Course Outline

1. Cryptocurrency and Block chain
2. Delving into BlockChain
3. Bitcoin and Block chain
4. Bitcoin Mining
5. Ethereum
6. Setting up private Blockchain Environment using Ethereum Platform
7. Hyperledger
8. Setting up Development Program using Hyperledger composer
9. Create or Deploy our private Blockchain on Multi chain
10. Prospect of Blockchain

IntelliPaat

Cryptocurrency & Blockchain

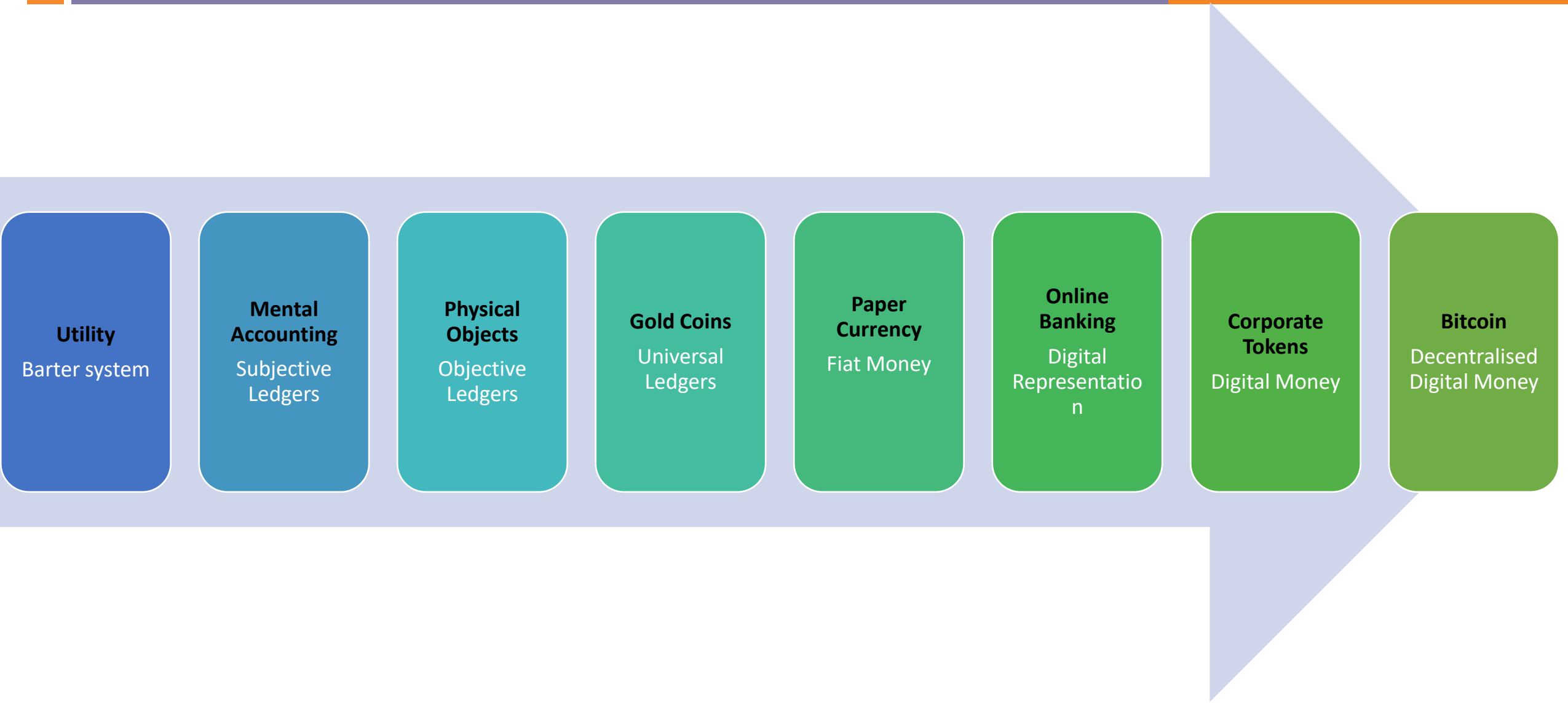
Agenda

At the end of this session you will be able to:

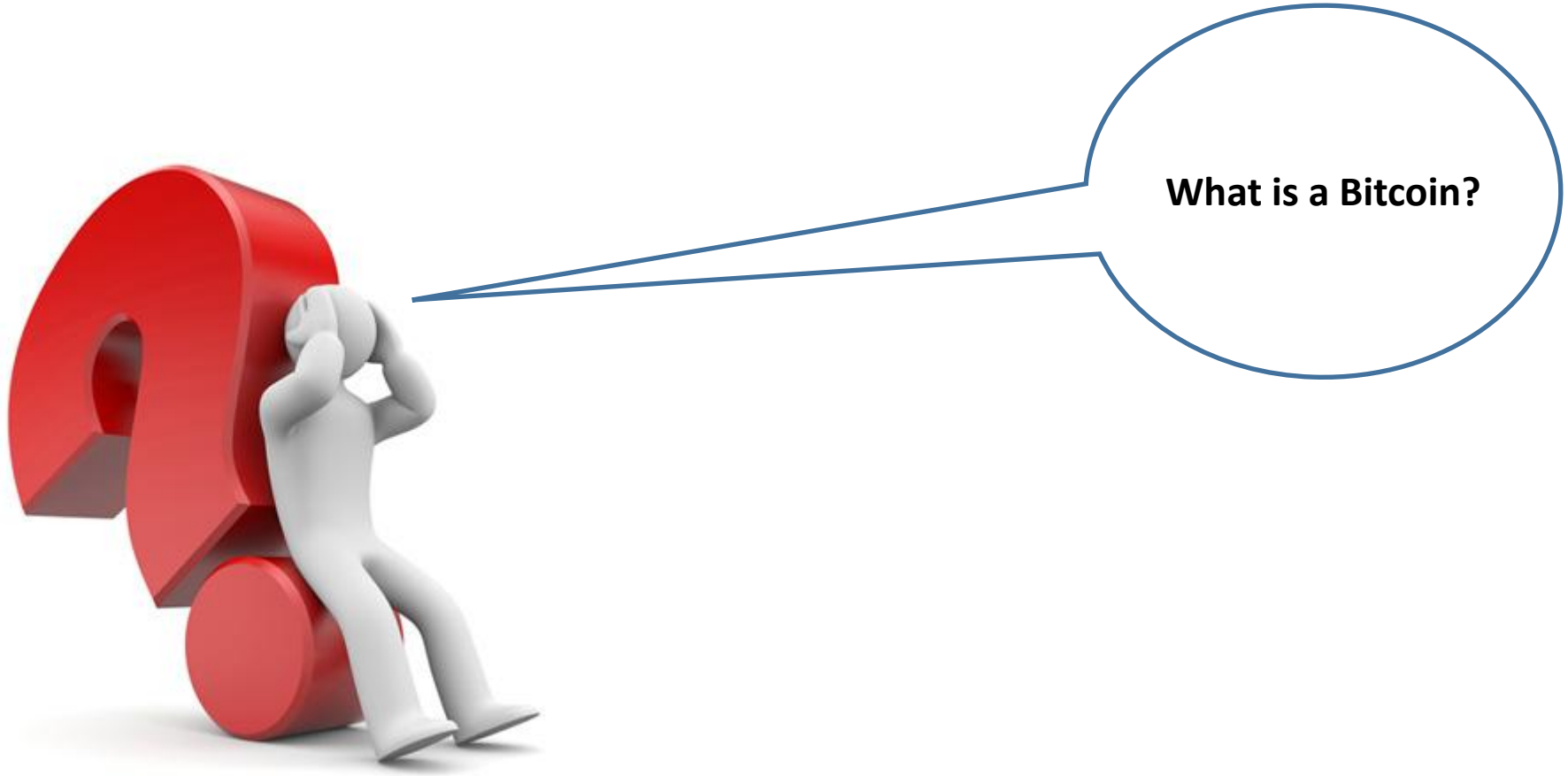
- Understand the drawbacks in current financial system
- Infer how spectrum of finance can be secured using distributed system
- Induce the key concepts which constitutes the Distributed System
- Infer various types of cryptocurrencies
- Deduce various uses of cryptocurrencies

Transformation in Trading Units

Transformation of Money



Bitcoin-A brief note



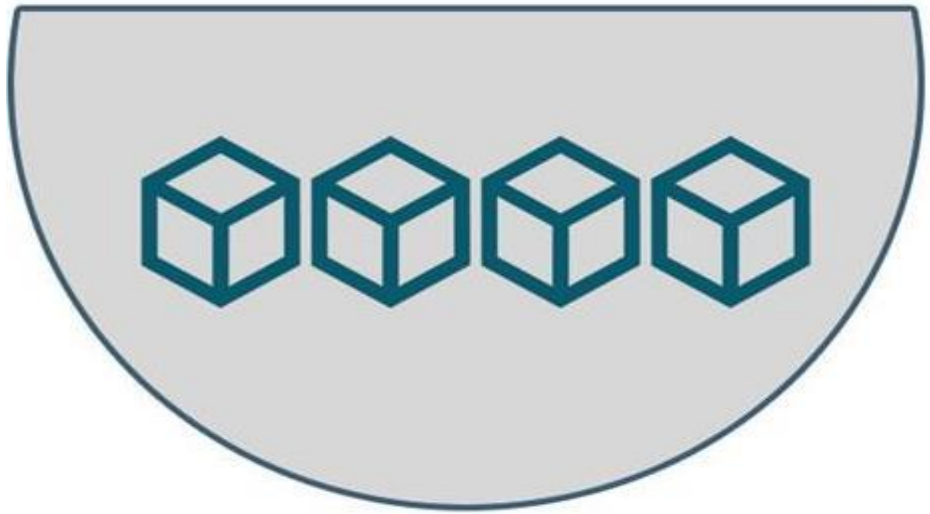
Bitcoin-A brief note

> **Bitcoin** is a type of cryptocurrency which is nothing but "**digital money".**
> And the underlying technology that enables moving of digital coins or assets among individuals is **Blockchain**

Blockchain

What is Blockchain?

> The blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value.



Definition Of Blockchain

Blockchain is simply a data structure where each block is linked to another block in a time stamped chronological manner.

It is a distributed digital ledger of an immutable public record of digital transactions.

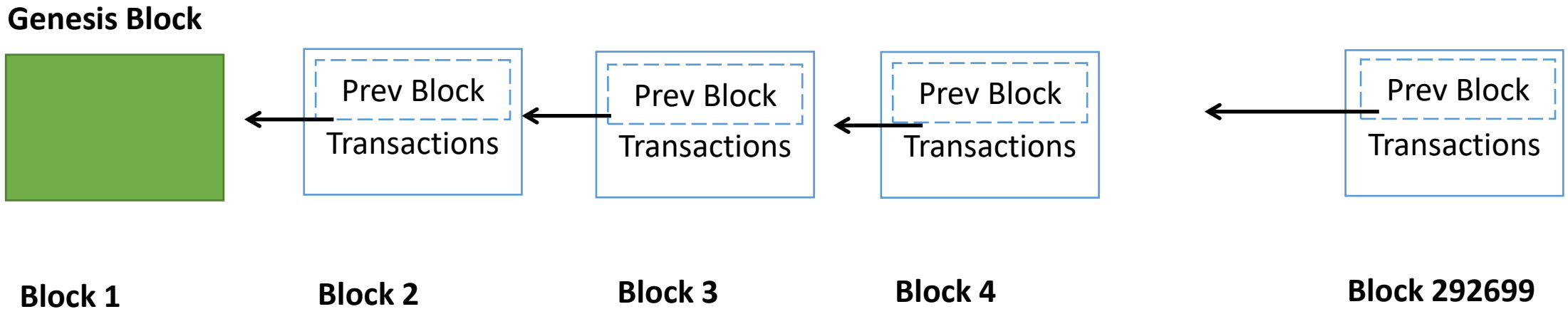
Every new record is validated across the distributed network before it is stored in a block .

All information once stored on the ledger is verifiable and auditable but not editable.

Each block is identified by its cryptographic signature.

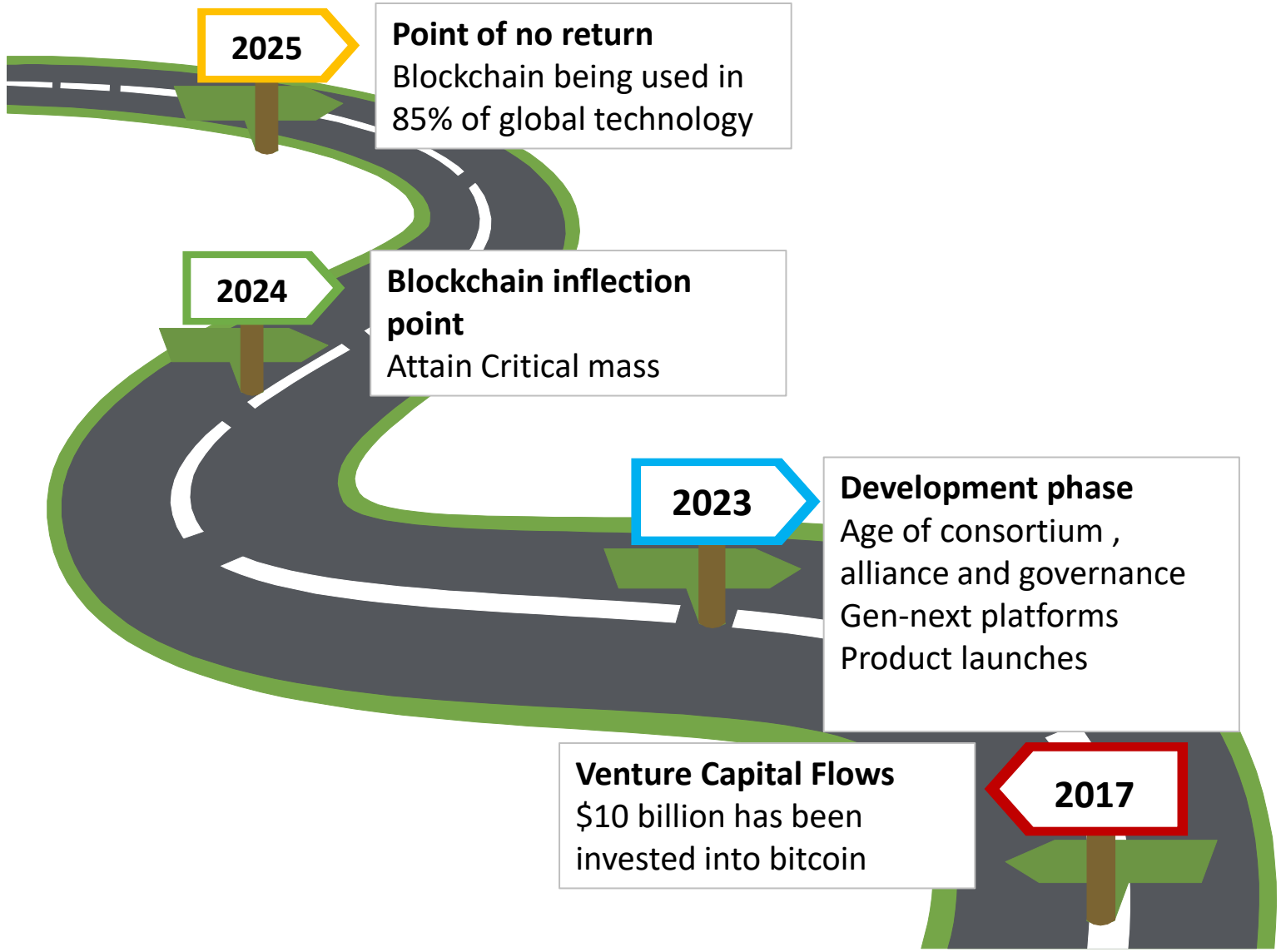
The first block of the Blockchain is know as the Genesis block.

Definition Of Blockchain



To access data of the first ever created block, you have decussate from the last block created to the first block.

Blockchain Tectonic Shift



Blockchain Tipping Point & Societal Impact

2023

Tax collected by Govt.

