Blockchain Honor Degree Sem VII

HBCC 601 : Blockchain Platforms

Module - 2 : Public Blockchain
(6 Hours)

Instructor : Mrs. Lifna C S

Topics to be covered

- **Introduction to Public Blockchain**
- **Characteristics of Public Blockchain,**
- **Advantages of Public Blockchain**
- **Examples of Public Blockchain**
  - **Bitcoin: Terminologies and Transaction**
  - Ethereum: Smart contract (Already covered in Module 1)
- **Comparison of Bitcoin and Ethereum,**
- **Other public Blockchain platforms**

Self-learning Topics: Study any one case study on a public blockchain

Introduction to Public Blockchain

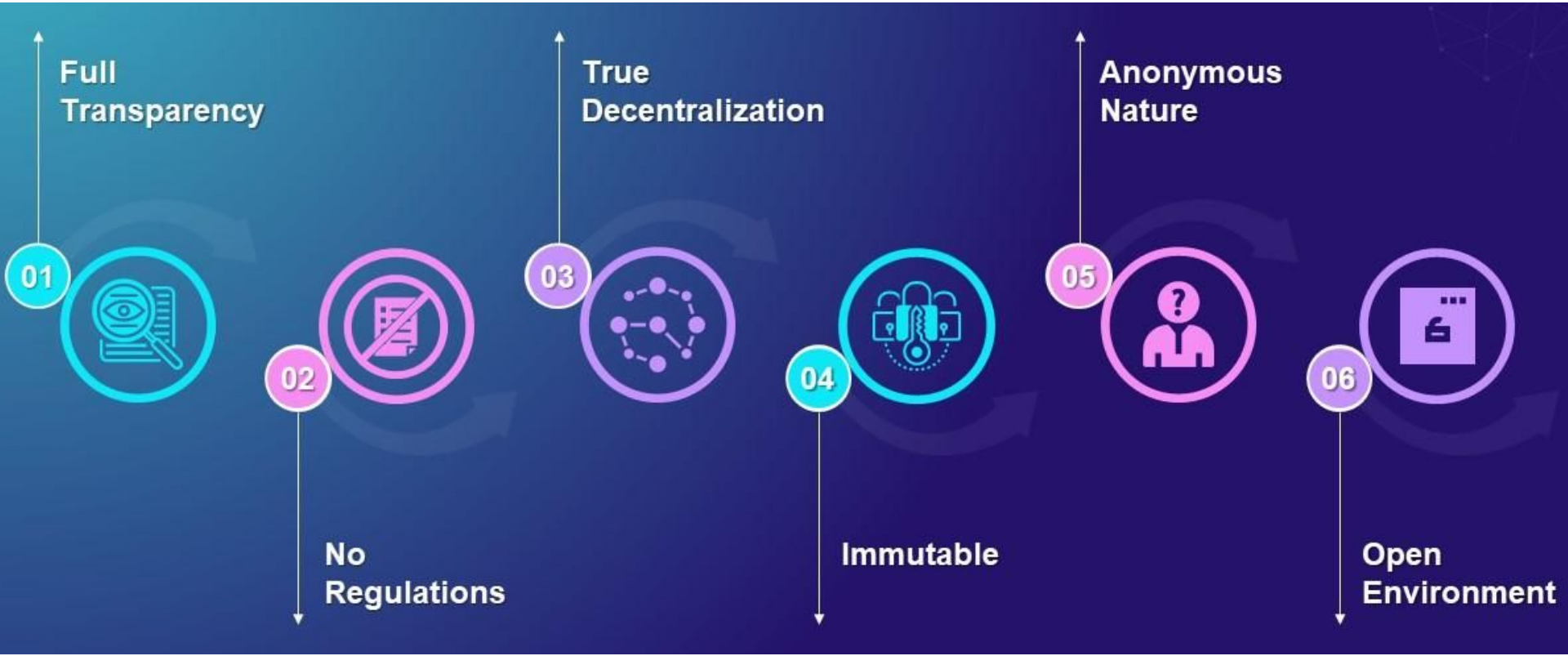
- **does not have restrictions.**
- **Anyone with an internet connection can get access to the network** and **start validating blocks and sending transactions.**
- Offers incentive for users who validate the blocks.
- The network tends to use **Proof of Work or Proof of Stake consensus algorithms** for validating the transactions.
- It is a “Public” network in a true sense.
- It was the model that **Satoshi Nakamoto suggested back in 2009**.
- Later, enterprise companies, tweaked the nature of the decentralized ledger and introduced the private blockchains.
- Anyone can download the protocol anytime, without any permission from anyone.
- **it’s completely decentralized, no single organization controls the ecosystem.**
- Whereas, a private blockchain can be changed and altered by the owning organization.
- A public blockchain surpassed the necessity of a third party.
- A **self-governed, purely decentralized and autonomous digital public ledger.**

Courtesy : 101 Blockchain

Introduction to Public Blockchain - Characteristics

- It is an **open network and permissionless**
  - where nodes can join and leave without the permission of anyone.
  - Every node **has access to read and write on the ledger**
  - Anyone can download and add nodes to the system
  - the ledger is shared and transparent.
- Includes a **protocol of incentive mechanism**
  - to ensure the correct operation of the blockchain system.
- It is **secure to the 51% rule.**
- It **offers anonymity**, which means no one can track your transactions back to you
- **No regulation** hence no limit to how one can use the platform for betterment.
- The technology is **fully decentralized in nature**
- **Everyone can change current business models** through the reduction in the use of middlemen.
- It is **not necessary to maintain servers or system administrators**.
- Hence there is **considerable cost reduction for the businesses**.

Introduction to Public Blockchain - Characteristics



Courtesy : Slide Team

Introduction to Public Blockchain - Advantages

- **Transparency**:
  - Public blockchains are transparent and open for everyone to access.
  - This makes the ledger accessible to all,
  - eliminating chances of corruption and ensuring transparency.
- **Security:**
  - Public blockchains are designed to operate with maximum security.
  - The decentralized nature of the network makes it difficult for hackers to compromise the system.
- **Empowerment:**
  - Allows all participants to validate transactions without any central authority overlooking their actions.
- **Immutability:**
  - meaning no one can tamper with the system, ensuring that transactions are secure.

Courtesy : Geeks4Geeks

Introduction to Public Blockchain - Disadvantages

- **Power Consumption:**
  - require a lot of computational power due to their decentralized nature.
  - This increases energy consumption and can be detrimental to the environment.
- **Scalability:**
  - With more users on the blockchain, the network becomes burdened with more transactions, leading to scalability issues.
- **Conspiracy:**
  - Due to decentralized nature, no one knows who validates the transactions,
  - increasing the risk of potential conspiracy.
- **Transactions:**
  - Can be slow due to the time it takes to process all transactions on the network.
- **Acceptance:**
  - Due to the openness and transparency, it can be difficult for governments to accept them as they are not controlled by authorities

Courtesy : Geeks4Geeks

Examples of Public Blockchain - Bitcoin

- "A **decentralized digital currency** enables instant payments to anyone, anywhere in the world"
- No central authority,
- uses peer-to-peer technology

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 - Key Feature

- **Decentralization:**
  - Operates on a peer-to-peer network of computers, known as nodes.
  - Eliminates the need for a central authority, allowing transactions to be conducted directly between users.
- **Blockchain Technology:**
  - Bitcoin transactions are recorded on a public ledger called the blockchain.
  - The blockchain is a distributed and immutable database that ensures transparency and security.
- **Limited Supply:**
  - Bitcoin has a capped supply of 21 million coins, which creates scarcity.
  - To control inflation and mimic the scarcity of precious metals like gold.
- **Mining**:
  - Bitcoin transactions are verified and added to the blockchain through a process called **mining.**
  - This involves solving complex mathematical problems, and miners are rewarded with newly created bitcoins for their efforts.

Bitcoin - Key Features

- **Security:**
  - Bitcoin **uses cryptographic techniques** to secure transactions and control the creation of new units.
  - The decentralized nature of the network and the robustness of the underlying blockchain make it **resistant to censorship and fraud.**
- **Anonymity**:
  - While Bitcoin transactions are recorded on the public blockchain, users are identified by cryptographic addresses rather than personal information.
  - This provides a level of **privacy**, although it's not entirely anonymous.
- **Volatility:**
  - Bitcoin's value can be **highly volatile,** with its price subject to market demand and speculation.
  - This volatility has both attracted traders and investors seeking profit opportunities and **raised concerns about its use as a stable store of value.**

Bitcoin - Pros & Cons

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

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.

