

BlockChain and Cryptocurrencies

Block chain and Crypto Currencies
Dr. Ahlad Kumar

The Myth Busters

- Blockchain ≠ Bitcoin (or any other cryptocurrencies)
 - If you want to take this course to trade cryptocurrencies, this course is not for you !!
 - We do not want to make any comment on whether Bitcoin is good or whether Bitcoin should be blocked

Block chain and Crypto Currencies
Dr. Ahlad Kumar

The Myth Busters

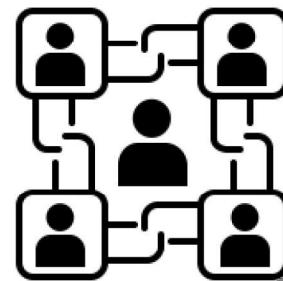
- Blockchain ≠ Bitcoin (or any other cryptocurrencies)
 - If you want to take this course to trade cryptocurrencies, this course is not for you !!
 - We do not want to make any comment on whether Bitcoin is good or whether Bitcoin should be blocked
- Anything and everything in the world cannot be solved using a blockchain
 - Blockchain is good but may not be so "stellar" the way it is projected



Then why should you take this course

- To avoid all the hypes and apply Blockchain as a solution at the right place ...

So, what is the
right place?



Let's explore the course !!

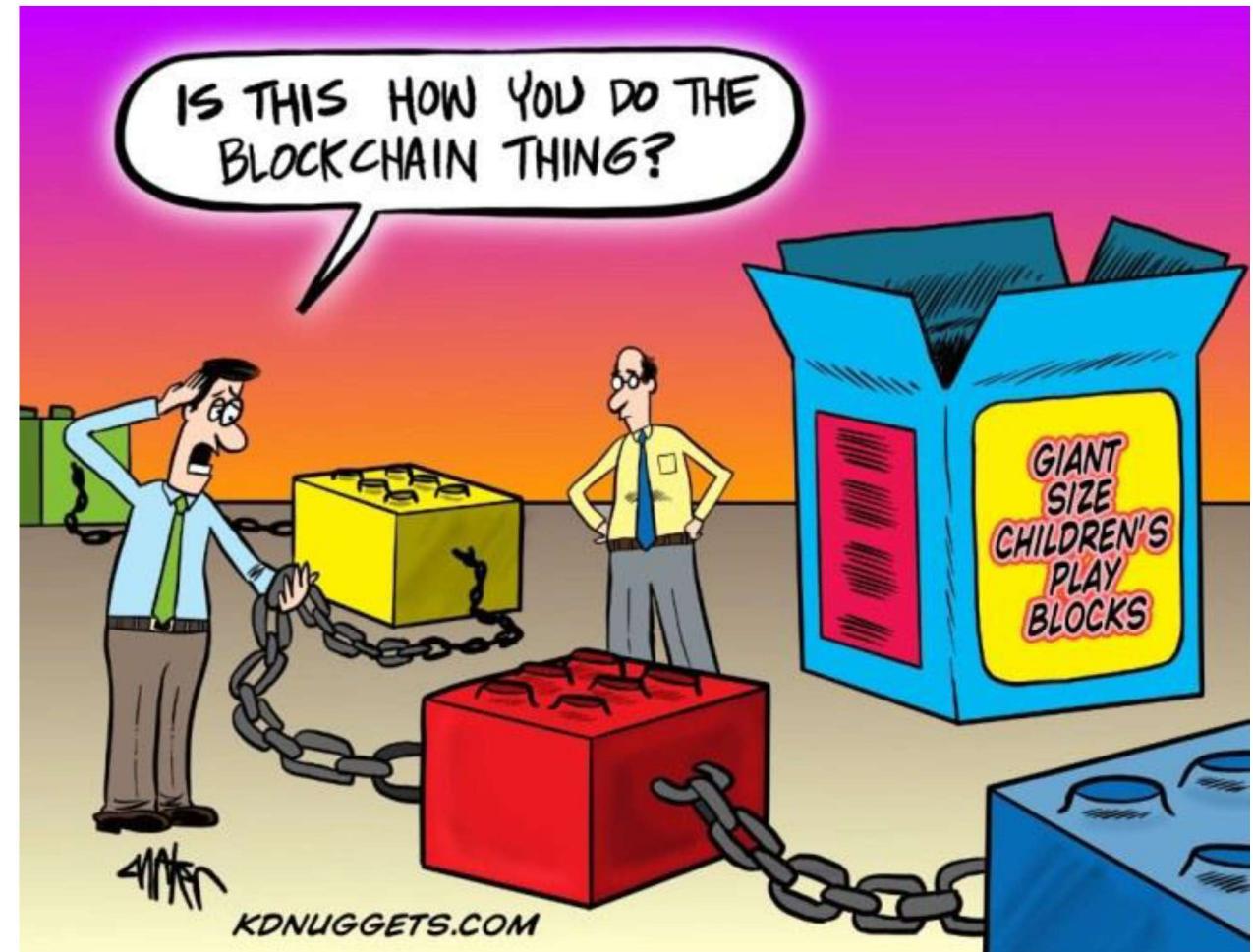
Block Chain and Crypto Currencies
Dr. Phlad Kumar