1 trillion lot sensor connected to internet

Digital transformation outreach 80% of population

2025

Sharing economy 2.0- P2p Economy Maturity

2026

Smart city fully operational

2027

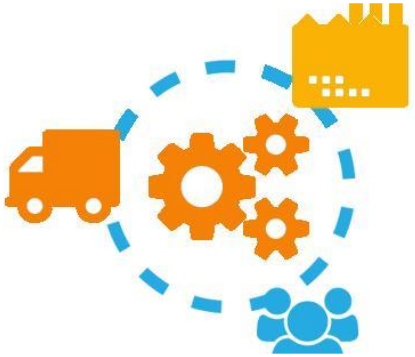
!0 % of world GDP will be on Block chain technology

Current System

How Current System Works?

> Before going Deeper into the details of Blockchain, let's see, how our current system works

How Trading Happens Using Current System



Trade is recorded in Bookkeeping(An offline ledger where transaction details are stored)

Bookkeeping is isolated and closed to public

For this reason we use trusted third parties or middlemen we trust to facilitate and approve our transactions

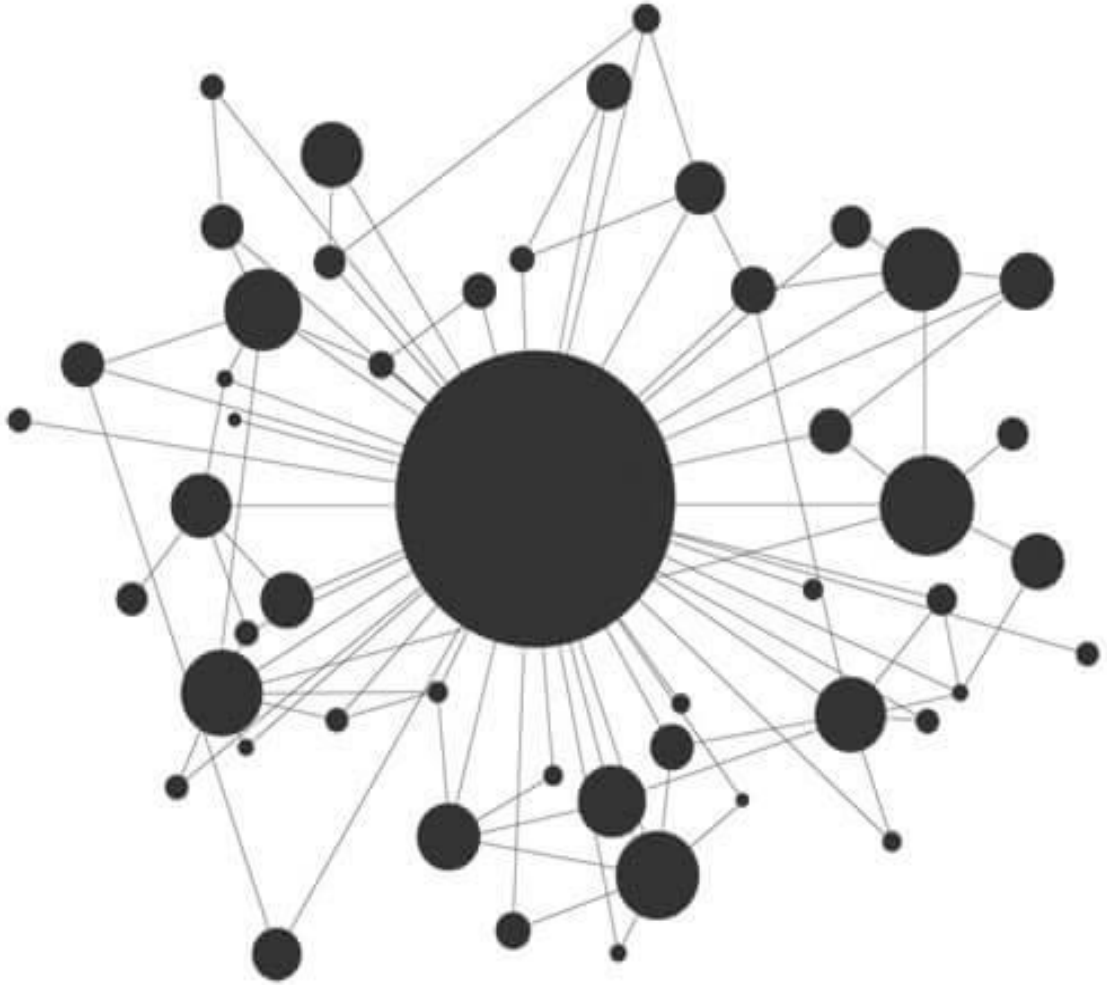
Problems which current system faces

1. Banks and other third parties take fees for transferring money
2. Mediating costs increases transaction costs
3. Minimum practical transaction size is limited; Cutting off the possibility for small casual transactions
4. Financial exchanges are slow. Checking and low cost wire services take days to complete
5. System is opaque and lacks transparency and fairness
6. Also, central authority in control can overuse the power and can create money as per their own will

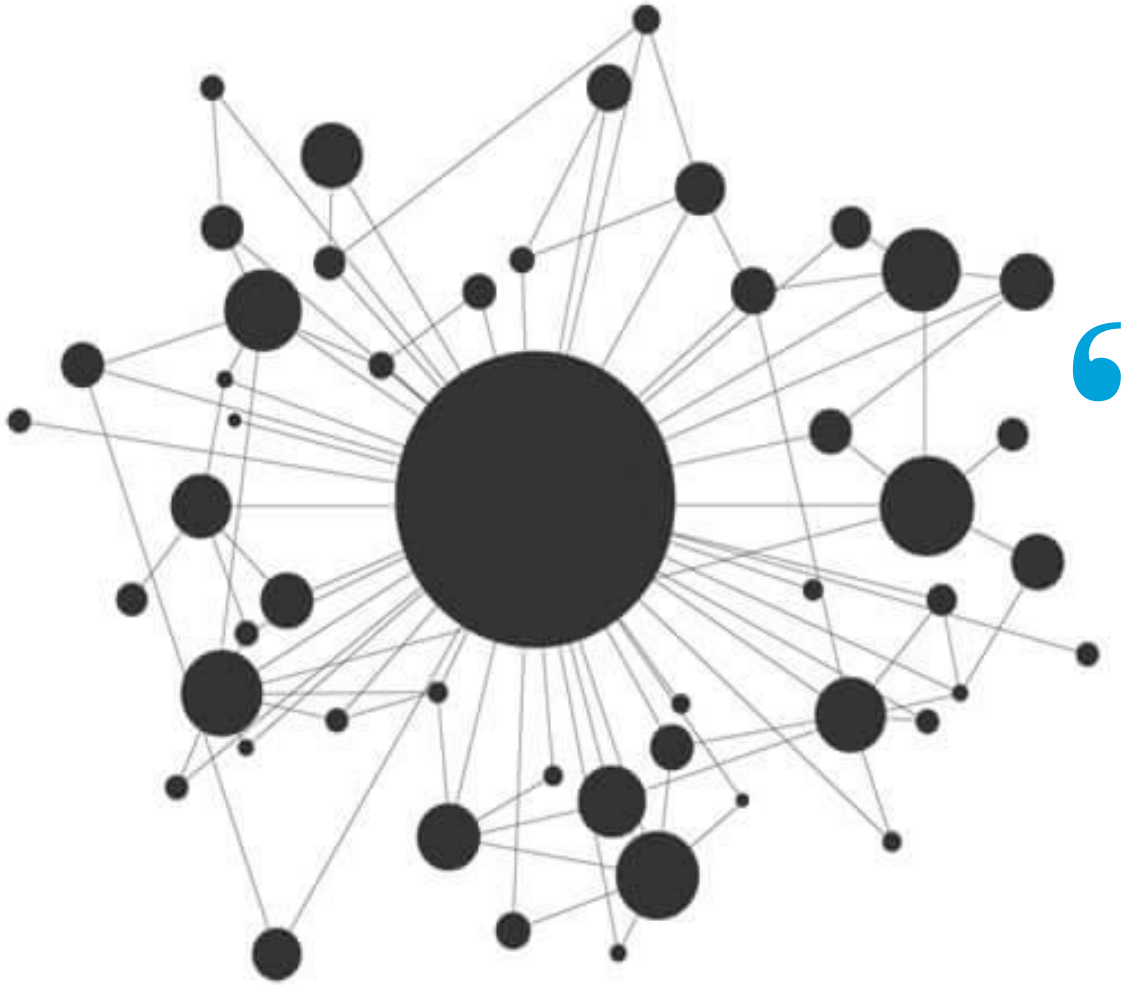
Possible solutions

We need a system which:

- Eliminates the need of middlemen or Third Parties thereby making transaction costs nil or negligible.
- Enhances transaction execution speeds and can facilitate instant reconciliation.
- Is Transparent and tamper resistant in order to avoid manipulation or misuse.
- Currency creation is not in control of any central authority.
- Is regulated to maintain the value of the currency.

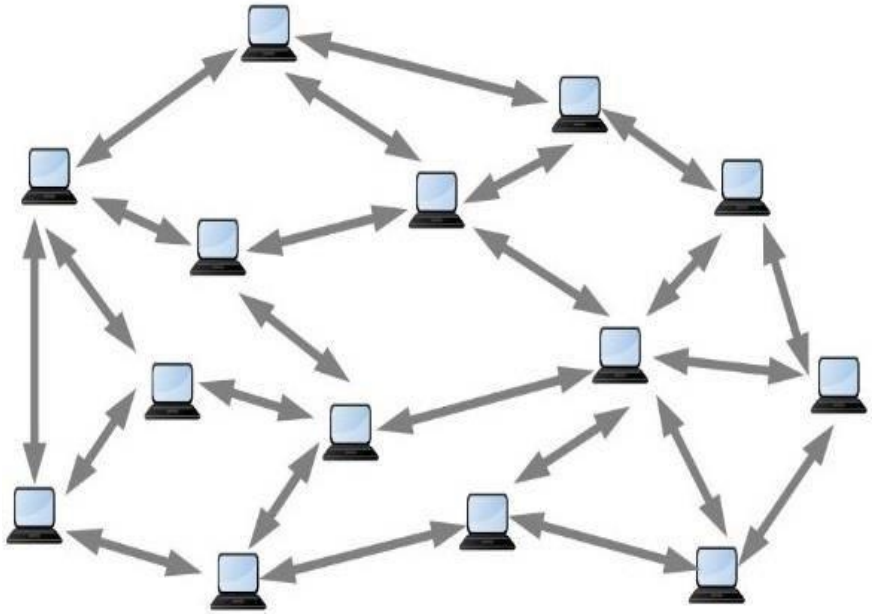


Distributed System to Solve the Problem



Distributed System enables a network of computers to maintain a collective bookkeeping via the internet
This is open and is not in control of one party
It is available in one ledger which is fully distributed across the network

Distributed System



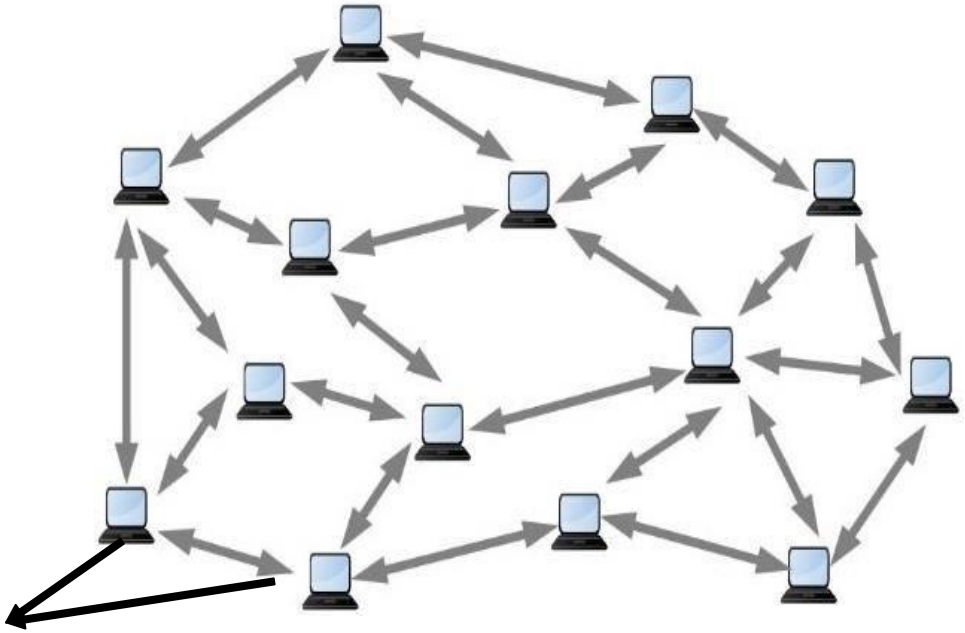
A system where two or more nodes work with each other in a coordinated fashion in order to achieve a common outcome

It's modelled in such a way that end users see it as a single logical platform.

What is a Node?

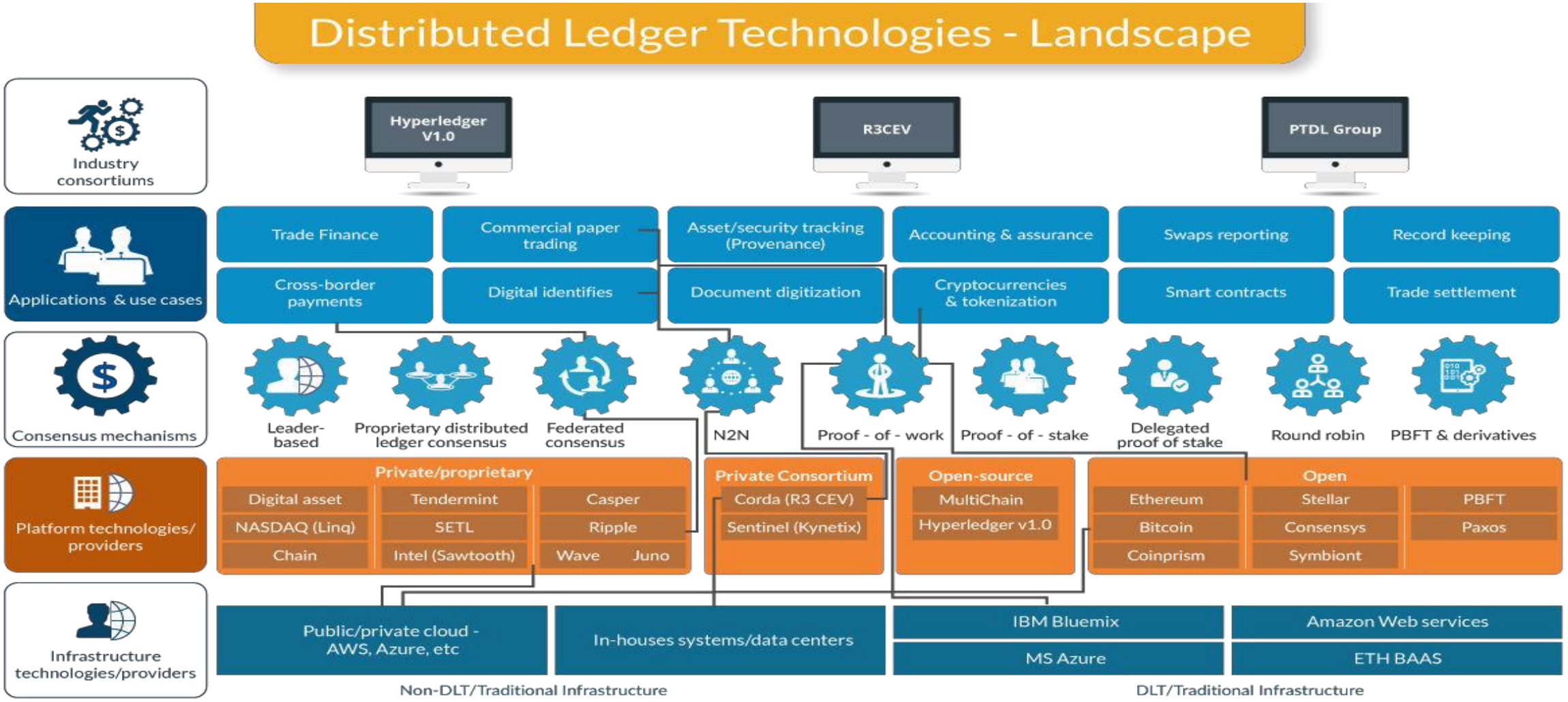
A node can be defined as an individual processing unit in a distributed system.