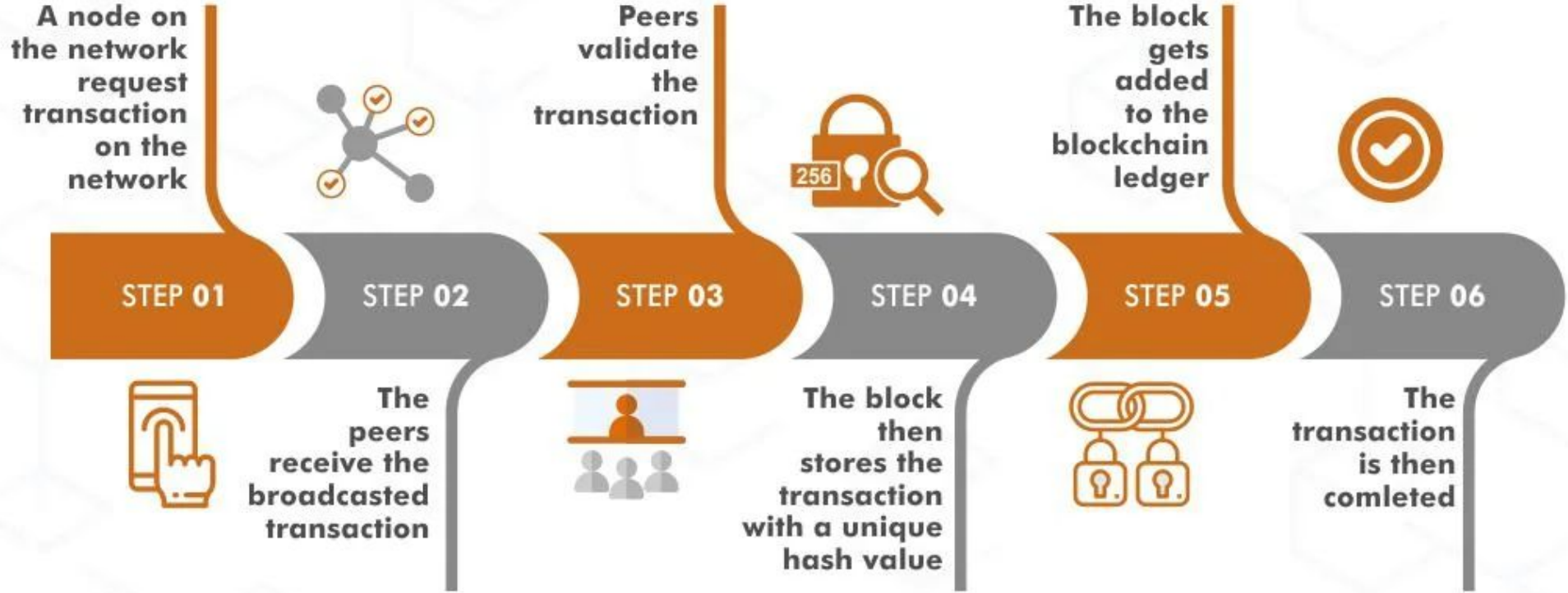
Courtesy : Ledger.com

Bitcoin - Properties of Transactions

- **Permissionless and borderless.** The software can be installed by anybody worldwide.
- **Anonymous.** Bitcoin does not require any ID to use making it suitable for the unbanked, the privacy-conscious, computers or people in areas with underdeveloped financial infrastructure.
- **Private**. When used with care bitcoin can support strong financial privacy.
- **Censorship-resistant.** Nobody is able to block or freeze a transaction of any amount.
- **Fast.** Transactions can be made almost as fast as data can travel over the Internet.
- **Cheap.** Fees can be very very low.
- **Irreversible** once settled, like cash. (but consumer protection is still possible.)
- **Online and available 24 hours a day, 365 days per year.**

Courtesy : Bicoin - Wiki

Transactions 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

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

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
TX	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
TX	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
TX	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
TX	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
TX	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
TX	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
TX	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 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)

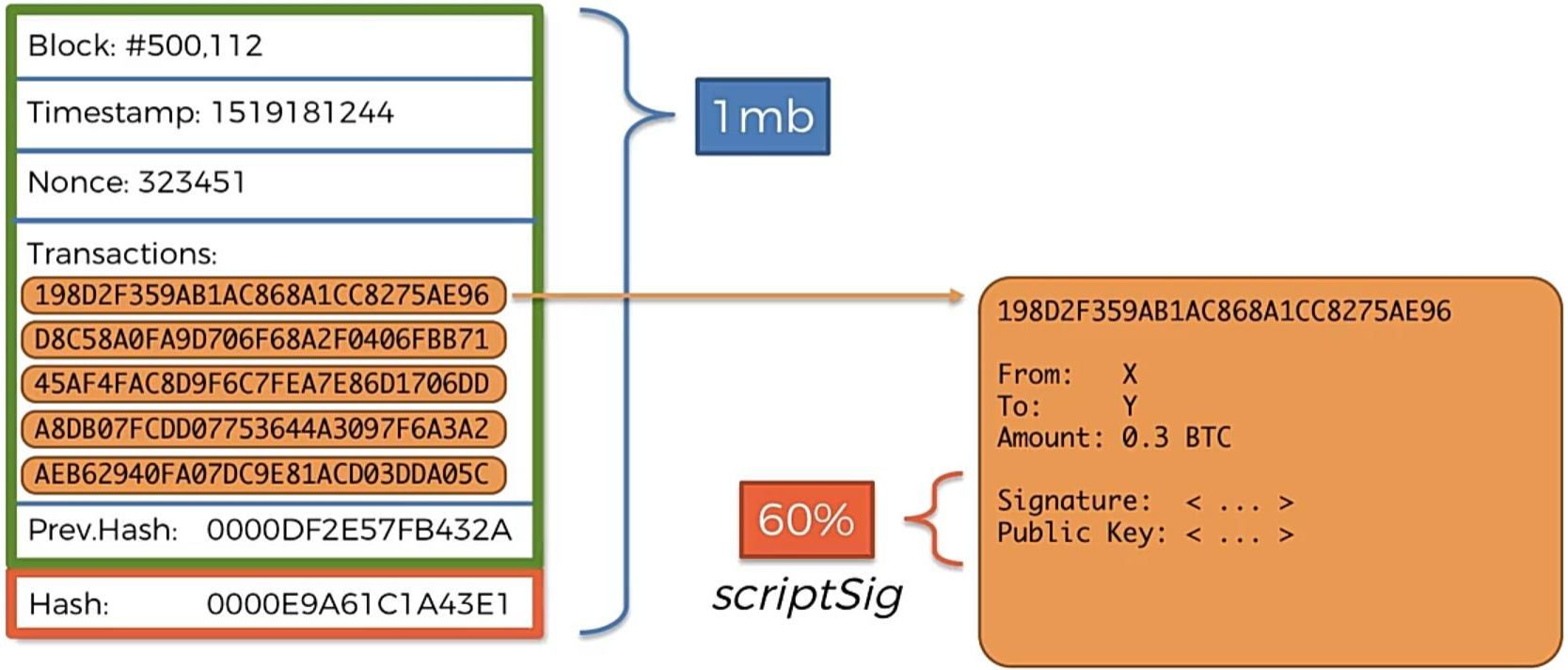
- collected 50 BTC as thousands of UTXO as TxInputs
- Pay the purchaser as one UTXO
- Pay higher TxFees as there are many small TxInputs so that transaction is processed promptly.

