What is BlockChain?

- Block Chain is a philosophy
- As the name suggests it is a list of blocks, a distributed collection of immutable data or code
- It is linked and secured with some **crypto-hash(Fingerprint)** and is publicly available over the INTERNET.
- Each child block has a crypto-hash of its parent block.
- Bitcoin and other cryptocurrencies are the most popular examples of blockchain usage.
- Applications include: Financial transactions, real estate, asset management, health-care services, and many more.

Dr. Devarshi Mehta

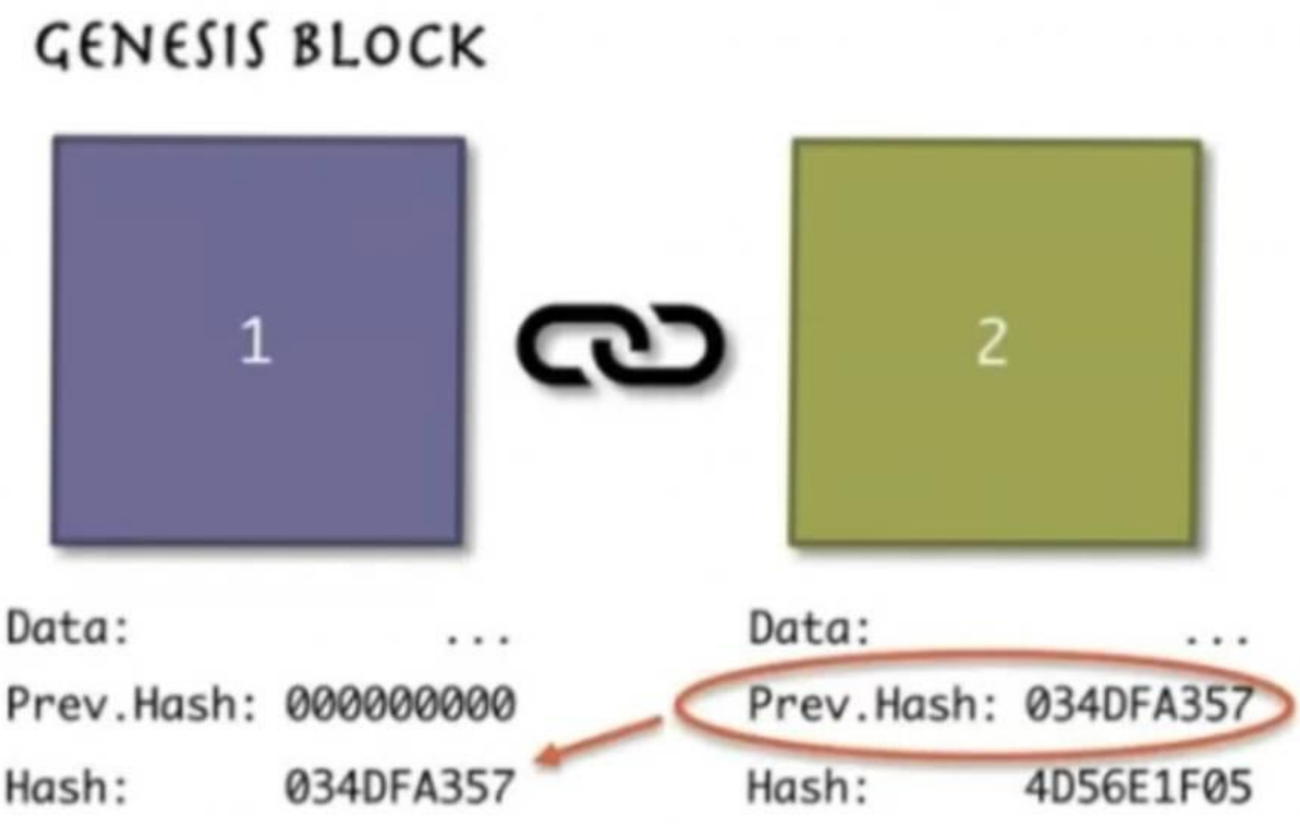


Figure-1: GENESIS_BLOCK is the first block in BlockChain, without having previous hash

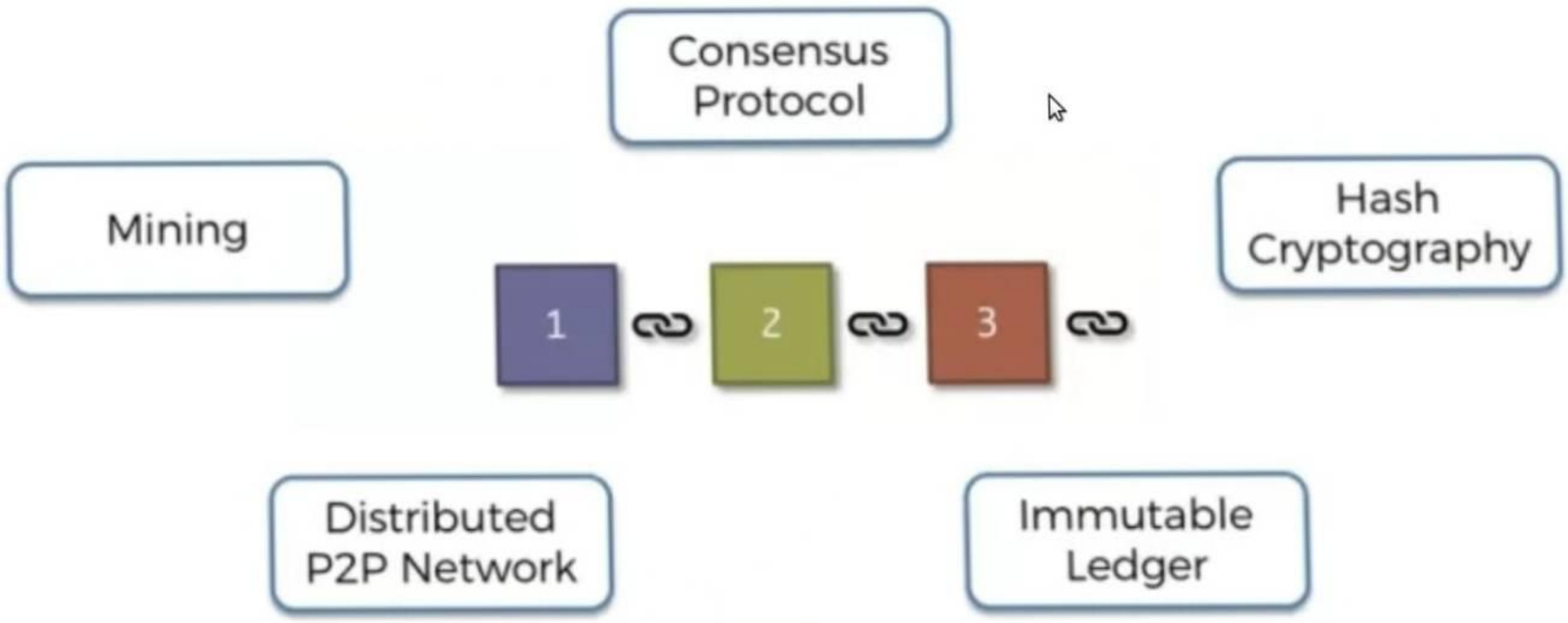


Figure-2: Fundamental building blocks for BlockChain technology

Blockchain in India

- The Indian government is preparing a national framework to support the wider deployment of blockchain use cases.

- While the country might be embracing blockchain, it has created regulatory challenges for cryptocurrency businesses.

- Minister of state for electronics and IT (MeitY) said that the government is drafting for Framework for different use cases like:
  - **Governance**
  - **Banking and Finance**
  - **Cyber Security and so on.**

Blockchain in India

- The Indian government has already built the Distributed Center of Excellence in Blockchain Technology.

- A piloted project on a blockchain system **for property registration** at Shamshabad District, Telangana State,
  - developed proof-of-concept solutions for Cloud Security Assurance, C-KYC for financial sector and trade finance.

- **Other ongoing projects include**
  - **authentication of academic certificates with a proof-of-existence framework**
  - **Vehicle life cycle**
  - **Hotel registry management**

Blockchain in India

- **Tech Mahindra** announced it was teaming up with Netherlands-based blockchain application incubator Quantoz to provide secure digital payments.

- **Tata Consultancy Services** has also launched a multi-brand consumer loyalty platform on R3's enterprise blockchain Corda

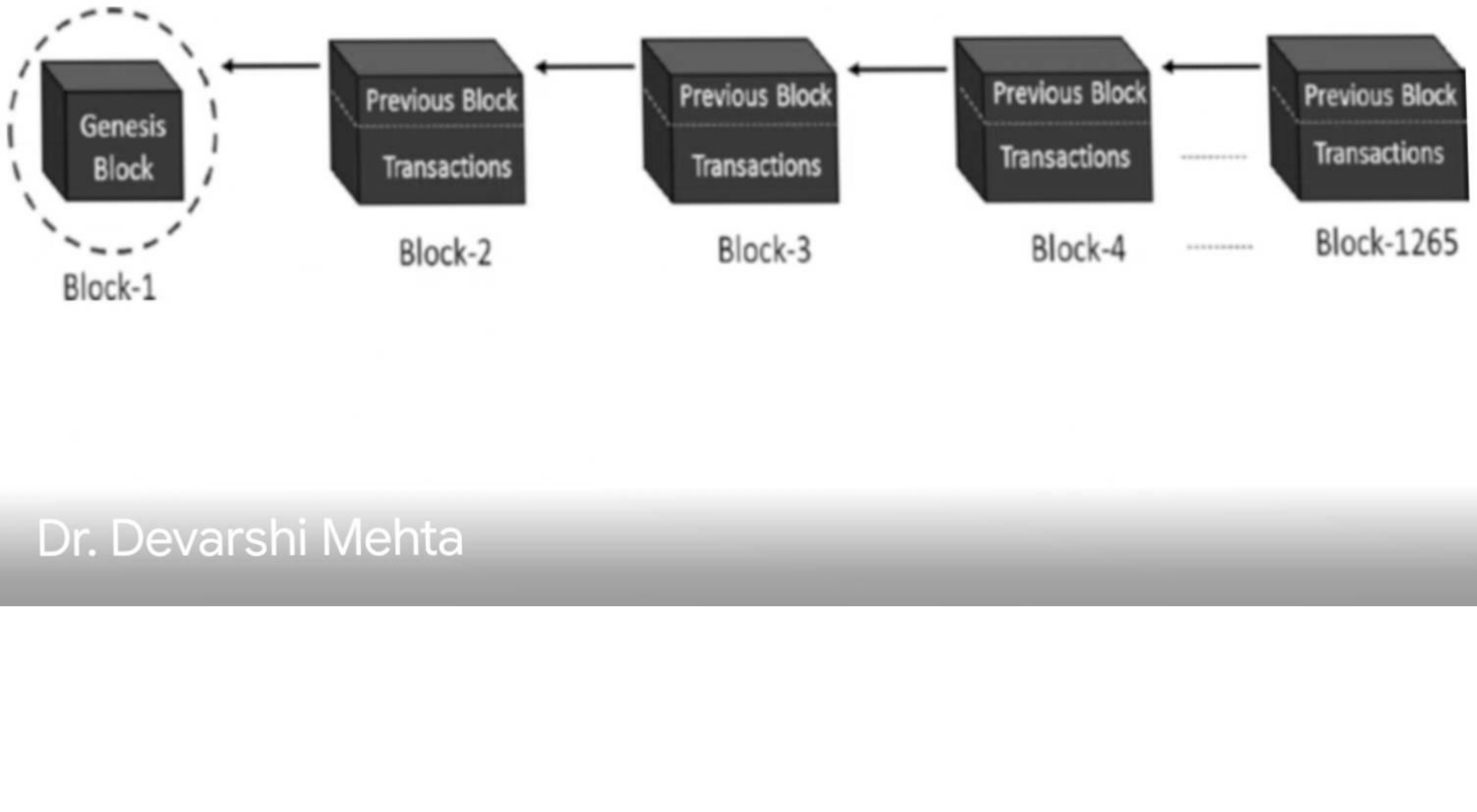
- **India's defense minister** also stressed the potential use cases of blockchain in the defense industry .