What We'll Cover in This Course?

- Blockchain as a Data Structure
 - How does a blockchain look like?
 - How do we efficiently store data in a blockchain?
 - How can we efficiently manage data insertion in a blockchain? What is the complexity of data insertion and searching a data item within a blockchain?

Block chain and Crypto Currencies
Dr. Ahlad Kumar

So, What is a Blockchain?





Supply Chain Management: The Players and the Game

Supply Chain in Petroleum Industry



Crude Purchase

Block chain and Crypto Currencies
Dr. Ahlad Kumar

Supply Chain in Petroleum Industry



Crude Purchase

Crude Transportation

Block chain and Crypto Currencies
Dr. Ahlad Kumar

Supply Chain in Petroleum Industry



Crude Purchase



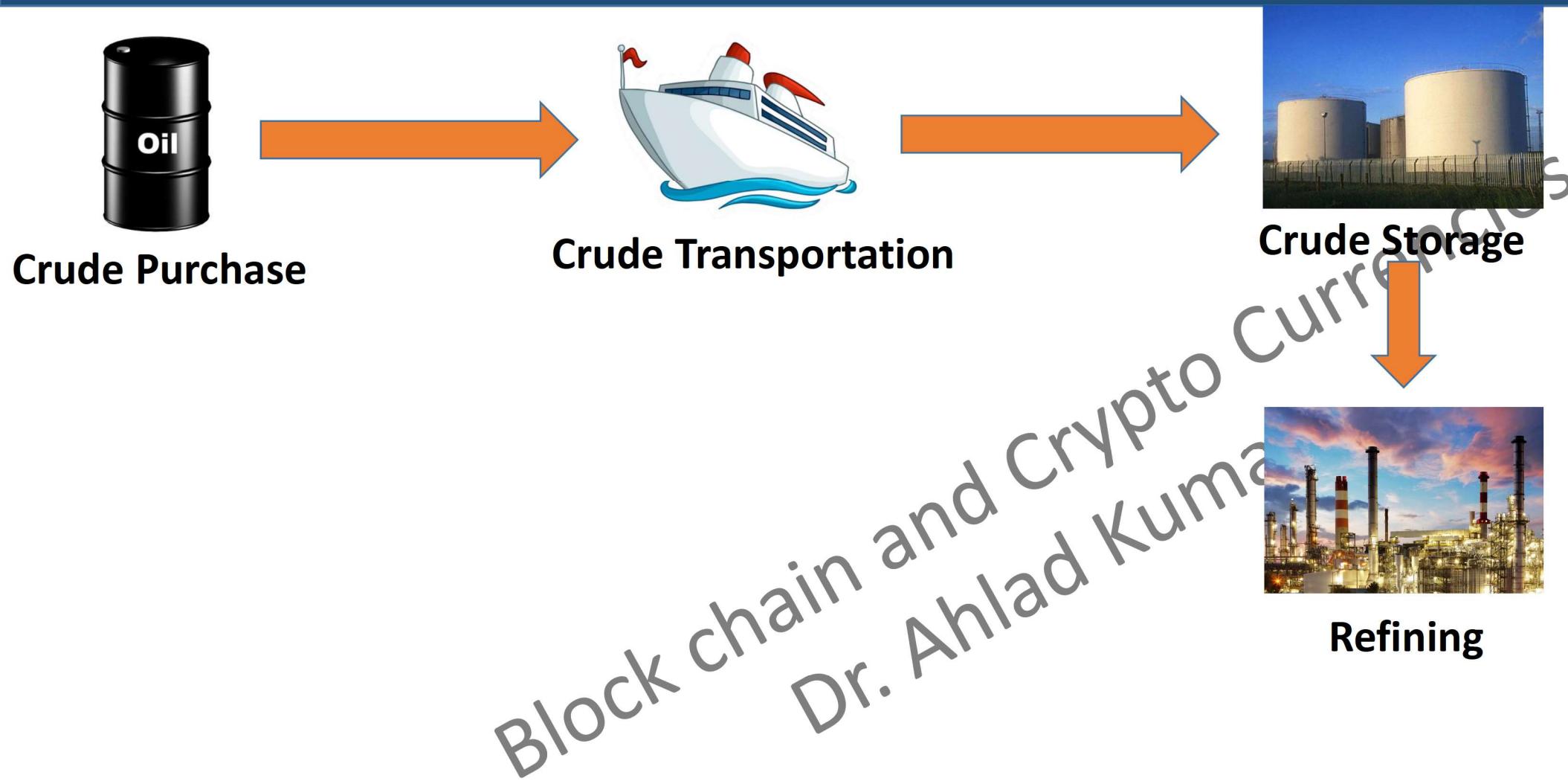
Crude Transportation



Crude Storage

Block chain and Crypto Currents
Dr. Ahlad Kumar

Supply Chain in Petroleum Industry



Supply Chain in Petroleum Industry



Crude Purchase



Crude Transportation