All nodes are capable of sending and receiving messages to and from each other



Nodes in Distributed System

Distributed Ledger Technologies



Transaction in Distributed Network

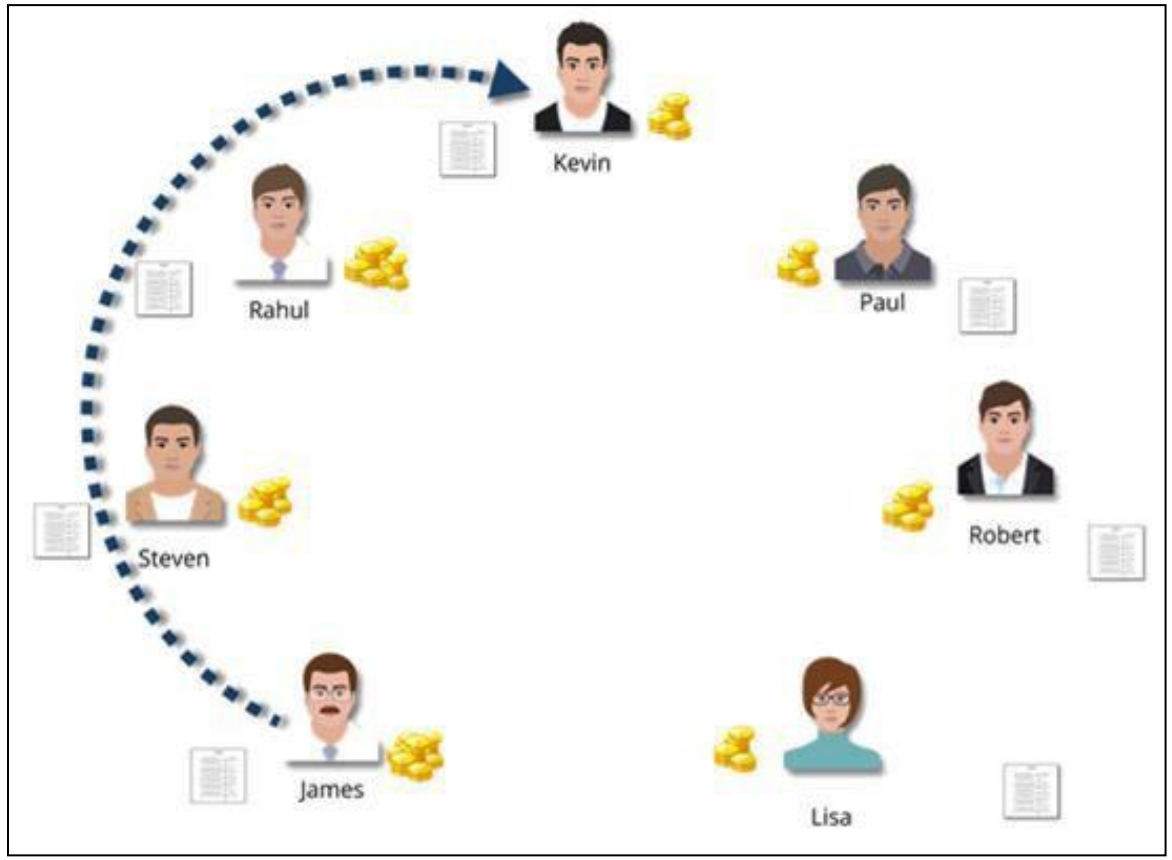
Transaction in a Distributed Network

Now that you have understood what is a role of a distributed system. Let's see how transaction happens in a distributed system.

Initiating a Transaction in a Network

Scenario:
Let's say James wants to transfer money to his friend, Kevin?

Now, since there is no central authority in the system, there can be certain questions that might cross your mind.



Curiosity Questions?

How to verify from where the transaction is initiated and to whom it is sent?

How is the transaction faster than the present system?

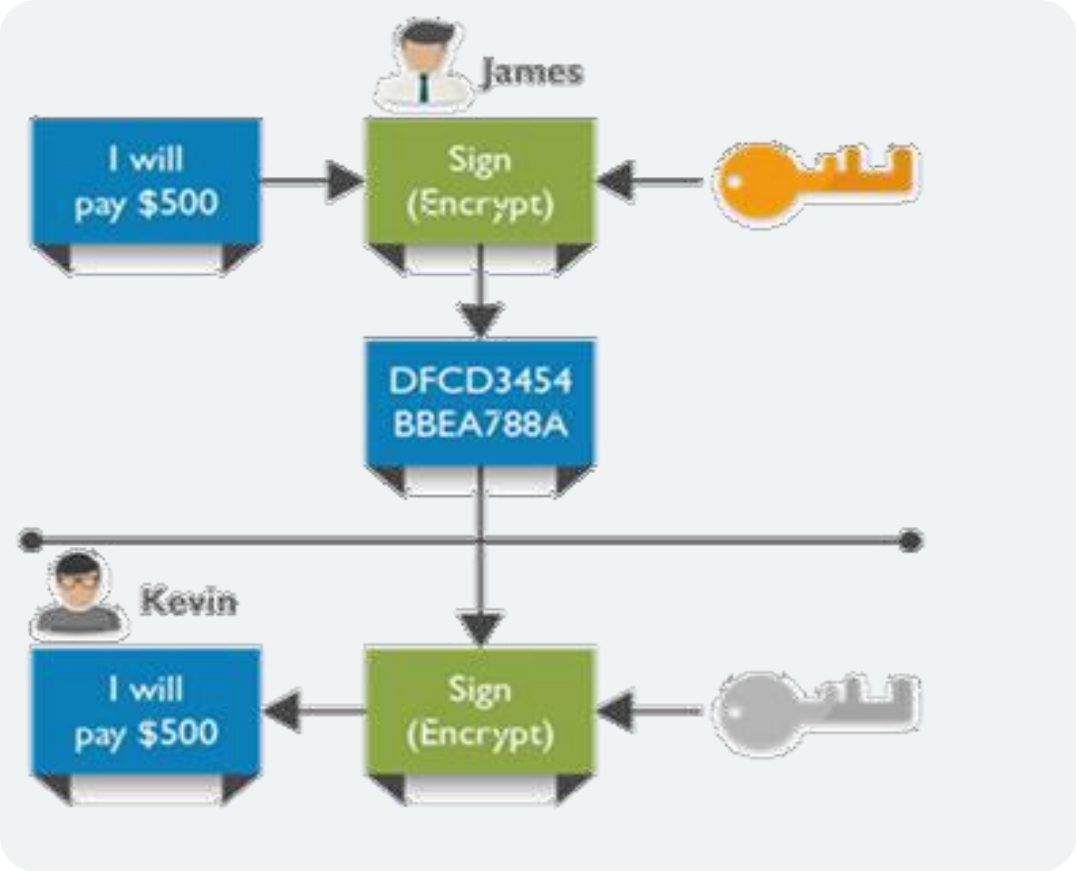
Who validates the transactions as there is no central authority?

How is currency generated?

Encountering your Curiosity

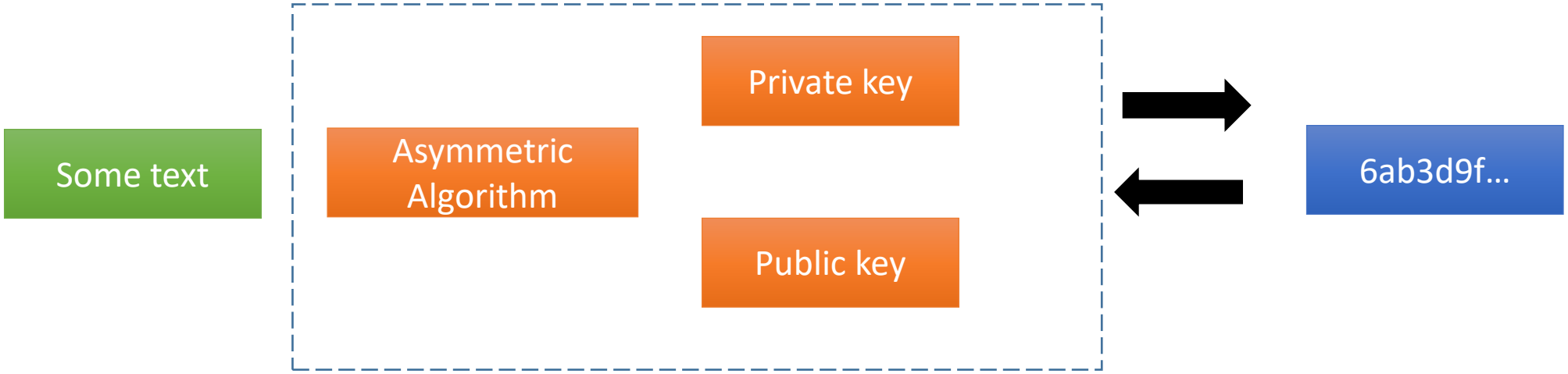
To satisfy your curiosities, first let's see how a transaction is initiated in a distributed network.

Initiating Transaction



To initiate a transaction **James** uses two piece of information **private key** and **public key**

Public Key Cryptography



This approach involves two different keys:

- One key is purposely kept private, the other is provided to the other party(or often the public)
- If you use private key to encrypt then the public key can decrypt
- If you use the public key to encrypt then you use the private key to decrypt. This is called asymmetric encryption

Storing of Keys

Question:
Where are these keys stored when James transfer money to his friend, Kevin?

The Keys are stored in James's wallet.

Bitcoin Address and Wallet

Bitcoin Address

> An identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3. Represents a possible destination for a bitcoin payment.

1GPaJQLww88wLsrcNNzHjFjLaJBsT58awX

Specimen of a Bitcoin Address

Bitcoin Wallet

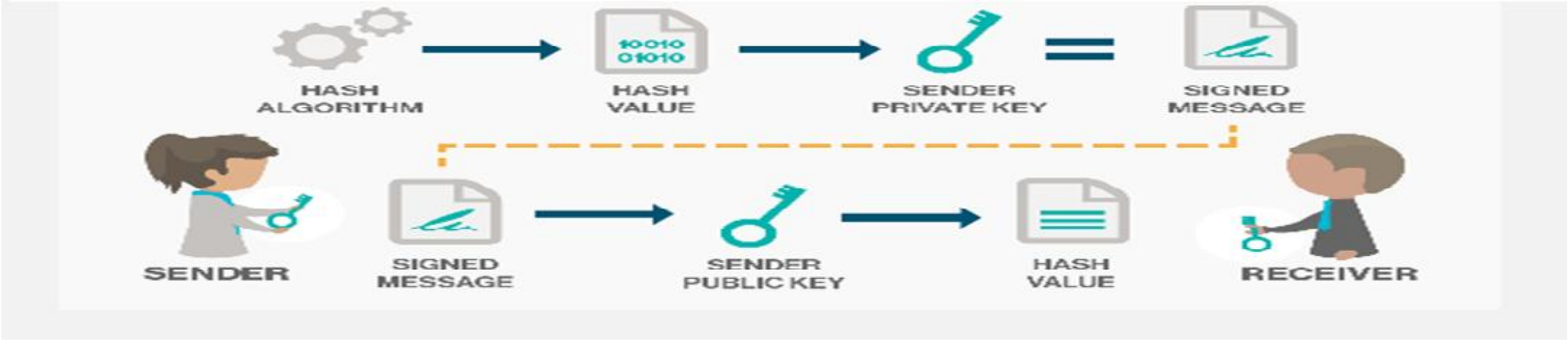
A “wallet” is basically the Bitcoin equivalent of a bank account.

- It allows you to receive bitcoins, store them, and then send them to others
- Once a bitcoin wallet is installed on your computer or mobile device, it will generate your first bitcoin address
- Each address has its own balance of bitcoins
- However the address can be changed whenever you want to.

Types of Bitcoin Wallet

Transaction

Sending a Transaction



Transaction is broadcasted in the form of a **Digital message**.

Just like your signature provides the proof of ownership on the document, similarly, **digital signature** provides the proof that the **transaction is genuine.**

Unlike a handwritten password, digital signature is **unique** for every transaction.

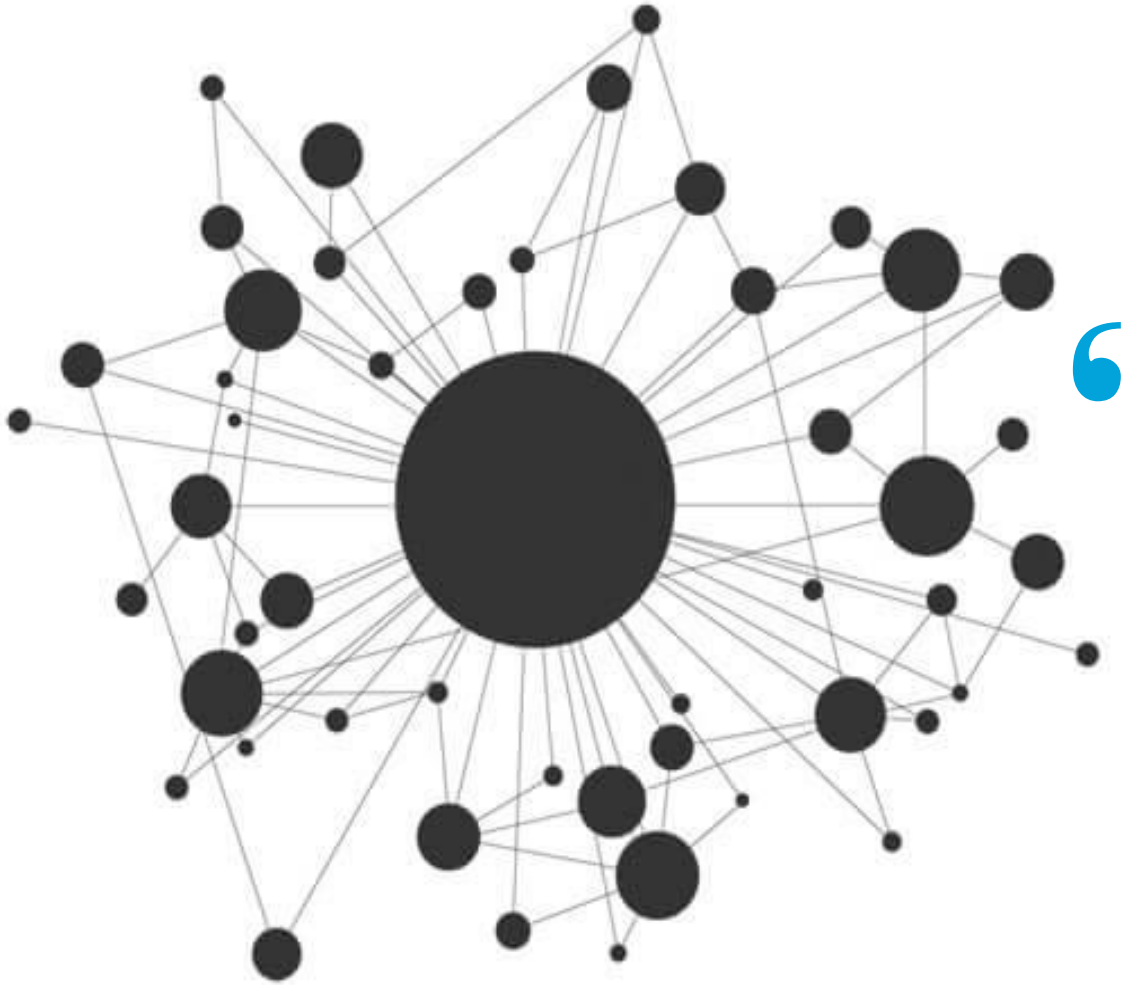
Transaction Propagation

> After the transaction is created it propagates in a distributed Network.

Curiosity Questions?

How is the transaction faster than the present system?