Dr. Devarshi Mehta

Chapter 1

- Peer-to-peer system of transacting values
  - with no trusted third parties in between.
- It is a shared, decentralized, and open ledger of transactions.
- This ledger database is an append-only
- Every entry is a permanent entry.
- Any new entry on it gets reflected on all copies of the databases hosted on different nodes.

Dr. Devarshi Mehta



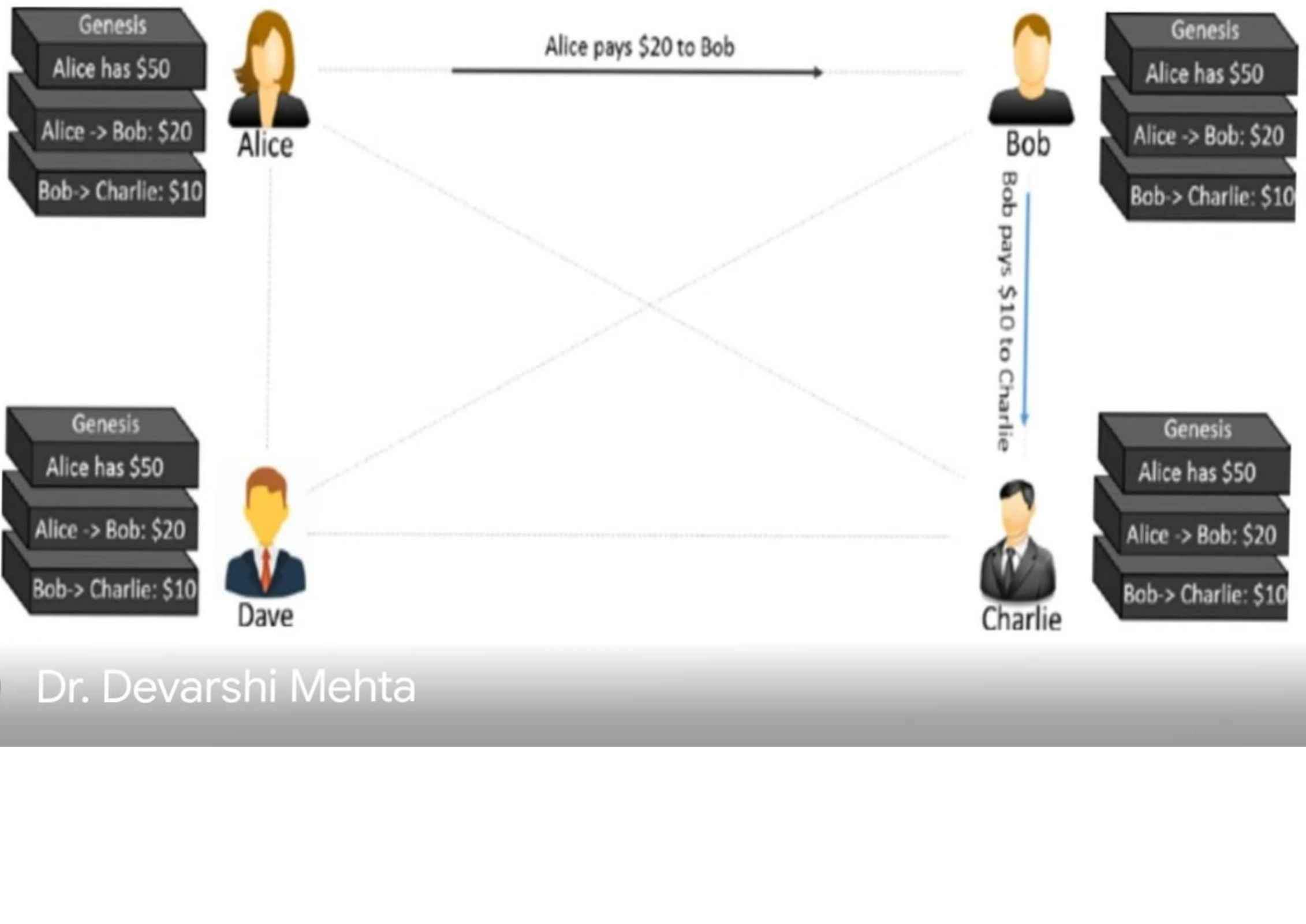
- Just the way TCP/IP was designed to achieve an open system,
  - blockchain technology was designed to enable true decentralization.

- Every node on the blockchain network has an identical copy of the blockchain

- Here every block is a collection of transactions.

Dr. Devarshi Mehta

Dr. Devarshi Mehta



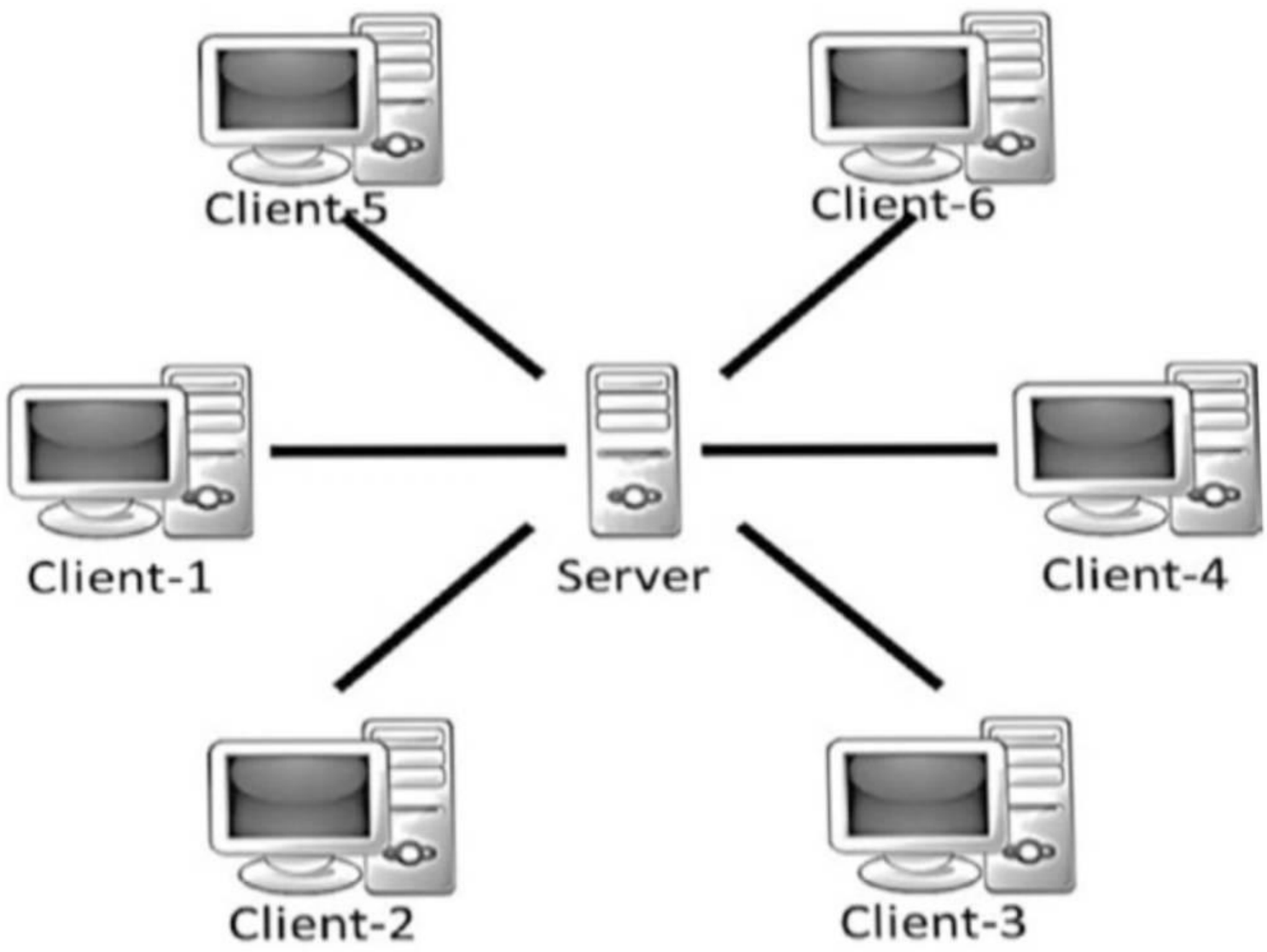
Centralized Systems

- Systems with a centralized control & all administrative authority.
- Such systems are easy to design, maintain, impose trust, and govern

Limitations:

- They have a central point of failure, so are less stable.
- They are more vulnerable to attack and hence less secured.
- Centralization of power can lead to unethical operations.
- Scalability is difficult most of the time.

