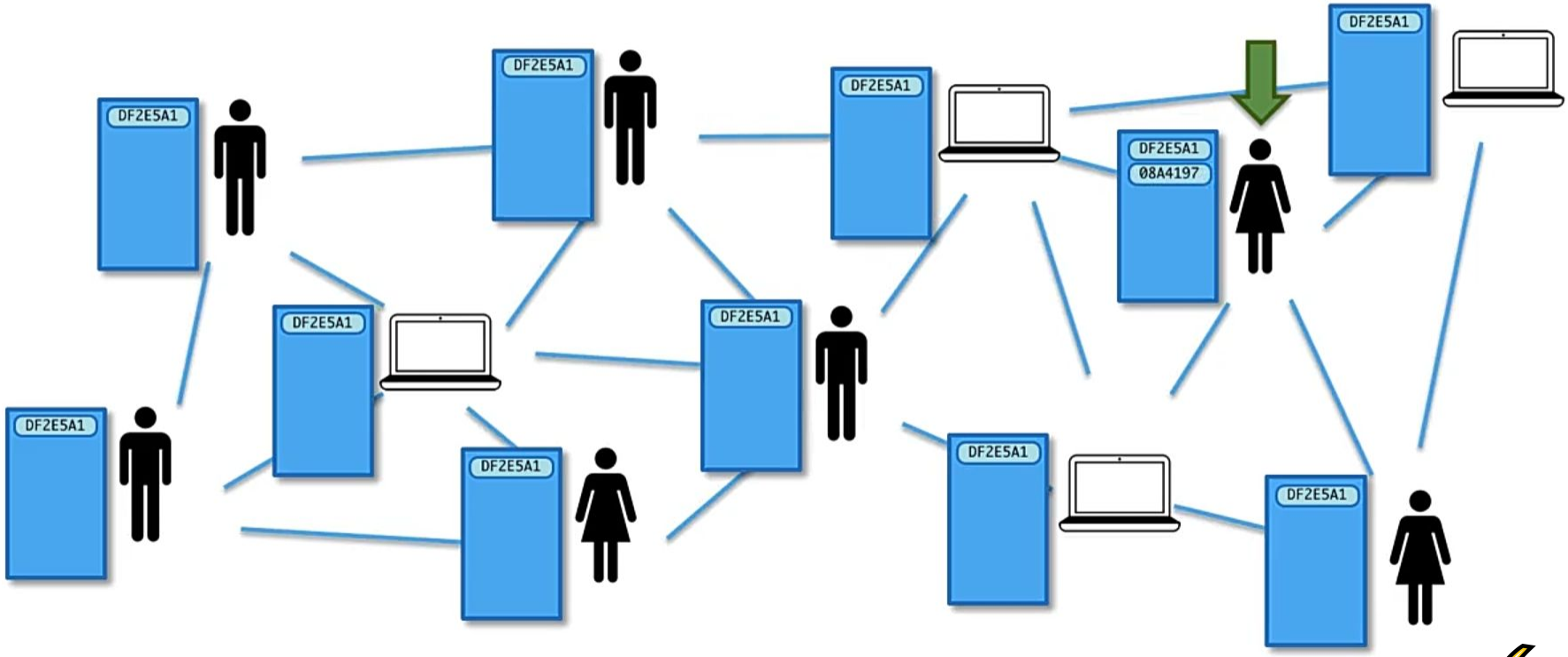
Courtesy : Super Data Science

How do Mempools work?



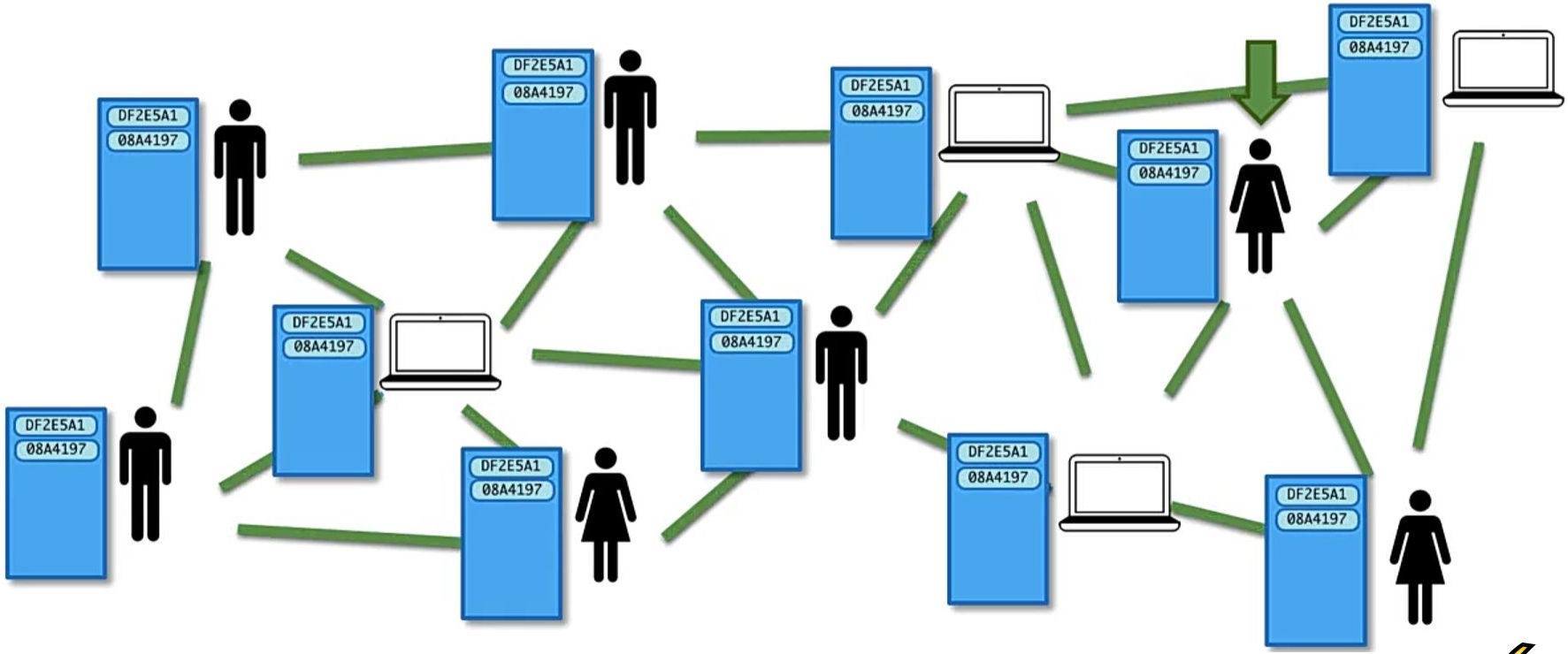
Courtesy : Super Data Science

How do Mempools work?



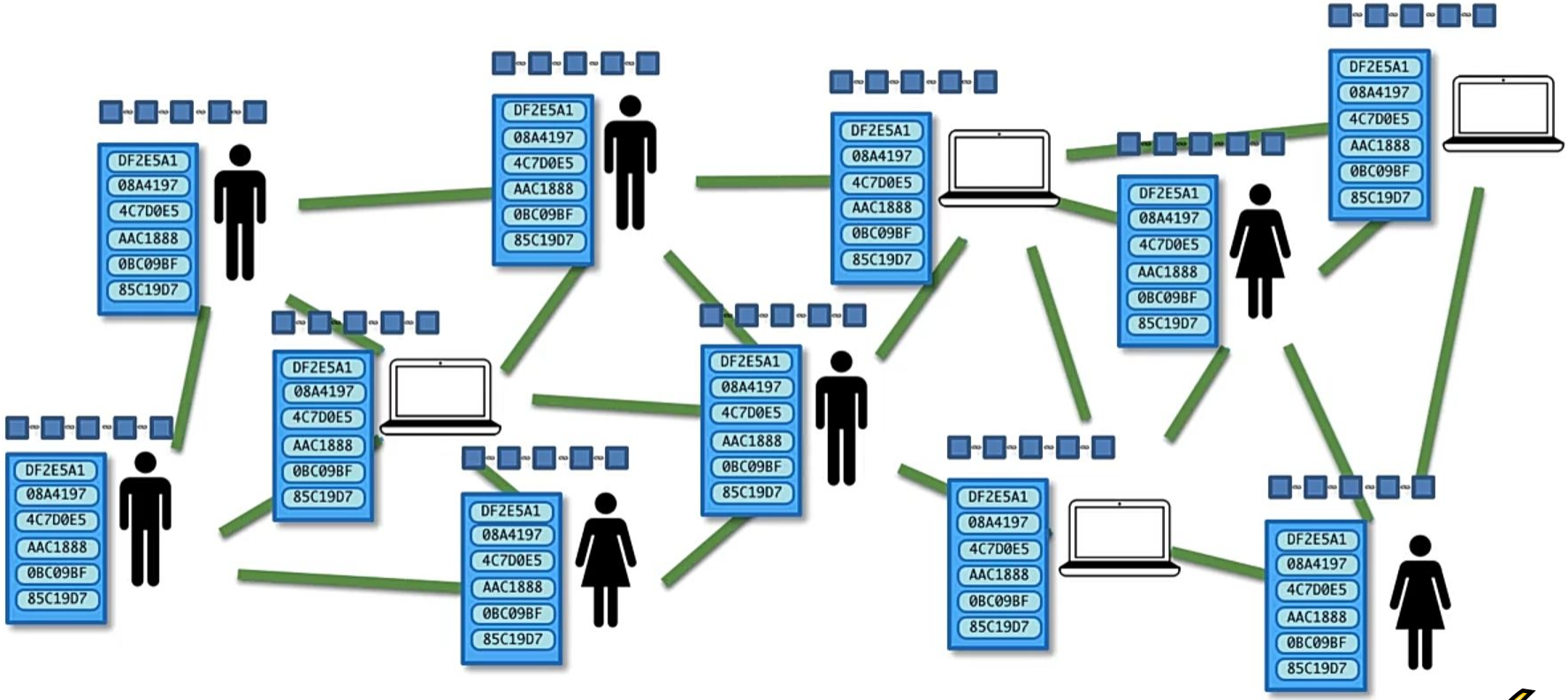
Courtesy : Super Data Science

How do Mempools work?



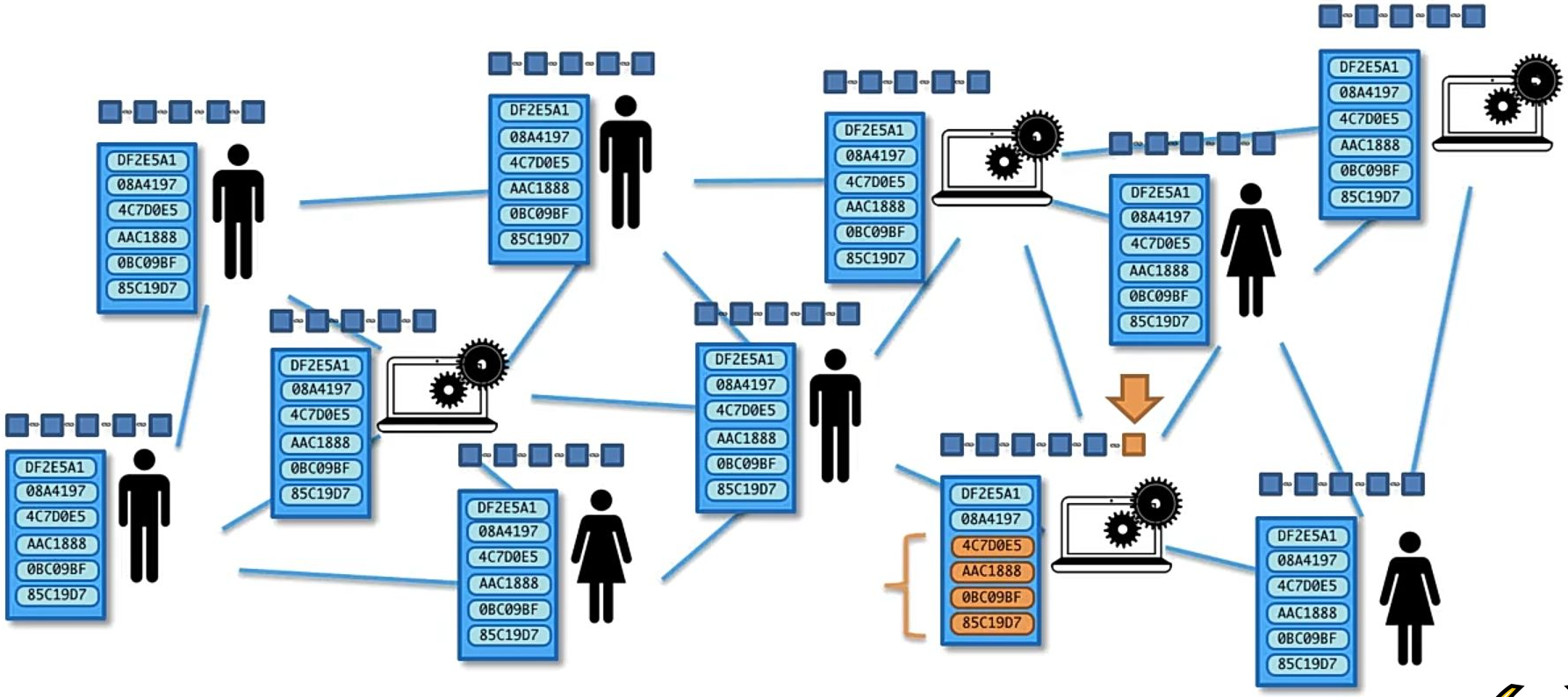
Courtesy : Super Data Science

How do Mempools work?