Transaction Propagation in Distributed Network



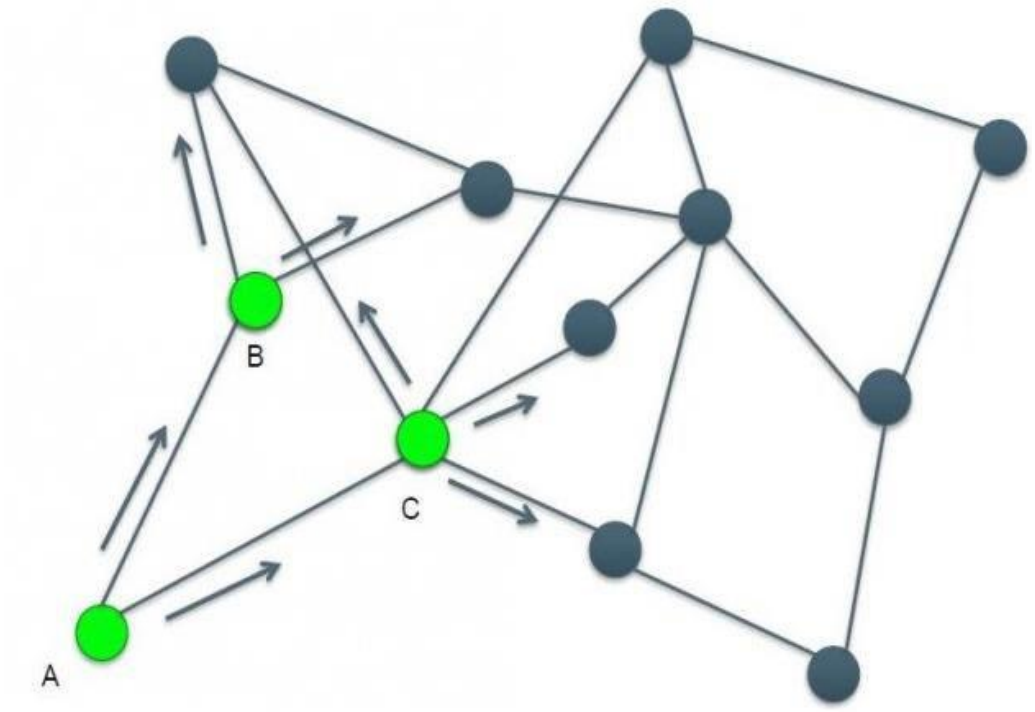
In a distributed architecture, transaction is transmitted peer-to-peer

Transmission of the transaction across the network takes around 1-2 seconds

Transaction Propagation in Distributed Network

Scenario:
Suppose A (a node in the Network) finds the transaction: Kevin pays 5 coins to James.

Node A broadcasts to the Peers B and C in the network.
Nodes (A, B, and C) check for the basic formats of the transaction and forward the transaction to their Peers. Like this the transaction propagates rapidly across the network.
Hence, it is faster and cost efficient as there is no middle-man.



Validation

Curiosity Questions?

Who validates the transactions as there is no central authority?

Who Validates?

There are some special nodes in the network who verify the transactions and maintains the ledger.
They are called Miners.

Miners (or Validators)

Miners are special Nodes which hold the copy of the ledger and verify the transactions happening in the network

Using state of the art cryptographic algorithm, miners validate the transactions across the network

In order for our digital monetary system to work, the miners must be able to confirm that:

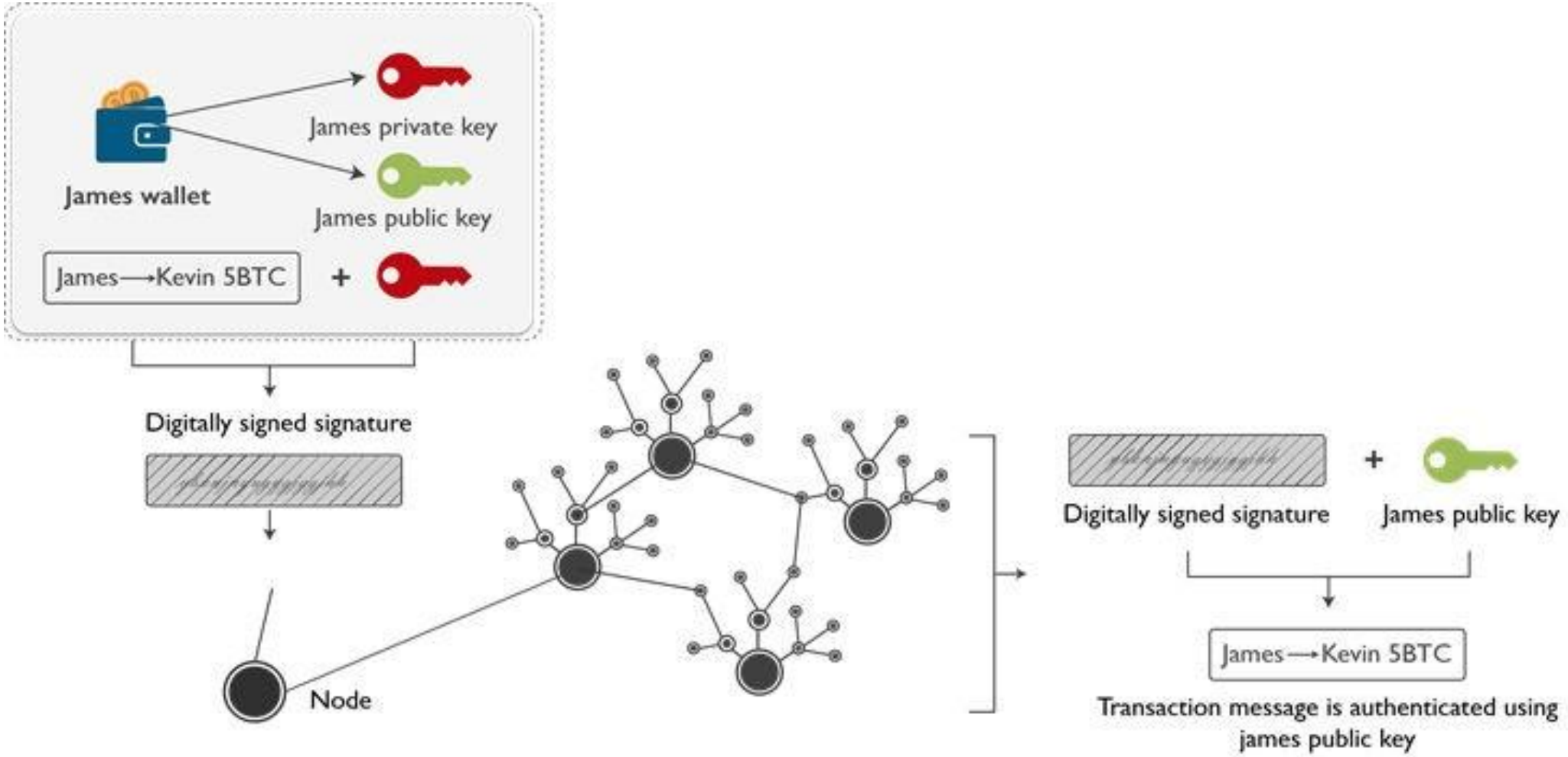
- The originator of the transaction possesses the funds being transferred.
- The originator of the transaction has obtained the funds by one of the means commonly recognized as valid

Verification

Curiosity Questions?

How to verify from where the transaction is initiated and to whom it is sent?

Digital Signature is used in Transaction Verification

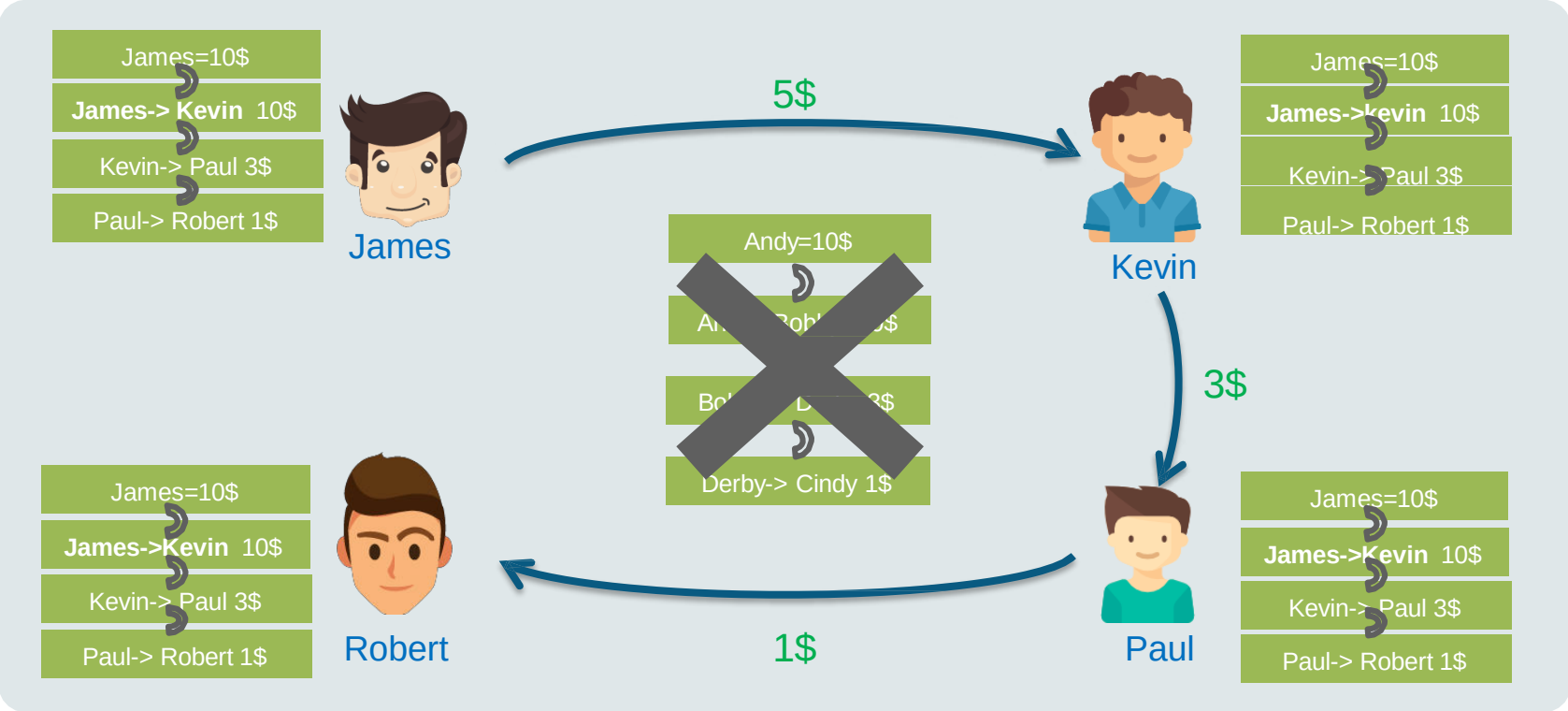


Storage

Transactions are stored in a ledger

> Once the transaction is verified it is stored in a shared ledger across the network

Distributed Ledger

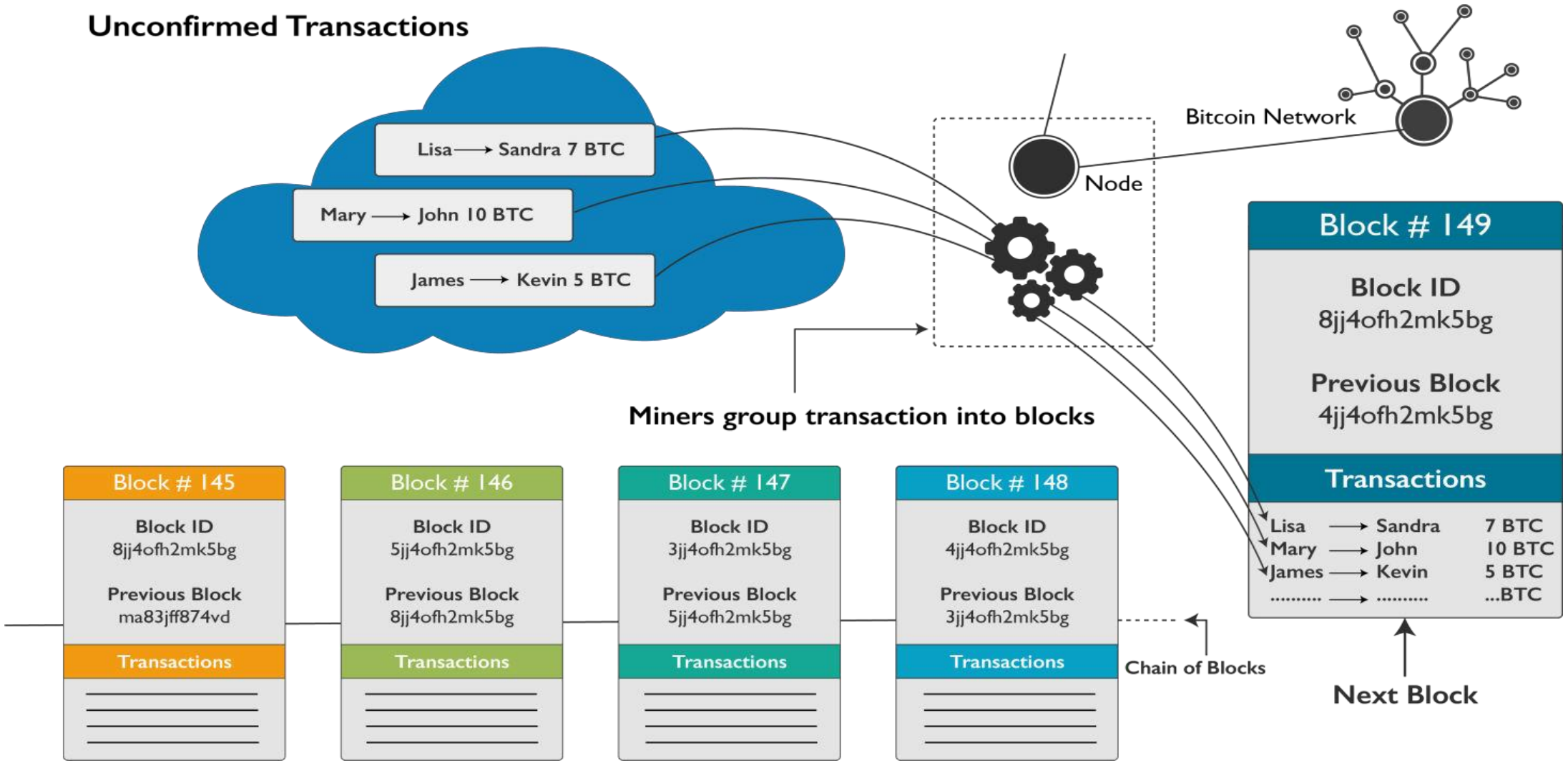


Ordering of Transactions

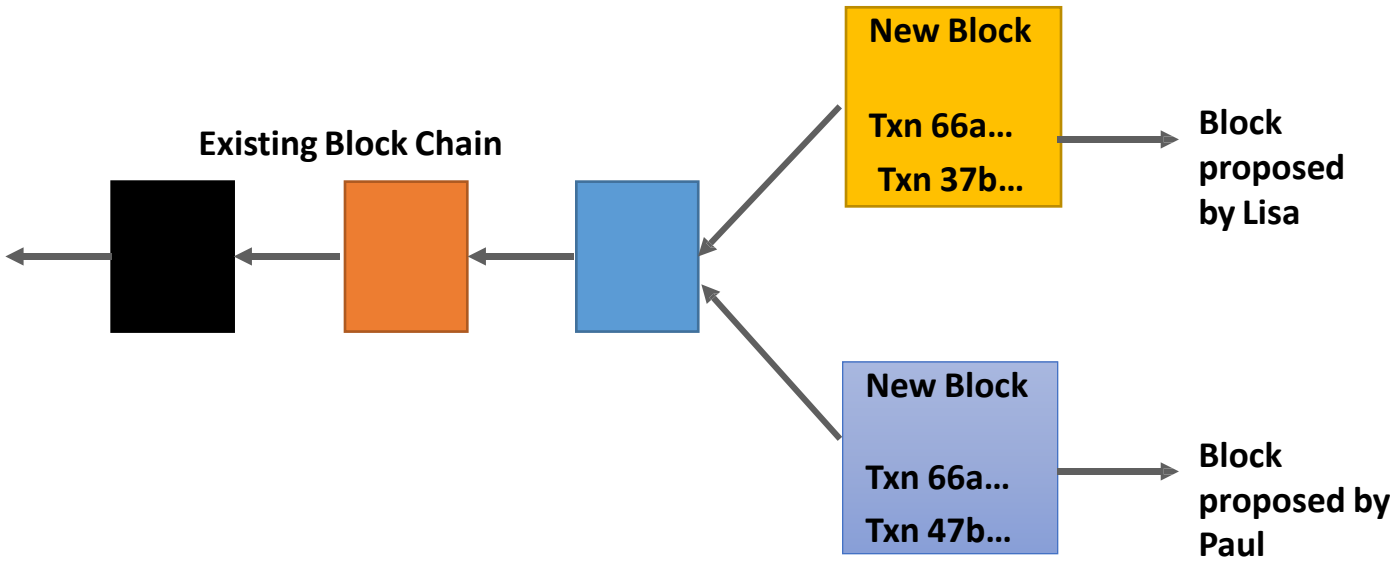
- Since, Transactions are passed from node to node, there is no guarantee that the order in which you receive them represents the order in which they are created
- To agree about the order of transaction is a challenge in a decentralized system

> **Therefore, cryptocurrency system orders transactions by placing them in groups called blocks and then links them in a chain.**

Miners Group the Transactions in a Block



Miners in the Network



- Various miners are constructing blocks, there could be several options to choose from. How does the network decides which block should be the next in the chain?