Crude Storage



Distribution



Refining

Block chain
Dr. Ahmad Kumar
Crypto Currents

Supply Chain in Petroleum Industry



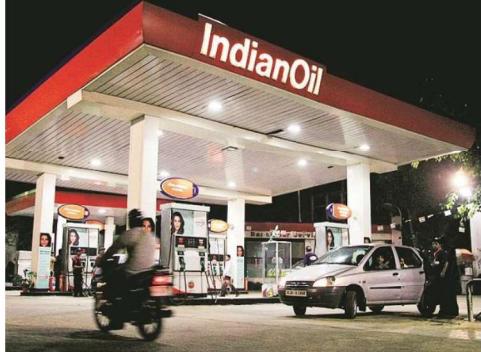
Crude Purchase



Crude Transportation



Crude Storage



Retail



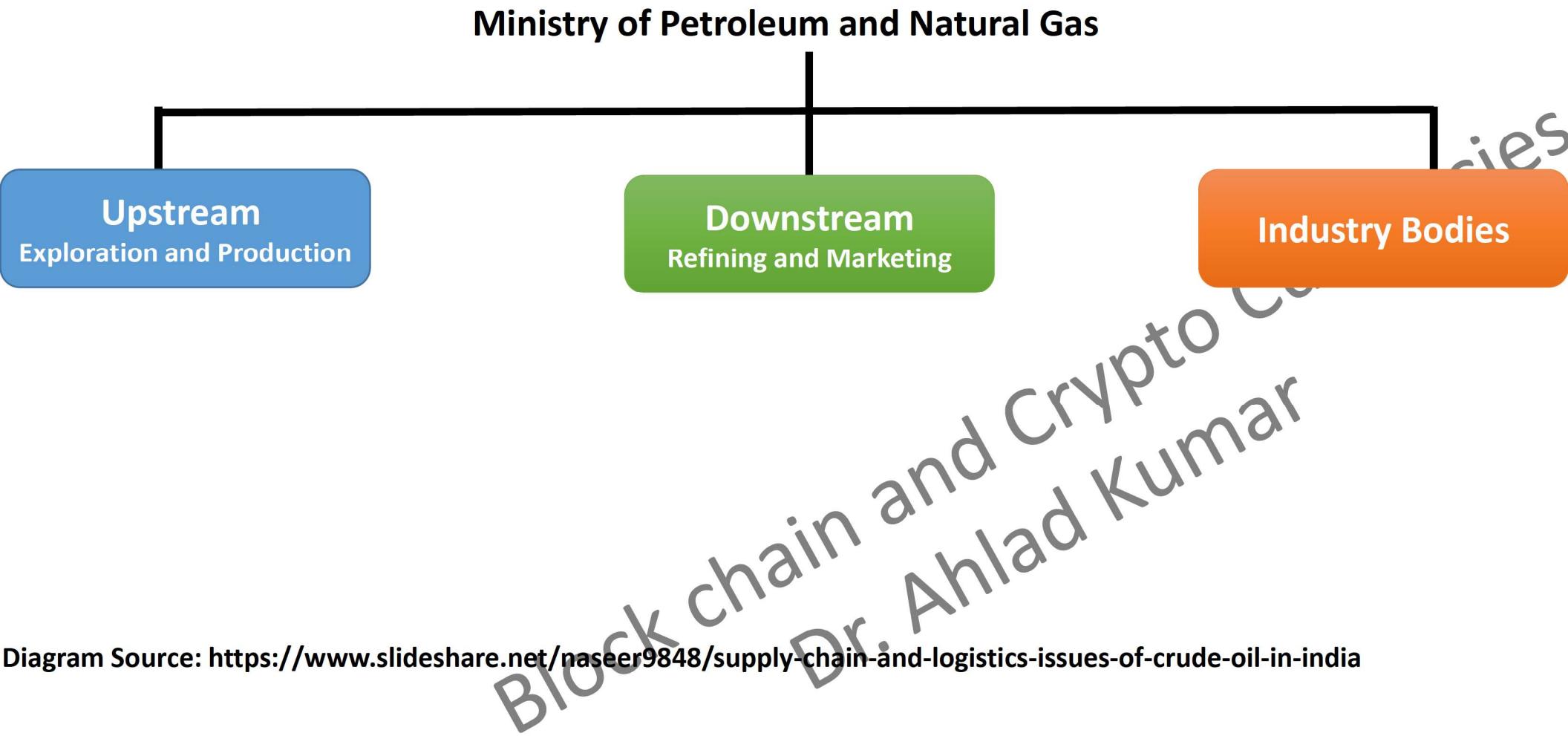
Distribution



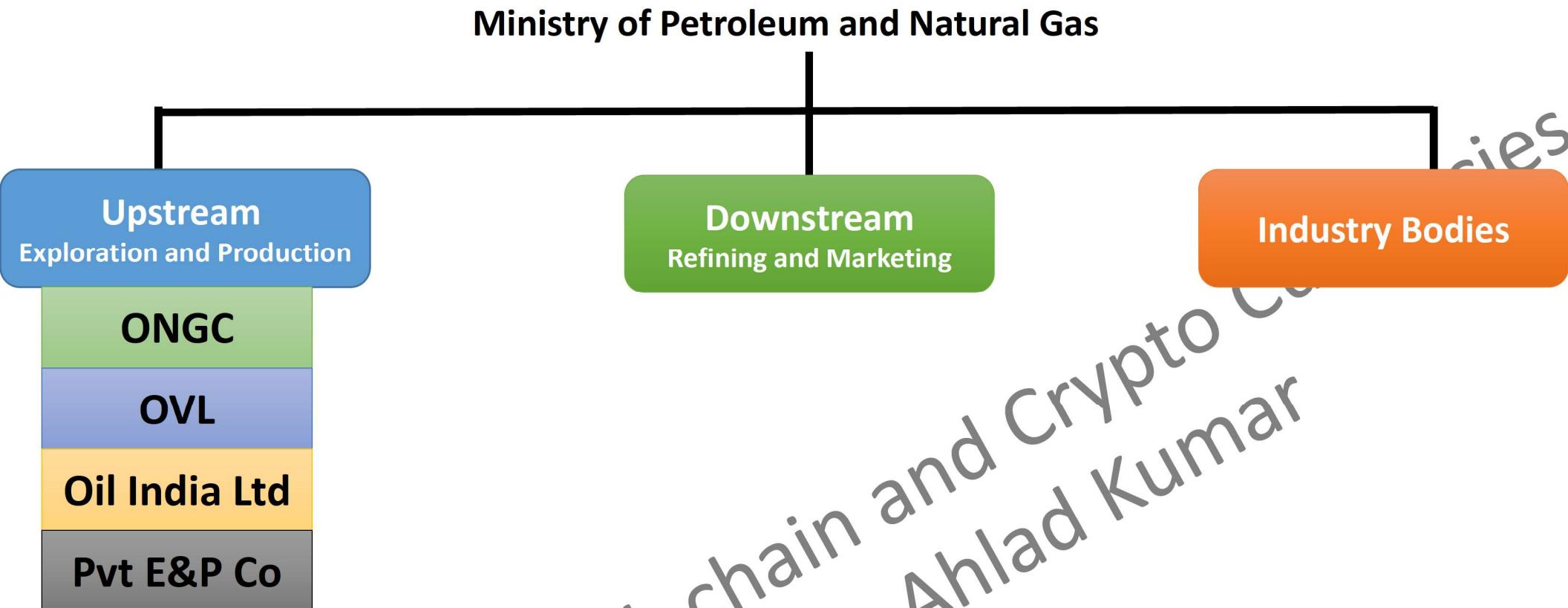