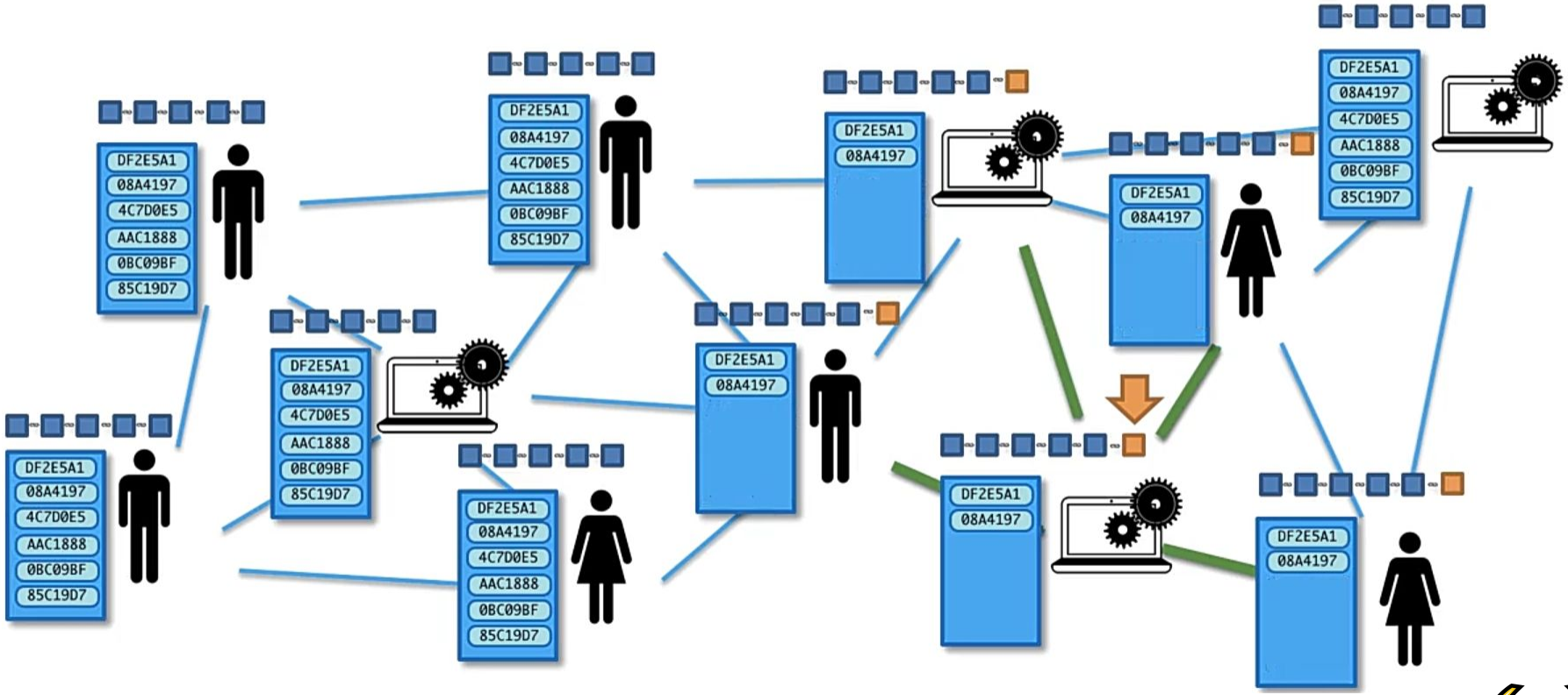
Courtesy : Super Data Science

How do Mempools work?



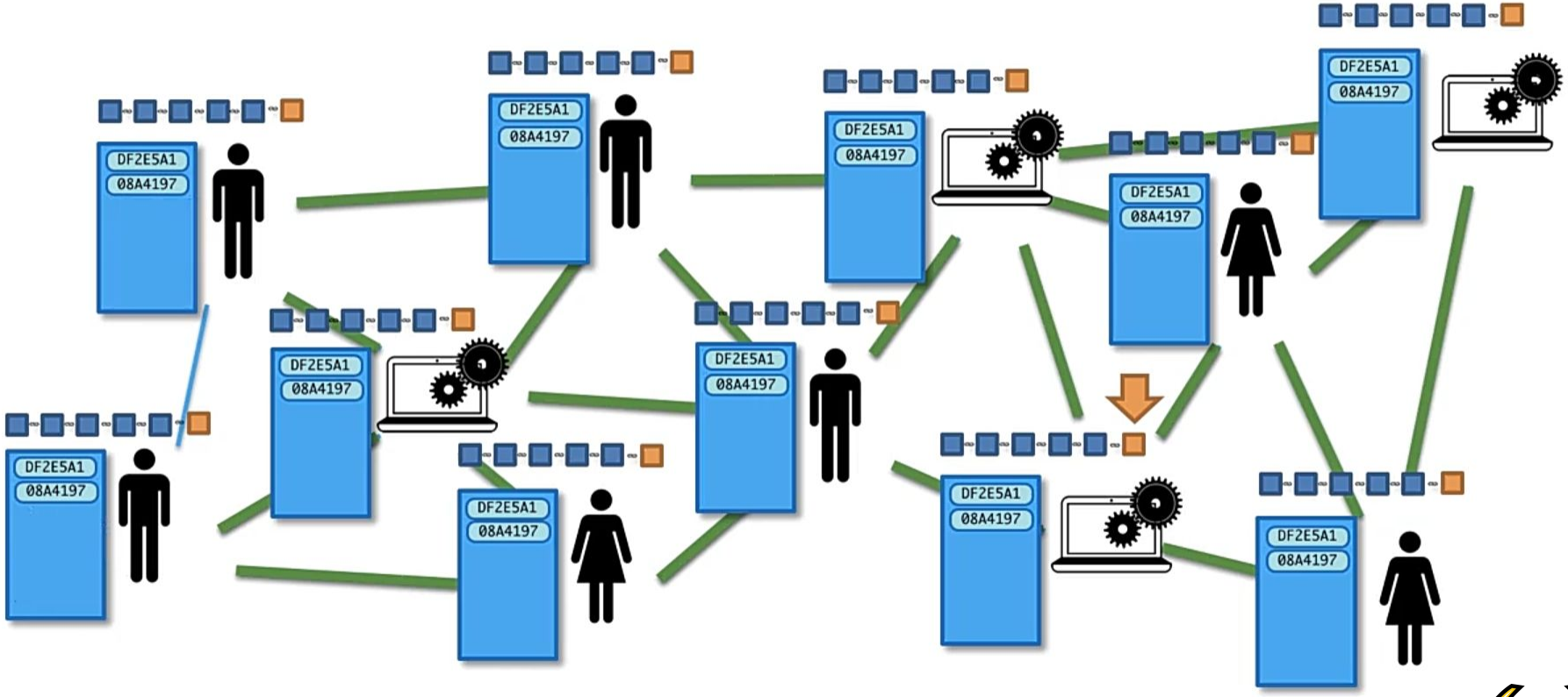
Courtesy : Super Data Science

How do Mempools work?



Courtesy : Super Data Science

How do Mempools work?



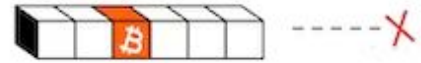
Courtesy : Super Data Science

Double Spending Problem

d why is it such a problem?

Alice

Without exception, all Bitcoin transactions are included in a block of transactions.
Each block has a timestamp with encoded information that makes it more difficult to manipulate the blockchain.



Katy

Double spending is a type of deceit where the same money is promised to two parties but only delivered to one.

John

The mechanism of the blockchain ensures that the party spending the bitcoins is the real owner.

Bob

The technology behind Bitcoin ensures that the party who spends the bitcoins is the real owner by only processing verified transactions.

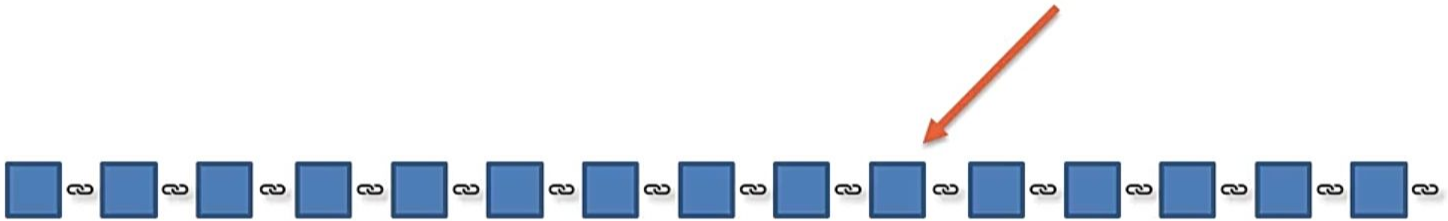
Courtesy : BitPanda

Double Spending Problem

- **Risk that a cryptocurrency can be used twice or more.**
- **Transaction information** within a blockchain **can be altered if specific conditions are met**.
  - The conditions allow modified blocks to enter the blockchain;
  - if this happens, the person that initiated the alteration can reclaim spent coins.
- occurs when someone alters a blockchain network and inserts a special one that allows them to reacquire a cryptocurrency.
- Double-spending can happen, but it is more likely that a cryptocurrency is stolen from a wallet that wasn't adequately protected and secured.
- Many variations of attacks could be used for double-spending—**51% is one of the most commonly cited attacks,** while the unconfirmed transaction attack is most commonly seen.