Whose block to consider?

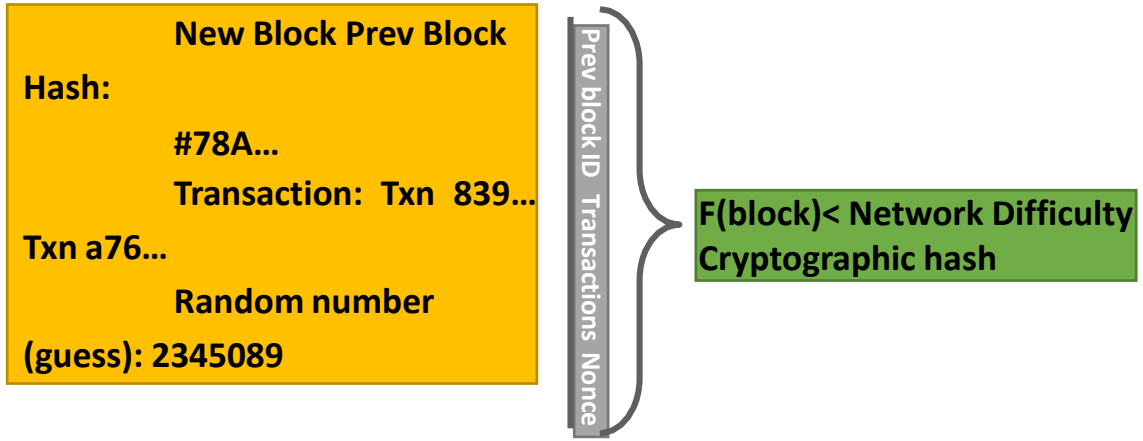
> There can be a number of miners constructing a block whose block is chosen by the network?

Proof of Work – Block Puzzle

Proof of work is a piece of data which is difficult(costly, time consuming) to produce but easy for others to verify and which satisfies certain requirements.

To keep the coin distribution predictable , puzzles becoming increasingly difficult to solve when more people work on them.

Part of Bitcoin solution is that each block must contain the answer to a special math problem



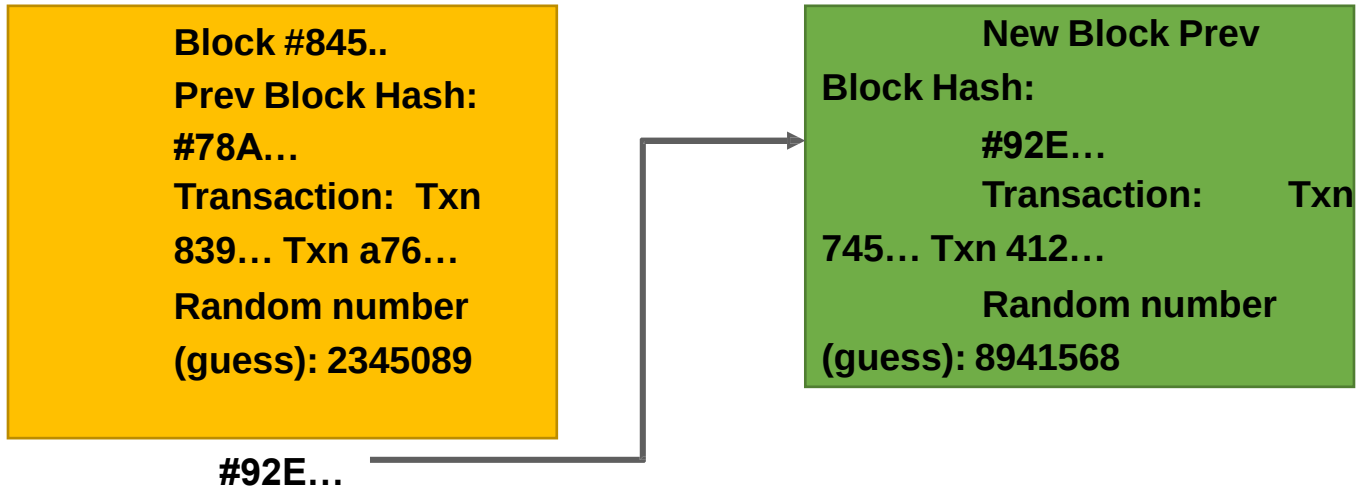
Proof of Work

There are 3 components which help in achieving the proof of work solution:

NONCE: A random number whose value is set so that the hash of the block will contain a run of leading zeros. The rest of the fields may not be changed, as they have a defined meaning.

HASH: A “fixed length “ number which results in large unchanged data when read.

TRANSACTION: Authentic transfers of Bitcoin ownership collected and recorded in BLOCKCHAIN



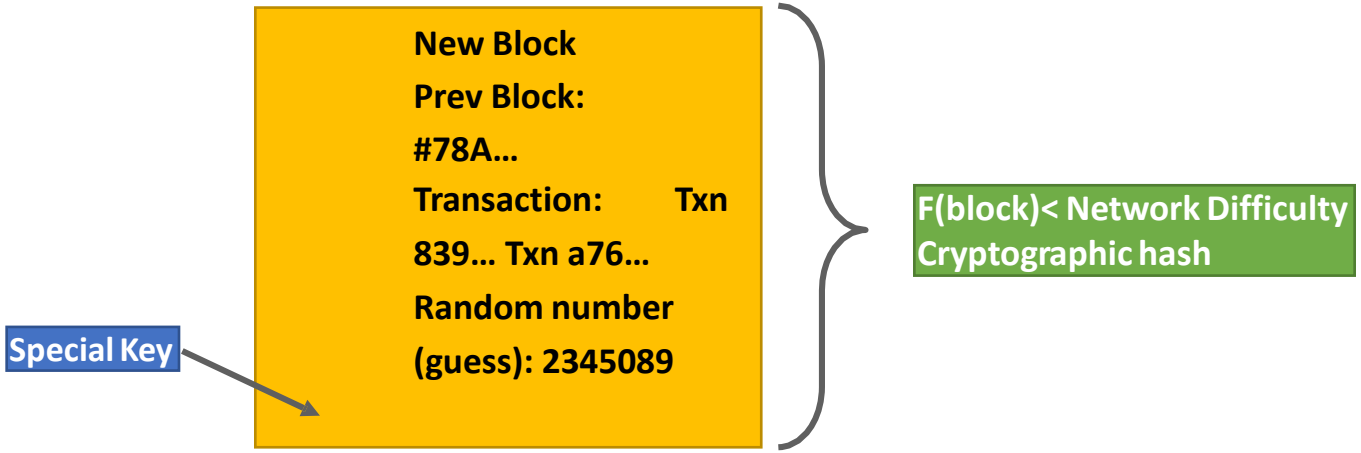
Finding the Puzzle – Why is it Hard?

The SHA-256 is a one-way function hence, brute force is the only way to a particular output value

On an average, it takes many random guesses to find a solution and thus the challenge is tough

It takes around 10 minutes on an average for someone to find the special key to the solution

Hence, a new block is created after every 10 minutes in the bitcoin network.



Security Properties of Hash Functions

Collision Free:

Given an input a it should be difficult to find different input b such that hash(a) = hash(b)

Hiding

A hash function H is hiding if: when a secret value r is chosen from a probability distribution that has high entropy, then given H(r , x) it is infeasible to find x. means concatenation of two strings.

Puzzle Friendly

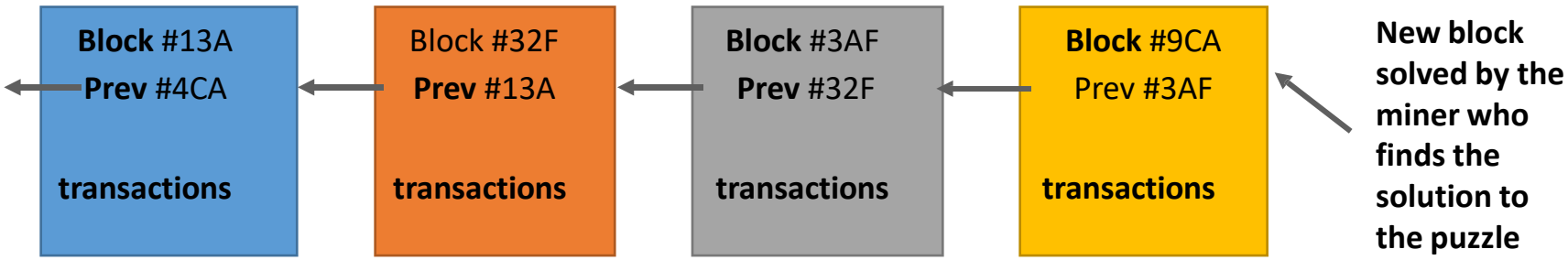
For all probable output value b, If m is chosen from a very high spread probability distribution, then it is not feasible to find the |alue̲å suÐh that hash of ŵ+dž=a

Why do Miners Invest their Resources in Validation?

> There is an incentive for a successful solving of a block.

Miners Reward – What do they do to get this?

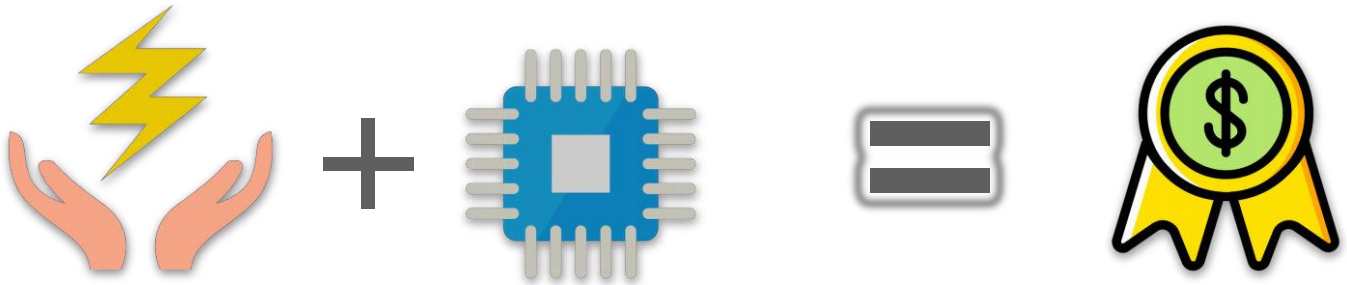
- Miners tries to find the key to the complex puzzle as per the algorithm
- Search for this key is random, hence a Miner needs to invest huge computational power and Electricity
- The miners are repeatedly guessing new keys until the first key is found that matches the puzzle
- The miner who finds this key, publishes the block to the network
- Other Miners stops creating their blocks and will take the published block, validate it, and add it to its ledger



The Reward

Since Miners use their valuable resources to validate the block, they are given monetary award

In case of bitcoin they get some newly created bitcoins as a reward



Electricity **Computational Work** **Monetary Reward**

Exhausting resources to solve the puzzle means the miner has actually solved the puzzle- **proof of work**

Currency Generation

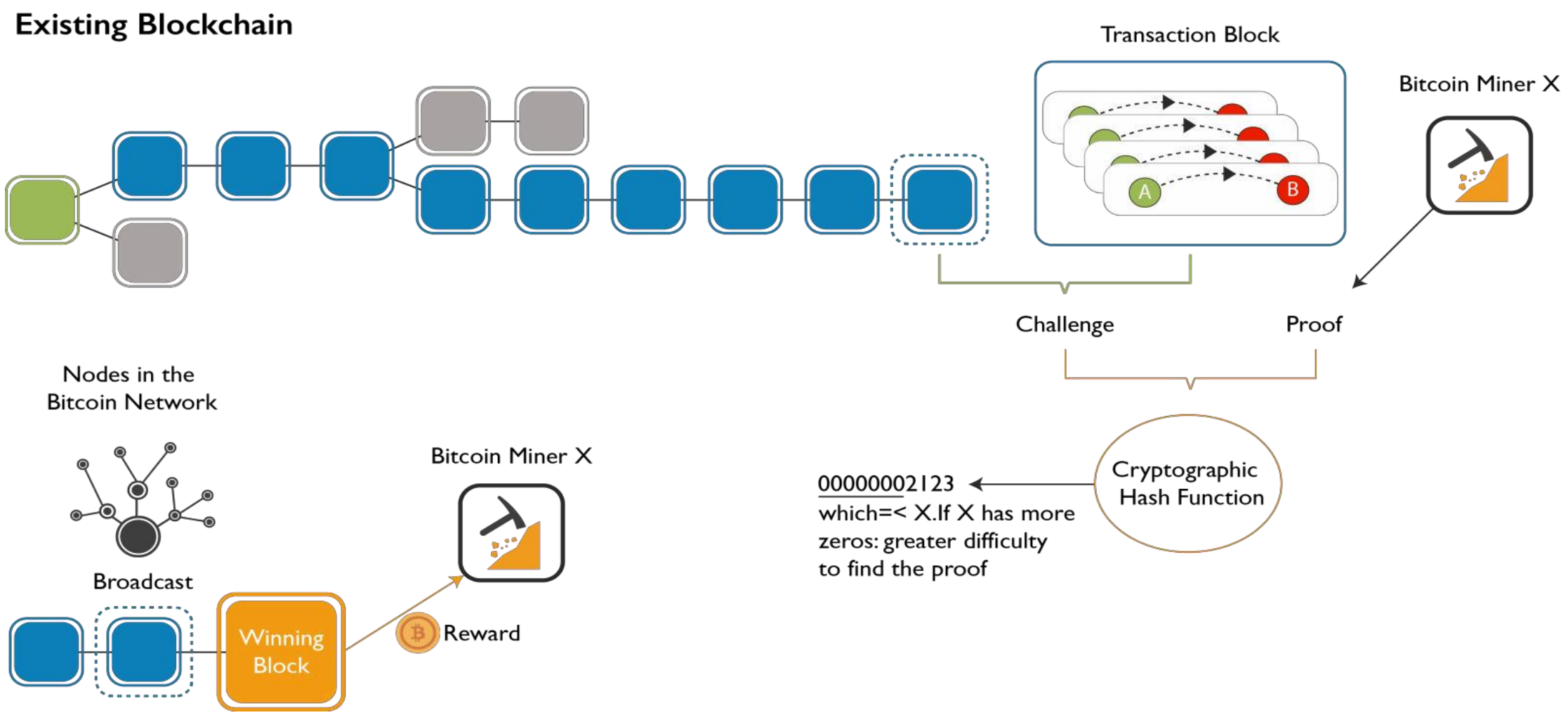
Curiosity Questions?

How is currency generated?

Currency Generation

- As a result of incentive to Miner’s, new bitcoins are generated and sent to the Miner’s address.
- A pre-defined schedule limits the total number of bitcoins so that they gradually approach a total of 21 millions.
- The limit of 21 million bitcoins is "hard-wired" in to the protocol, and there will never be more bitcoins than this. Unless of course, if they update the protocol in future.

Illustrating the Proof-of-Work



If more than One Block get Solved in the Same Time

I have understood that the first miner to provide proof of work will get the reward. What happens in the case when more than one block gets solved in the same time

If more than One Block get Solved in the Same Time

> Yes, this is possible indeed! Such a contradiction is solved by the consensus rules.