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 = 0000000000000000005d97dc0000000000000000000000000000000000000000

Max target = 00000000FFFF0000000000000000000000000000000000000000000000000000

Difficulty is adjusted every 2016 blocks (2 weeks)

Current target = 0000000000000000005d97dc0000000000000000000000000000000000000000

18 zeros

Let's do some estimations:

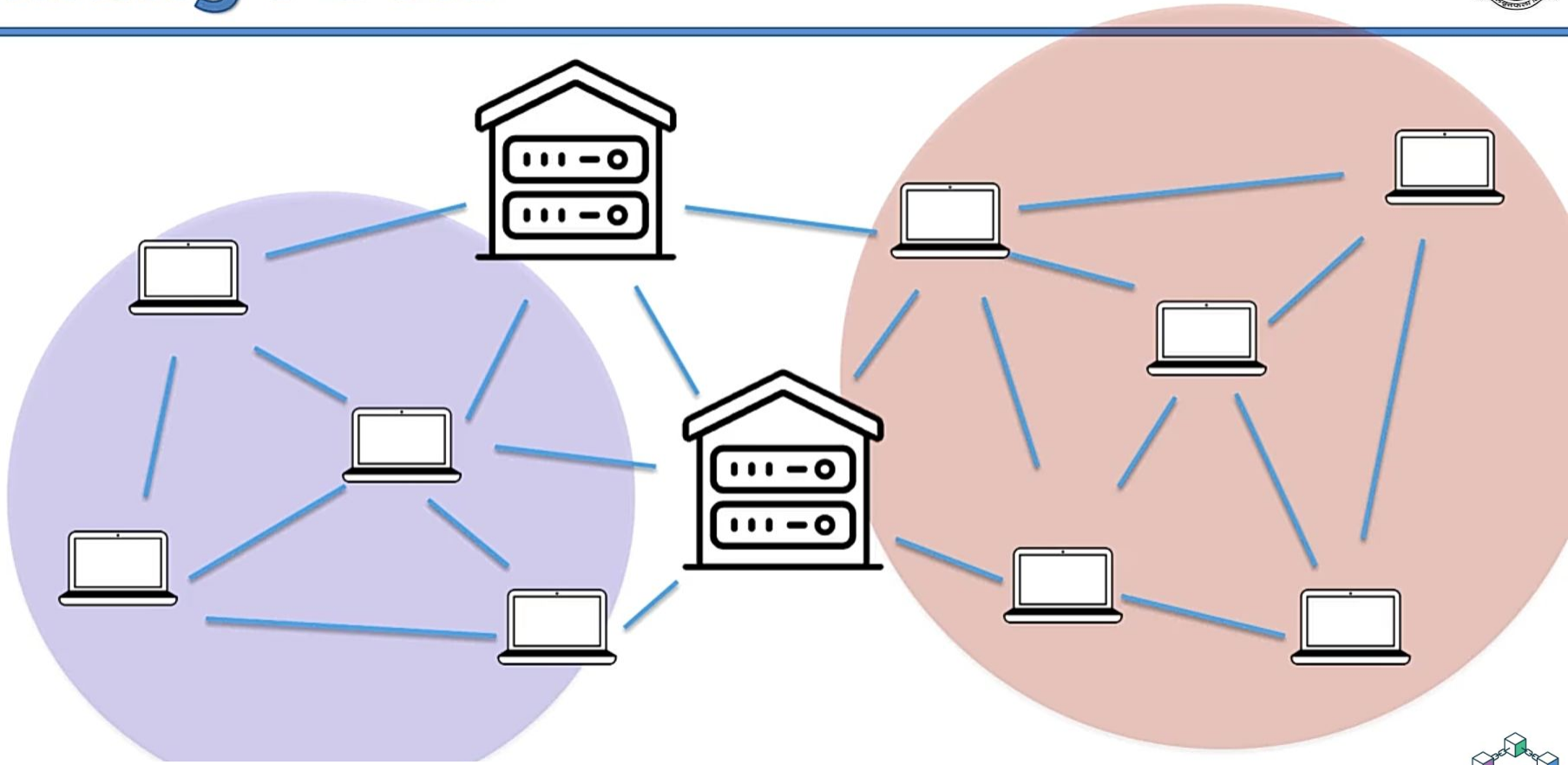
Probability:

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): $16 \times 16 \times \ldots \times 16 = 16^{64-18} \approx 2.4519 \times 10^{55} \approx 2 \times 10^{55}$

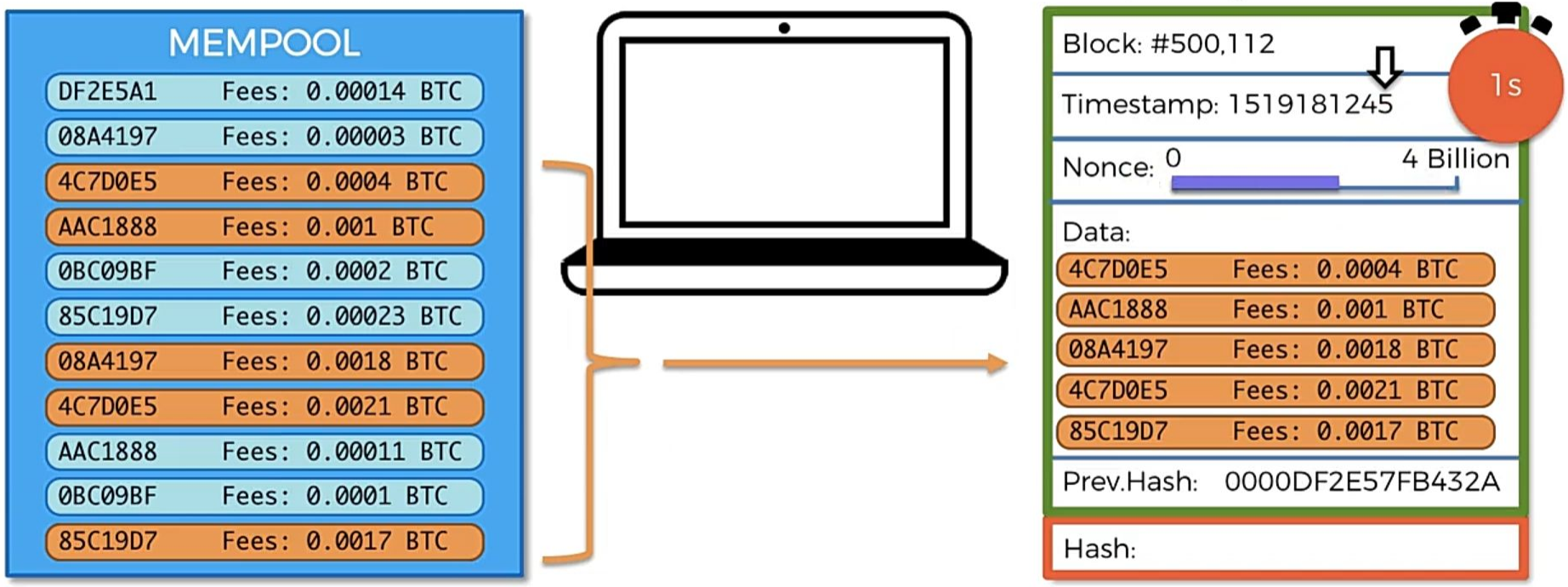
Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Mining Pools

