KIET Group of Institutions, Delhi-NCR, Ghaziabad
Department of Computer Applications
(An ISO – 9001: 2015 Certified & 'A+' Grade accredited Institution by NAAC)

PRESENTATION ON
<<BLOCKCHAIN >>

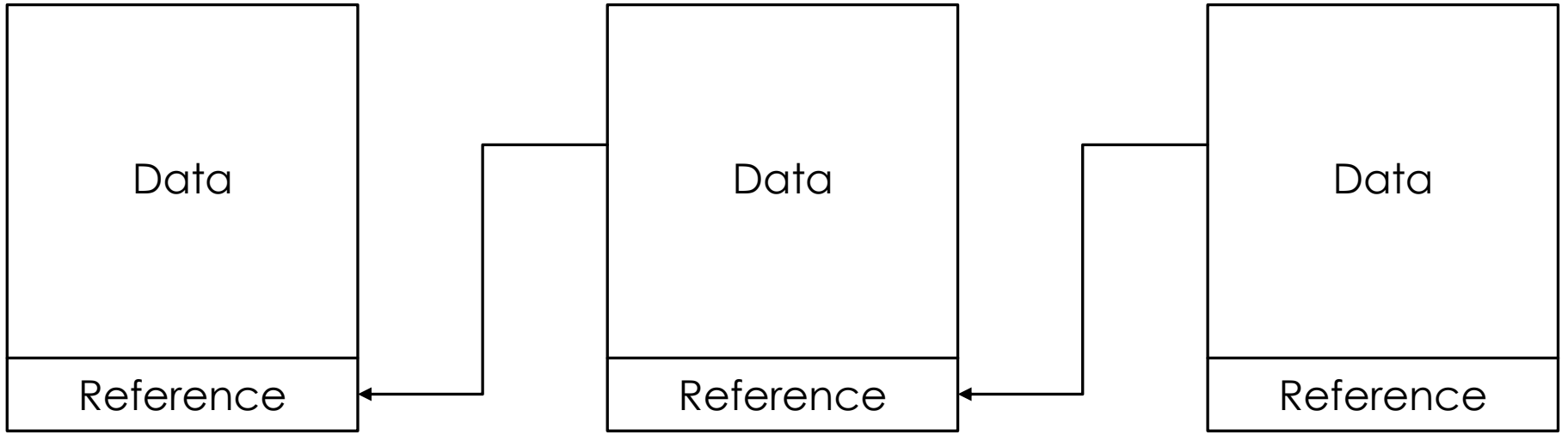
SUBMITTED BY

UNIVERSITY ROLL NO. :- 1900290140008
NAME :- Apoorva Srivastava
SEMESTER :-VIth
SECTION :- A
DATE:-26-03-2022

WHAT IS A BLOCKCHAIN?

- A blockchain is a data structure, which is a growing list of data blocks.

- The data blocks are linked together, such that old blocks cannot be removed or altered.



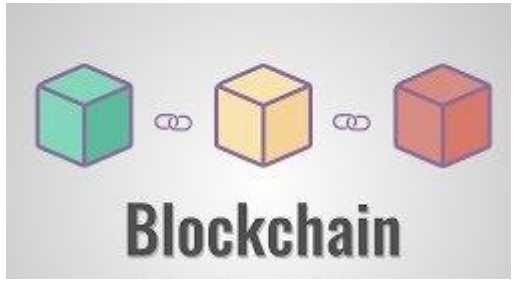
A technology that permits transactions to be gathered into blocks and recorded; cryptographically chains blocks in chronological order; and allows the resulting ledger to be accessed by different servers

Blockchain transactions are immediately validated and cleared, then settled shortly thereafter, automatically without a Central Authority

In the financial world, cash transactions only are cleared and settled automatically without a Central Authority

BITCOIN ≠ BLOCKCHAIN

- Bitcoin does not equal Blockchain.
- Bitcoin is a currency and a system that uses a blockchain as underlying data structure, which can be used for many things, including cryptocurrencies.
- Blockchain is the underlying data structure.