Consensus Algorithm

Consensus algorithms are central to the functioning of any blockchain.
There is a contradiction among the nodes about the blocks in the network, such a contradiction is resolved by the Consensus rules

01 **Consensus is the task of getting all processes in a group to agree on some specific value based on the votes of each processes**

02 **With a consensus algorithm, we need to get unanimous agreement**

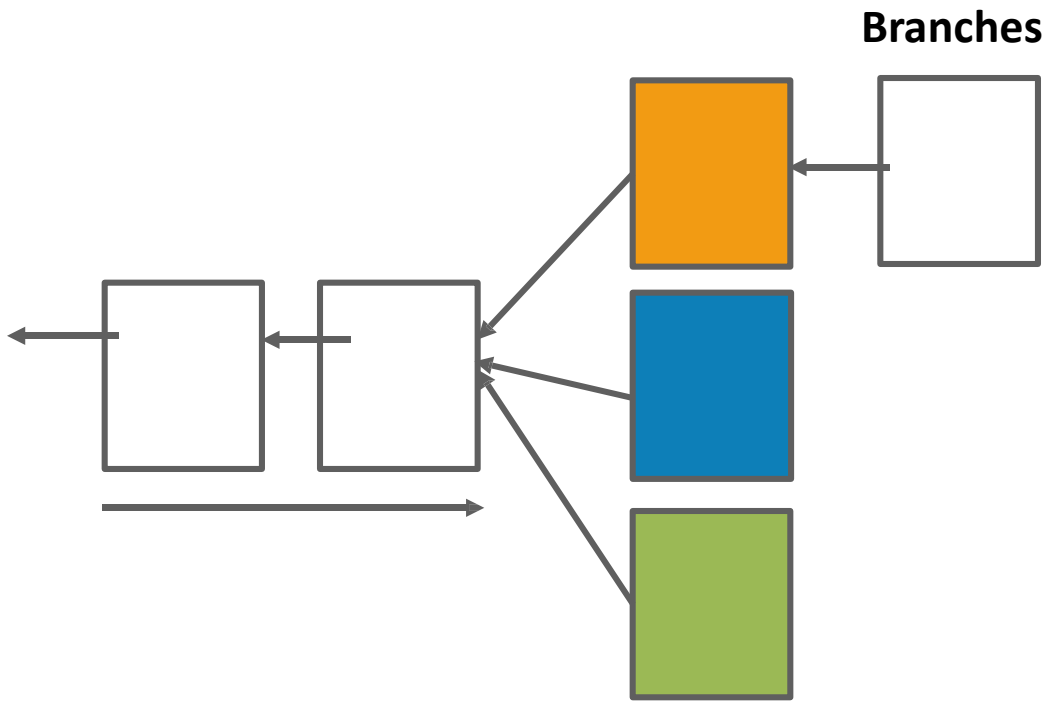
03 **Any algorithm that relies on multiple processes maintaining common state relies on attaining a consensus**

Several Branches

Although, the problem is tough, however there are chances that more than one block will be solved at the same time

Several branches in the blockchain are possible in such cases

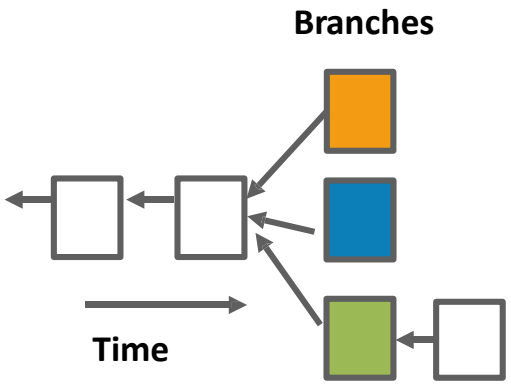
Everyone should simply build the blocks on top of the first block that they receive



Several Branches

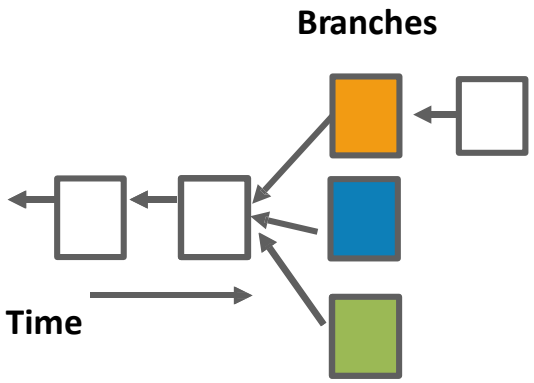
Other Nodes may have received the blocks in different order

They will be building on the block they first receive



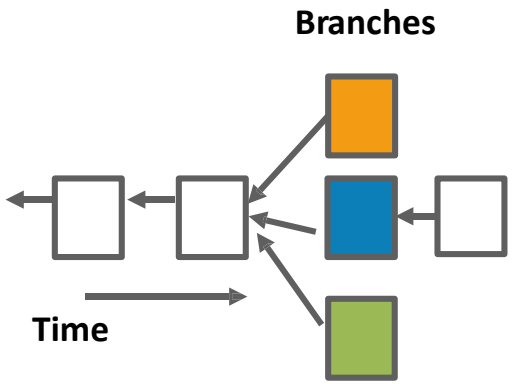
Paul's Blockchain

Paul received green block first, hence he builds the next block on top of green



Robert's Blockchain

Similarly, Robert received orange first, hence he builds the next block on top of orange

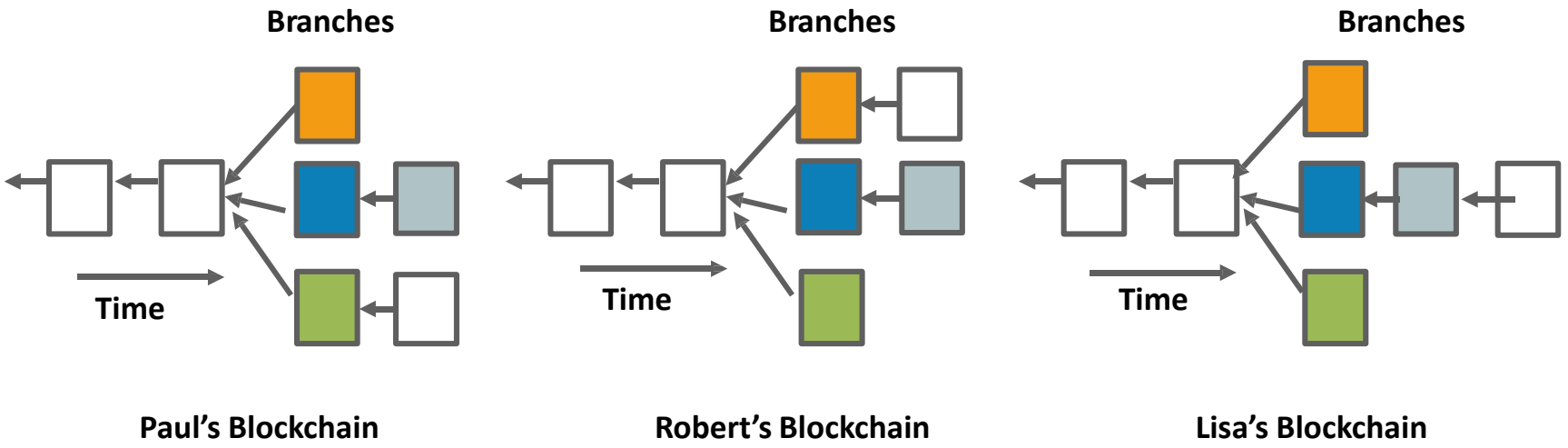


Lisa's Blockchain

Also, Robert received blue first, hence he builds the next block on top of blue

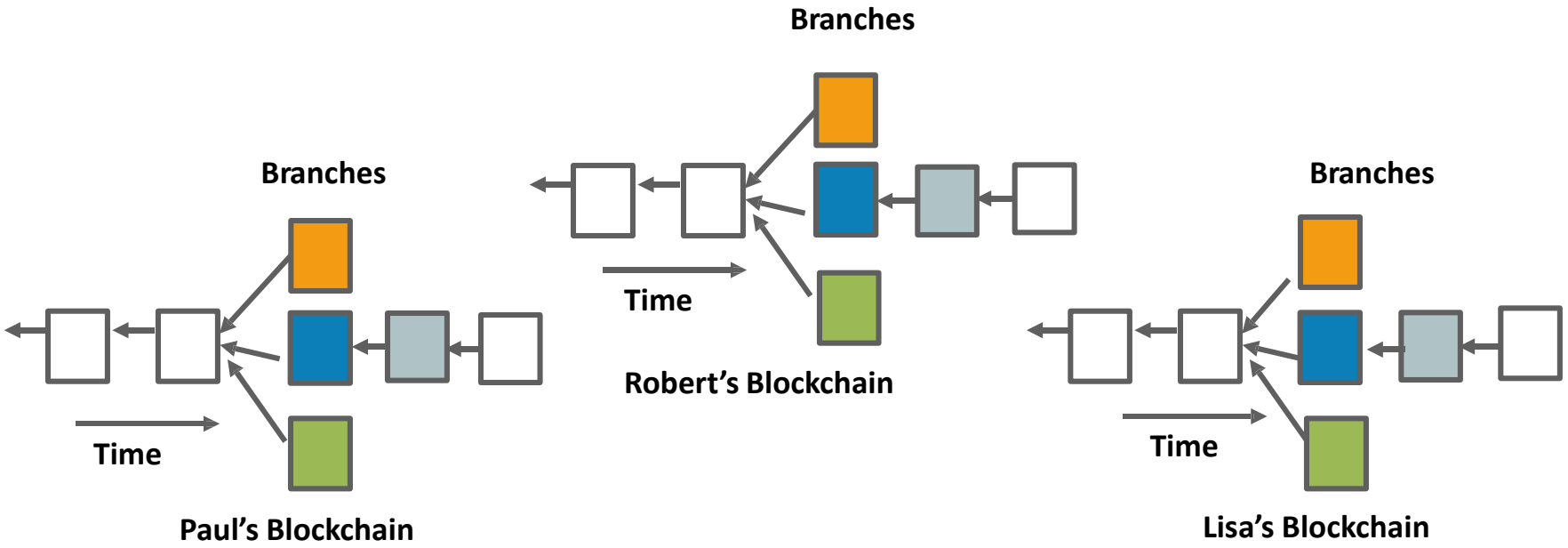
What Happens When the Next Block is Solved?

The tie gets broken when someone solves the next block, because it is very rare for this situation to happen multiple times in a row



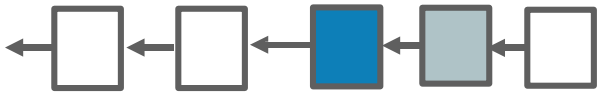
Switch to Longest Chain Available

Blockchain quickly stabilizes in this situation. The general rule is to switch to the longest chain available.

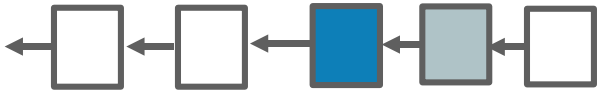


Longest Chain

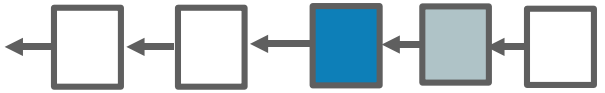
Paul's Blockchain



Robert's Blockchain



Lisa's Blockchain



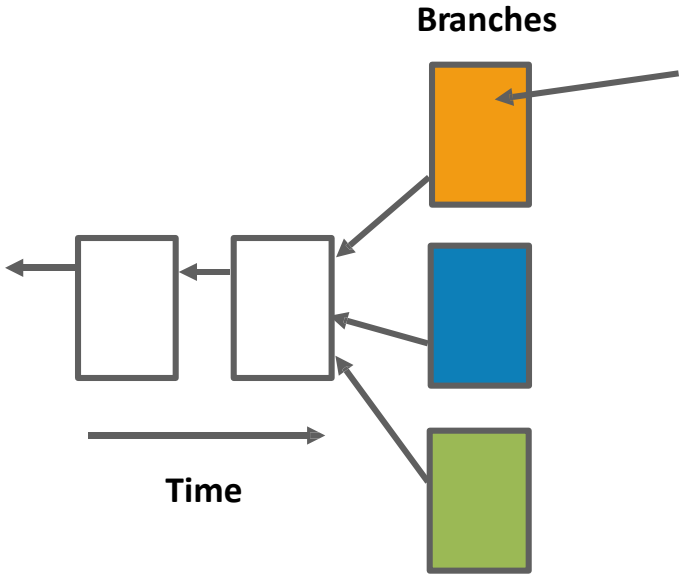
The Blockchain quickly Stabilizes. Every node is in agreement with the current state of the ledger

Transaction in Shorter Branches

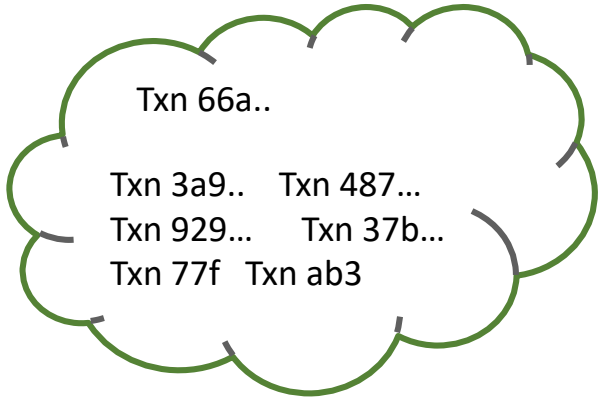
I What happens to the transactions which finds themselves in shorter branches?

Transaction in Shorter Branches

Such transactions go back to the pool of unconfirmed transactions and will be picked later in the block by the Miners



Transaction in the shorter branches lose its place in the longer chain



Transaction in the Shorter branch go back to the pool of unconfirmed transaction and will be included later in the block

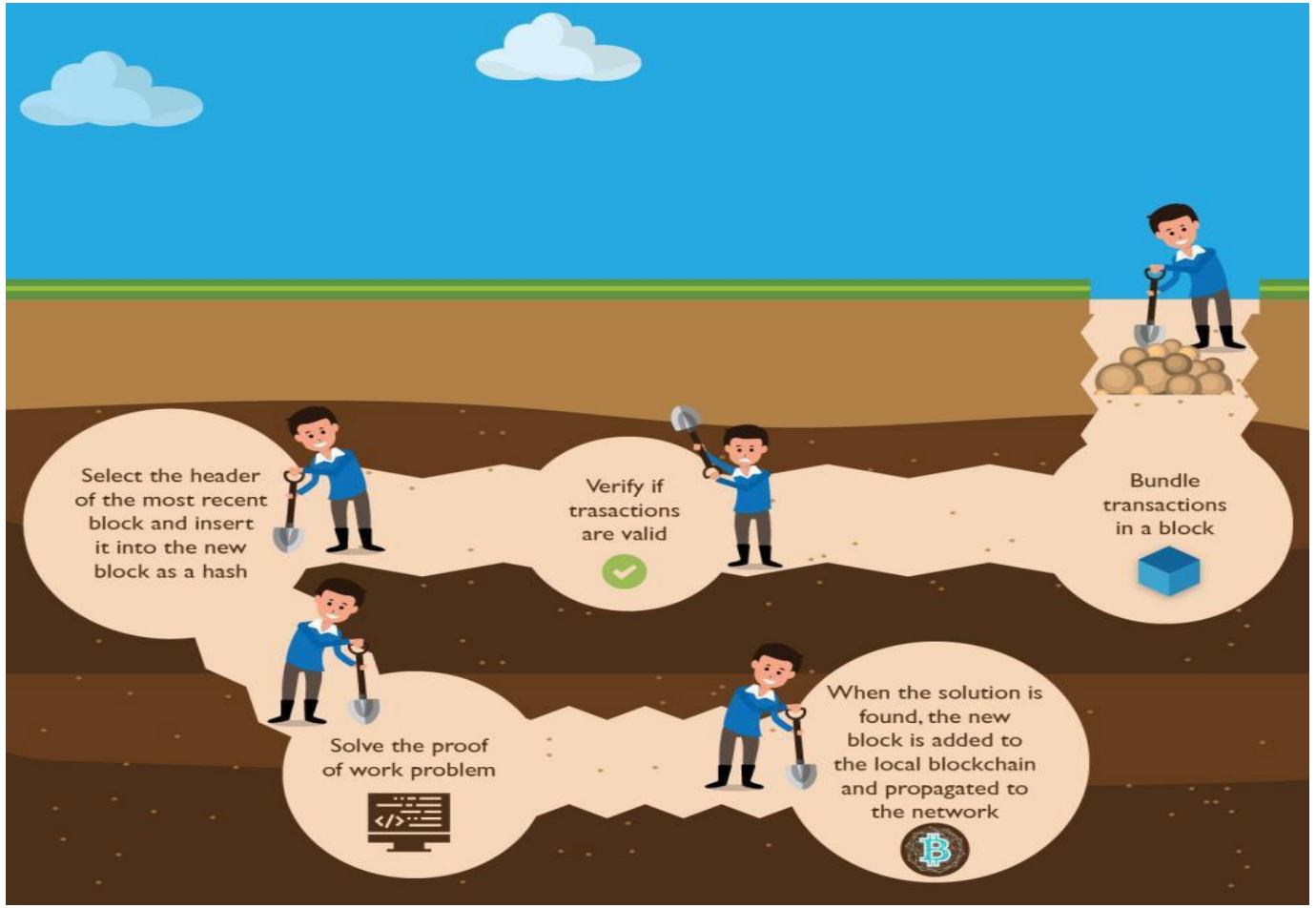
What if a Miner tries to Cheat with the System

Since there is a reward for solving a block, there are chances that a miner might gives a wrong solution to the block. What happens in such case?