Dr. Devarshi Mehta



Dr. Devarshi Mehta

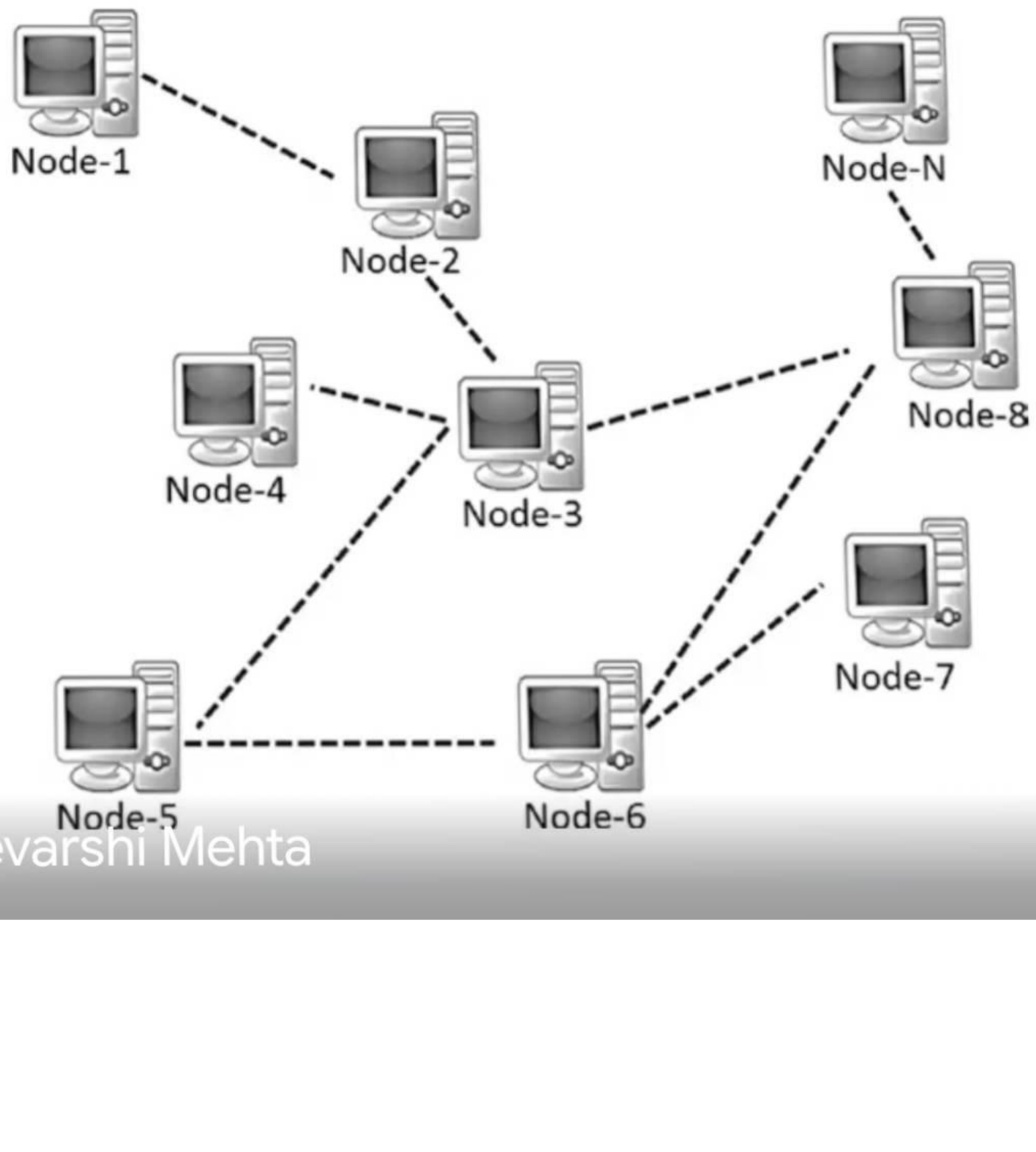
Decentralized Systems

- System does not have a centralized control and every node has equal authority.
- Such systems are **difficult** to design, maintain, govern, or impose trust.

Advantages:

- They do not have a central point of failure, so more stable and fault tolerant
- **Attack resistant**, as no central point to easily attack and hence more secured
- Symmetric system with equal authority to all, so less scope of unethical operations and usually democratic in nature

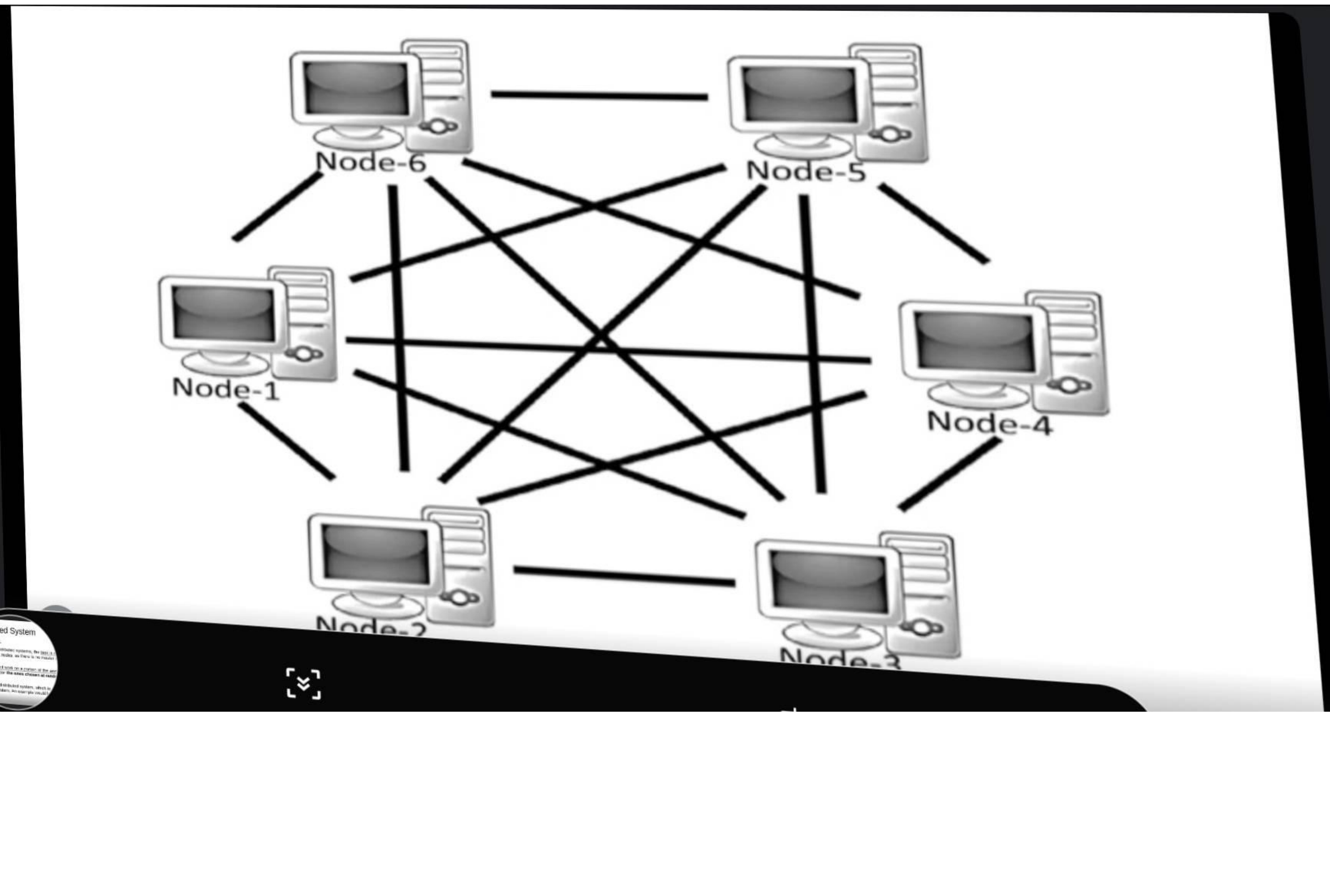
Dr. Devarshi Mehta



Distributed System

- It can also be **decentralized**.
- However, unlike common distributed systems, the task is not subdivided and delegated to nodes, as there is no master in blockchain.
- The contributing nodes do not work on a portion of the work, rather, the interested nodes (or **the ones chosen at random**) perform the entire work.
- A typical decentralized and distributed system, which is effectively a peer-to-peer system, An example would be blockchain!

Dr. Devarshi Mehta



Centralized vs. Decentralized Systems

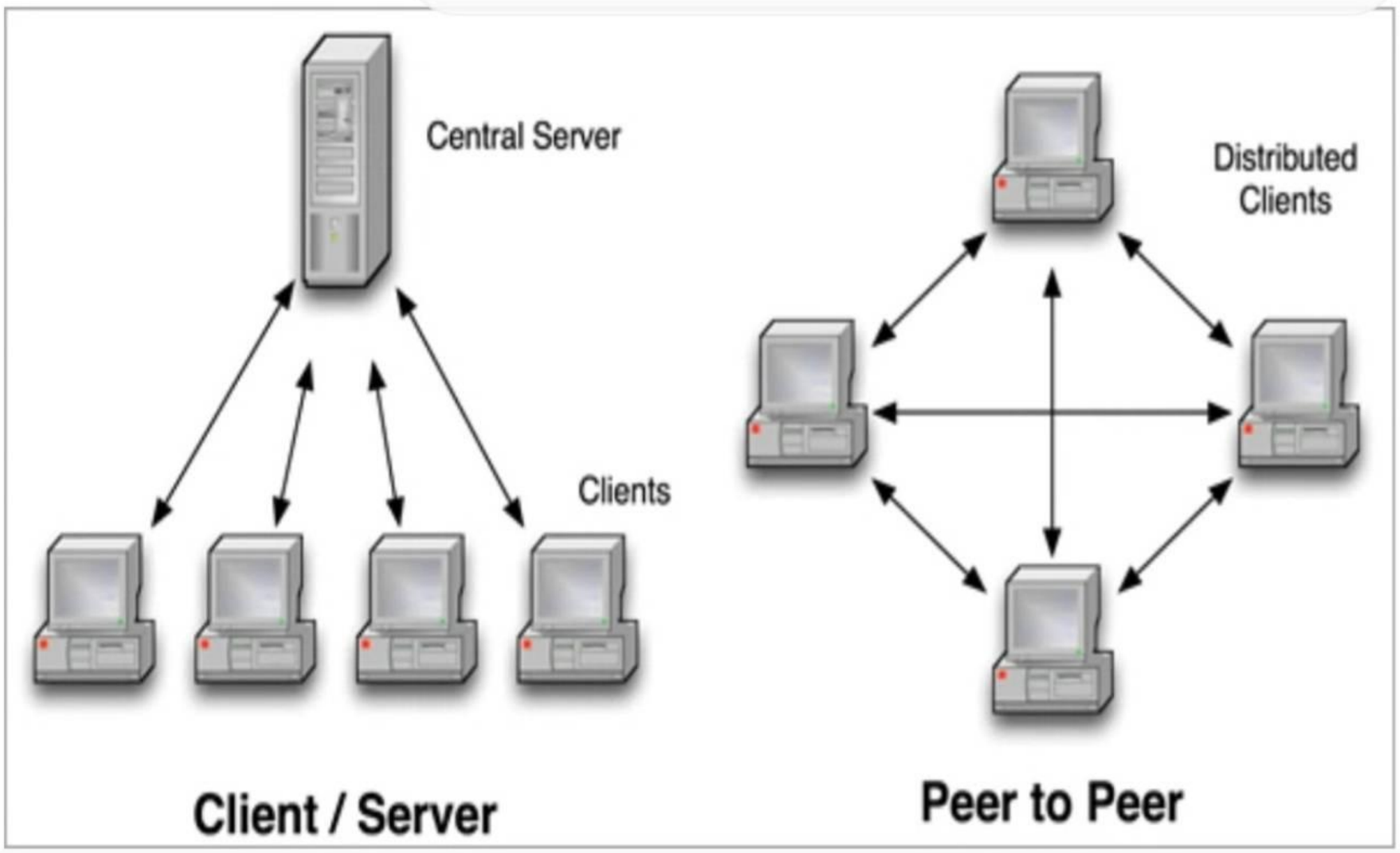
- Blockchain is designed to be decentralized, **but there is almost no system that is purely centralized or decentralized.**
- What is a distributed system then?
- Whether a system is centralized or decentralized, it can still be distributed.
- **A centralized distributed system** is one in which there is a master node responsible for breaking down the tasks or data and distribute the load across nodes.
- On the other hand, a **decentralized distributed system** is one where there is no “master” node as such and yet the computation may be distributed.