BITCOIN
Is an application of blockchain technology

BLOCKCHAIN
Is the underlying data structure, which can be used for many things, including cryptocurrencies

THE HISTORY OF BITCOIN

2008
Idea was published under the pseudonym Satoshi Nakamoto

2009
Start of the Bitcoin Network

2010
First cryptocurrency stock exchange is launched

2011
One Bitcoin equals one USD

2013
1 Bitcoin equals 100 USD

2014
Microsoft accepts Bitcoin

2017
1 Bitcoin equals 10,000 USD

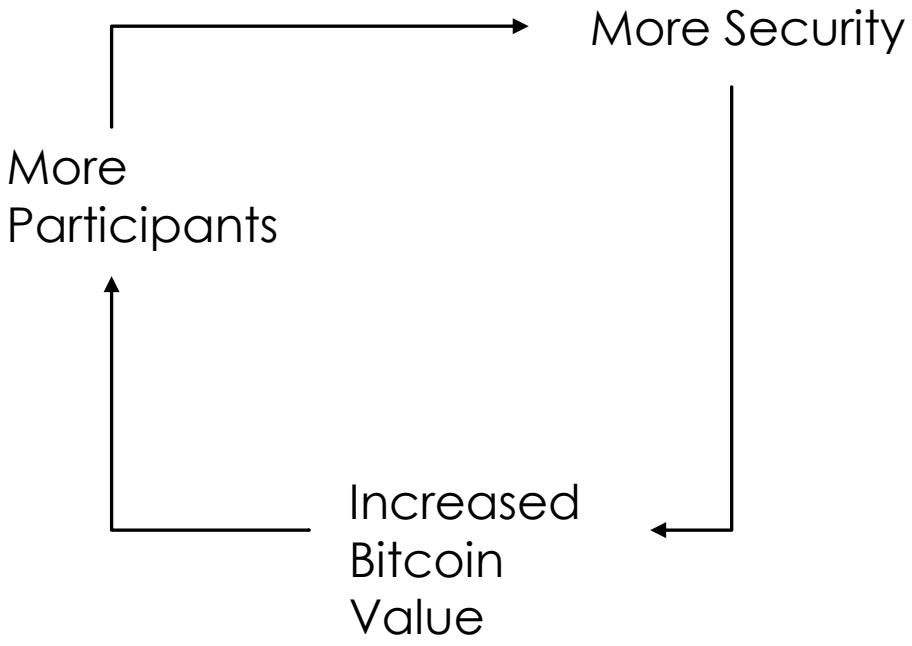
- 2008: The first description of Bitcoin was published in 2008 by an individual or a group under the pseudonym “Satoshi Nakamoto” in a now very famous white paper.
- 2009: The Bitcoin Network goes live and the first Bitcoins are mined.
- 2010: The first cryptocurrency stock exchange for trading Bitcoin is launched.
- 2011: One Bitcoin equals one USD.
- 2013: One Bitcoin now equals 100 USD.
- 2014: Microsoft starts accepting Bitcoin as payments.
- 2017: One Bitcoin equals 10'000 USD.

BITCOIN ECOSYSTEM

•The Bitcoin ecosystem contains a public network in which anyone, including a malicious participant, can participate without restriction.

•Even though it is not organized by a central authority, it works!

BITCOIN ECOSYSTEM



- The Bitcoin ecosystem is self-stabilizing.
- The more participants the system has, the more difficult manipulations become. And the more difficult manipulations become and the more participants there are, the greater the demand for Bitcoins.
- This results in a price increase, which in turn attracts new participants.

BASIC COMPONENTS OF BITCOIN

The basic components of bitcoin are:
1.Software
2.Cryptography
3.Hardware
4.Miners(Gaming Theory)

BASIC COMPONENTS OF BITCOIN

First Component: Software

Bitcoin is basically a software at the core that defines what a bitcoin is, as well as how a bitcoin gets transferred. It identifies what the rules of a valid bitcoin, who can be inside bitcoin, who cannot be inside bitcoin, what is valid, what is not, etc. Everything is based on software, which is the bitcoin software. The bitcoin software is always operated in 24*7.