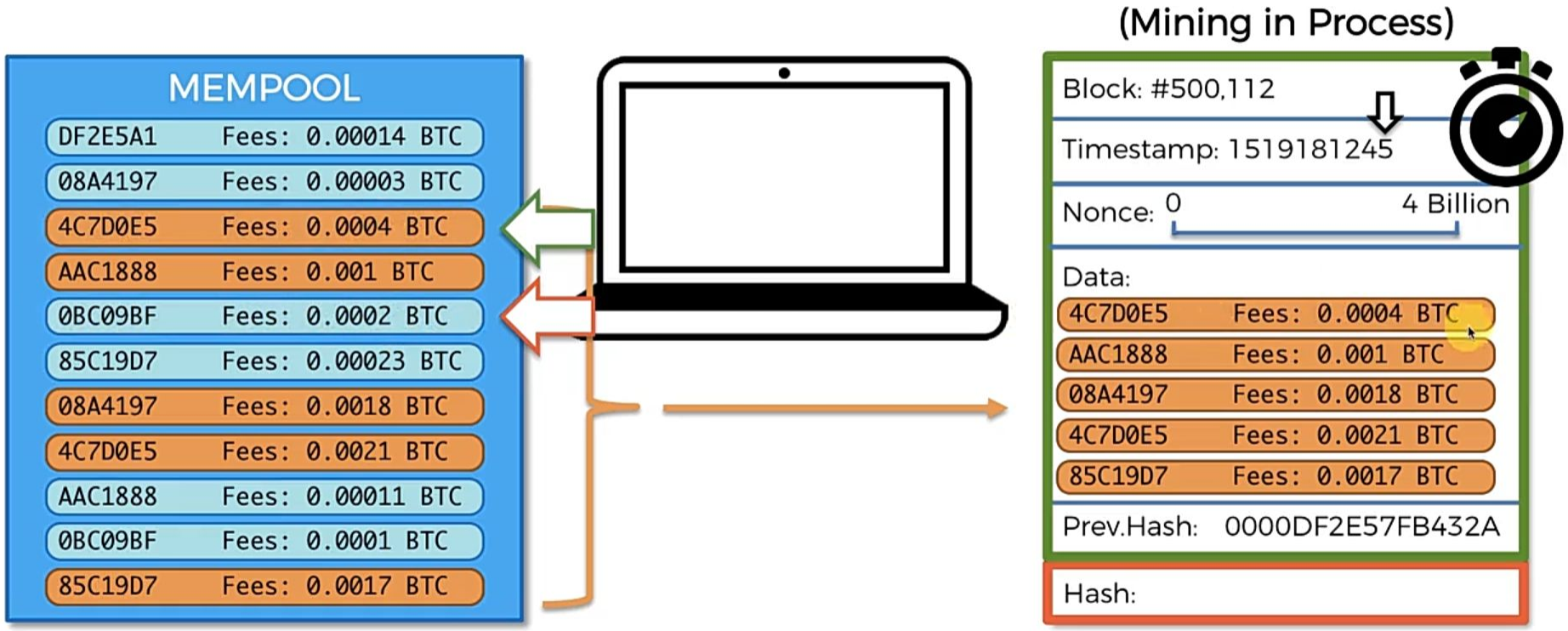


Courtesy : Super Data Science

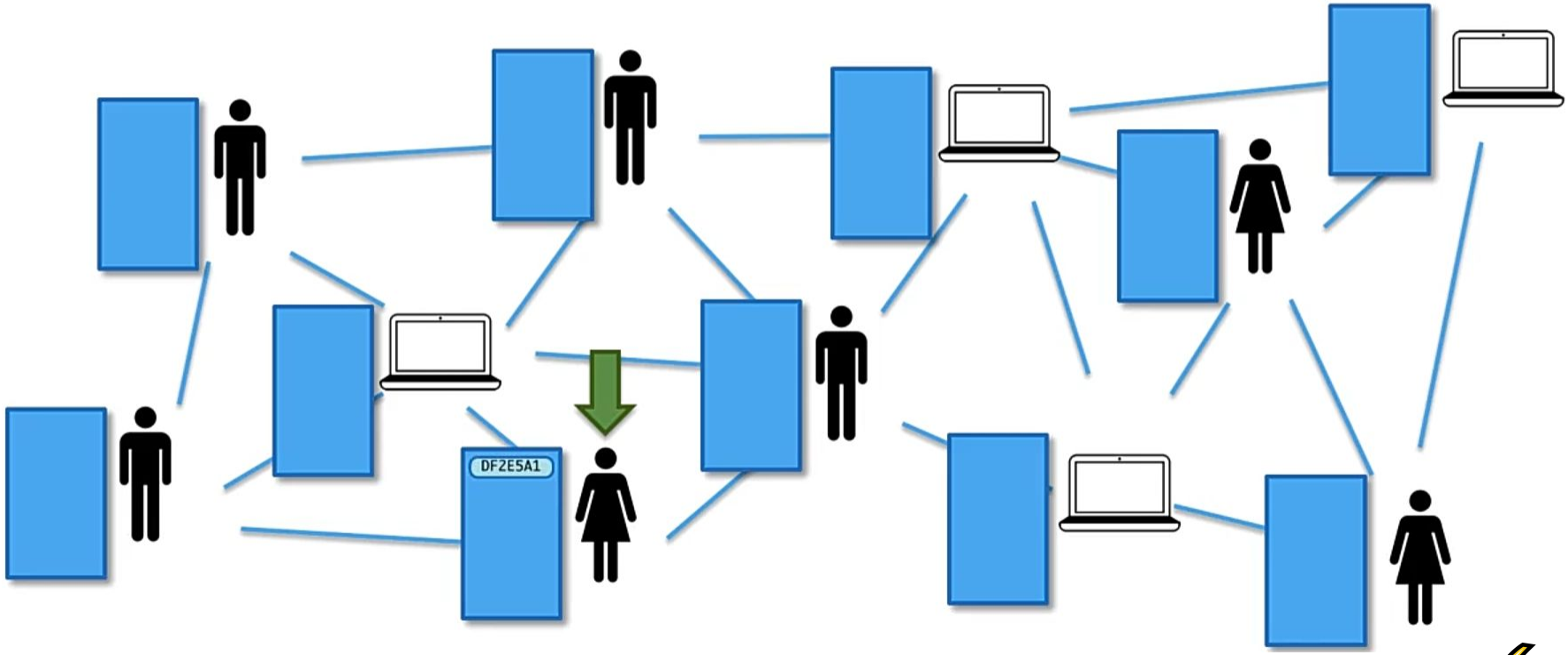
How Miners Pick Transactions



How Miners Pick Transactions

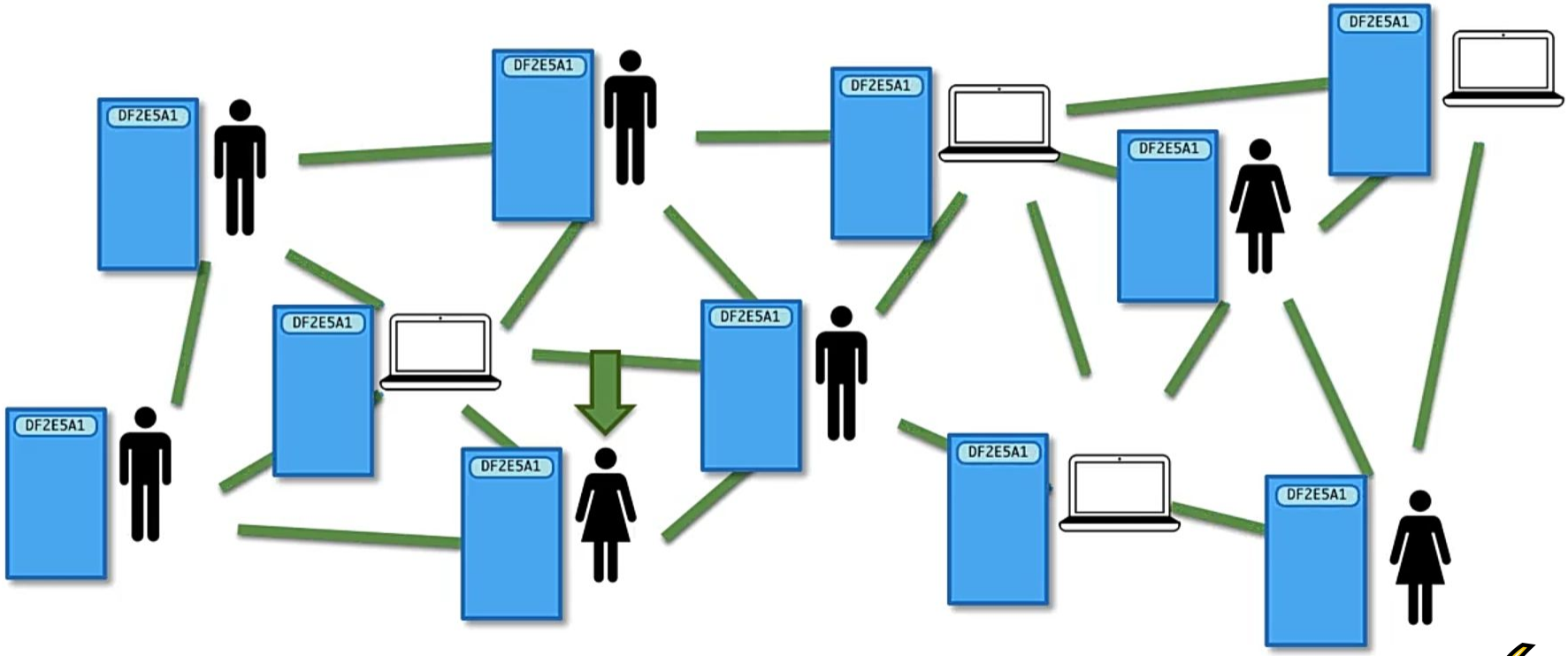


How do Mempools work?