Dr. Devarshi Mehta

Centralized vs. Decentralized Systems

- Blockchain is designed to be decentralized, **but there is almost no system that is purely centralized or decentralized.**
- What is a distributed system then?
- Whether a system is centralized or decentralized, it can still be distributed.
- **A centralized distributed system** is one in which there is a master node responsible for breaking down the tasks or data and distribute the load across nodes.
- On the other hand, a **decentralized distributed system** is one where there is no “master” node as such and yet the computation may be distributed.

Dr. Devarshi Mehta



Limitations of Centralized systems

- Trust issues / Privacy issue of data
- Security issue
- Cost and time factor for transactions

Dr. Devarshi Mehta

Advantages of decentralized systems over centralized

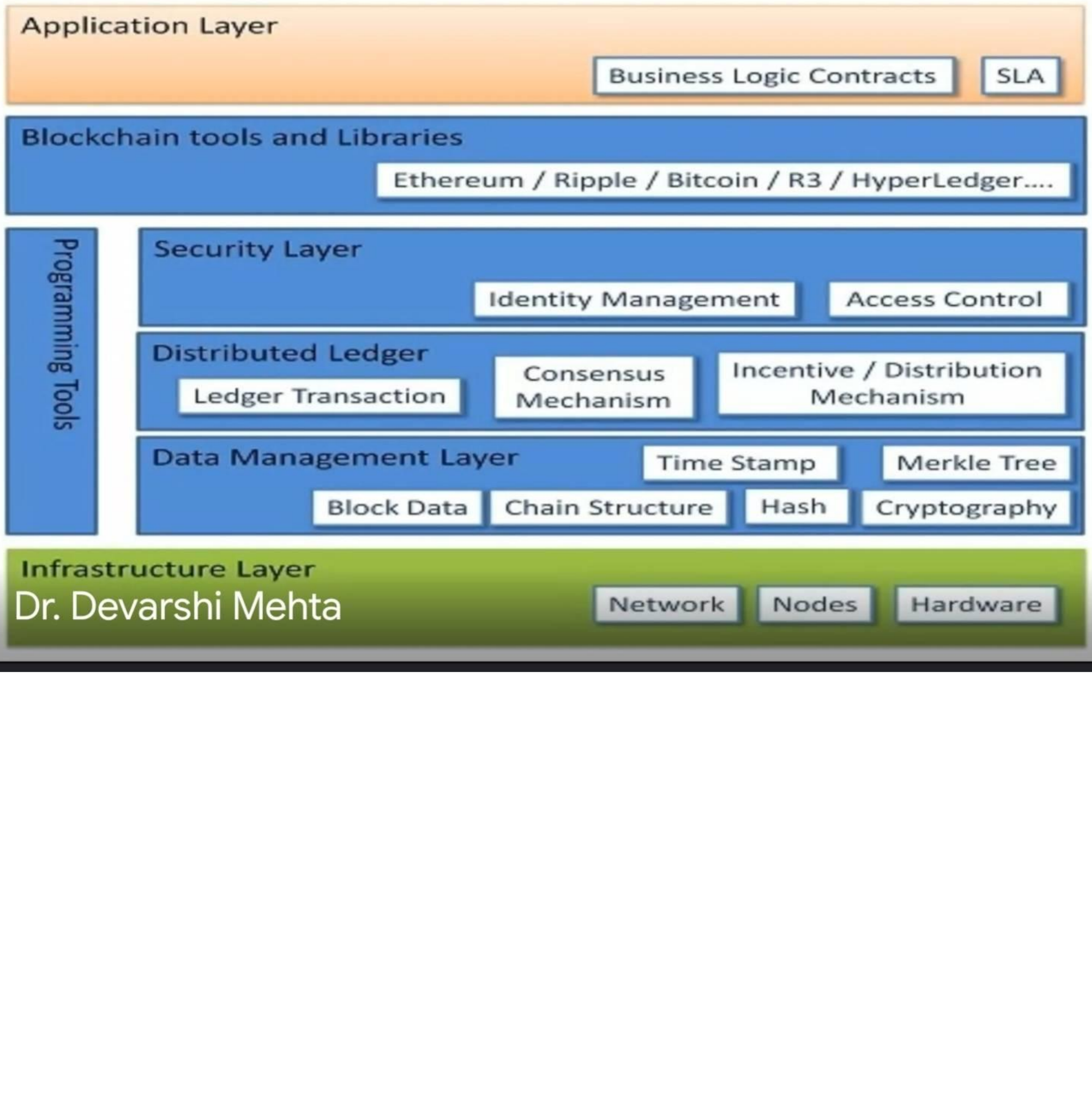
- Elimination of intermediaries
- Easier and genuine verification of transactions
- Increased security with lower cost
- Greater transparency
- Decentralized and immutable

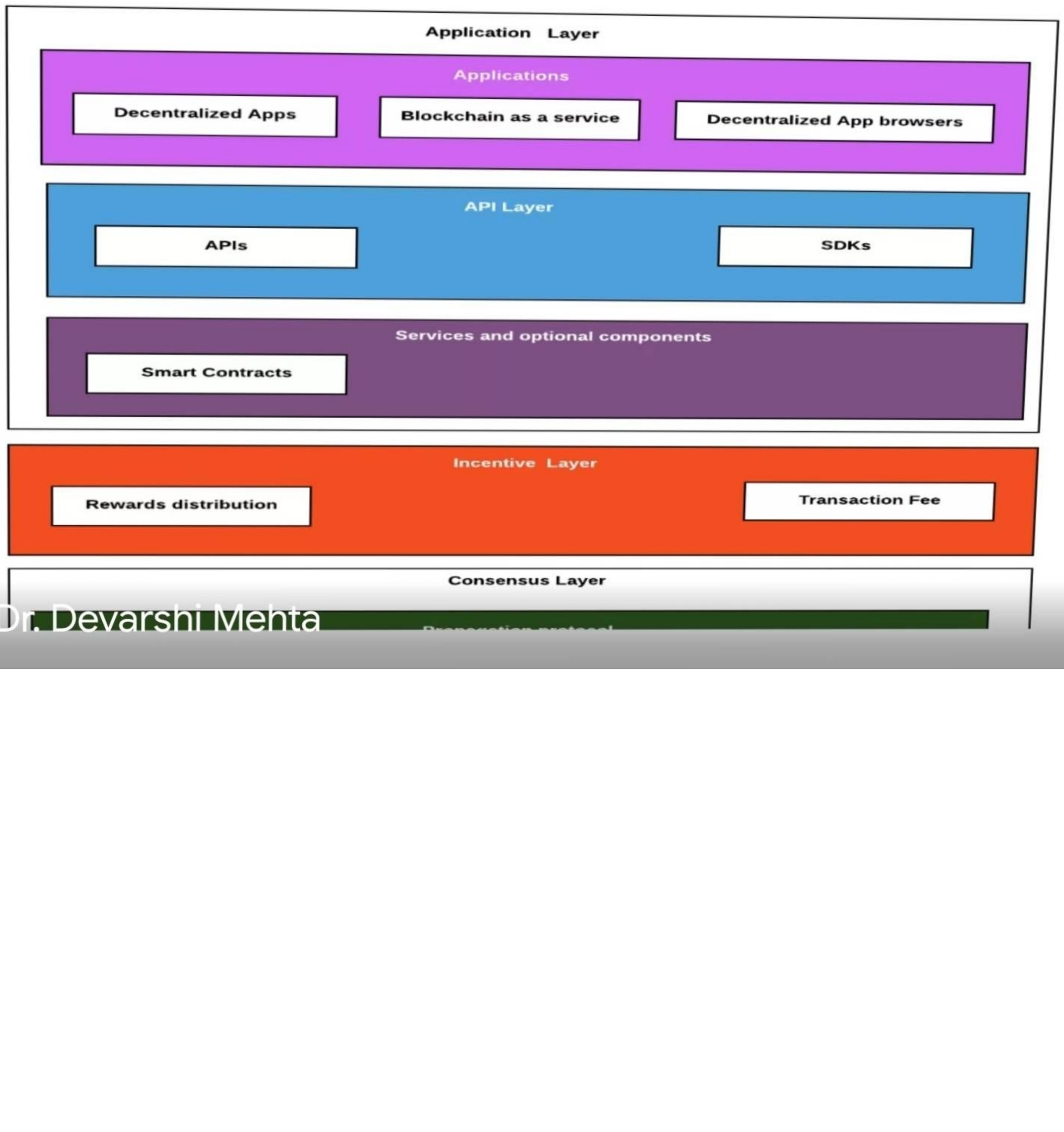
Dr. Devarshi Mehta

Layers of Blockchain

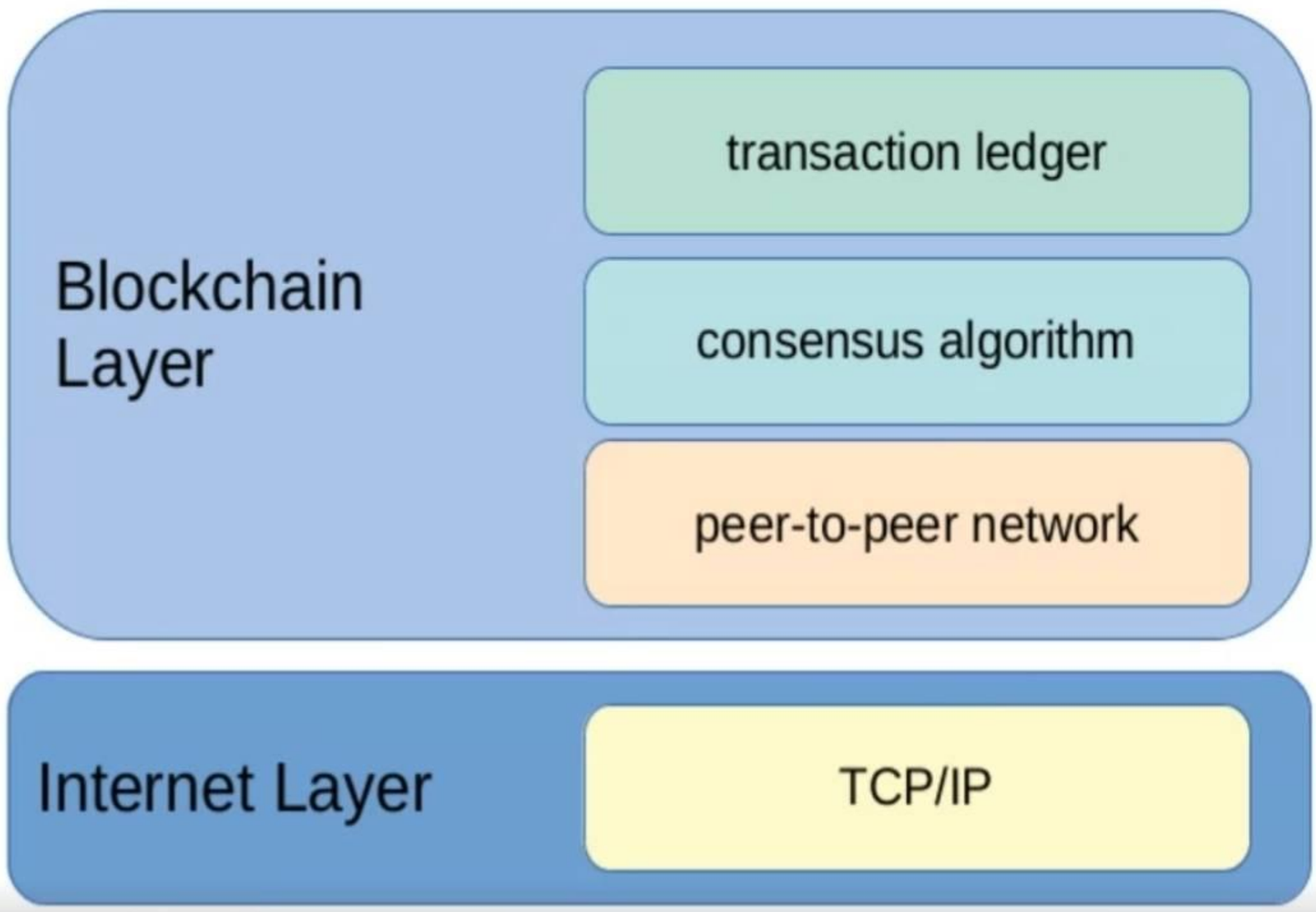
- Blockchain is never just a piece of technology, but a **combination of:**
  - business principles
  - Economics
  - game theory
  - Cryptography
  - computer science engineering
- The layered approach in the TCP/IP stack is actually a standard to achieve an open system.
- In the blockchain, there are no agreed global standards.
- **A layered heterogeneous architecture is needed in future.**
- All these layers are present on all the nodes.