Second component: Cryptography

The software, at its core, uses cryptography and bitcoin as a cryptocurrency. Bitcoin uses cryptography to regulate the transfer of bitcoin between parties, as well as the creation of new units of bitcoin. Without cryptography, Bitcoin would simply not be possible. So, we've got that this software uses cryptography to control the transfer of bitcoin over the internet.

Cryptography is a mathematical approach which is solvable by computers and not by humans. So all the stuff that protects your data is served by the cryptography.

Third Component: Hardware

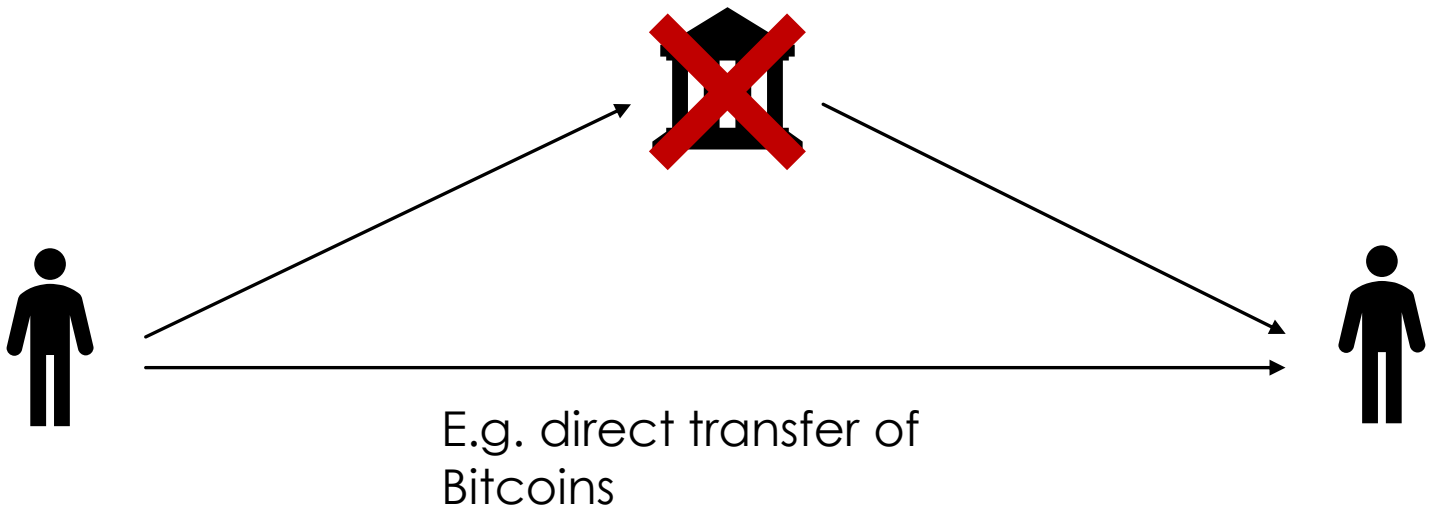
To run and solve cryptography, it needs HARDWARE. This hardware is composed of those thousands of miners around the world running their computers. So there are thousands of computers around the world that are basically running the Bitcoin software or the Bitcoin client. This hardware is specially designed for finding Nonce to validate block and hash. It requires a lot of CPU power to complete a simple task on the bitcoin blockchain.

If you try to mine bitcoin right now with your smartphone or home computer, then you will End up losing your computer along with a hefty electric bill.