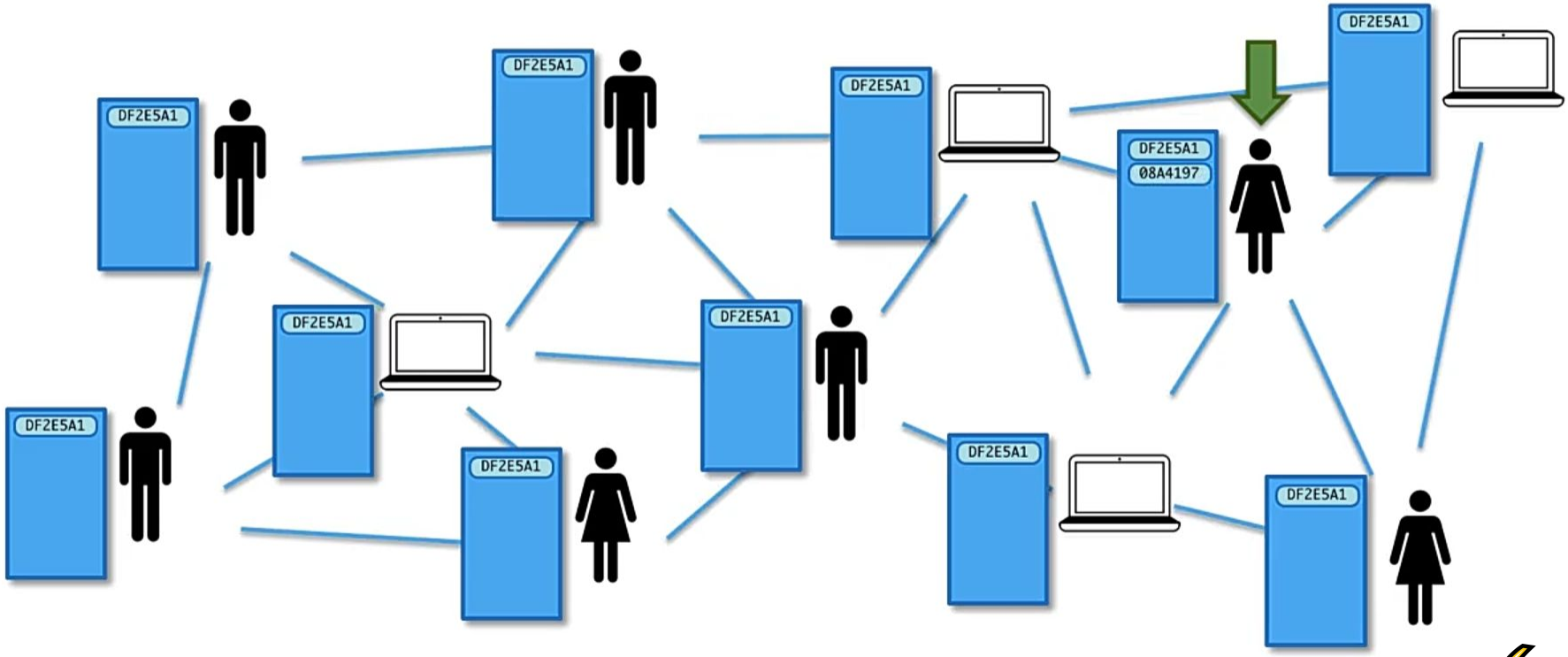
Courtesy : Super Data Science

How do Mempools work?



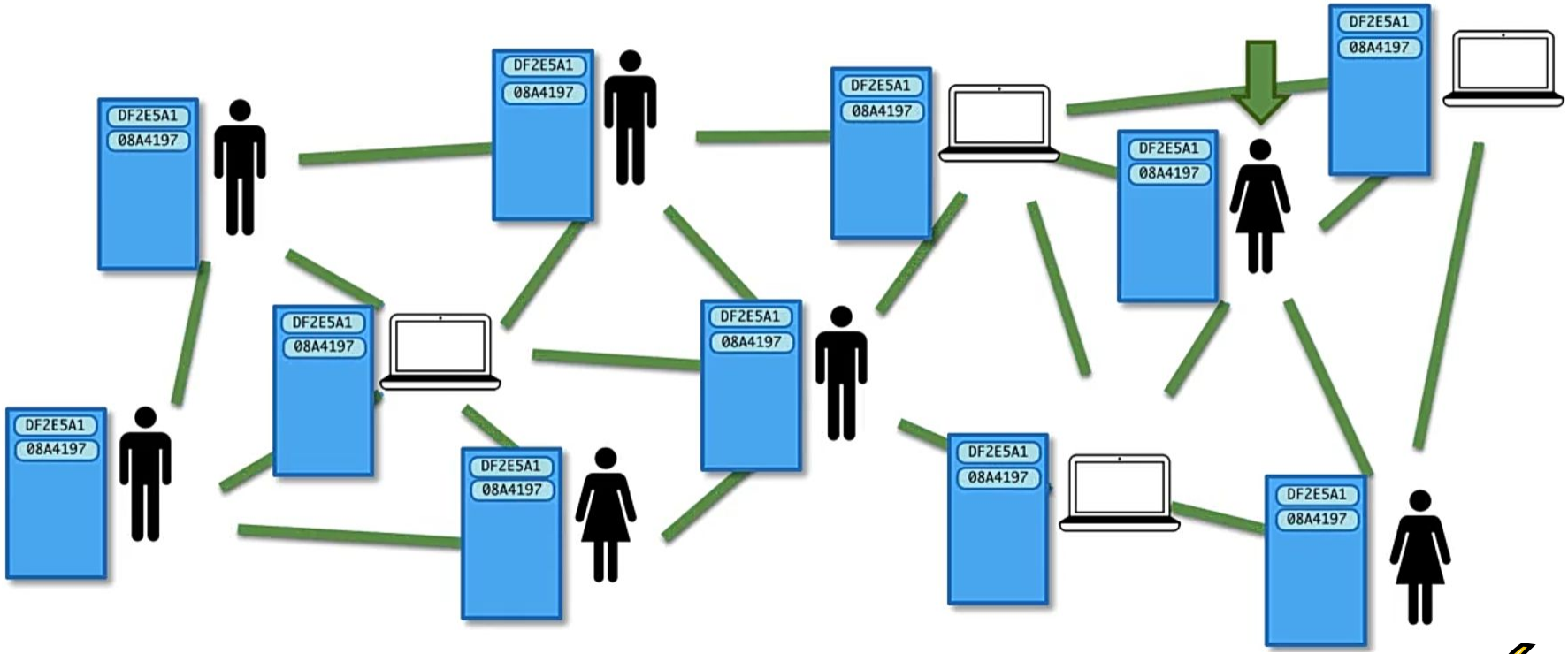
Courtesy : Super Data Science

How do Mempools work?



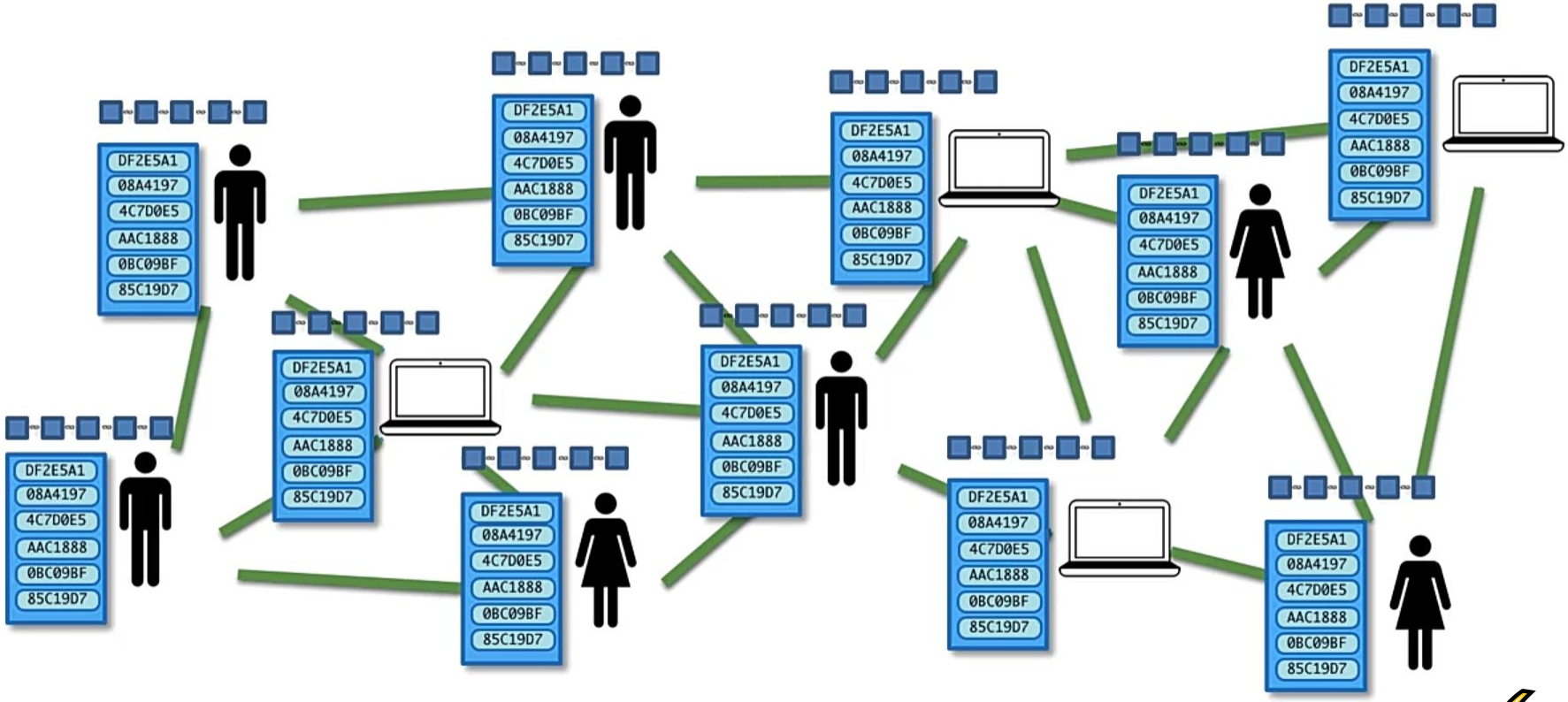
Courtesy : Super Data Science

How do Mempools work?