Dr. Devarshi Mehta





Dr. Devarshi Mehta



Dr. Devarshi Mehta

High-level, layered representation of blockchain

Coding level functionality: for front end & Backend	Application Layer
Execution of Single or set of Instruction by nodes	Execution Layer
Validating the transaction	Semantic Layer
Allows the nodes to discover each other, talk and sync	Propagation Layer
Assuring Safety and security	Consensus Layer

Application Layer

- Is used to code up the desired functionalities for software development
  - client-side programming constructs
  - scripting, APIs
  - development frameworks
- Blockchain as a backend: **applications to be hosted on web servers:**
  - web application development
  - server-side programming
  - APIs, etc
- **Off-chain networks is used**:
  - To ensure heavy lifting is done at the application layer
  - so core blockchain is light and effective
  - network traffic is less

Execution Layer

- Executions of instructions ordered by the Application Layer
- Instructions could be
  - simple instructions
  - or a set of multiple instructions
  - in the form of a ***smart contract***
- All the nodes execute the **programs /scripts independently.**

Dr. Devarshi Mehta

Execution Layer at various cryptocurrency

- **Bitcoins** uses simple scripts and allow few set of instructions.
- **Ethereum** allow complex executions that gets executed on its own **EVM**(Ethereum Virtual Machine).
- **Hyperledger** uses smart contracts using inside docker(list of many executable files) images
  - supports languages such as **Java and Go**.

Dr. Devarshi Mehta

Semantic Layer

- Is a **logical layer**
- A transaction, whether valid or invalid, gets validated in the Semantic Layer.
- In Bitcoin it will check:
  - legitimate transaction
  - double-spend attack
  - Is the node authorized to make this transaction
  - Check one or more previous transactions

What are smart contracts?

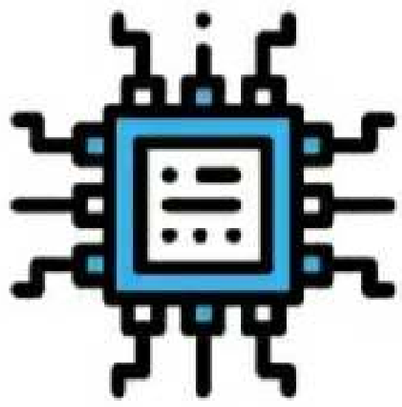
- Lines of code that are stored on a blockchain
- **Automatically execute** when predetermined terms and conditions are met.
- They are programs run by the people who developed them.
- In business collaborations, used to enforce some type of agreement
- So that all participants can be **certain of the outcome without an intermediary's involvement**.

Blockgeeks

1

Smart Contracts are **written as code** and committed to the blockchain. The code and conditions in the contract are **publicly available** on the ledger.

2



When an *event* outlined in the contract is triggered, like an expiration date or an asset's target price is reached-- the **code executes**.

3

Regulators can watch contract activity on the blockchain to **understand the market** while still **maintaining the privacy** of individual actors.

DAPPS or Smart Contracts

- A decentralized application is a **computer application** that runs on a distributed computing system.
  - DApp, dApp, Dapp, or dapp
- It uses distributed ledger technologies (DLT) such as
  - Ethereum
  - Blockchain
  - often referred to as smart contracts.

Blockchain Middleware Creates Connectivity

Connect Smart Contracts to
critical external data, so they
can include real world events.

Connect Smart Contracts to
widely accepted bank payments
so they can pay in local currencies.

Connect Smart Contracts from
different networks to each other
for **critical combined functionality.**

Propagation Layer

- Peer-to-peer **communication layer, allows the nodes to sync**
- When a transaction is made, it gets broadcasted to the entire network.
- When a **node wants to propose a valid block**, it gets immediately propagated to the entire network as the latest block.
- **Latency issues for transaction or block:** Some propagations occur within seconds or after some time, depending on the
  - capacity of the nodes
  - network bandwidth

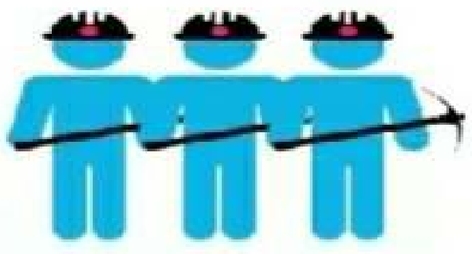
Process of verifying the transactions in the block to be added:

- **Organizing** these transactions in a chronological order in the block
- **Announcing** the newly mined block to the entire network
- **The energy consuming part is solving the 'hard mathematical problem'**
- **Link** the new block to the last block in the valid blockchain.
- **Find the right solution by miners** the node broadcasts it to the whole network at the same time
- **The rewards**, receiving by miners as a cryptocurrency prize **provided by the PoW protocol**
- **12.5 bitcoins** winning miner will get prize for a mining block in the bitcoin network

Proof of Work vs. Proof of Stake

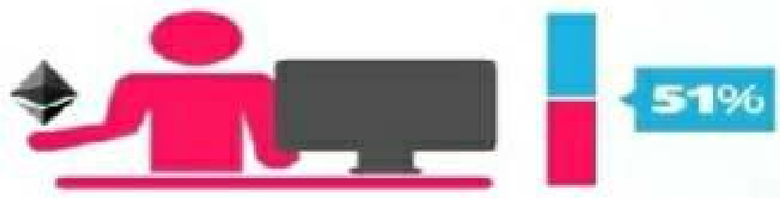
To add each block to the chain, miners must compete to solve a difficult puzzle using their computers processing power.

In order to add a malicious block, you'd have to have a computer more powerful than 51% of the network.



The first miner to solve the puzzle is given a reward for their work.

There is no competition as the block creator is chosen by an algorithm based on the user's stake.



In order to add a malicious block, you'd have to own 51% of all the cryptocurrency on the network.

There is no reward for making a block, so the block creator takes a transaction fee.

Consensus(general agreement) Layer

- It is a base layer assuring Safety and security
- Allow to get all the nodes to agree on one consistent state of the ledger.
- In Bitcoin or Ethereum,
  - it is used through “mining”
  - It use a **Proof of Work (PoW)** consensus mechanism to randomly select a node that can propose a block.

Proof-of-Work

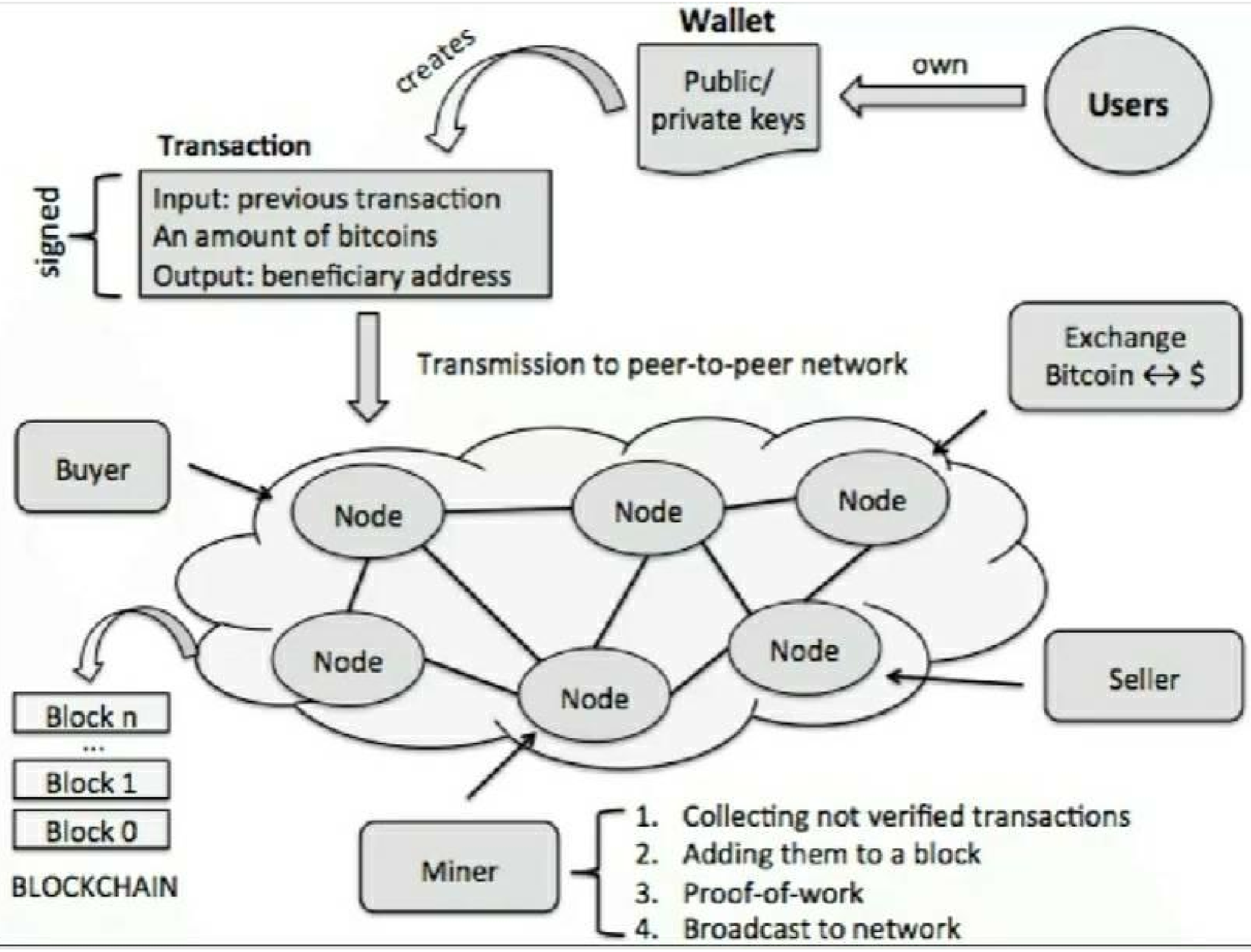
- Proof-of-Work, or PoW, is the original consensus algorithm(mathematical Puzzle) in a Blockchain network.
- With PoW, **miners compete against each other** to complete transactions on the network and get rewarded.
- When a miner finally finds the right solution they announces it to the whole n/w
- Receiving a crypto currency prize provided by the protocol PoW.
- Miners use more and more powerful machines due to increase of complexity
- This PoW is verified by other Bitcoin nodes each time they receive the block