Fourth Component: Mining(Gaming Theory)

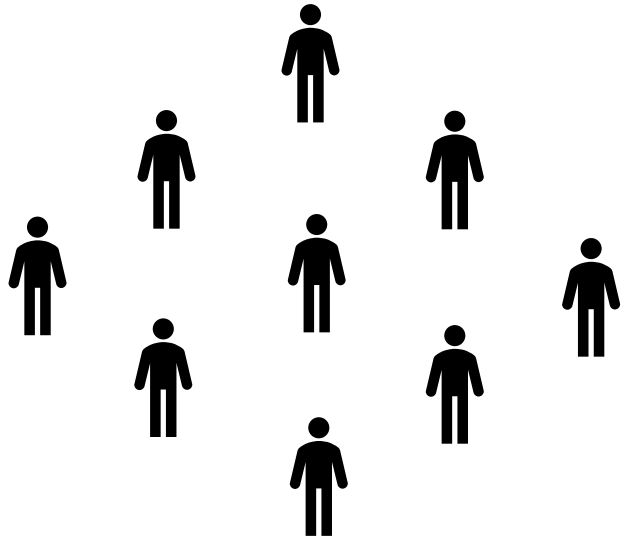
Miners are users who involved in a gaming theory because bitcoin is truly a game which is run by these miners around the world. In the above, we have seen that the first component is **software for bitcoin** that issues a cryptography challenge in every 10 minutes. The cryptography challenge involves in trying to find a Nonce which will make the hash for a specific block valid. All the hashes and validations are done by these miners. After successful creation of the block, the new block is added to the blockchain.

CUTTING THE MIDDLEMAN



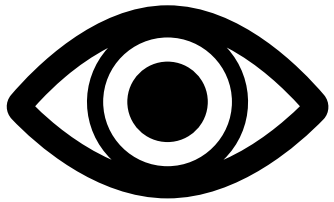
- Blockchain technology makes middlemen (so-called trusted third parties) obsolete in many applications.
- Bitcoin can serve as an example here.
- Bitcoins are not routed via a central instance, e.g. a bank, but can be transferred directly between the parties.

BUILDING CONSENSUS



- Blockchain technology has a wide range of applications for consensus building.
- In a finite timeframe, all participants of the blockchain agree on a proposal, which was worked out by a participant.
- At Bitcoin, for example, all participants agree on who owns how many bitcoins. But many applications are also conceivable in industry.
- After a finite time, all participants agree on a single state.
- E.g. on who owns how many Bitcoin.