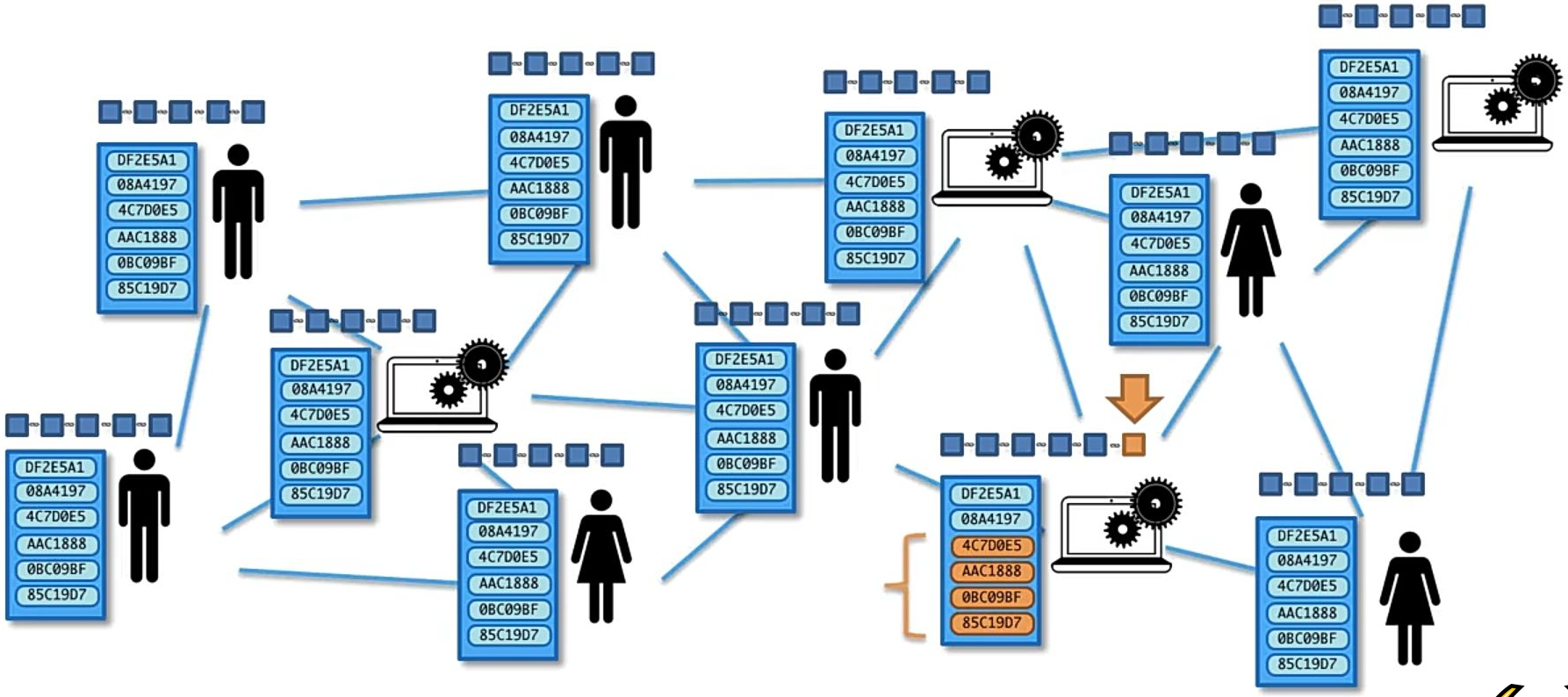
Courtesy : Super Data Science

How do Mempools work?



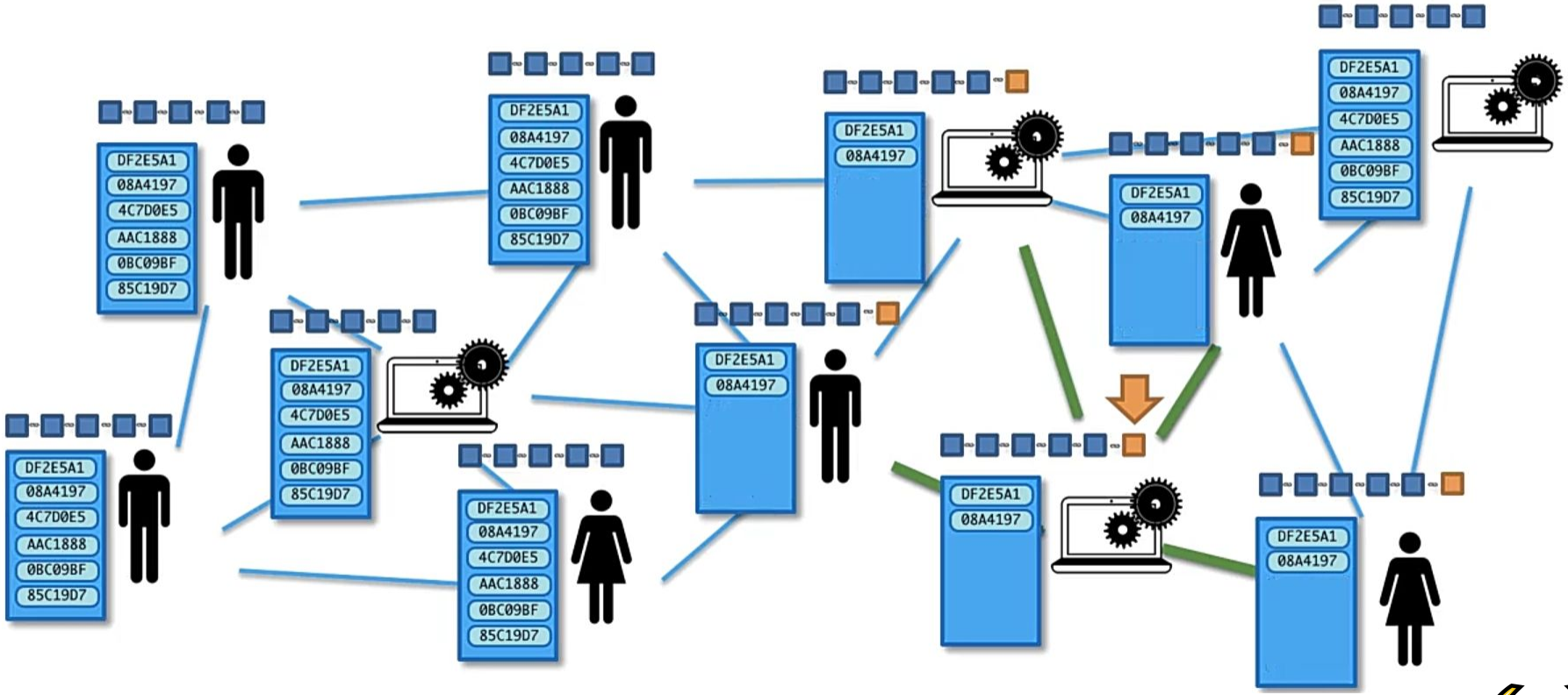
Courtesy : Super Data Science

How do Mempools work?