Consensus Layer

- If the PoW puzzle was solved properly
- They add this block to their own copy of blockchain and build further on it.
- There are many different variants of consensus protocols such as
  - **Proof of Stake (PoS)**
  - **deligated PoS (dPoS)**
  - **Practical Byzantine Fault Tolerance (PBFT)**
  - **etc**

Other Applications of BC

- Financial market
- Media and entertainment
- Energy trading
- Prediction markets
- Retail chains
- Loyalty rewards systems (helps businesses to meet target and give incentives to the right customers)
- Insurance
- Logistics and supply chains(transporting goods to customers)
- Medical records
- Government and military applications



Mining

- Process of **adding** transactions to the large **distributed** public **ledger** of existing transactions, known as the blockchain.
- Miners(**special computers on the network**) perform computation work in solving a complex mathematical problem
- With time, the mathematical problem becomes **more complex**.
- **Bitcoin** has introduced Proof of Work model for mining:
  - To verify the legitimacy of a transaction
  - To avoid double spending
  - To create new digital currencies by rewarding miners

Wallet

- A cryptocurrency wallet digitally stores a user's public and private keys
- Also programmatically helps in sending and receiving digital currency

Threats & Challenges

- **Double Spending:** One can play with cryptocurrencies trying to spend the same money twice in quick succession.
- The transaction is evaluated by miners and takes some time to get confirmed.
- But before confirmation, person may send the same amount again to another one.
- So there are 2 unconfirmed transactions in pool called double spending
- In order to avoid this:
  - BC keeps a timestamp of each transaction

Centralized vs. Decentralized Systems

- Blockchain is designed to be decentralized, **but there is almost no system that is purely centralized or decentralized.**
- What is a distributed system then?
- Whether a system is centralized or decentralized, it can still be distributed.

- **A centralized distributed system** is one in which there is a master node responsible for breaking down the tasks or data and distribute the load across nodes.
- On the other hand, a decentralized distributed system is one where there is no "master" node as such and yet the computation may be distributed.

Centralized Systems

- Systems with a centralized control & all administrative authority.
- Such systems are <u>easy to design, maintain, impose trust, and govern</u>
- **Limitations:**
- They have a central point of failure, so are less stable.
- They are more vulnerable to attack and hence less secured.
- Centralization of power can lead to unethical operations.
- Scalability is difficult most of the time.

Layers of Blockchain

- Blockchain is never just a piece of technology, but a **combination of:**
  business principles, economics, game theory, cryptography, and computer science engineering.
- The layered approach in the TCP/IP stack is actually a standard to achieve an open system.
- In the blockchain, there are no agreed global standards.
- **A layered heterogeneous architecture is needed in future.**
- All these layers are present on all the nodes.

high-level, layered representation of blockchain

Coding level functionality: for front end & Backend

Execution of Single or set Instruction by nodes

Validating the transaction

allows the nodes to discover each other, and talk and sync

assuring Safety and security

Execution Layer

- Executions of instructions ordered by the Application Layer
- Instructions could be
  - simple instructions
  - or a set of multiple instructions
  - in the form of a ***smart contract***
- All the nodes execute the **programs /scripts independently.**

Execution Layer at various cryptocurrency

- **Bitcoins** uses simple scripts and allow few set of instructions.
- **Ethereum** allow complex executions that gets executed on its own **EVM**(Ethereum Virtual Machine).
- **Hyperledger** uses smart contracts using inside docker(list of many executable files) images

  –supports languages such as **Java and Go**.

Semantic Layer

- Is a **logical layer**
- A transaction, whether valid or invalid, gets validated in the Semantic Layer.
- In Bitcoin it will check:
  - legitimate transaction
  - double-spend attack
  - Is the node authorized to make this transaction
  - Check one or more previous transactions

What are smart contracts?

- lines of code that are stored on a blockchain
- **automatically execute** when predetermined terms and conditions are met.
- they are programs run by the people who developed them.
- in business collaborations, used to enforce some type of agreement
- so that all participants can be **certain of the outcome without an intermediary's involvement**.

Propagation Layer

- peer-to-peer **communication layer, allows the nodes to sync**
- When a transaction is made, it gets broadcast to the entire network.
- When a **node wants to propose a valid block**, it gets immediately propagated to the entire network as the latest block.
- **latency issues for transaction or block:** Some propagations occur within seconds or after some time, depending on the
  - capacity of the nodes
  - network bandwidth

- **<u>Process of verifying the transactions in the block to be added:</u>**
- **organizing** these transactions in a chronological order in the block
- **announcing** the newly mined block to the entire network
- **The energy consuming part is solving the 'hard mathematical problem'**
- **Link** the new block to the last block in the valid blockchain.
- **Find the right solution by miners** the node broadcasts it to the whole network at the same time
- **The rewards**, receiving by miners as a cryptocurrency prize
- **provided by the PoW protocol**
- **12.5 bitcoins** winning miner will get prize for a mining block in the bitcoin network

Consensus(general agreement) Layer

- It is base layer assuring Safety and security
- Allow to get all the nodes to agree on one consistent state of the ledger".
- In Bitcoin or Ethereum,

  –it is used through "mining."

  –It use a **Proof of Work (PoW)** consensus mechanism

  –to randomly select a node that can propose a block.

Consensus Layer

- If the PoW puzzle was solved properly
- they add this block to their own copy of blockchain and build further on it.
- There are many different variants of consensus protocols such as
  - **Proof of Stake (PoS)**
  - **deligated PoS (dPoS)**
  - **Practical Byzantine Fault Tolerance (PBFT)**
  - **etc**

Limitations of Centralized systems

- Trust issues / Privacy issue of data
- Security issue
- Cost and time factor for transactions

Advantages of decentralized systems over centralized

- Elimination of intermediaries
- Easier and genuine verification of transactions
- Increased security with lower cost
- Greater transparency
- Decentralized and immutable

Mining

- Process of **adding** transactions to the large **distributed** public **ledger** of existing transactions, known as the blockchain.
- Miners(**special computers on the network**) perform computation work in solving a complex mathematical problem
- With time, the mathematical problem becomes **more complex**.
- **Bitcoin** has introduced Proof of Work model for mining:
  - To verify the legitimacy of a transaction
  - To avoid double spending
  - To create new digital currencies by rewarding miners

Proof-of-Work

- Proof-of-Work, or PoW, is the original consensus algorithm(mathematical Puzzle) in a Blockchain network.
- With PoW, **miners compete against each other** to complete transactions on the network and get rewarded.
- When a miner finally finds the right solution they announces it to the whole n/w
- Receiving a crypto currency prize provided by the protocol PoW.
- Miners use more and more powerful machines due to increase of complexity
- This PoW is verified by other Bitcoin nodes each time they receive the block

DAPPS or Smart Contracts

- A decentralized application is a **computer application** that runs on a distributed computing system.
  - DApp, dApp, Dapp, or dapp
- It uses distributed ledger technologies (DLT) such as
  - Ethereum
  - Blockchain
  - often referred to as smart contracts.