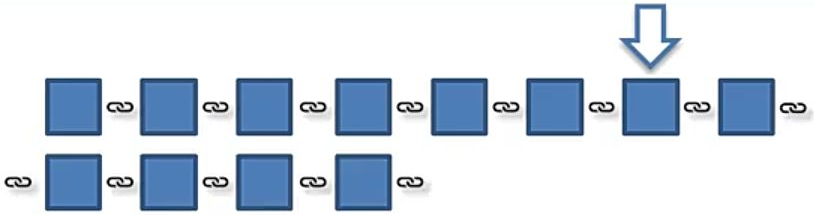
Courtesy : Investopedia

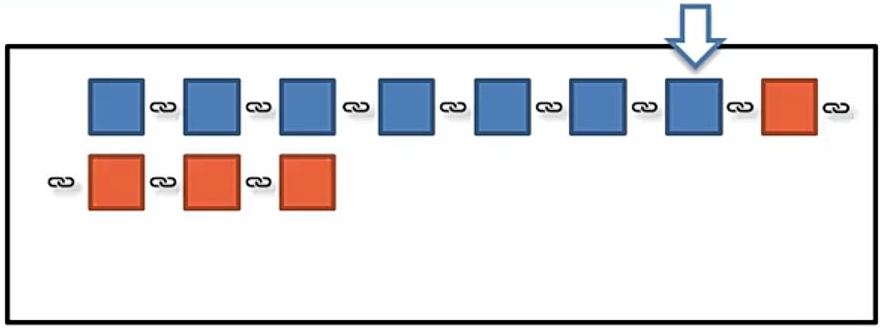
The 51% Attack

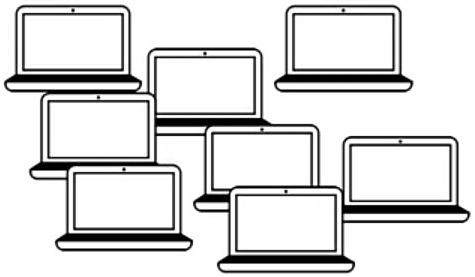


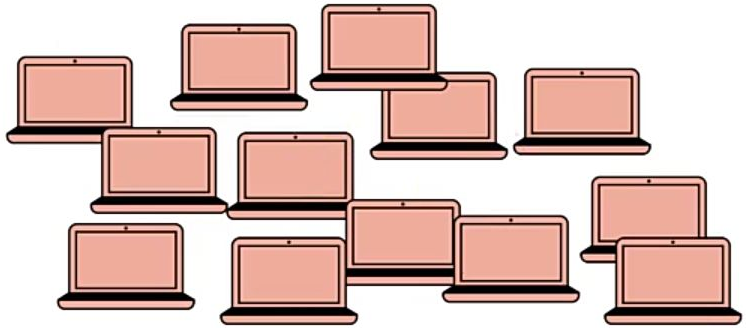
This is NOT the 51% attack

The 51% Attack



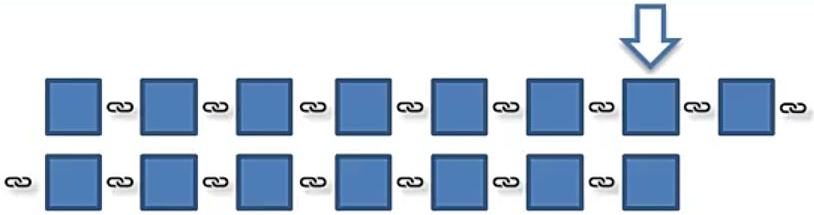


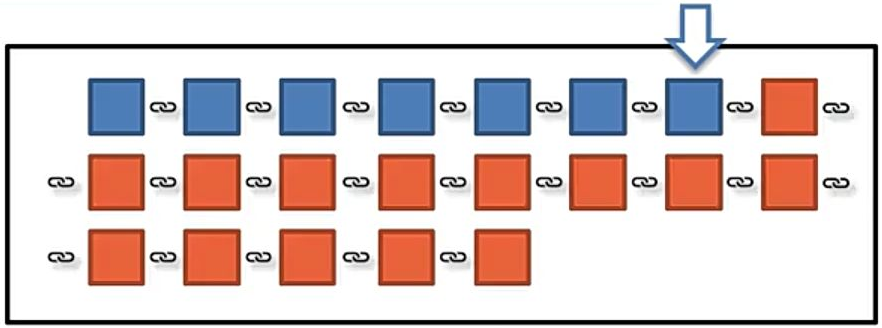


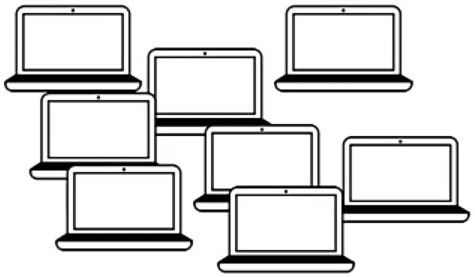


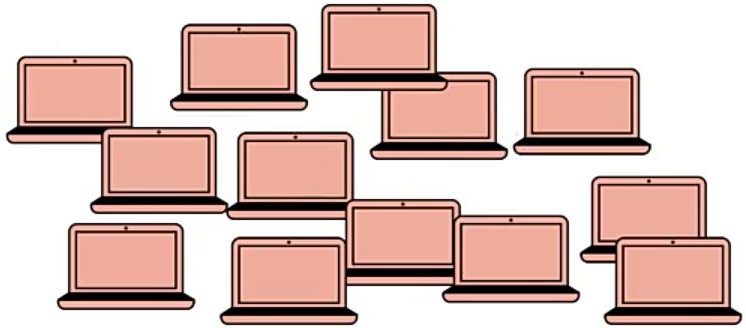
Courtesy : Super Data Science

The 51% Attack



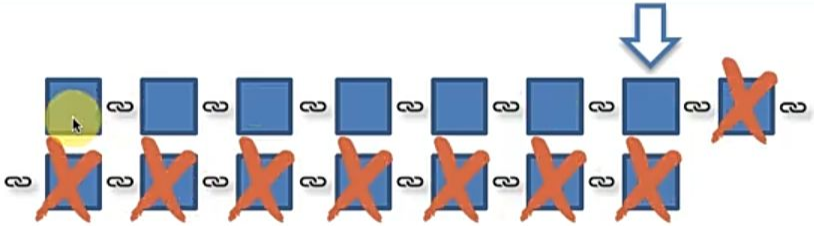


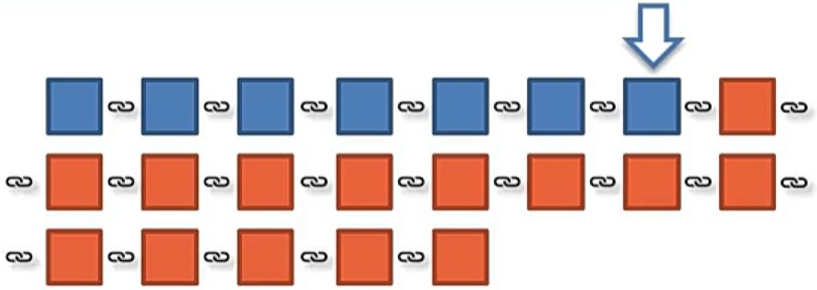


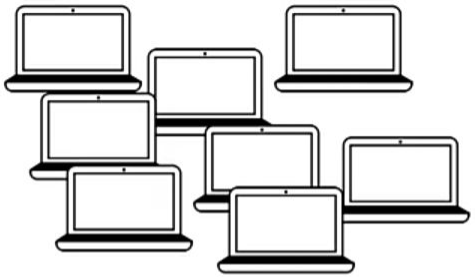


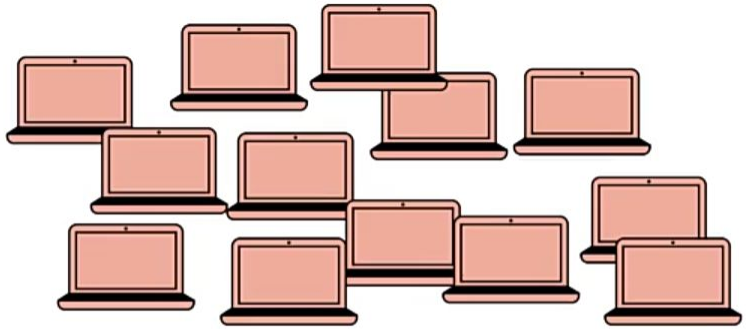
Courtesy : Super Data Science

The 51% Attack









Courtesy : Super Data Science

Bitcoin Blockchain- “Bitcoin: A Peer-to-Peer Electronic Cash System”.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

- 9 pages Research Paper · Cited by **28186**
- Propose a solution to the double-spending problem using a **peer**-to-**peer** network.

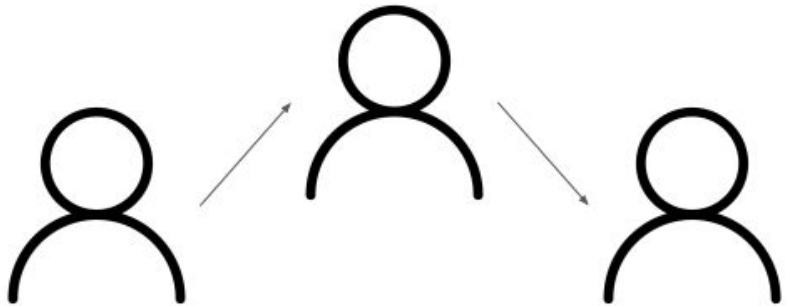
Courtesy : Bitcoin - WhitePaper

Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Electronic Payment Background

Online commerce rely on trusted third parties

- Reversible
- Have minimum transaction limits
- Not applicable for small amount transactions



Courtesy : University of Michigan - PPT

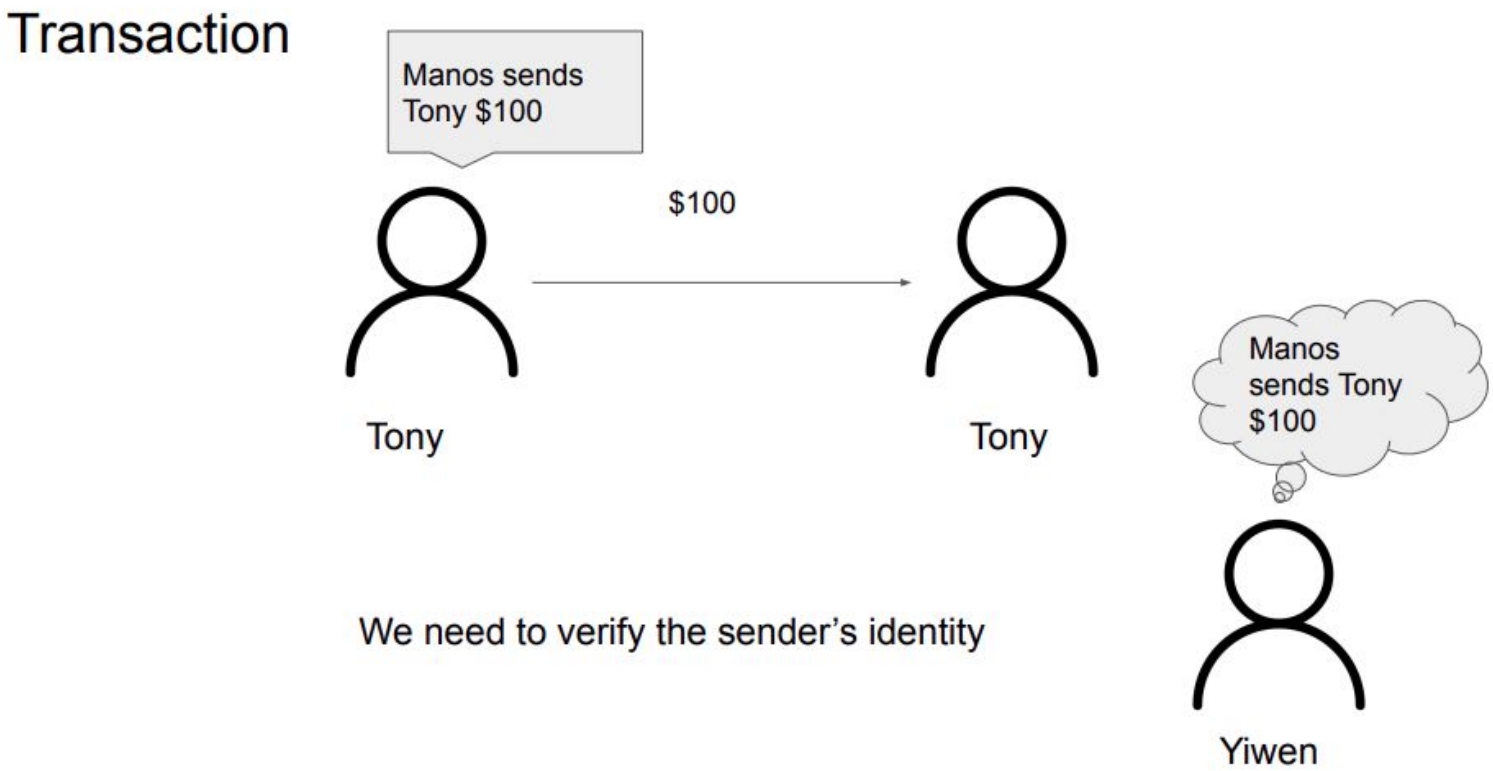
Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Motivation of Bitcoin

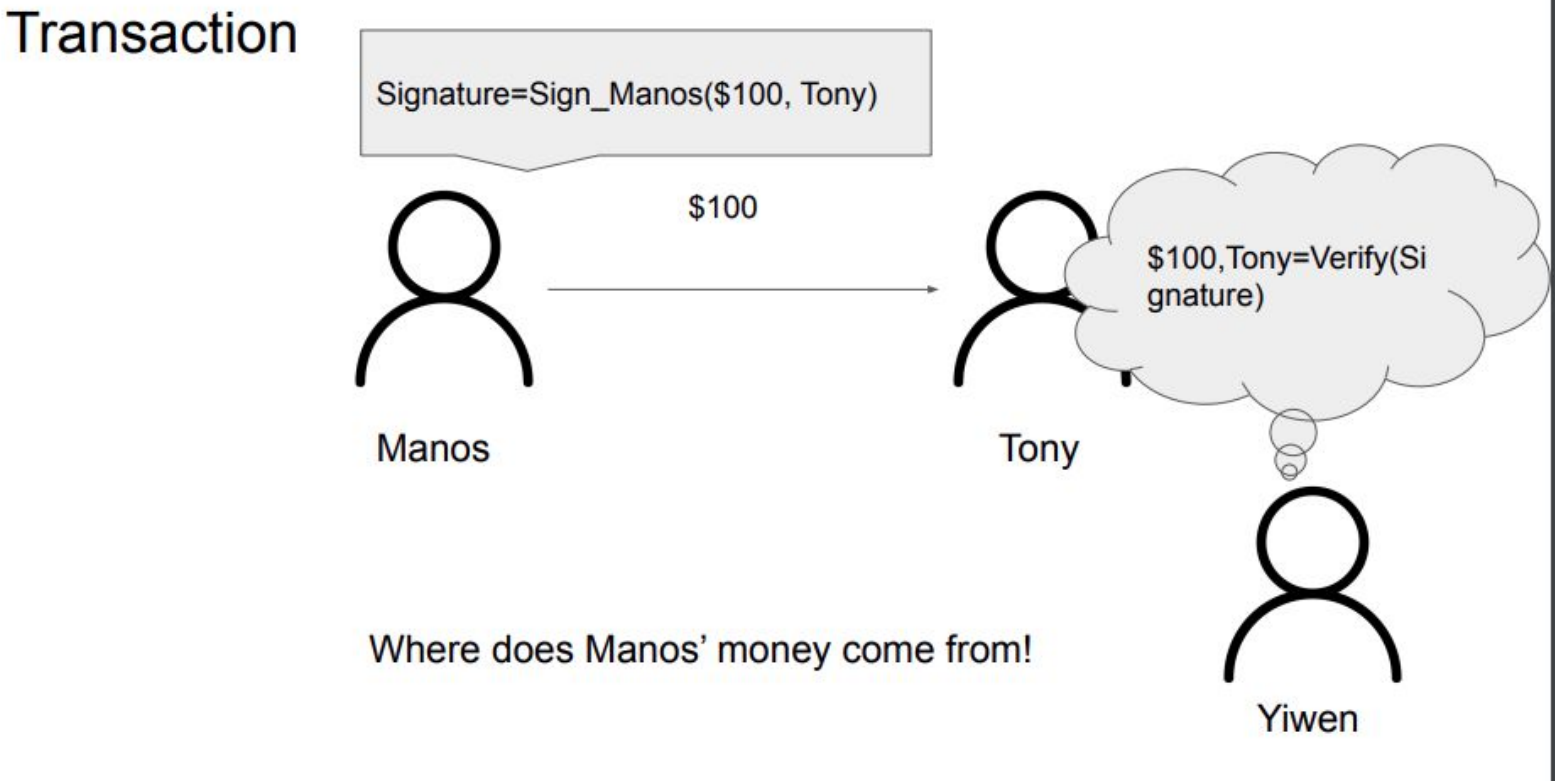
Electronic payment system based on cryptographic proof instead of trust