CREATING WITNESSES

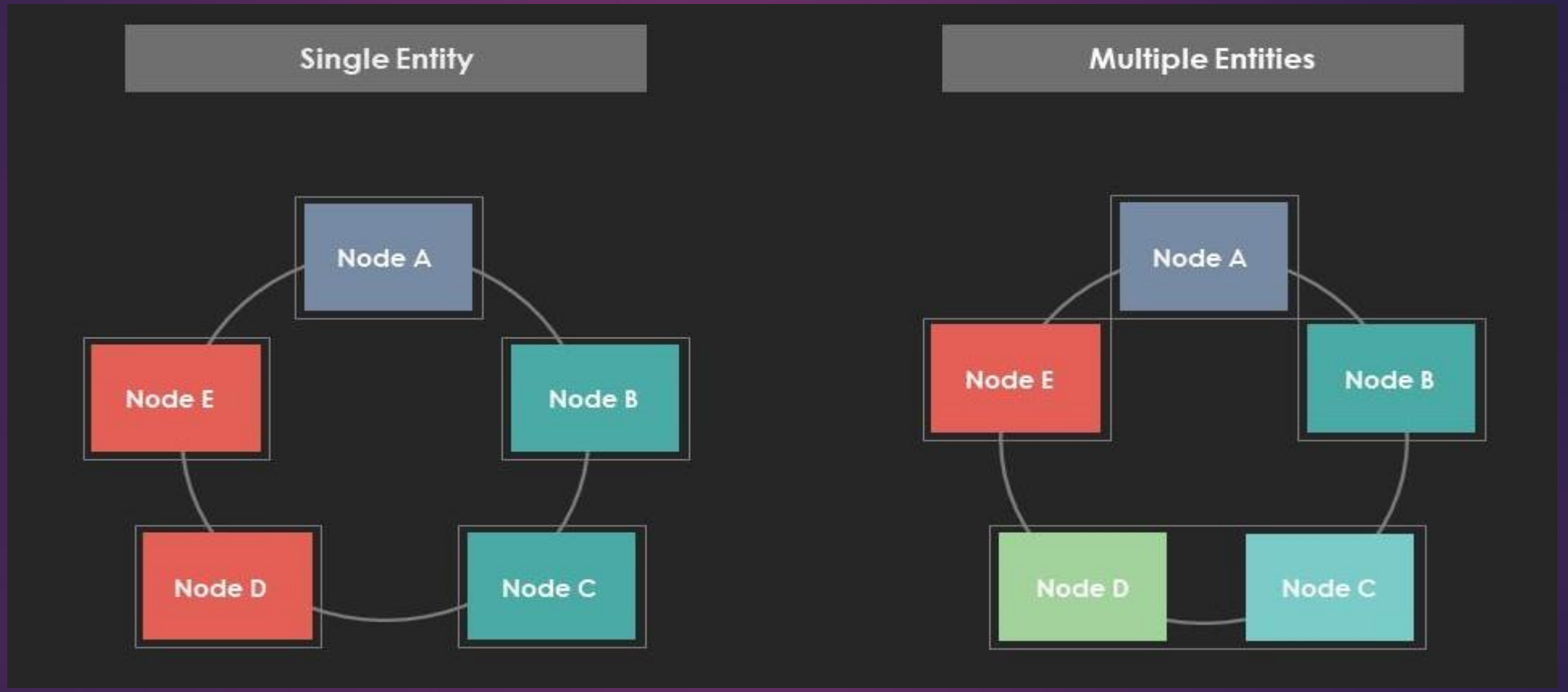


- A public blockchain can be used for the automated creation of witnesses.
- If something is published on a public blockchain, all participants become witnesses.
- This is used, for example, by OriginStamp to create a secure timestamp for documents.