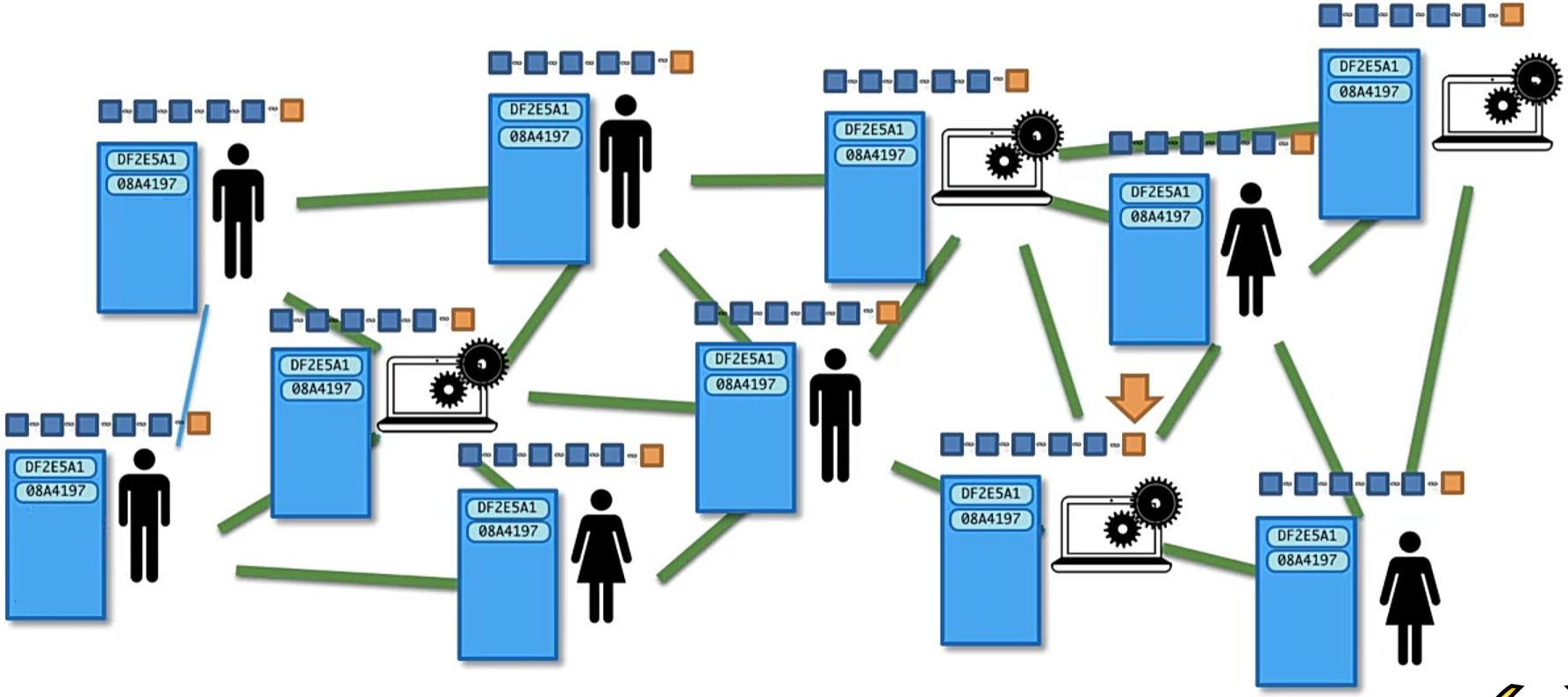
Courtesy : Super Data Science

How do Mempools work?



Courtesy : Super Data Science

How do Mempools work?



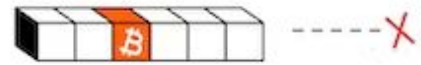
Courtesy : Super Data Science

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.

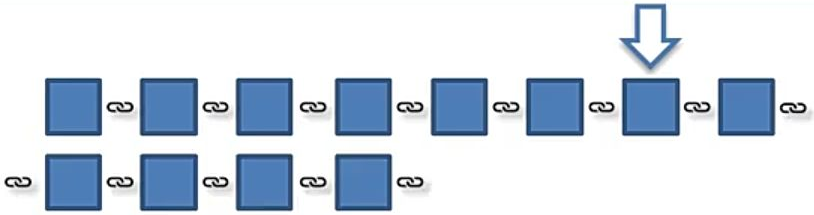
Courtesy : BitPanda

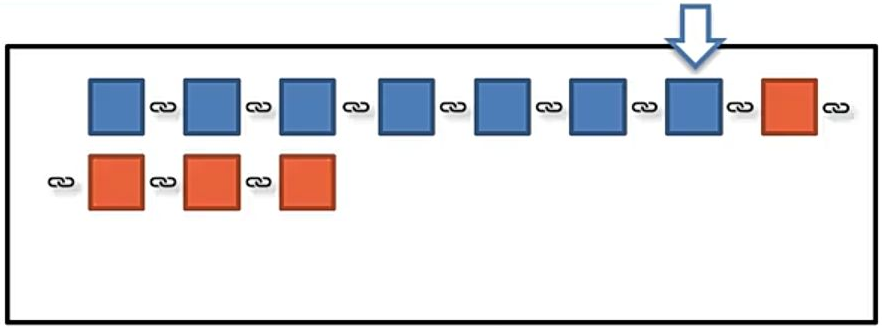
Double Spending Problem

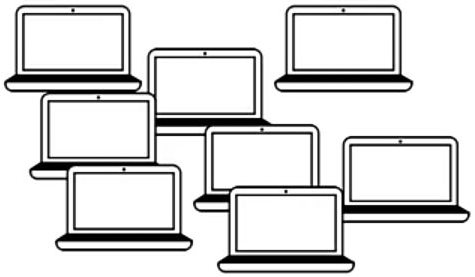
- **Risk that a cryptocurrency can be used twice or more.**
- **Transaction information** within a blockchain **can be altered if specific conditions are met**.
  - The conditions allow modified blocks to enter the blockchain;
  - if this happens, the person that initiated the alteration can reclaim 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.