- Non-reversible
- Peer-to-peer
- Solves double-spending

Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

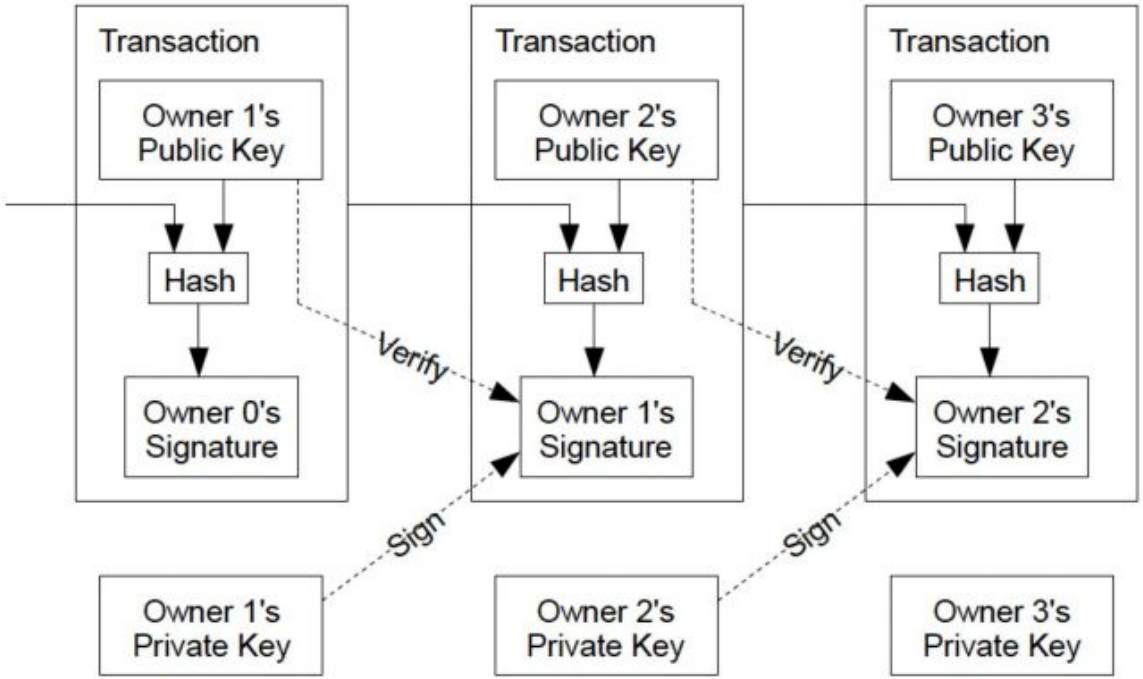


Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".



Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Transaction



Courtesy : University of Michigan - PPT

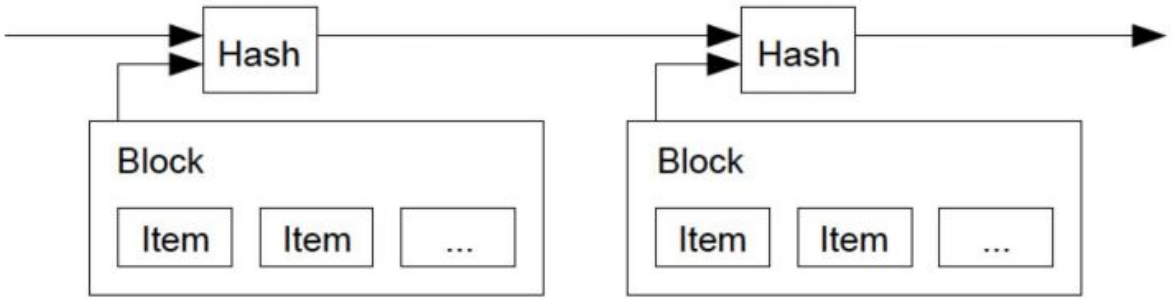
Requirements of Transactions

- Transactions must be publicly announced
- Need a system to agree on a single history of the order
- Need to prove that at the time of each translation, the majority nodes agreed

Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

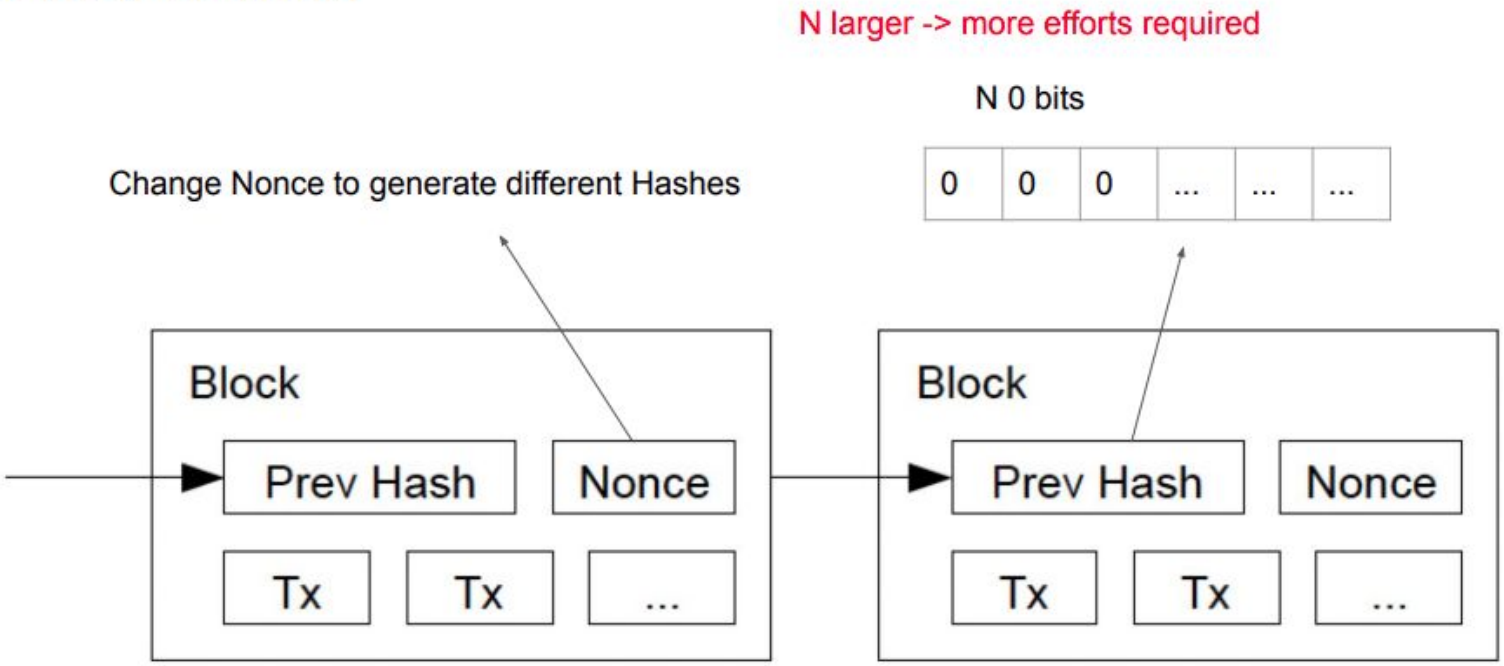
Timestamp Server

Takes a hash of a block of items to be timestamped and widely publishes the hash



Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Proof-of-work



Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Proof-of-work

- Makes the blockchain difficult to be changed
  - To change a block, need to recalculate the hash values of the target block and all blocks after
- Solves the problem of determining representation in majority decision making
  - If the majority is based on number of IP addresses -> Attacker with many IP addresses can break the system
  - CPU based majority makes the honest chain to grow fastest -> Immense efforts required to attack

Hardware speed develops fast, maybe attackers can catch up in future?

Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Nakamto

The proof-of-work difficulty is determined by a moving average targeting an average number of blocks per hour. **If they are generated too fast, the difficulty increases.**

Network

1. New transactions are broadcast to all nodes.
2. Each node collects new transactions into a block.
3. Each node works on finding a difficult proof-of-work for its block.
4. When a node finds a proof-of-work, it broadcasts the block to all nodes.
5. Nodes accept the block only if all transactions in it are valid and not already spent.
6. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

Incentive

- The first translation in a block
  - A new coin
- Transaction fees
  - Difference of output value and input value
  - When the number of coins reaches some predetermined value, incentive transition entirely to transaction fees to prevent inflation

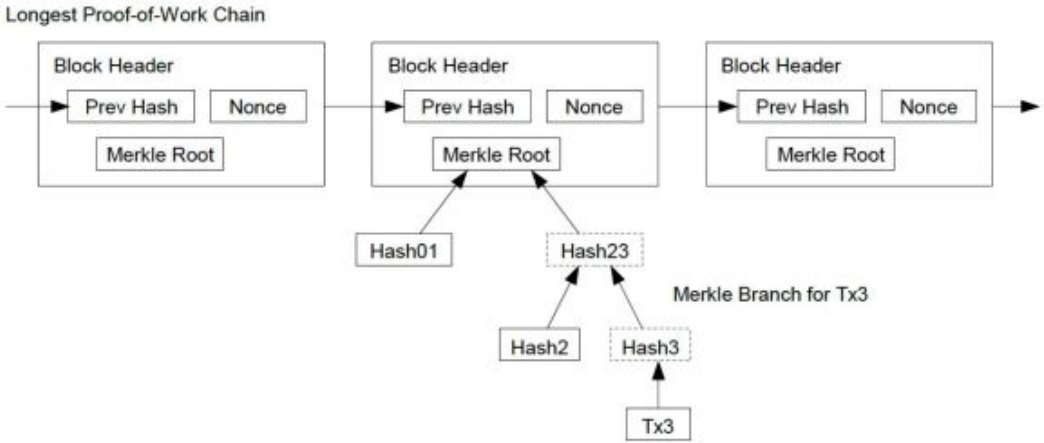
Since you have powerful, why not be honest? You will get rewards!

Nakamto

Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Simplified Payment Verification

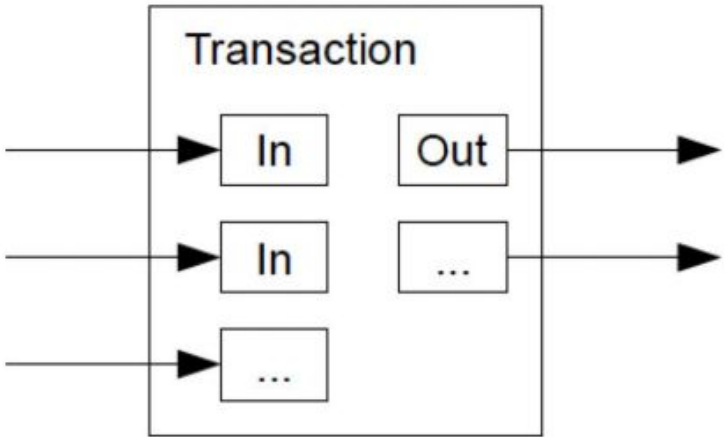
- Keep a copy of the block headers of the longest proof-of-work chain
- Link the transaction to a space in the chain, if it is accepted by a network, then the transaction is valid
- Vulnerable if the network is overpowered by an attacker



Courtesy : University of Michigan - PPT

Combining and Splitting Value

- A single input from a larger previous transaction or multiple inputs combining smaller amounts
- At most two outputs: payment -> payee and charge -> sender



Bitcoin Blockchain- "Bitcoin: A Peer-to-Peer Electronic Cash System".