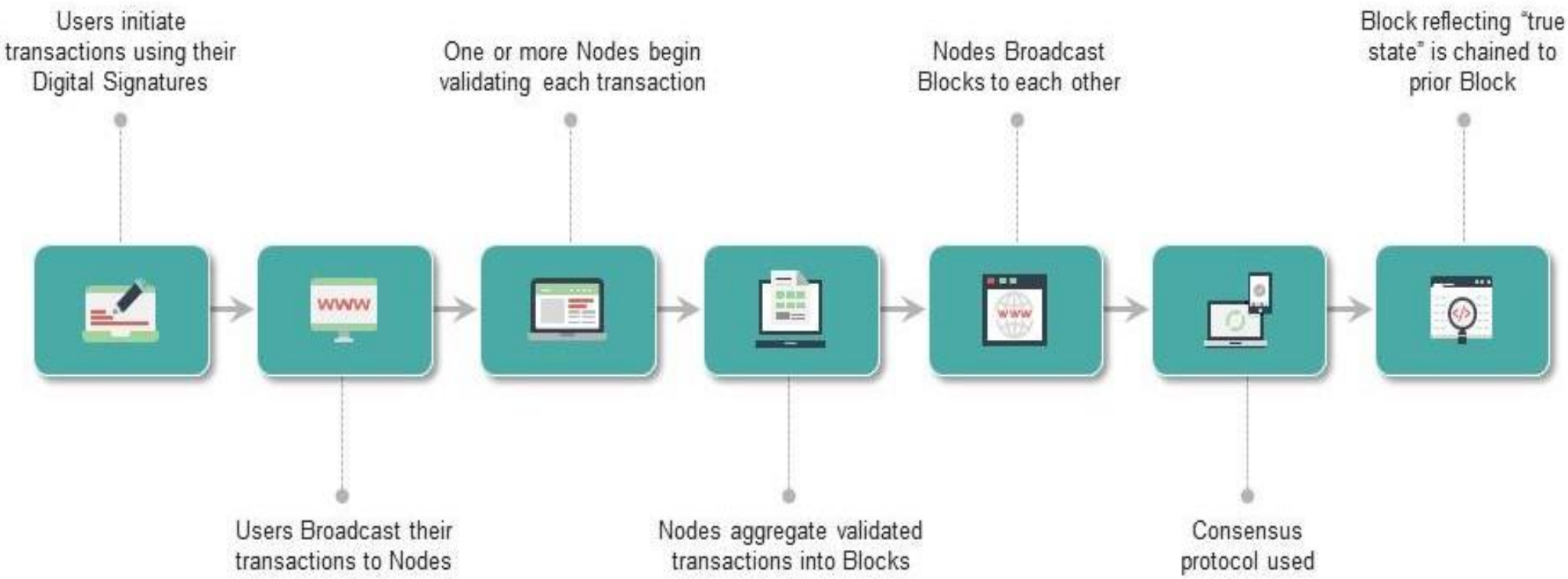
DISTRIBUTED LEDGER

- It is a database that is **shared**, **replicated**, and **synchronized among** the members of a decentralized network.
- All the information on this ledger is securely and accurately stored using **cryptography**.
- The distributed ledger allows transactions to have public **witnesses**, which makes cyberattack more difficult
- There is no **central authority**, or third-party mediators. Every record in the distributed ledger has a **timestamp** and **unique** cryptographic signature.
- It makes the ledger an auditable, and immutable history of all transactions in the network.
- When any modifications happen in the ledger, each node constructs the new transaction, and then the nodes **vote by consensus algorithm** on which copy is correct.
- Once a consensus algorithm has been determined, all the other nodes update themselves with the new and correct copy of the ledger.

DISTRIBUTED LEDGER



WORKING OF A DISTRIBUTED LEDGER



SMART CONTRACT

Business rules implied by the contract embedded in the Blockchain & executed with the transaction

Verifiable, signed

Encoded in programming language

PRIVACY

- Ledger is shared , but participants require privacy.
- Participants need : Transactions to be private . Identity not linked to a transaction.
- Transactions need to be authenticated.
- Cryptography central to these processes.

KEY FEATURES

- Write-only, immutable, transparent data storage.
- Decentralized, no need for intermediaries.
- Consistent state across all participants.
- Resistant against malicious participants.
- Open to everyone.

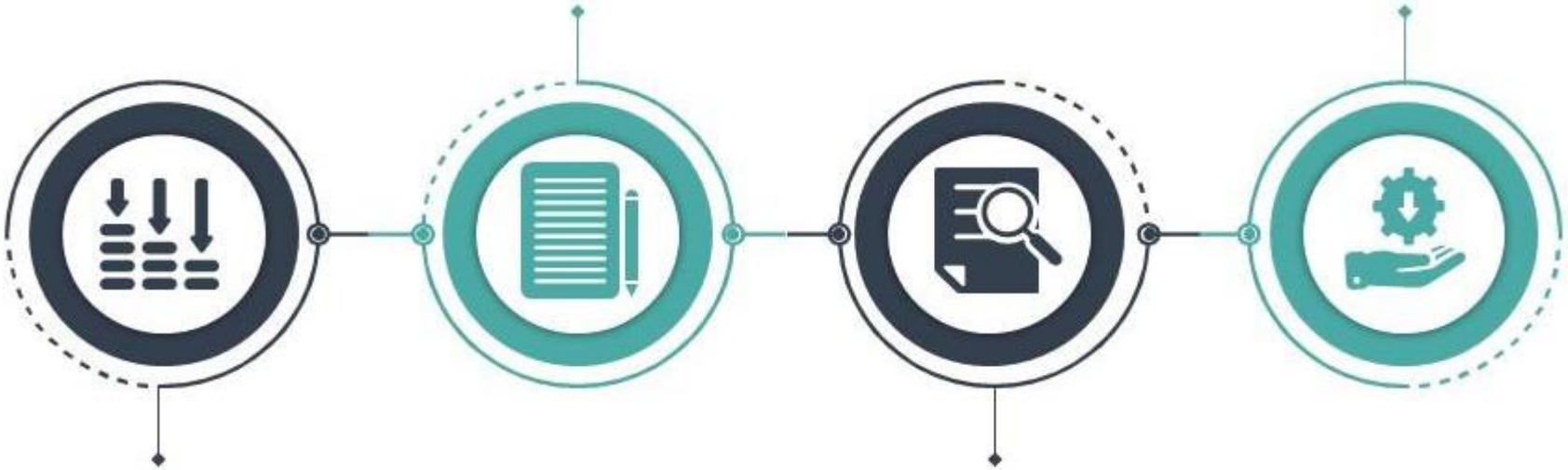
INDUSTRIAL BLOCKCHAIN BENEFITS

Trusted Recordkeeping

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Share Trusted Processes

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.