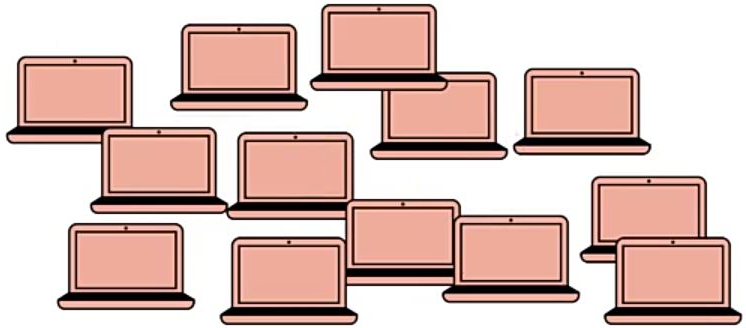
Courtesy : Investopedia

The 51% Attack

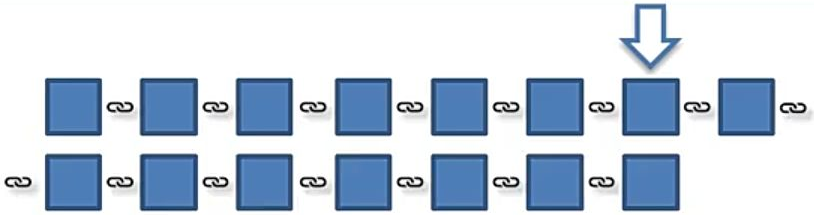


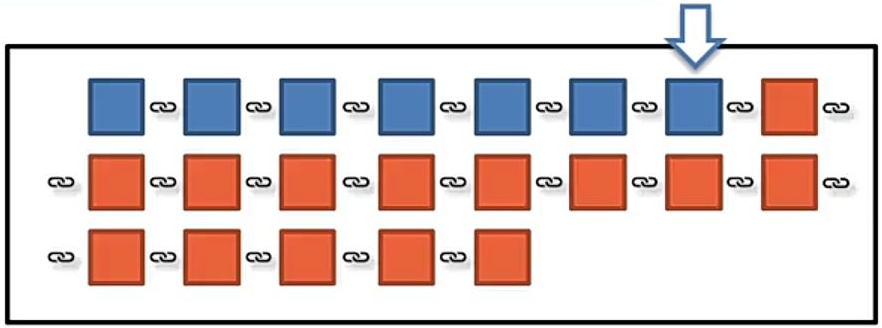


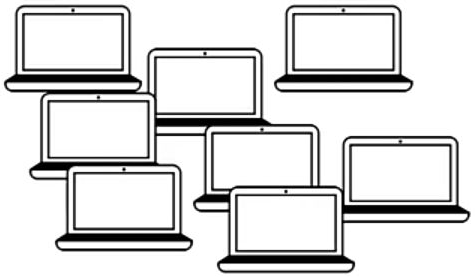


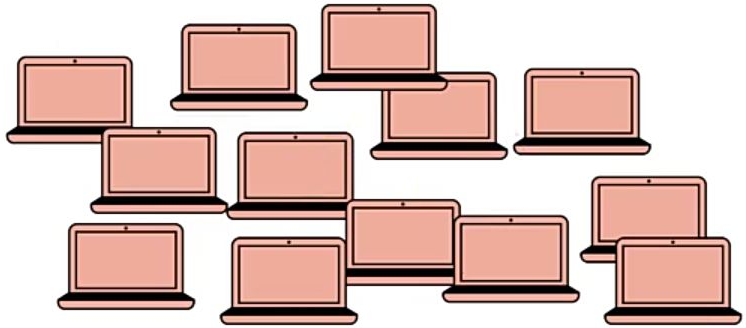


The 51% Attack

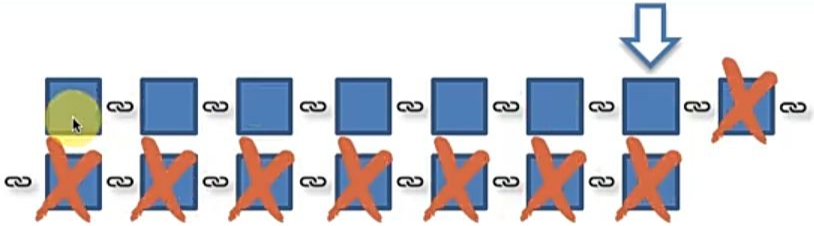


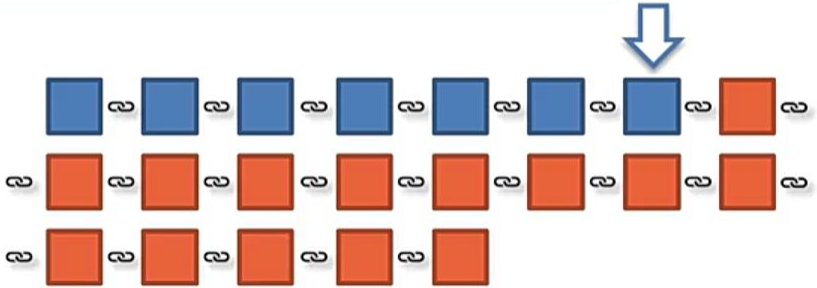


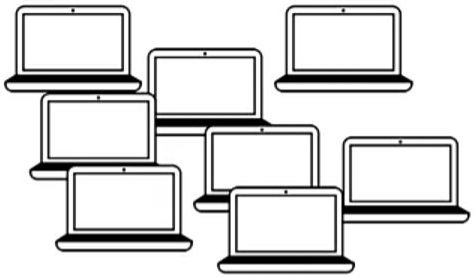


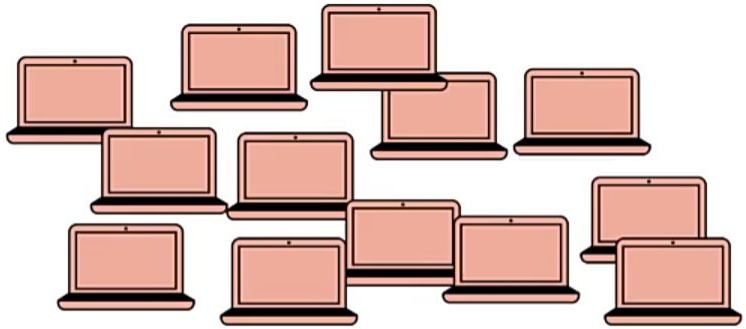


The 51% Attack









Ethereum Vs Bitcoin

Basis	Bitcoin	Ethereum
Smart Contracts	Although bitcoin do have smart contracts, they are not as flexible or complete as Ethereum smart contracts. Smart contracts in Bitcoin does not have all the functionality that a programming language would give them.	Ethereum allows us to create smart contracts. Smart contracts are computer codes that is stored on a blockchain and executed when the predetermined terms and conditions are met.
Smart Contract Programming Language	Smart contracts on Bitcoin are written in programming languages like Script, Clarity.	Smart contracts on Ethereum are written in programming languages like Solidity, Vyper, etc.
Transactions	Generally, bitcoin transactions are only for keeping notes.	Ethereum transactions may contain some executable code.

Ethereum Vs Bitcoin

Basis	Bitcoin	Ethereum
Definition	Bitcoin (abbreviation: BTC; sign: ₿) is a decentralized digital currency that can be transferred on the peer-to-peer bitcoin network.	Ethereum is a decentralized global software platform powered by blockchain technology. It is most commonly known for its native cryptocurrency, ether (ETH).
History	The word bitcoin was defined in a white paper published on 31 October 2008. The currency began use in 2009.	Ethereum was conceived in 2013 by programmer Vitalik Buterin, and then went live on 30 July 2015.
Purpose	The purpose of bitcoin was to replace national currencies during the financial crisis of 2008.	The purpose of Ethereum was to utilize blockchain technology for maintaining a decentralized payment network and storing computer code.

Ethereum Vs Bitcoin

Basis	Bitcoin	Ethereum
Hash Algorithm	Bitcoin runs on the **SHA-256** hash algorithm.	Ethereum runs on the **Keccak-256** hash algorithm.
Consensus Mechanism	The Proof-of-Work (PoW) is the consensus mechanism used by the Bitcoin network.	The Proof-of-Stake is the consensus mechanism used by Ethereum.
Block Time	The block time of bitcoin is 10 minutes.	The block time of Ethereum is 14 to 15 seconds.
Block Limit	The bitcoin blockchain has a block limit of 1 MB.	The Ethereum blockchain does not have a block limit.

Ethereum Vs Bitcoin

Basis	Bitcoin	Ethereum
Popularity	Bitcoin is the most popular digital currency in the market to date.	Ether, native currency of Ethereum is the second-largest cryptocurrency after bitcoin to date.
Energy Consumption	Energy consumption is very high.	Energy consumption is very low as compared to bitcoin
Energy Consumption rate	Energy consumption rate of bitcoin mining system 3.2 Million household.	Energy consumption rate of bitcoin mining system 1.2 Million household.
Structure	Structure of bitcoin is simple and robust.	Structure of Ethereum is complex and feature rich

Ethereum Vs Bitcoin

Basis	Bitcoin	Ethereum
Rewards	Miner got nearly 6.25 BTC on successfully adding new block in network.	Miner got nearly 5 BTC along with same additional rewards on successfully adding new block in network.
Assets	Assets of Bitcoin is BTC.	Assets of Ethereum is Ether.

Other Public Blockchain Platforms

1. **Ethereum (ETH):**
   - Ethereum is a decentralized platform that enables the creation of smart contracts and decentralized applications (DApps).
   - Ether (ETH) is its native cryptocurrency.
   - Ethereum's flexibility has made it a popular platform for various blockchain-based projects.
2. **Binance Smart Chain (BSC):**
   - Binance Smart Chain is a blockchain network created by the cryptocurrency exchange Binance.
   - It supports smart contracts and decentralized applications, aiming to provide a faster and cheaper alternative to Ethereum.
3. **Ripple (XRP):**
   - Ripple is designed for fast and low-cost international money transfers.
   - It operates on a consensus ledger and is known for its focus on facilitating cross-border payments for financial institutions.
4. **Cardano (ADA):**
   - a more secure and scalable infrastructure for the development of decentralized applications and smart contracts.
   - It emphasizes a research-driven approach to development.

Other Public Blockchain Platforms

5. **Polkadot (DOT):**
   - Polkadot is a multi-chain blockchain platform that enables different blockchains to transfer messages and value in a trust-free fashion.
   - It was created to facilitate interoperability between different blockchains.
6. **Litecoin (LTC):**
   - Created as the "silver to Bitcoin's gold."
   - Litecoin is a peer-to-peer cryptocurrency that shares many similarities with Bitcoin but with faster block generation times and a different hashing algorithm.
7. **Tezos (XTZ):**
   - Tezos is a blockchain platform that focuses on self-amendment and on-chain governance.
   - It allows stakeholders to vote on changes to the protocol, providing a mechanism for the evolution of the network.
8. **Chainlink (LINK):**
   - decentralized oracle network that connects smart contracts with real-world data.
   - It enables smart contracts to interact with external information, such as market prices or weather conditions.

Other Public Blockchain Platforms

9. **Stellar (XLM):**
   - Stellar is a blockchain platform designed to facilitate fast and low-cost cross-border payments.
   - It targets individuals and institutions, aiming to provide financial services in regions with limited access to traditional banking.
10. **EOSIO (EOS):**
   - EOSIO is a blockchain platform that aims to provide a scalable and user-friendly environment for decentralized applications.
   - It emphasizes high transaction throughput and low latency.

Online References

- https://www.spiceworks.com/tech/tech-general/articles/top-five-blockchain-platforms/
- https://aws.amazon.com/what-is/blockchain/?aws-products-all.sort-by=item.additionalFields.productNameLowercase&aws-products-all.sort-order=asc
- https://blogs.opentext.com/blockchain-platform/
- https://101blockchains.com/best-blockchain-platforms/