Pros of Bitcoin

- The first system of blockchain
  - A success on decentralization
- Privacy
- Hard to modify previous records
- Transparent
- Against inflation
  - Limited throughput

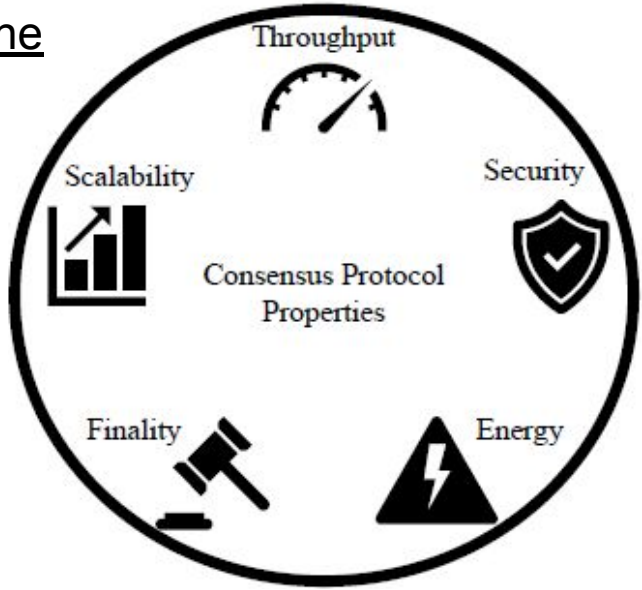
Cons of Bitcoin

- Long transaction time
  - Average of 10 mins
- Limited throughput
  - 21,000,000 in total
  - 3,000,000 remaining
- Large energy consumption
  - about 80 terawatt-hours
  - ~ Annual output of 23 coal-fired power plants
- Graphics cards out of stock

Courtesy : University of Michigan - PPT

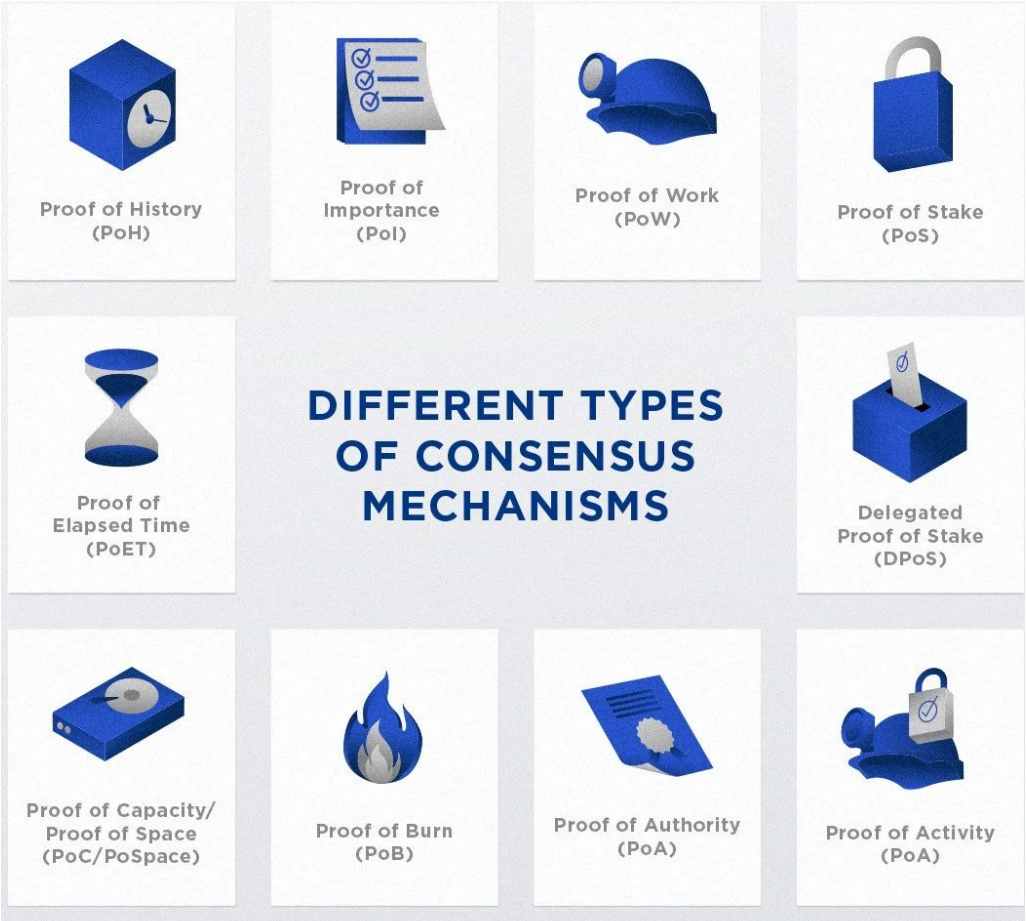
Consensus Mechanism

- A **procedure** in which the **peers** of a blockchain network reach agreement about the present state of the data in the network.
- Establish **reliability and trust** in the blockchain network.
- **backbone of all cryptocurrency** blockchains,
- what make **Blockchains secure.**
- Helps to **determine which blockchain transactions are valid and which are not**.
- **Sets of rules that help to protect networks from malicious behaviour and hacking attacks.**



Courtesy : Crypto.com

Consensus Mechanisms



Courtesy : Crypto.com

Types of Consensus Mechanisms - Proof of Work (PoW)

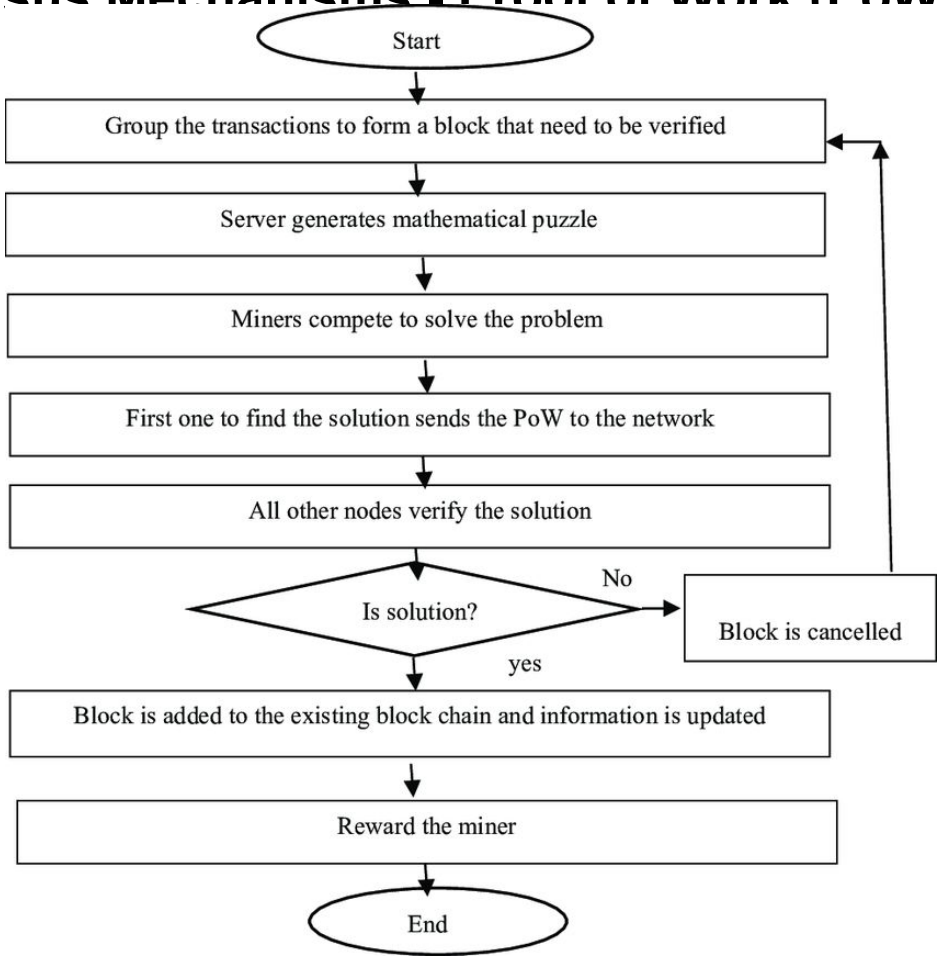
- Used by Bitcoin and many other public blockchains,
- very first consensus mechanism created.
- most reliable and secure of all the consensus mechanisms
- was first coined in the early 1990s,
- it was Bitcoin founder Satoshi Nakamoto who first applied the technology in the context of digital currencies.

Algorithm

- ‘miners’ essentially compete against one another to solve extremely complex computational puzzles using high-powered computers.
- The first to come up with the 64-digit hexadecimal number (‘hash’) earns the right to form the new block and confirm the transactions.
- The successful miner is also rewarded with a predetermined amount of crypto, known as a ‘block reward’.

Courtesy : Crypto.com

Types of Consensus Mechanisms - Proof of Work (PoW)



Courtesy : Research Gate

Types of Consensus Mechanisms - Proof of Work (PoW)

Advantages of Proof-of-Work

- A **hard-to-find solution**. Still, easy verification.
- As an initial consensus mechanism, PoW **does not need initial stakes of coins before mining.** One can start with 0 coins and it will only be positive.
- Ease of implementation compared to other blockchain consensus mechanisms.
- It is **fault tolerant.** It means that the failure of one component will not shut down the entire blockchain network.
- **Give miners the opportunity to earn by adding a block.**
- PoW is the **oldest, most trusted, and most popular consensus protocol.**

Types of Consensus Mechanisms - Proof of Work (PoW)

Limitations of Proof-of-Work

- A **lot of energy is wasted** because only one miner can finally add their block.
- It requires a **lot of computing power** and, therefore, massive consumption of resources and energy.
- **51% risk of network attack**. A controlling person can get 51% to control the network.
- Spread environmental hazards with attachment machines.
- PoW is a **time and energy wipe-out process.**
- It required a lot of hardware costs.
- **Risk of Denial of Service Attacks by Intruders**.

Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

- Nodes in the network, **stake a certain amount of cryptocurrency to become candidates for validating a new block and receiving a fee**.
- The algorithm then selects a node from the pool of candidates to verify the new block.
- This selection **algorithm combines the amount of deposit** (amount of cryptocurrency) **with other factors (such as selection based on coin age, and randomization process)** to make the selection fair for everyone in the network.

Coin-age-based selection:

- The algorithm keeps **track of how long each candidate validator node remains a validator.**
- The older the node, the higher the chance of becoming a new validator.

Random Block selection:

- The validator is **selected by combining "lowest hash value" and "highest stake."**
- The **node that has the best-weighted combination of them becomes the new validator.**

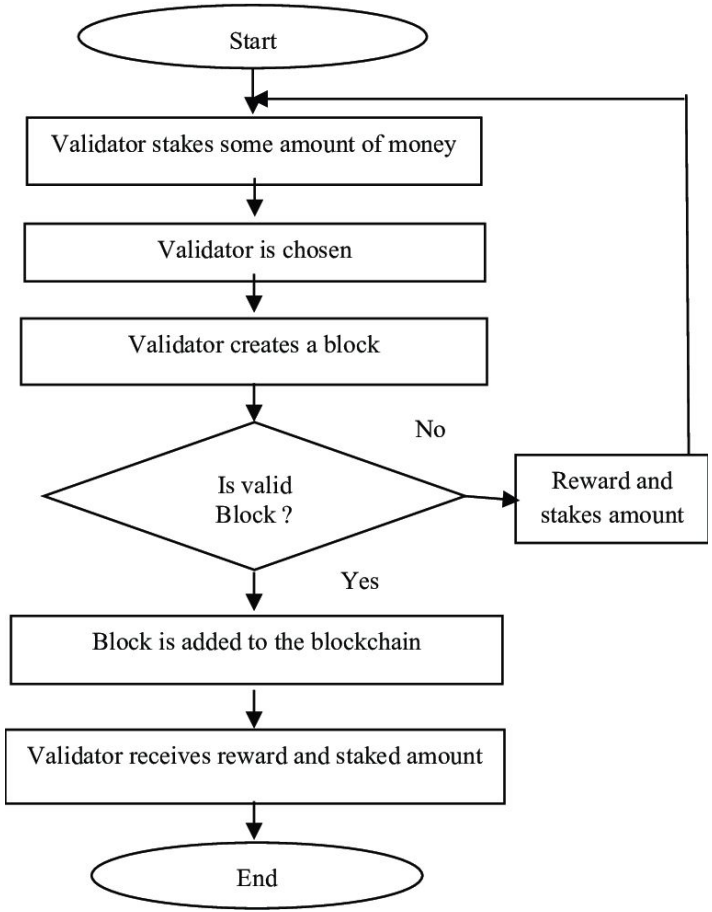
Types of Consensus Mechanisms - Proof of Stake (PoS)

Workflow of a PoS-based mechanism

1. Nodes perform transactions. The PoS algorithm puts all these transactions into a pool.
2. All nodes fighting to become validators for the next block **raise the stake**. This stake is combined with other factors such as “coin age” or “random block selection” to select a validator.
3. The validator verifies all transactions and publishes the block. His bet remains locked, and the forgery reward has also not yet been awarded. This is so that nodes in the network can “OK” a new block.
4. The **validator will get the stake back and the reward if the block is OK**. If the algorithm uses a mechanism based on coin age to select validators, the validator for the current block has its coinage reset to 0. This puts it in low priority for the next validator election.
5. **If other nodes in the network do not validate the block, the validator loses his stake and is marked as “bad” by the algorithm**. The process starts again from step 1 to create a new block.