Reduce Costs and Complexity

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

Improve Discoverability

This slide is 100% editable. Adapt it to your needs and capture your audience's attention.

BLOCKCHAIN LIMITATIONS

- Need high performance (millisecond) transactions
- Small Organization (no business network)
- Looking for a database replacement
- Looking for a messaging solution
- Looking for transaction processing replacement

CHALLENGES

•The high energy consumption - Bitcoin uses a lot of energy.

•The scalability issue - Bitcoin supports far less transactions per second than e.g. VISA.

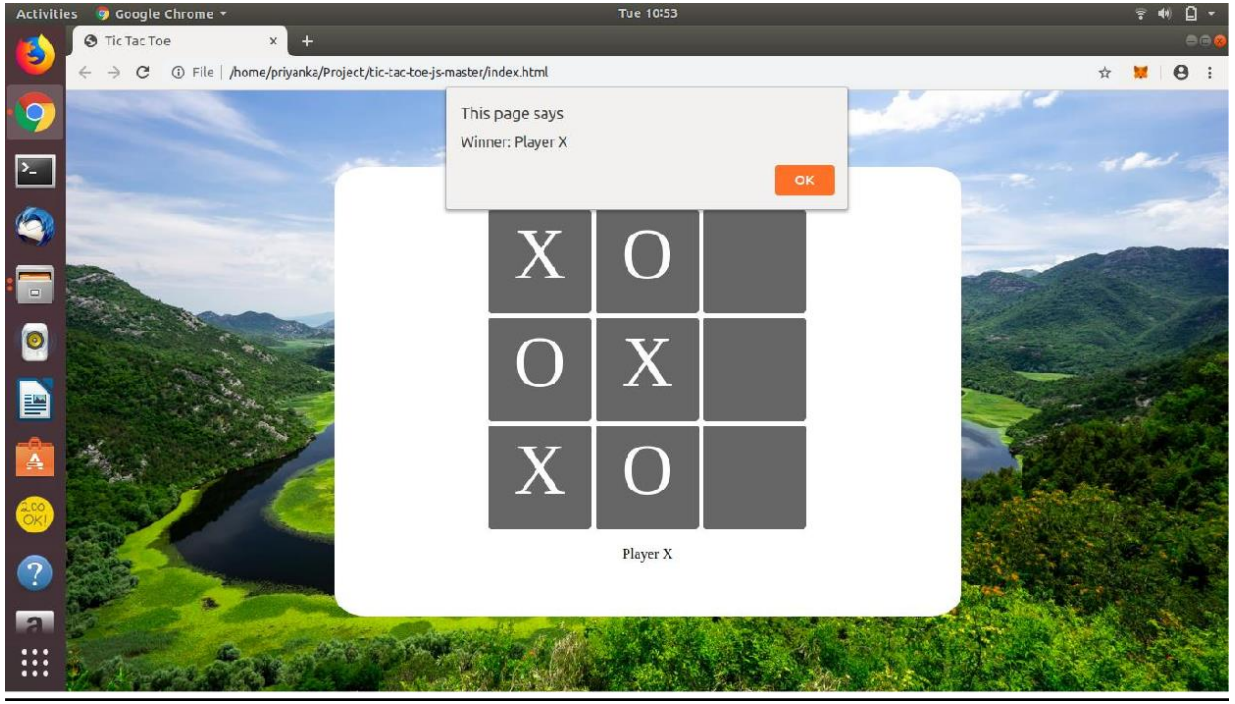
•It opens up possibilities for money laundering - Some blockchains as Monero are anonymous.