- After creating a block miner has to publish the block with the proof of work to the network
- Other miners validates the block to ensure the authenticity
- If the proof of work provided is wrong, the block is considered to be invalid
- As a result of which the miner end up exhausting their resources without getting any reward

Therefore, the consensus algorithm does not allow anyone to cheat the system.

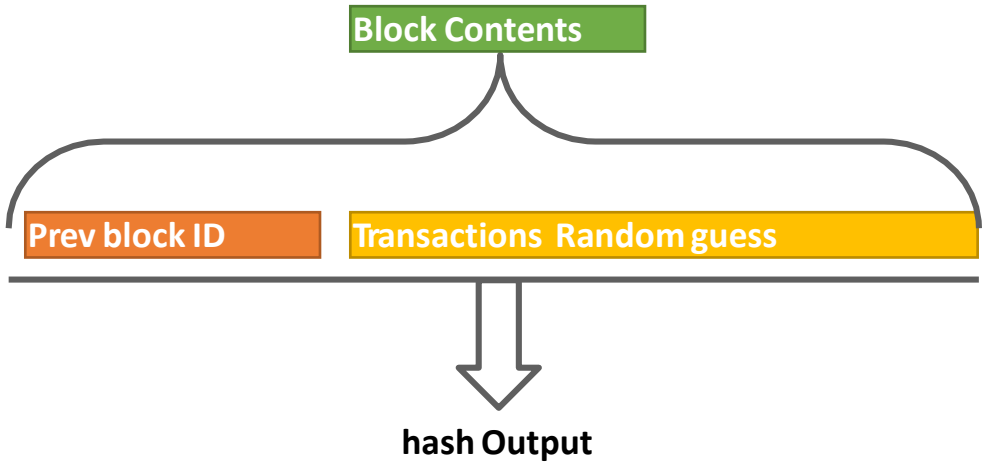
Mining at Glance



What if Someone tries to Hack the System?

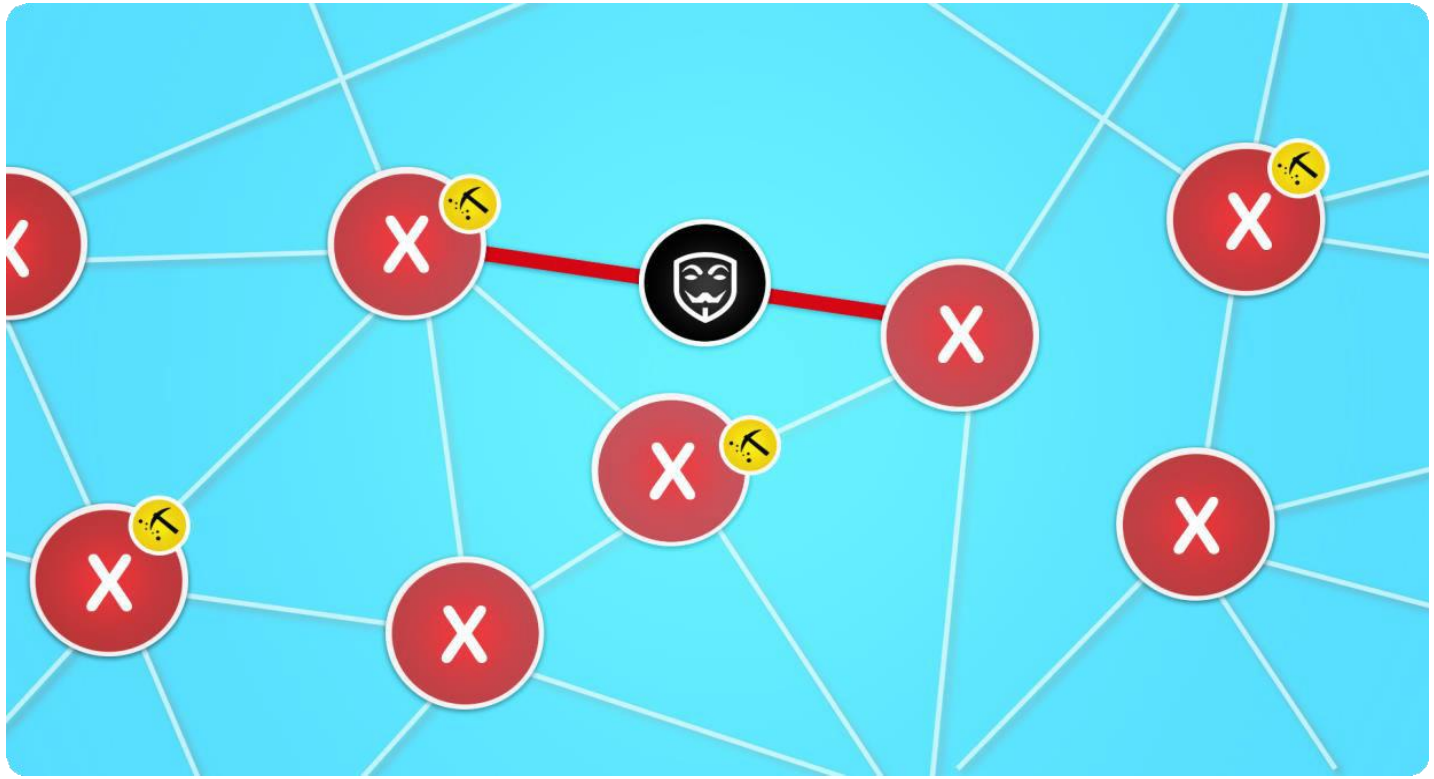
What if somebody tries to alter the transaction in the block?

Once a block is solved the cryptographic hash output becomes the identifier of that block



If someone tries to alter any transaction in any of the block , the hash of the block changes

Consequently, Hash of Every Block Changes



Nodes will not arrive at the consensus and hence the fraud can easily be detected

There is no Way to Alter the System

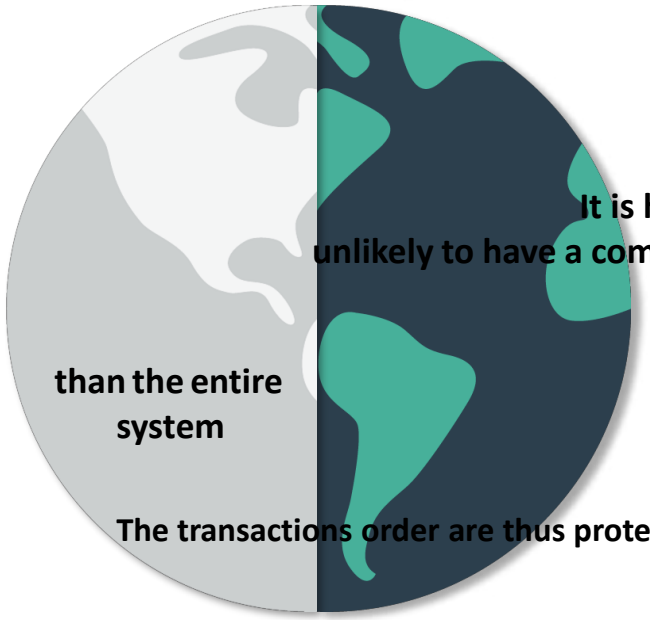
If you want to alter any transaction in a block, you have to out run the whole network

- Is it possible for someone with and extremely fast computer to outpace every other nodes ?

- It is highly unlikely that someone can do that
- even with a thousands of computers

Hence the Transactions are Protected by a Race

It would require more than 50 percent of the total computational power of the entire system to have a probability of solving 50 percent of the blocks faster than someone else.



than the entire system

It is highly unlikely to have a computing power stronger

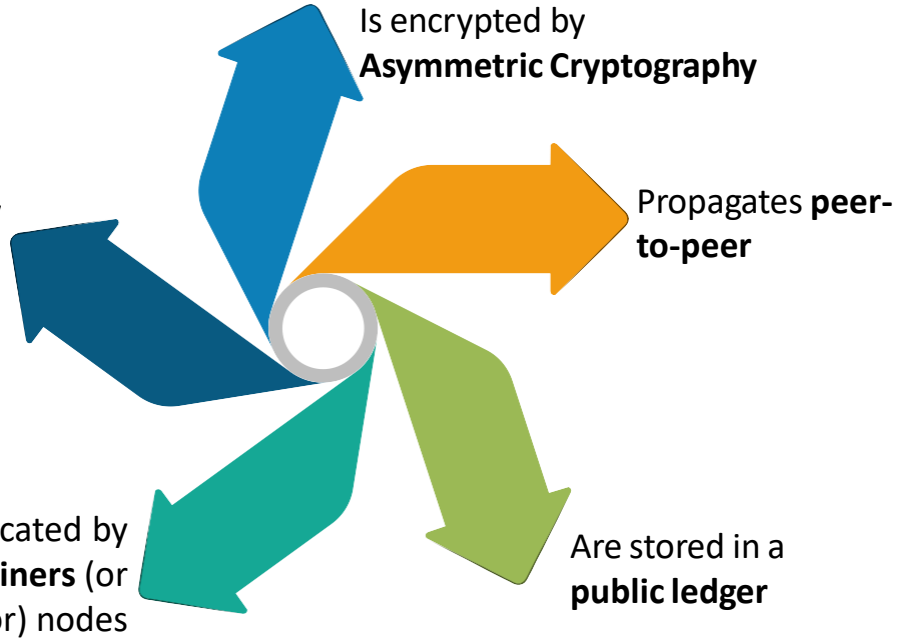
V/s

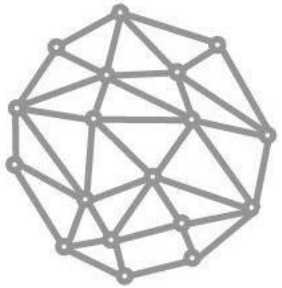
Against a mathematical race

The transactions order are thus protected by the mathematical race

To Sum up

In a Distributed system, transaction :



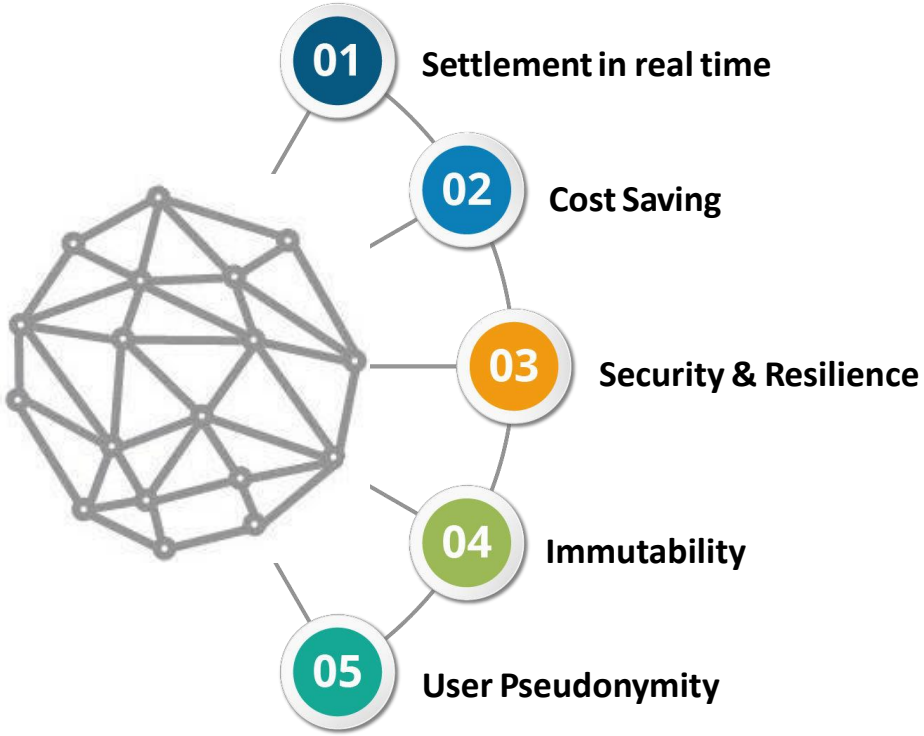


All these concepts constitutes Blockchain Technology

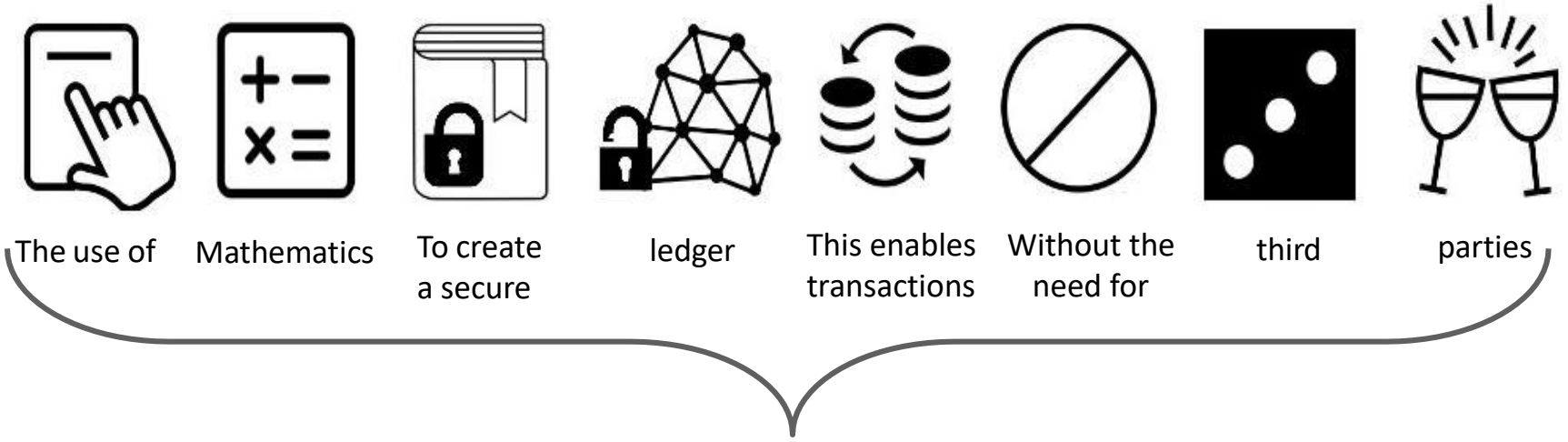
Benefits of Blockchain

Benefits of Blockchain Technology in Cryptocurrency

Removing the reliance on a trusted third party to maintain a central ledger has the following benefits:



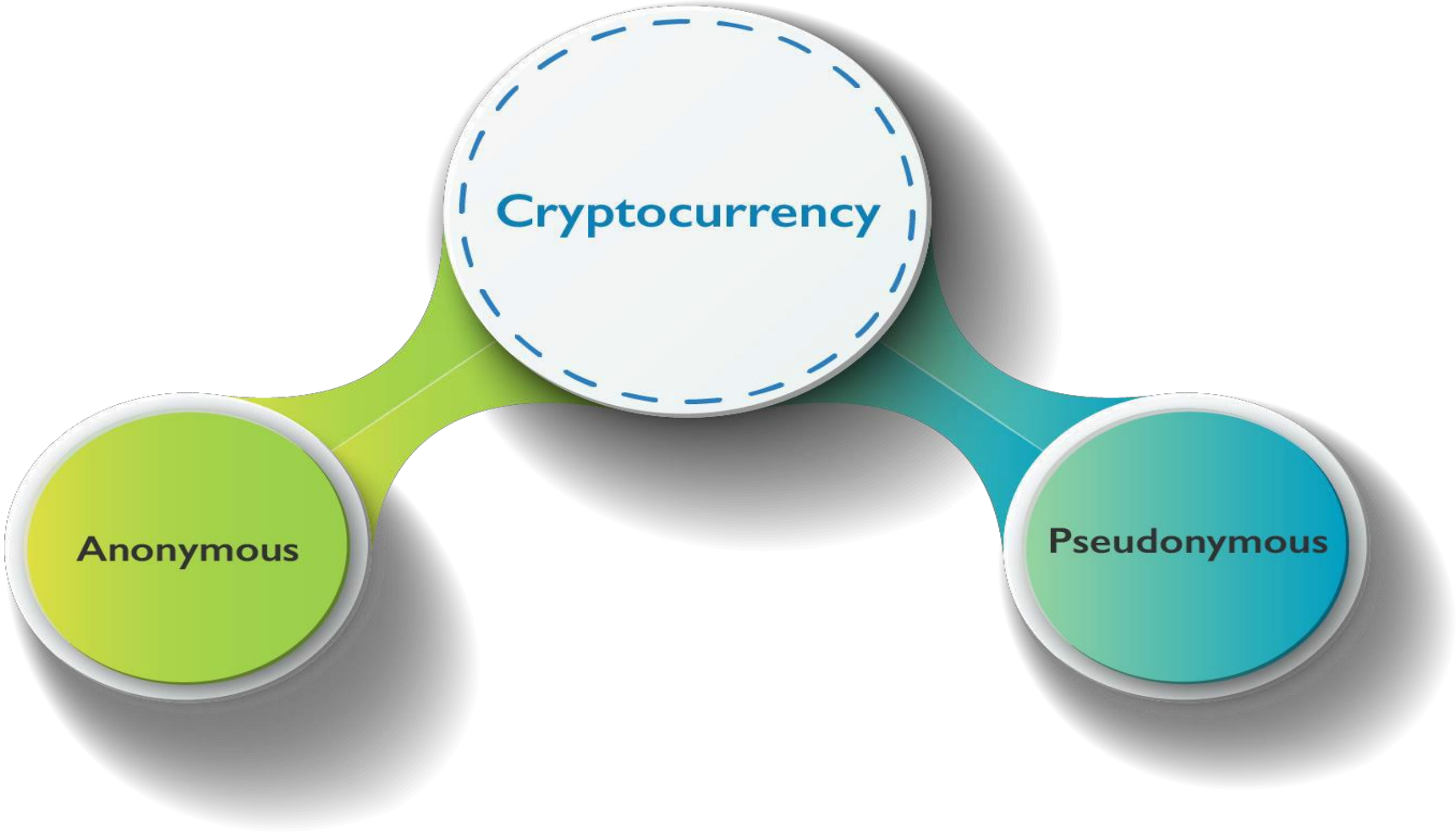
In a Nutshell



Access to shared single source of truth

Anonymity & Pseudonymity in Cryptocurrency

Types of Cryptocurrencies



Anonymity

- The state or quality of being anonymous
- Lacking a name; Lacking individuality
- An anonymous person is non-identifiable, unreachable, or untraceable
- Not bound or linked to any entity
- Example of anonymous dealings- unidentified individual telephoning an APP entity to inquire generally about its goods or services, and an individual completing a retail transaction and paying for goods in cash.

Anonymity Examples

formspring

Questions & Answers Sites

Anonymous
blogging & posting

omegle
Talk to strangers!

Anonymous chatting &
Networking

Being Anonymous on Cryptocurrency Network

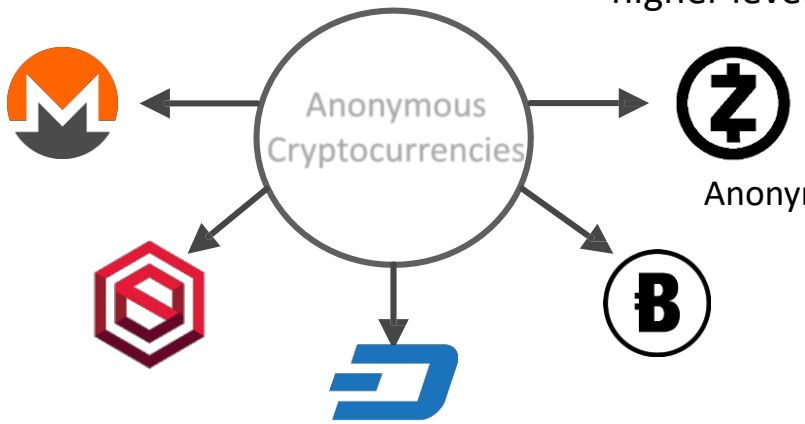
Being anonymous has its own rewards

But invisible exchange of values is a double-edged-sword

Extremely valuable (Example-some forms of truly anonymous communication, such as political speech, are considered valuable)

Electronic Harassment into trade and business this form of anonymity has exceptional potential for illegal acts because the message senders cannot be held accountable for their actions

Being anonymous makes it harder to trace transactions and giving higher level of privacy



Anonymous Cryptocurrencies

Discussing Anonymous Cryptocurrency- Z-cash

- First, totally anonymous crypto-currency
- Provides complete anonymity solution, hiding all knowledge about the transactions
- It is a concealed value exchange
- Provides user with private access control to their financial information
- It is an application of zk- SNARKs cryptography
- Only those with the correct view key can see the contents
- Users can provide view at their discretion
- Z-cash is a very interesting technology, provided the security is not being compromised

Pseudonymity

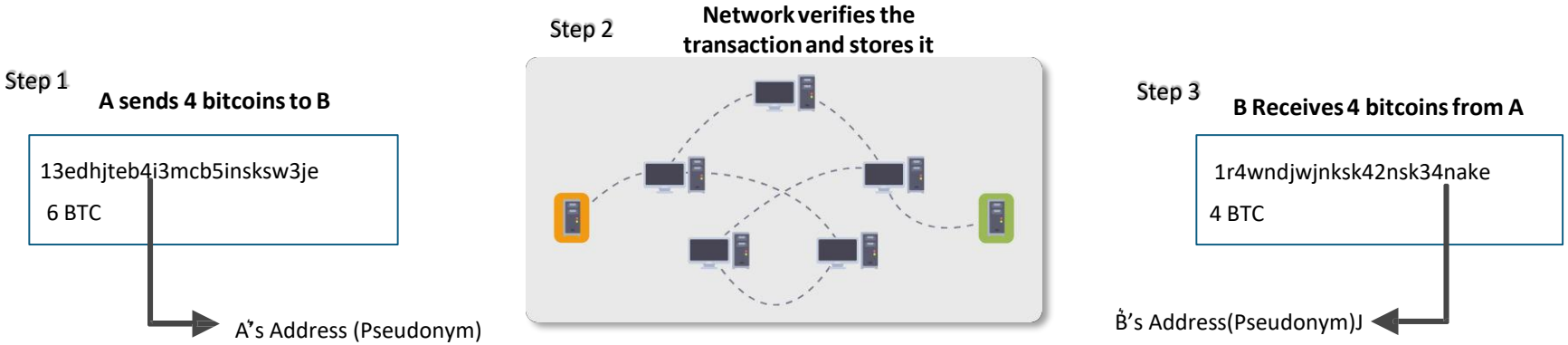
- Using a pseudonym to establish a long-term relationship with some other entity without disclosing personal identity to that entity
- A pseudonym is a unique identifier(example-nick name, credit card numbers, student numbers, bank account numbers, etc.)

- Using pseudonym, entity links different
- messages from the same person
- Pseudonyms are widely used in social networks and other virtual communication

I cant identify you. But I will single you out!

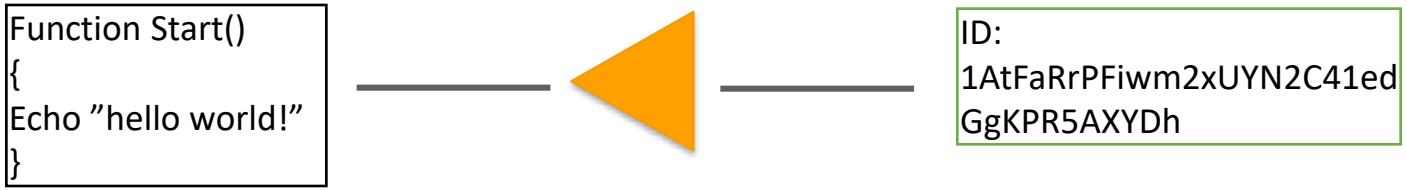
Importance of Pseudonymity in Cryptocurrency

- All the transactions in pseudonymous network are open and visible to all and thus it is widely acceptable
- The transactions have an origin and destination address and hence the flow of money can be observed
- Illegal use of the crypto-currency can be tracked by careful analysis of meta data



Programmable Money

Cryptocurrency is Programmable



- Each unit is individually identifiable and programmable
- Users can assign properties to each unit
- Users can program a unit to represent a eurocent or a share in a company, a kwh of energy or digital certificate of ownership
- Because of which cryptocurrency is much more than simply money and payments

Example of How Cryptocurrency can be Programmed

- For single transactions between two parties, programmable money can give the payer and payee a vastly greater range of parameters to use when exchanging value
- It also enables a huge array of different “valuables “ to be exchanged – far more than conventional money – time , contracts ,expertise , goods , services and more can all be traded.

Example of How Cryptocurrency can be Programmed

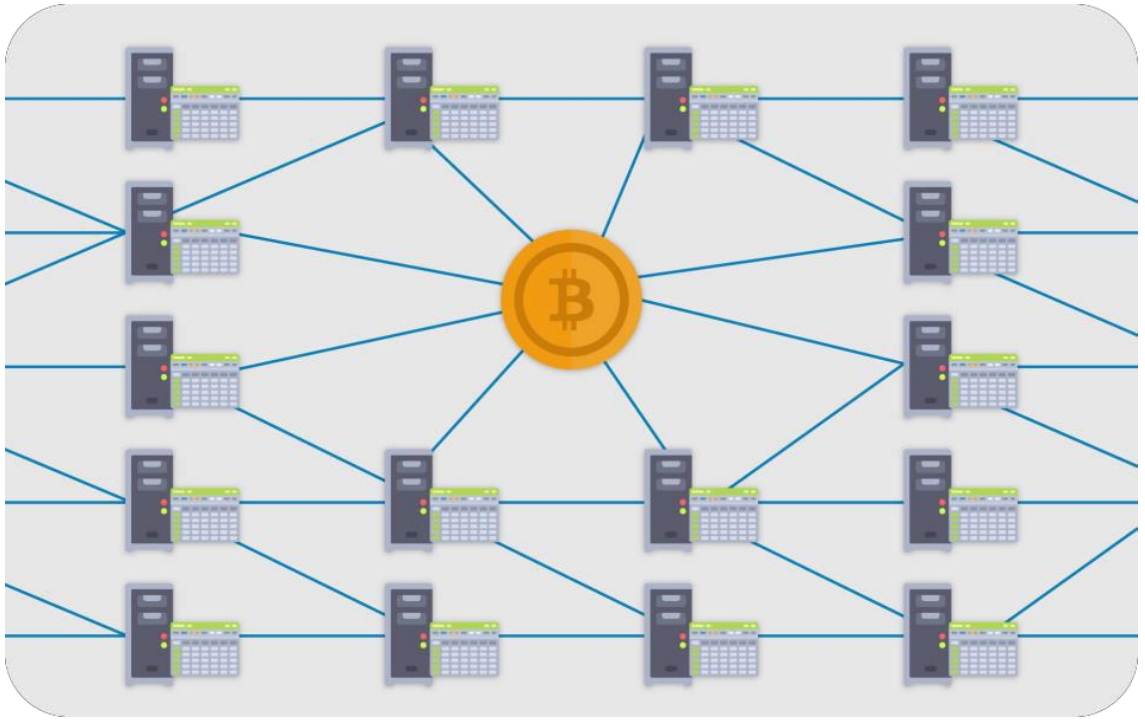
Example:
Alice buys a car online from Bob. The payment will only be executed after the car has been delivered and passes an emissions test

The terms verification is completed by the shipping agent and the emissions test agent. When both are complete , the transaction is authorized and the money changes hands

Is there any other Implementation of Blockchain?

Affirmatively, there are various ways in which blockchain can be implemented, let's see.

Bitcoin is the first Implementation of Blockchain

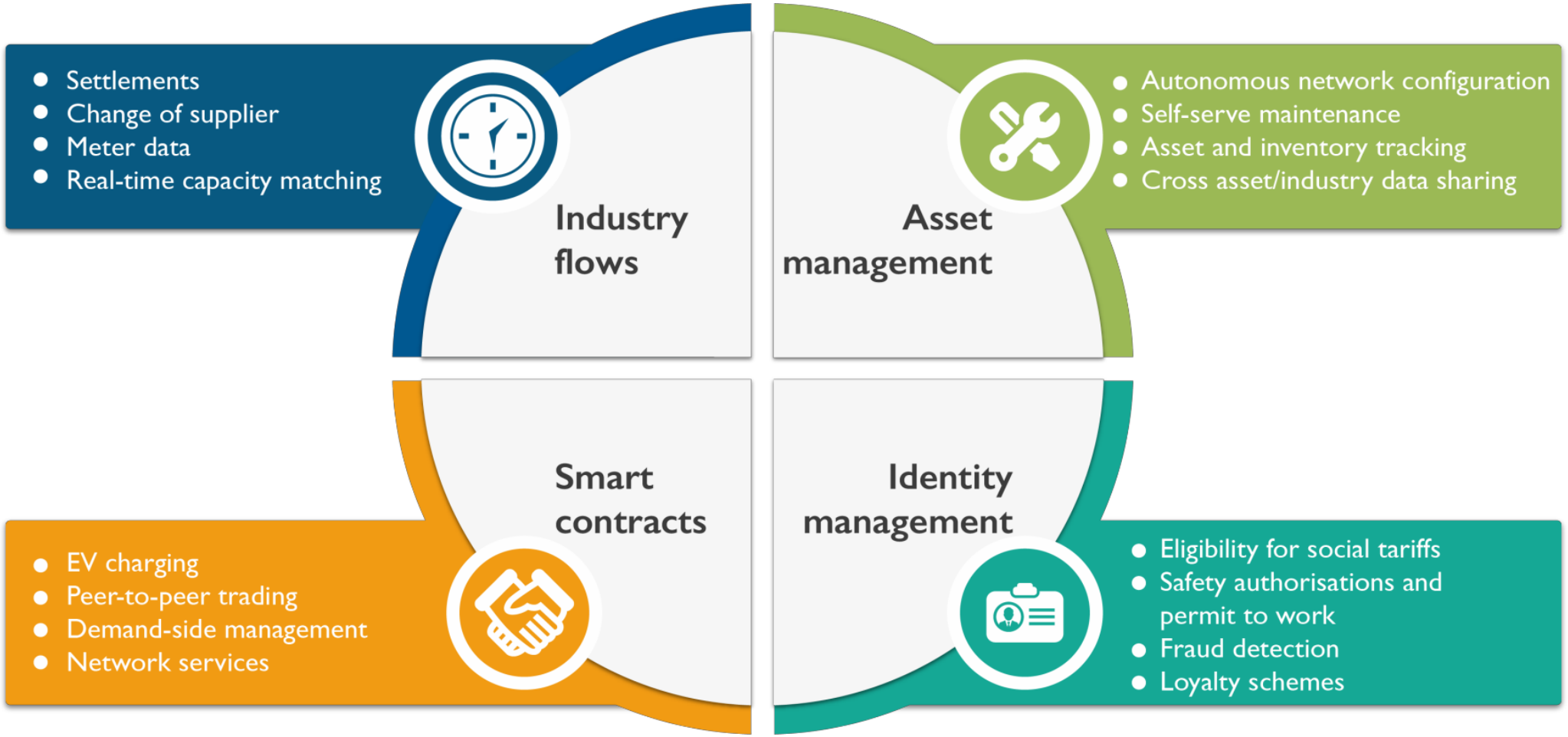


- Blockchain's foremost implementation was in the Bitcoin
- However, there are various ways in which the technology can be implemented

Blockchain Beyond Bitcoin

Monetary Aspect is just a tip of the iceberg of blockchain Technology
Blockchain is a ground-breaking technology for which money is merely one of the possible applications

Potential Applications of Blockchain



Thank You

Email us – support@intellipaat.com

Visit us - https://intellipaat.com