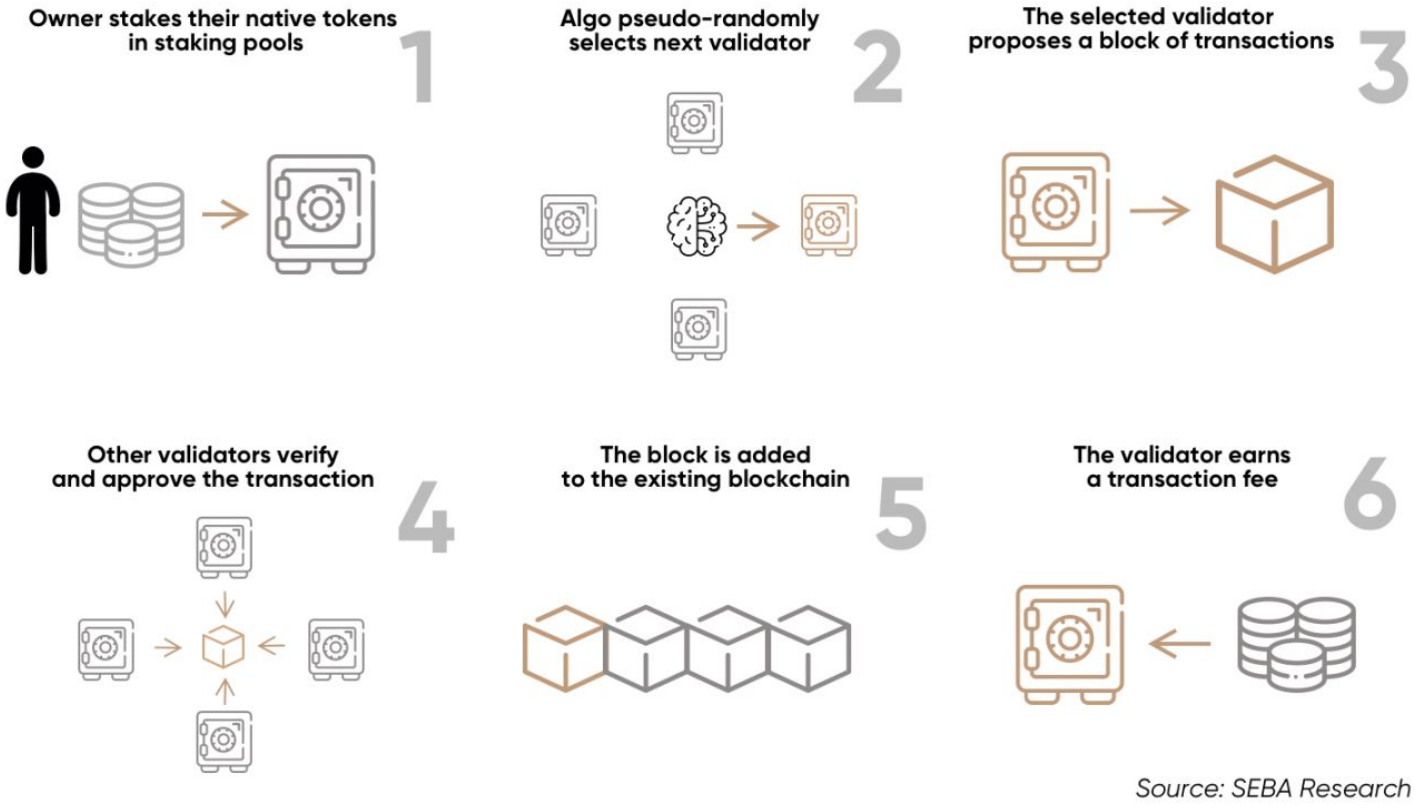
Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)



Courtesy : ResearchGate

Types of Consensus Mechanisms - Proof of Stake (PoS)



Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

Advantages of PoS

- **Energy saving:**
  - Since all nodes are not competing to add a new block to the blockchain, energy is saved.
  - No problem needs to be solved (as in the case of a Proof-of-Work system), thus saving energy.
- **Decentralization:**
  - **PoW** :
    - to achieve distributed consensus, there is the added incentive of exponential rewards for joining a mining pool, leading to a more centralized nature of the blockchain.
  - **PoS** (such as Peercoin),
    - the r**ewards are proportional (linear) to the deposit amount.**
    - no additional benefits for joining a mining pool, thereby supporting decentralization.
- **Safety:**
  - A **person trying to attack the net must own 51% of the stakes (quite expensive).**
  - This **leads to a secure network.**

Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

Weakness of PoS mechanism

- **Big Bet Validators:**
  - If a group of validator candidates come together and own a significant share of the total cryptocurrency, they will have a better chance of becoming validators.
  - The increased odds lead to bigger withdrawals, leading to more rewards being earned, which leads to owning a huge share of the currency. This can be the reason for the n**etwork to come to be centralized over time.**
- **New technology:**
  - PoS is still relatively new.
  - Research is ongoing to find the flaws, fix them, and make them viable for a live network with real currency transactions.
- **The "Nothing at Stake" Problem:**
  - This problem describes little to no disadvantage for nodes if they support multiple blockchains, in the case of blockchain forking.
  - In the worst case, **each fork will lead to multiple blockchains, and validators will work, and the nodes in the network will never reach a consensus.**

Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

Goals of Proof-of-Stake

- Proof-of-stake is designed to reduce network congestion and environmental sustainability concerns associated with the proof-of-work (PoW) protocol.
- Bitcoin miners earn bitcoins by validating transactions and blocks. However, they pay their operating costs such as electricity and rent in fiat currency. What happens then is that miners exchange energy for cryptocurrency, which makes PoW mining consume as much energy as some small countries.
- The PoS mechanism seeks to solve these problems by **effectively replacing computing power with staking, where the ability of an individual to mine randomly is the network**. This means there should be a drastic reduction in power consumption, as miners can no longer rely on massive farms of single-purpose hardware to gain an edge.

Courtesy : AnalyticsVidya

Types of Consensus Mechanisms - Proof of Stake (PoS)

Proof-of-Stake security

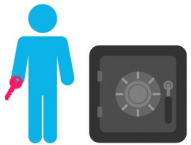
- Long touted as a threat to crypto fans, the 51% attack is concerning when using PoS, but there are doubts that it will happen. In PoS, **a group or individual would have to own 51% of the staked cryptocurrency.**
- **Controlling 51% of the cryptocurrency staked is very expensive.** Under Ethereum's PoS, if a 51% attack were to occur, honest validators on the network could vote to ignore the altered blockchain and burn the offender's staked ETH. This incentivizes validators to act in good faith for the benefit of the cryptocurrency and the network.

Courtesy : AnalyticsVidya

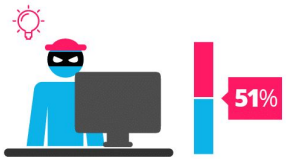
Consensus Mechanisms

Proof of Work vs Proof of Stake

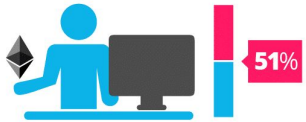
proof of work is a requirement to define an expensive computer calculation, also called mining



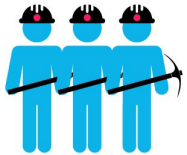
Proof of stake, the creator of a new block is chosen in a deterministic way, depending on its wealth, also defined as stake.



A reward is given to the first miner who solves each blocks problem.



The PoS system there is no block reward, so, the miners take the transaction fees.



Network miners compete to be the first to find a solution for the mathematical problem

Proof of Stake currencies can be several thousand times more cost effective.

Courtesy : Devopedia

Types of Consensus Mechanisms - Proof of Stake (PoET)

- used on permissioned blockchain networks,
- leverages trusted computing to enforce random waiting times for block construction.
- It was **developed by Intel** in early 2016,
- based on a special set of CPU instructions called **Intel Software Guard Extensions (SGXs).**
- **time-lottery-based consensus algorithm**

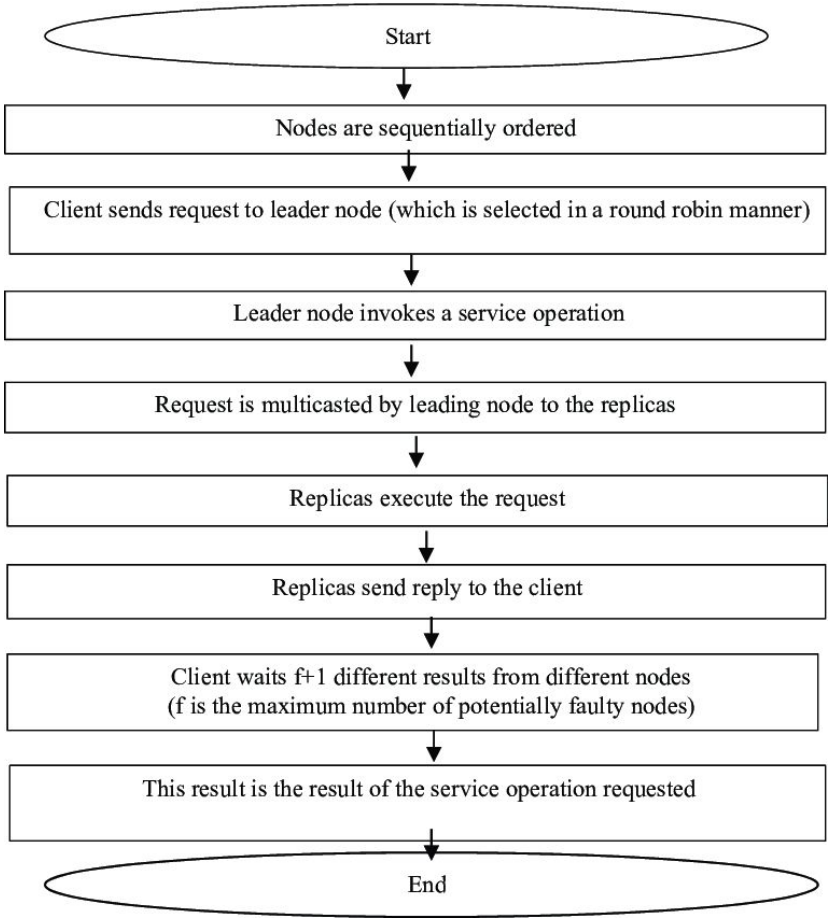
PoET Algorithm

1. randomly assigning different wait times to every node in the network.
2. During the waiting period, each of these nodes goes to 'sleep' for that specified duration.
3. The first to wake up (that is, the one with the shortest waiting time) is **awarded the mining rights.**

- This **randomisation guarantees that every participant is equally as likely to be the winner, ensuring fairness within the network.**
- highly efficient, less resource-intensive, and scalable.
- It has been implemented in **Hyperledger's Sawtooth.**

Courtesy : Crypto.com

Types of Consensus Mechanisms - Proof of Stake (PoET)



Courtesy : Research Gate

Types of Consensus Mechanisms - Proof of Stake (PoB)

- more sustainable alternative to Bitcoin's PoW algorithm is Proof of Burn (PoB),
- miners gain the power to mine a block by 'burning' (destroying) a predetermined amount of tokens in a verifiable manner — namely, sending them to an 'eater address' where they cannot be recovered or spent.
- The **more coins a miner burns, the greater their chances of being randomly selected.**
- **burned coins are irretrievable**.
- This method of requiring **miners to sacrifice short-term wealth in order to gain the lifetime privilege** of creating new blocks helps to encourage long-term commitment from miners.
- The act of burning coins also leads to coin scarcity, limiting inflation and driving up demand.
- Eg : Slimcoin (SLM), Counterparty (XCP), and Factom (FCT).

Courtesy : Devopedia

Compare Consensus Mechanisms - PoW, PoS, PoET, PoB

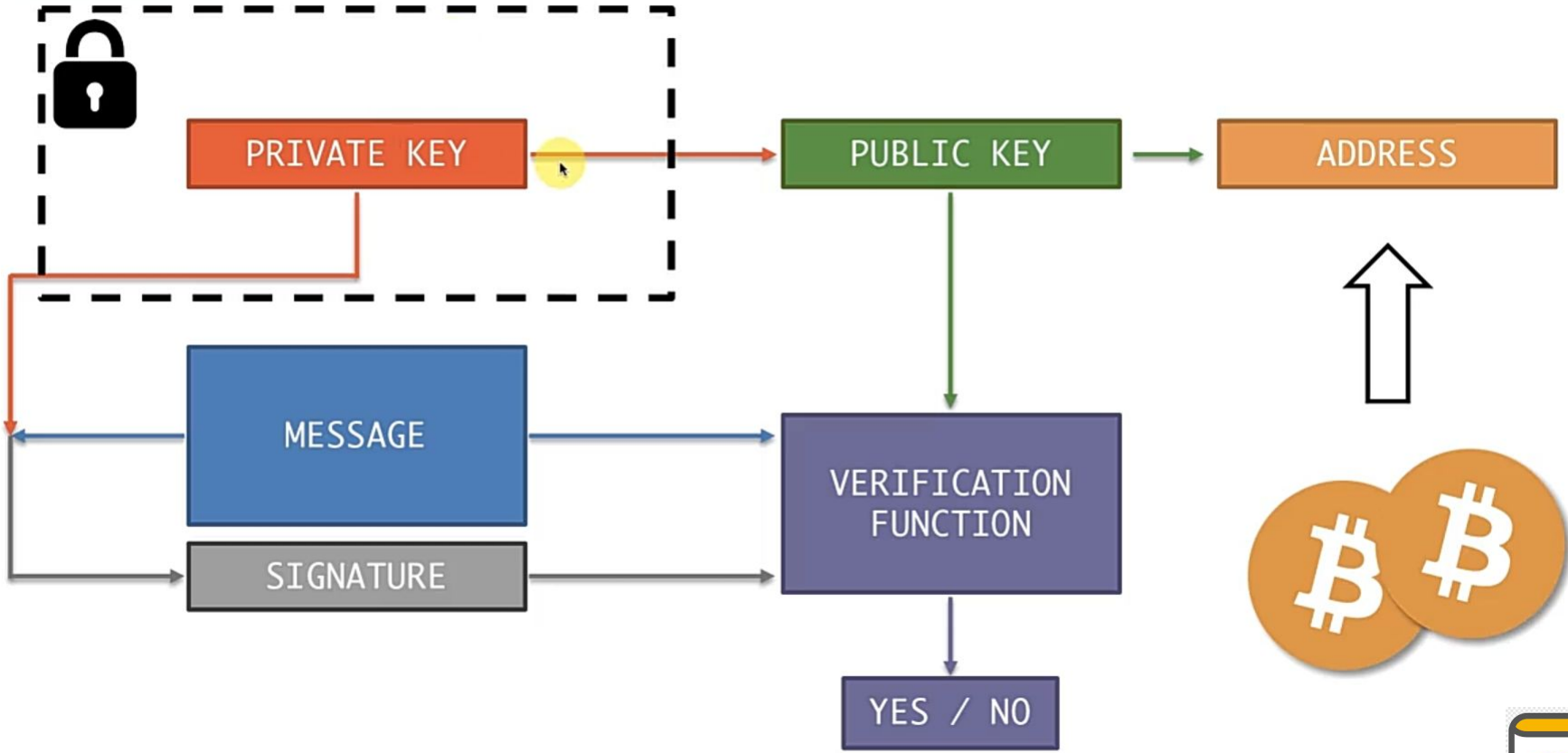
Proof of work (PoW)	Proof of stake (PoS) [11]	Proof of Burn (PoB)	PoET
Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level	Used for industries working on financial level
Using public key encryption (i.e. Bitcoin)	Using RSA algorithm for encryption	RSA algorithm for encryption	RSA algorithm for encryption
Miners having higher work done after investing higher power will have higher probability to mine the new block	It is some election type selection of miners for next block to be mined	PoB acquires some cryptocurrencies (wealth) to mine new block using virtual resource	Person spends some time and power to mine new block who finishes first the prior task will be the next miner
Power inefficient	Power efficient	Power efficient	Power efficient
Open environment	Open environment	Open environment	Open environment
Bitcoin script is used	Mostly Golong is used	Mostly Golong is used	