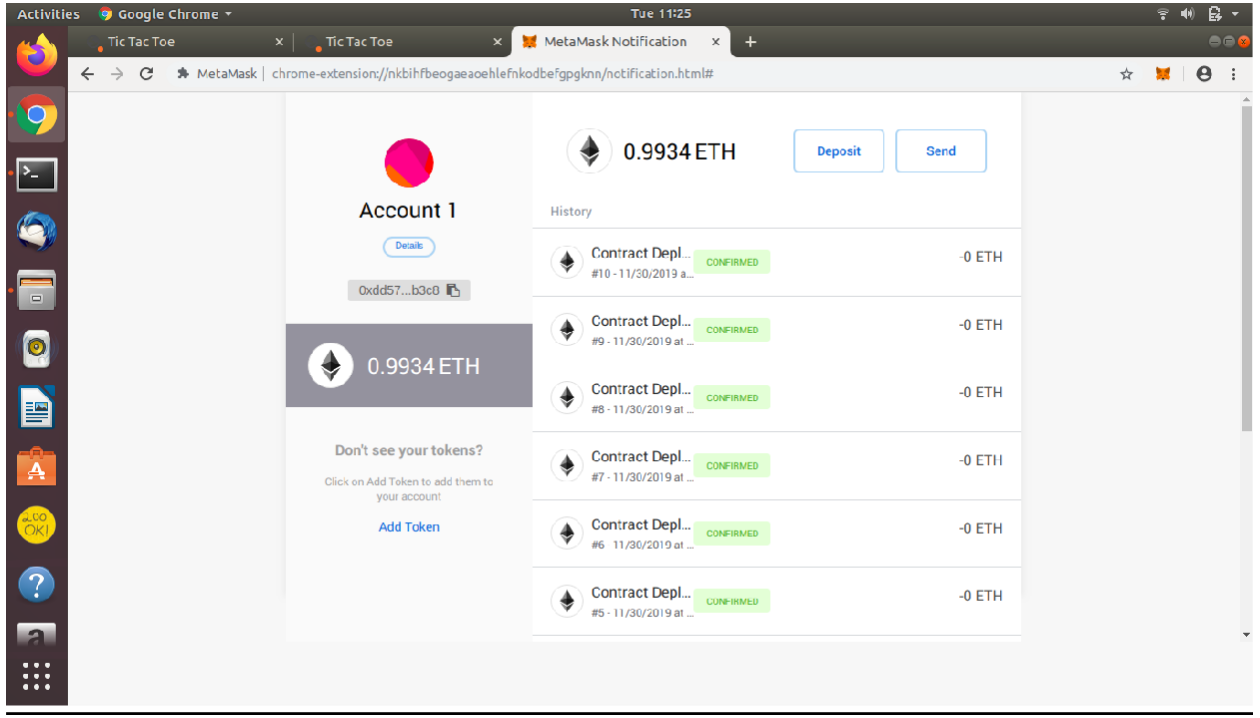
•Personal responsibility : The question remains as to how far we want to bypass the middleman. Often he can also protect us, e.g. a bank can protect us to the extend that we do not transfer the money to the wrong person.

TIC TAC TOE GAME USING BLOCKCHAIN

- There are two teams that play a game.
- Before starting the game, there is a contract between the teams - The winner gets money from the losing team.
- This transaction is done using blockchain which makes this transaction secured .
- The transaction done is immutable and no party can deny it.

TIC TAC TOE GAME USING BLOCKCHAIN





Ethereum enables the deployment of smart contracts and decentralized applications (dApps) to be built and run without any downtime, fraud, control, or interference from a third party.

MetaMask is a software cryptocurrency wallet used to interact with the Ethereum blockchain. It allows users to access their Ethereum wallet through a browser extension or mobile app, which can then be used to interact with decentralized applications.

Solidity is an object-oriented programming language for implementing smart contracts on various blockchain platforms, most notably, Ethereum.

THANKYOU