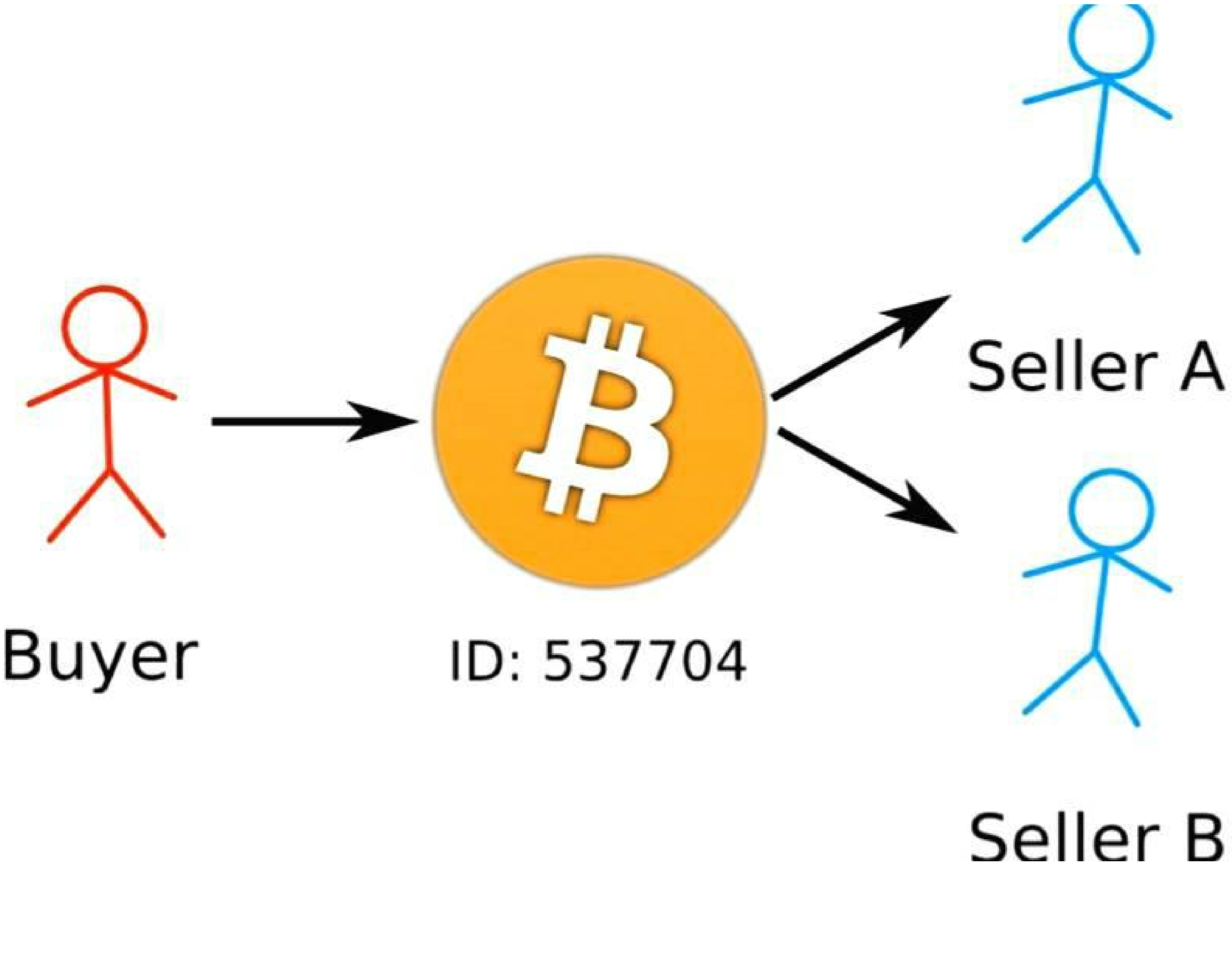
Wallet

- A cryptocurrency wallet digitally stores a user's public and private keys

- Also programmatically helps in sending and receiving digital currency

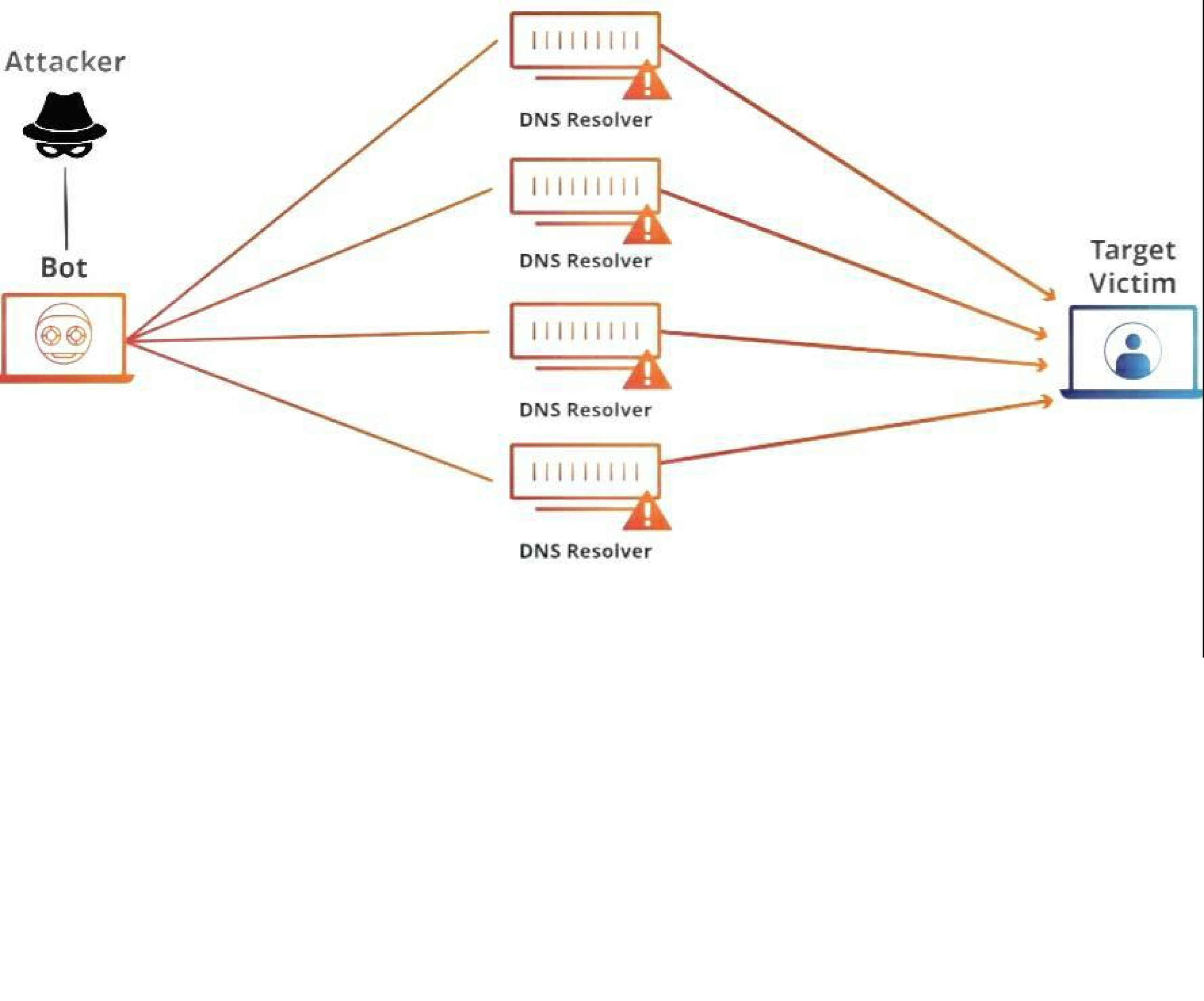
Threats & Challenges

- **Double Spending:** One can play with cryptocurrencies trying to spend the same money twice in quick succession.
- The transaction is evaluated by miners and takes some time to get confirmed.
- But before confirmation, person may send the same amount again to another one.
- So there are 2 unconfirmed transactions in pool called double spending
- In order to avoid this:
  - BC keeps a timestamp of each transaction



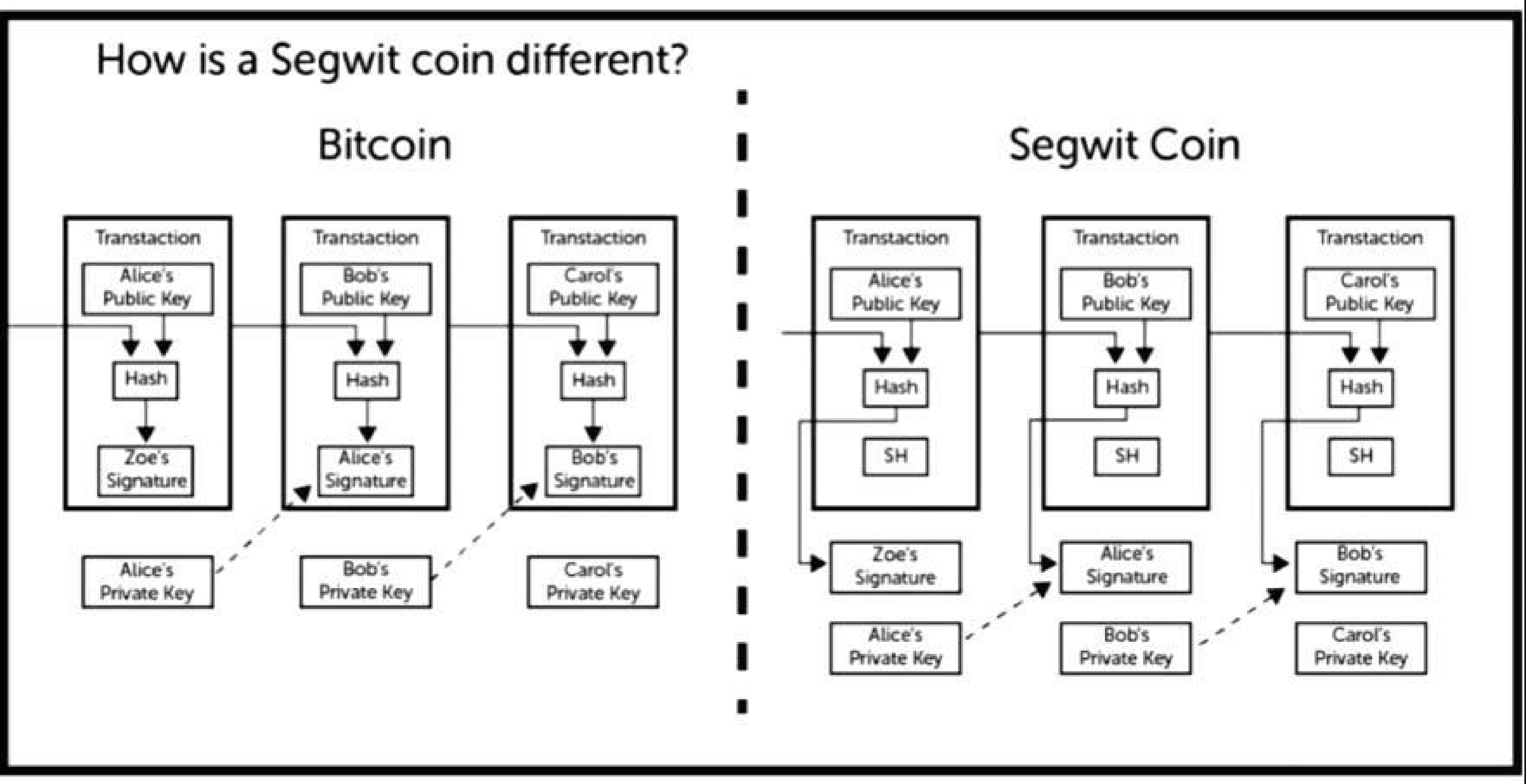
Threats & Challenges

- **Denial of Service Attack:** is a malicious attack on BC by **people who send fack blocks huge in length** to BC n/w.
- It takes **enormous amount of time for miners** to evaluate the block that reduces the transaction rate of adding blocks to the n/w.
- It happens due to:
  - BC is public and anyone can access
  - **There is no maximum limit to size of the blocks**
- Currently, Miners take almost **10 minutes** to mine a block which is much more.
- Some have created a **Private / Permissioned BC** where only **authorized** can access the BC
- While Public BC are used by anyone.



Segwit

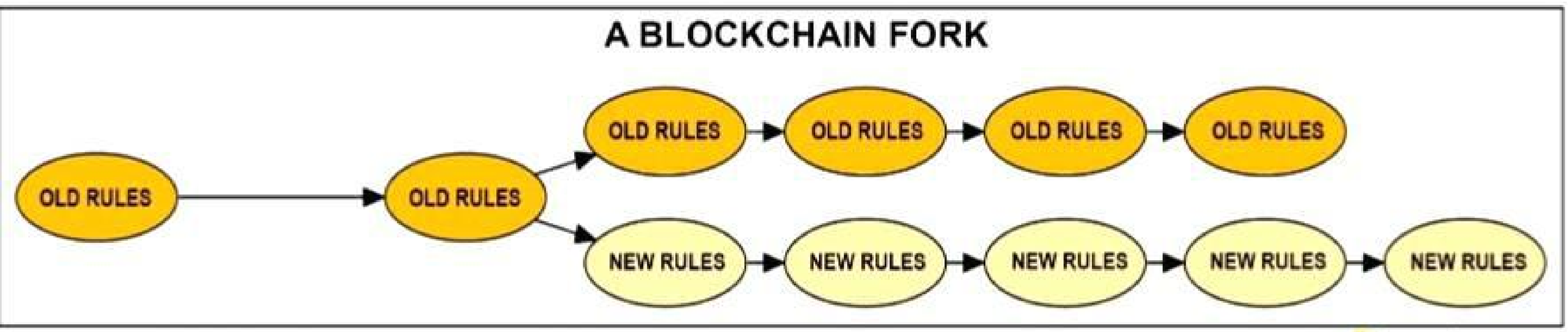
- Some Blockchainers applied a new technique called segwit (segregated Witness).
- Solution bitcoin proposed : Segwit **impose a restriction on block size** limiting in to only **1 MB**.
- Signature part of the block called "**witness**" would move to trailing part of the block.
- It makes mining much easier and faster due to small size of blocks
- This solution also implemented in crypto-currencies like:
  - Groestlcoin, Litecoin, DigiByte and Vertcoin
- **Segwit2X**: In november 2017, Segwit2X activated:
  - to increase the block size to 2 MB



Threats & Challenges

- **51% Attack**: every framework has a design flaw
- The transaction is confirmed and added to to BC only if a minimum percentage of all nodes accept it
- For bitcoin originally the % was 51%
- In a public BC **if a miner has 51% hashrate** then can manipulate the ledger
- So later on, people tried to increase this consensus % from 51 to higher
- **Ripple uses 80% consensus model.**