Courtesy : Research Gate

Extra Reading Materials

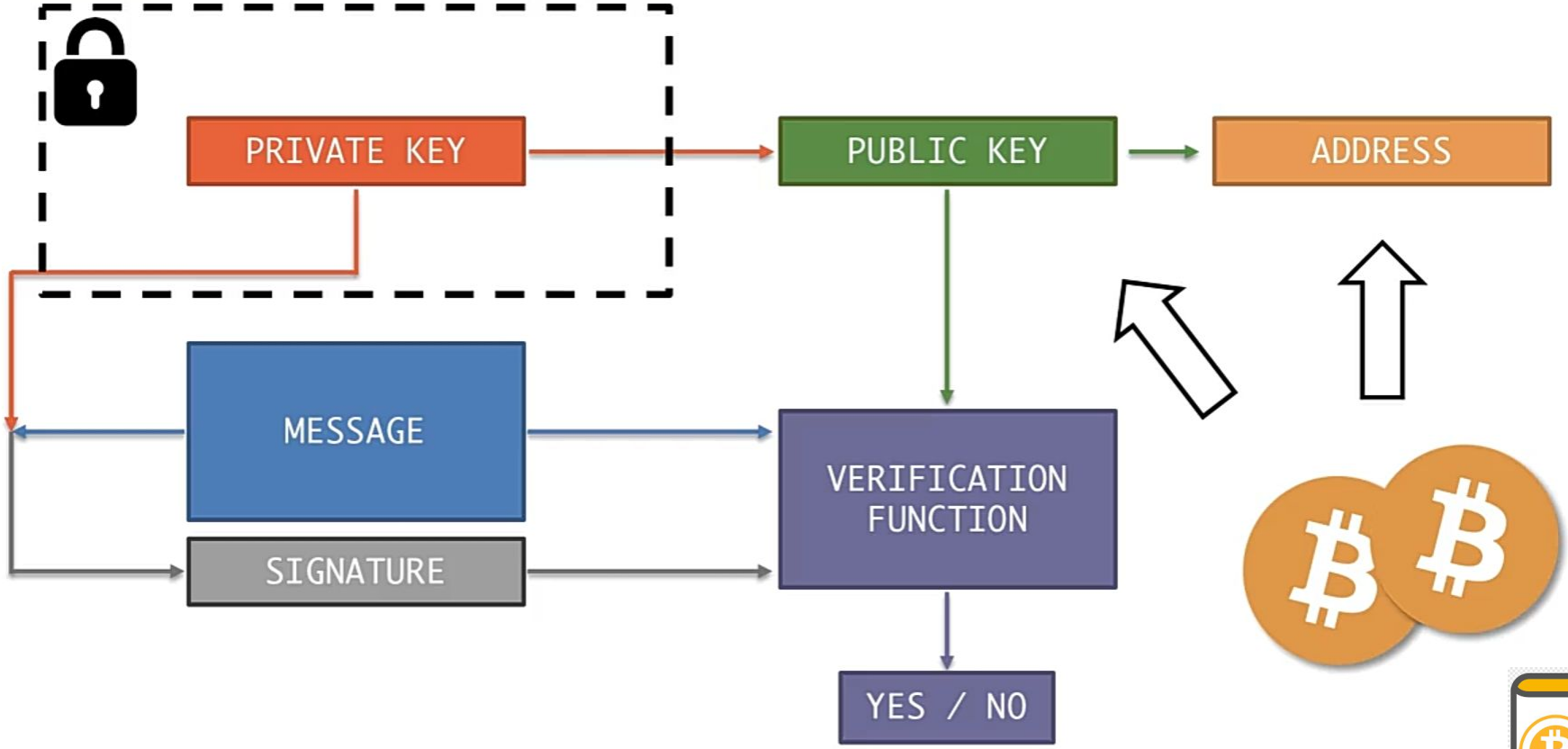
1. Public Key Vs Bitcoin Address
2. Hierarchical Deterministic (HD) Wallets - Demo
3. BIP - Bitcoin Improvement Proposal Demo
4. Consensus Mechanisms

Public Key Vs Bitcoin Address



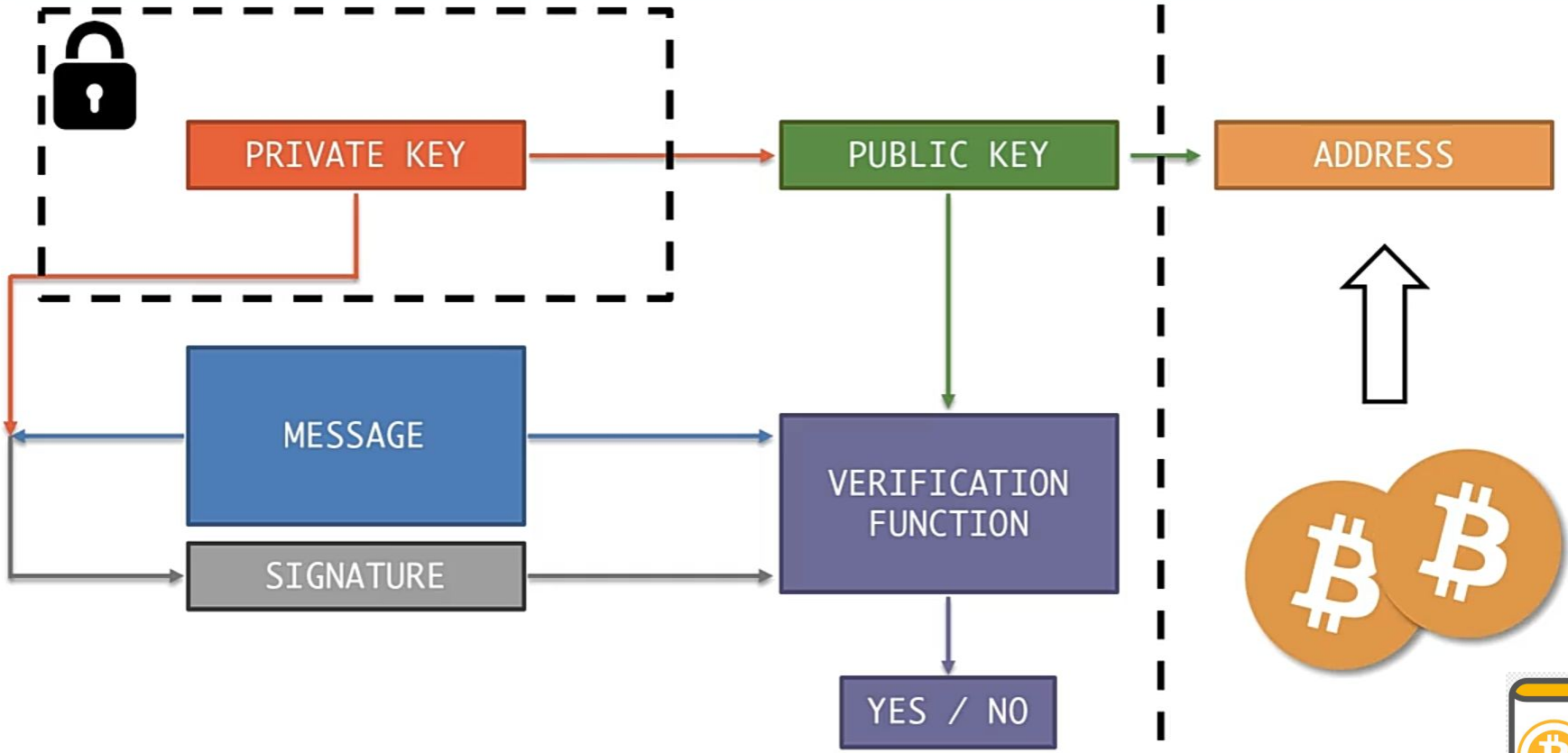
Courtesy : Super Data Science

Public Key Vs Bitcoin Address



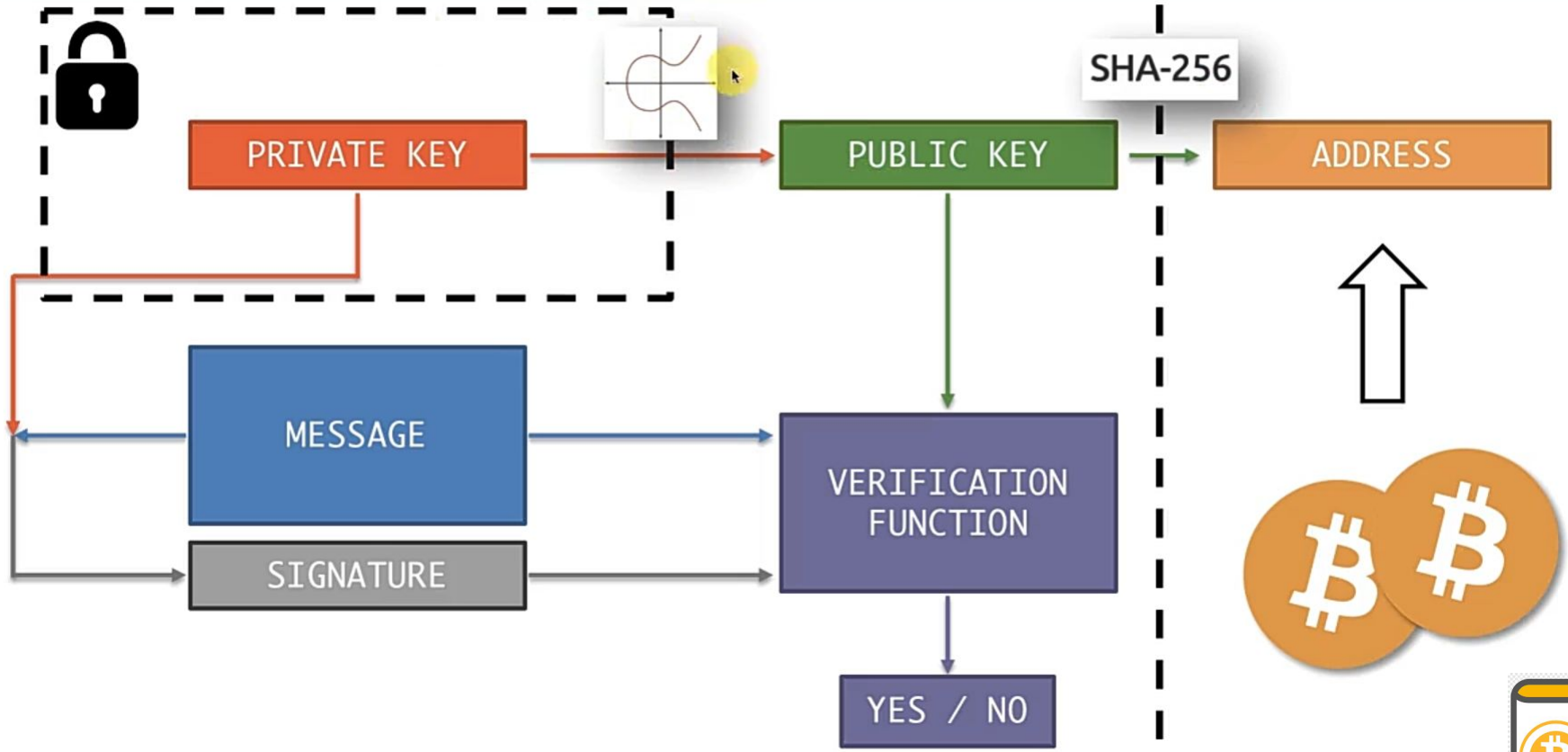
Courtesy : Super Data Science

Public Key Vs Bitcoin Address



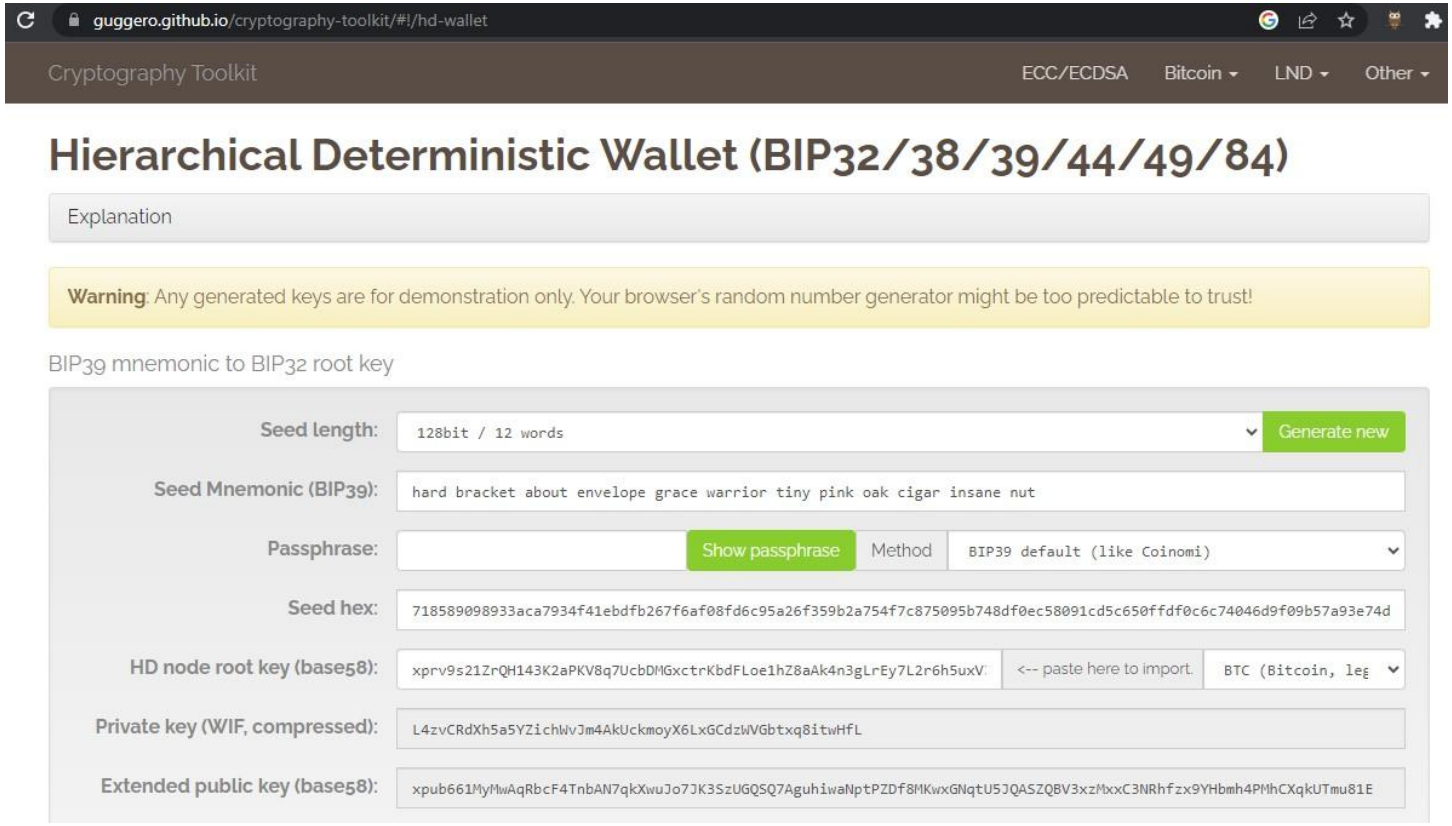
Courtesy : Super Data Science

Public Key Vs Bitcoin Address



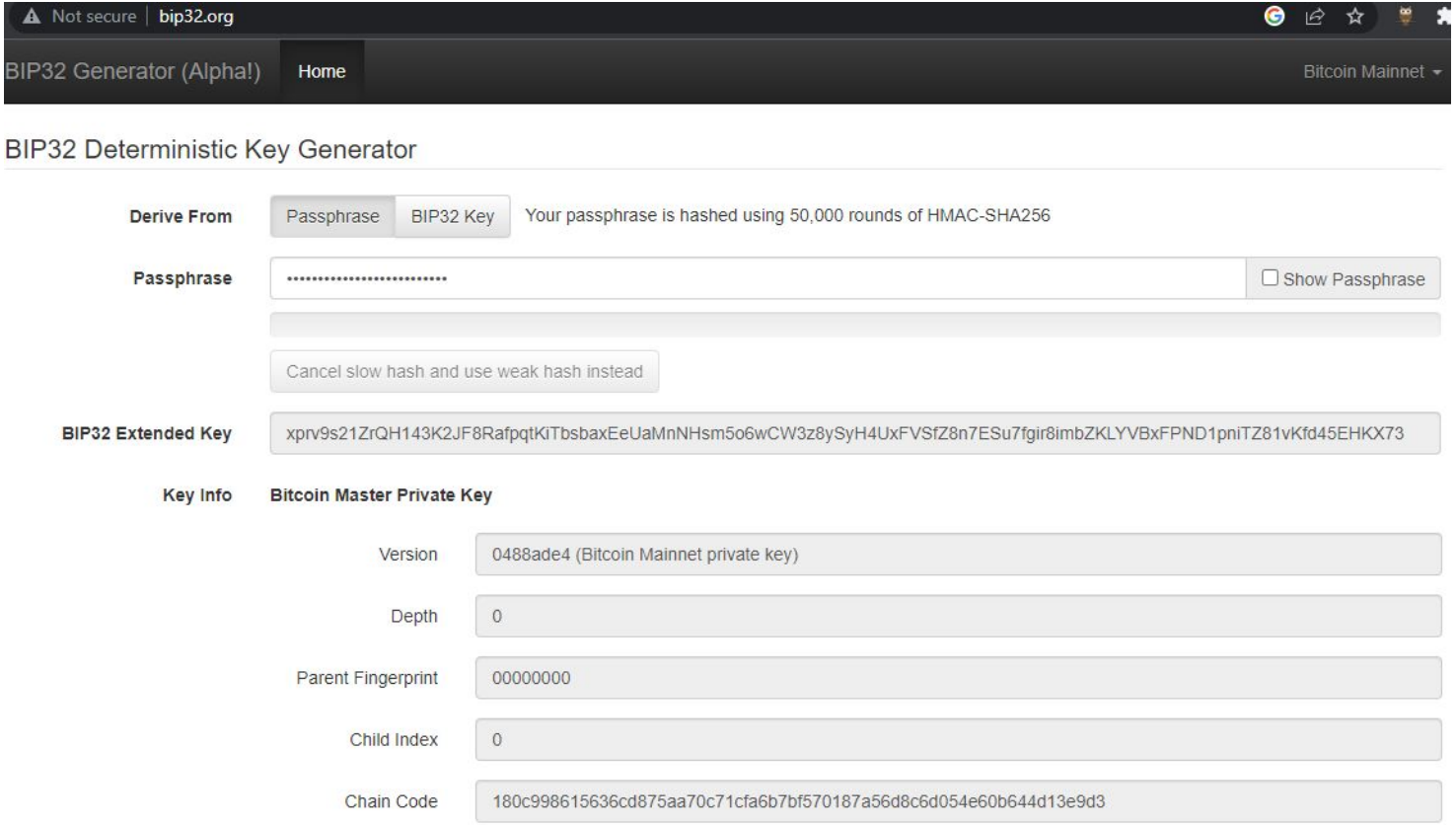
Courtesy : Super Data Science

Hierarchical Deterministic (HD) Wallets - Demo



Courtesy : [Cryptographic Toolkit]

BIP - Bitcoin Improvement Proposal



BIP 32 Demo

BIP - Bitcoin Improvement Proposal

BIP - 32

- **Introduced the standard of Hierarchical Deterministic (HD) wallets**
- improved the **interoperability of wallets**, as a set of **keys could be transferred between wallet software** with a single extended private key (xprv).
- **recoverability of wallets** was improved, **as a single seed could recover the entire wallet.** This improvement was **extended with BIP 39, which made seeds easier to store and remember.**
- **Enabled watch-only wallets**
  - to store and generate new addresses,
  - **allowing the user to receive payments**
  - **check their balances without ever needing to use private keys.**
  - Enhance a user's security by allowing them to **keep their private keys in cold storage**, while continuing **to receive bitcoin, track balances, and craft transactions**.

Github : BIP 32

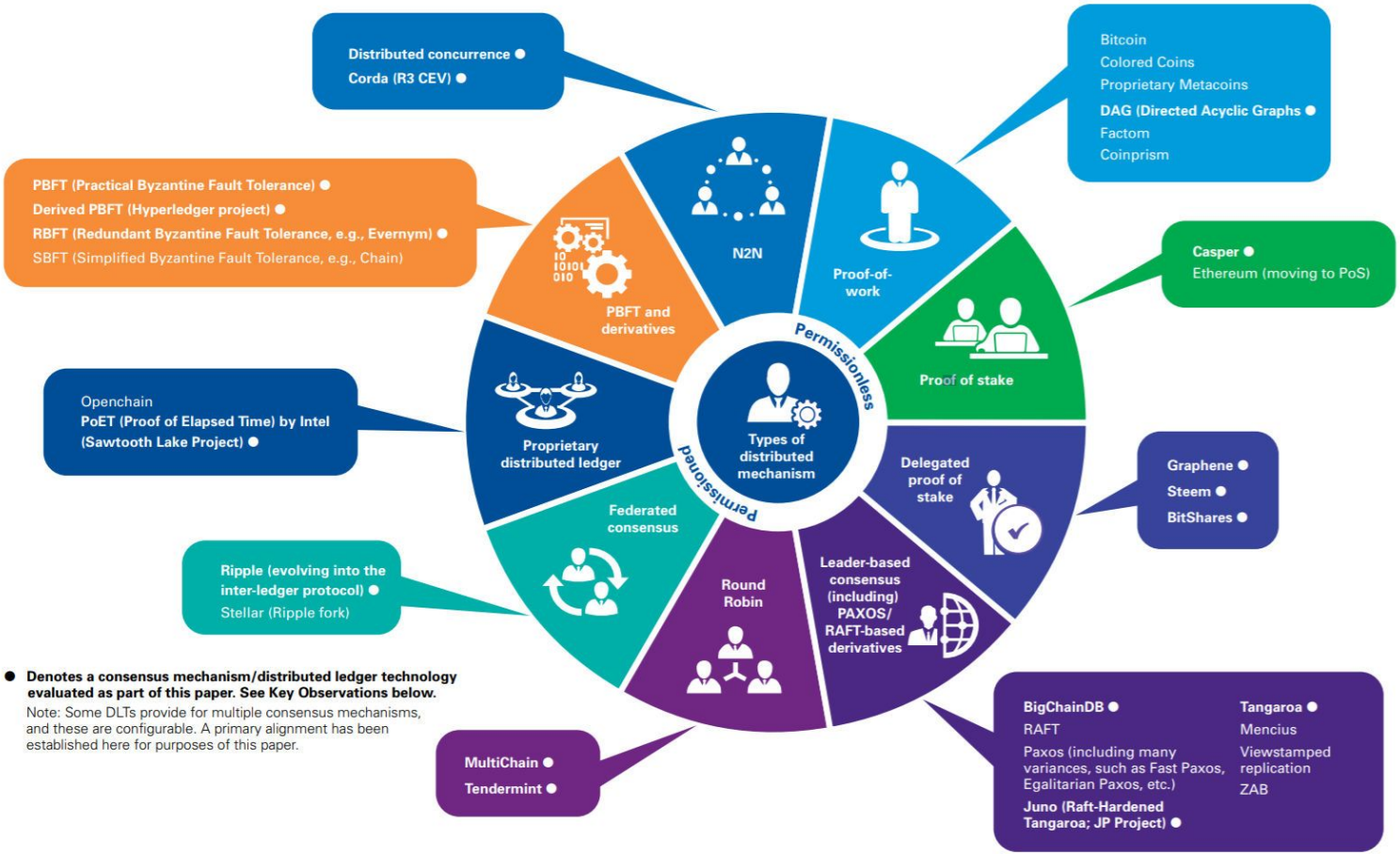
BIP - Bitcoin Improvement Proposal

BIP - 39

- **standardized set of words for the recovery and backup of a bitcoin or cryptocurrency wallet**.
- **Each word in the list is unique** within the first four letters of each word, meaning no two words on the list share the same first four letters.

Github : BIP 39,

Consensus Mechanisms



Courtesy : Devopedia

Consensus Mechanisms

PROOF OF WORK (PoW)
- PoW lets miners add a new block to the network based on the computation done to find the correct block hash.

PROOF OF STAKE (PoS)
- PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition.

DELEGATED PROOF OF STAKE (DPoS)
- In DPoS mechanism, the block delegates' selection is based on voting. It's an additional layer to PoS.

PROOF OF IMPORTANCE (PoI)
- PoI rewards users with importance scores which eventually helps them to become block harvesters.

PROOF OF CAPACITY (PoC)
- PoC uses the storage capacity for mining a block in a decentralized network.

PROOF OF ELAPSED TIME (PoET)
- PoET uses a time-lottery-based consensus mechanism, distributing wait time to each participating node.

PROOF OF ACTIVITY (PoA)
- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.

PROOF OF AUTHORITY (PoA)
- Proof of Authority (PoA) relies on the validator's reputation to make the blockchain work properly.

PROOF OF BURN (PoB)
- PoB allows miners to add their block by sending some of their coins to an unspendable account.

BYZANTINE FAULT TOLERANCE (BFT)
- BFT works on system to stay intact even if one of the nodes fails with constant communication among nodes.

Courtesy : Devopedia

Thank you