Fork in BC(Soft Fork & Hard Fork)



Fork in BC(Soft Fork & Hard Fork)

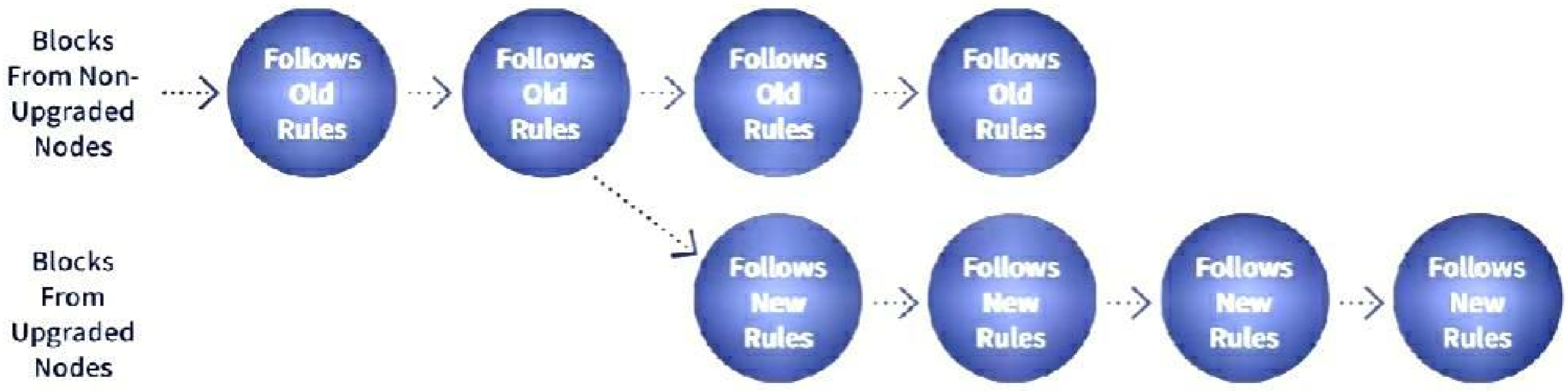
- **Fork means** blocks of different version of BC
- Transactions are added to block and the new block is finally added to the BC n/w
- Combined effort of **miners and a distributed consensus to validate** the everyone in n/w using **same version of BC**
- As people are using different version of BC, In such case a temporary or accidental fork is created.
- If we use **Ethereum as BC framework, chances are more for fork**
- However soon is sorted out by getting rid of the faulty blocks. It is called a **soft fork.**

Hard Fork

- From time to time there is a need in the s/w to change or upgrade

- So two different versions of BC are created sharing the same origin

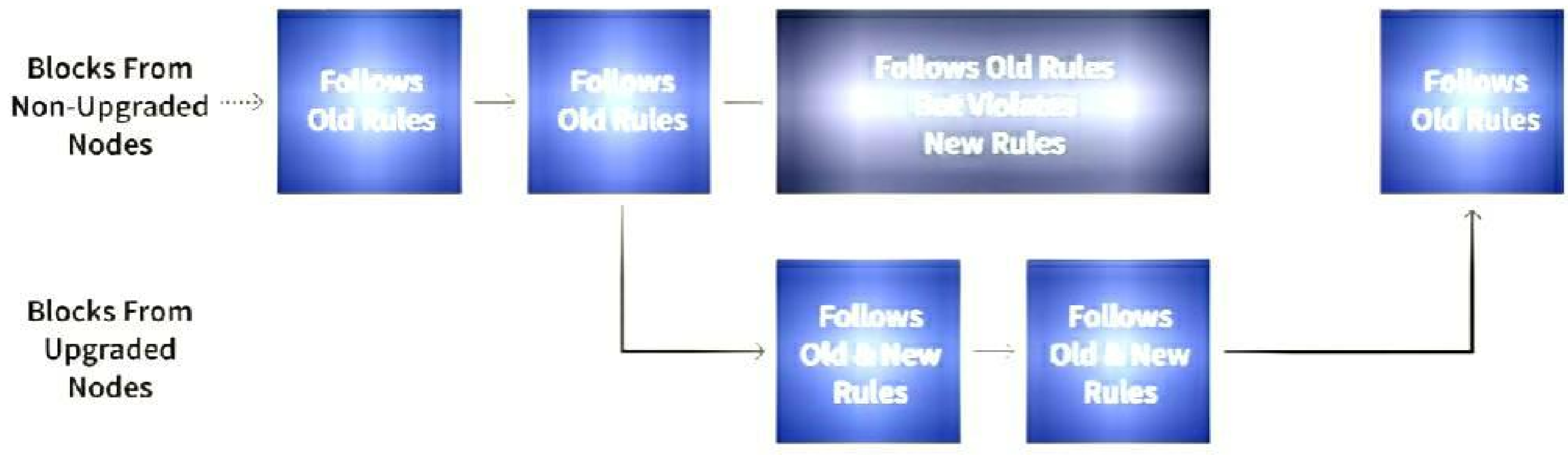
- It is called hard fork



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

soft fork

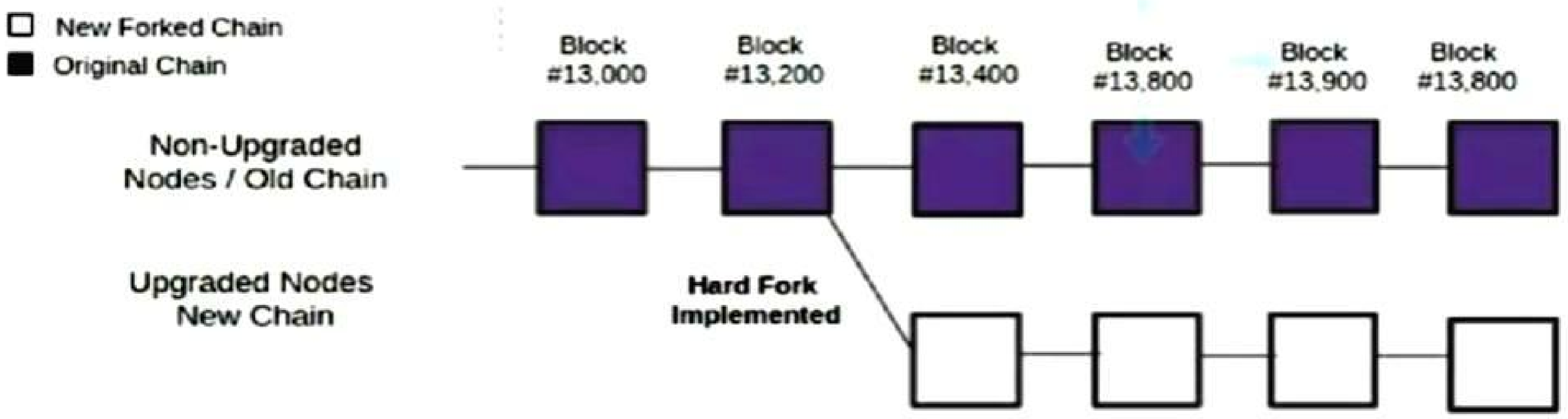
- A soft fork is a change to the software protocol where only previously valid transaction blocks are made invalid.
- Because old nodes will recognize the new blocks as valid, a soft fork is backwards-compatible.
- A soft fork can also occur at times due to a temporary divergence in the blockchain when miners using non-upgraded nodes violate a new consensus rule their nodes don’t know about.

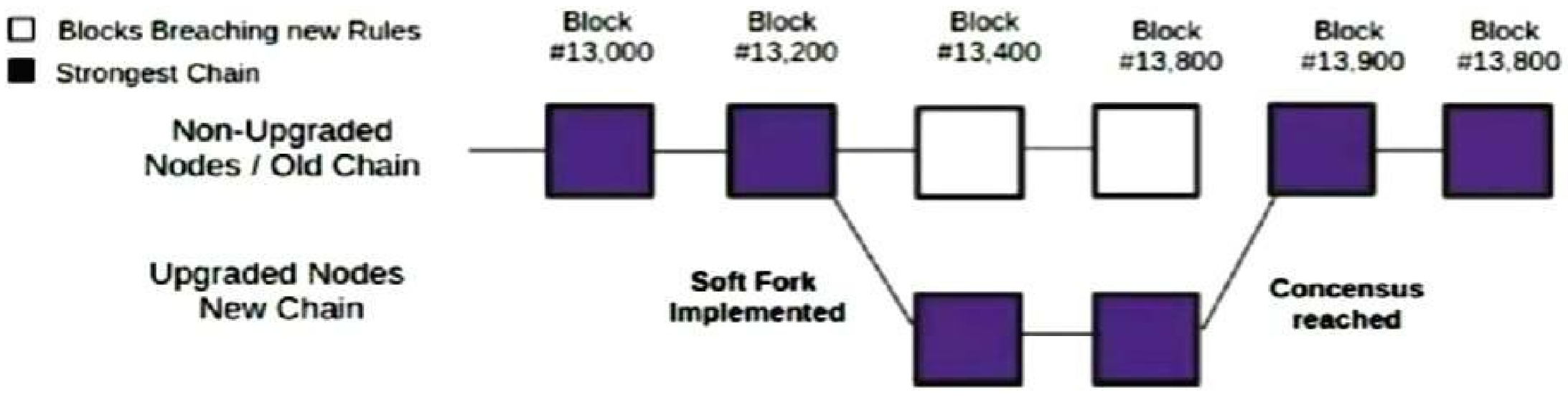


A Soft Fork: blocks violating new rules are made stale by the upgraded mining majority

Fork in BC(Soft Fork & Hard Fork)

- Hard forks and soft forks are essentially the same
- When a cryptocurrency platform's existing code is changed, an old version remains on the network while the new version is created.
- With a soft fork, only one blockchain will remain valid as users adopt the update.
- Whereas with a hard fork, both the old and new blockchains exist side by side, which means that the software must be updated to work by the new rules.
- Both forks create a split, but a hard fork creates two blockchains and a soft fork is meant to result in one.





Fork in BC(Soft Fork & Hard Fork)

- Considering the differences in security between hard and soft forks, almost all users and **developers call for a hard fork**, even when a soft fork seems like it could do the job.

- As the blocks in a blockchain requires a tremendous amount of computing power, but the privacy gained from a hard fork makes more sense than using a soft fork.

Property / Assets

- Any type of property or asset can be registered on blockchain.
  - physical or digital:
  - Laptops, mobile phones, diamonds, Automobiles
  - real estate, E-registrations, digital files,etc.

- From one person to another: maintain the transaction log, and check validity or ownerships.

Other Financial Applications

- cross-border payments
- Share trading
- loyalty and rewards system
- Know Your Customer (KYC) among banks, etc.
- Initial Coin Offering (ICO) is one of the most trending use cases:

  (just like IPOs : as a means to increase the amount of available financing to the company.)

  - ICO (small portion of cryptocurrency / BabyCoin) is the best way of crowdsourcing today by using cryptocurrency as digital assets.
  - **A coin in an ICO can be thought of as a digital stock in an enterprise, which is very easy to buy and trade.**