Refining

Block chain
Dr. Ahsad Kumar
Crypto Currents

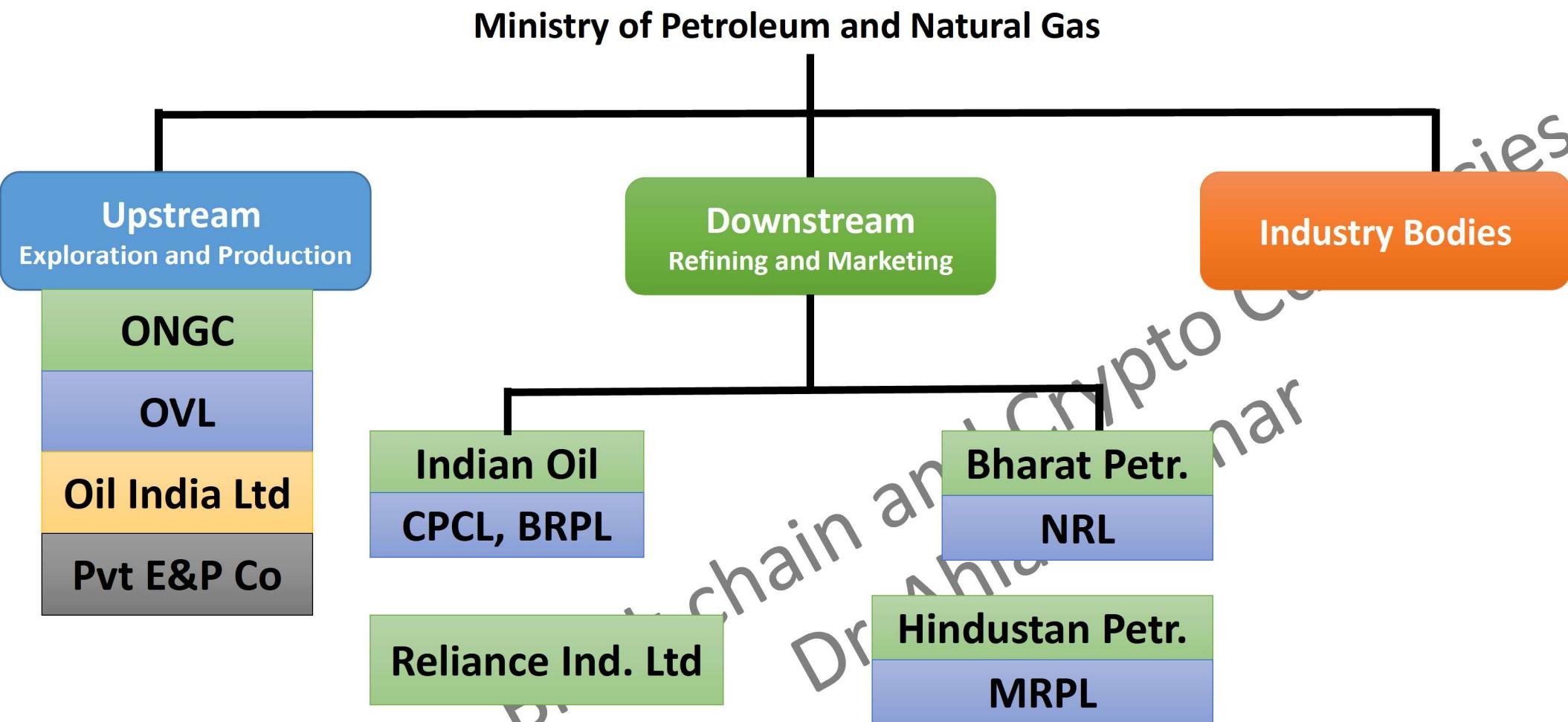
Petroleum Supply Chain in India



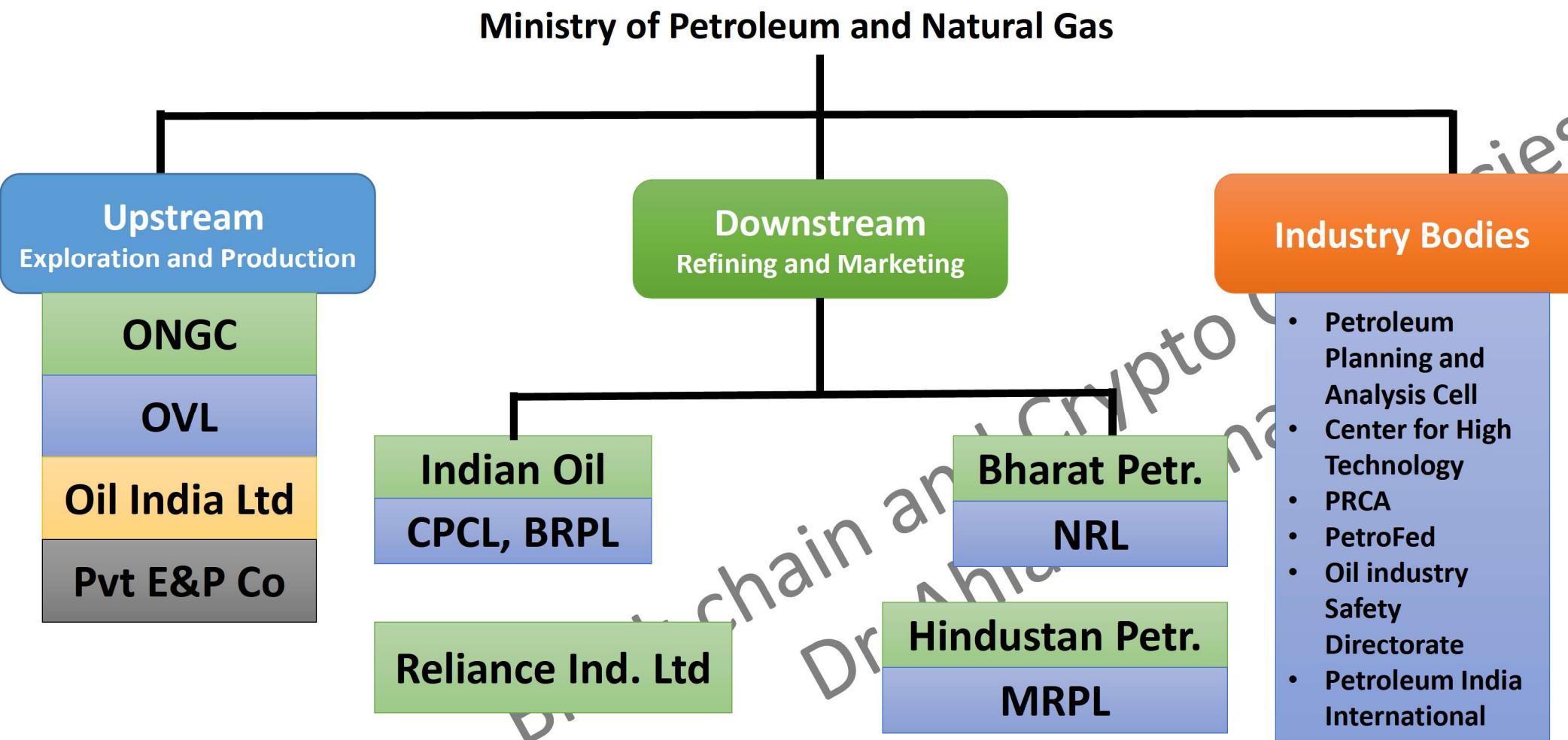
Petroleum Supply Chain in India



Petroleum Supply Chain in India



Petroleum Supply Chain in India



Requirements of a Successful Supply Chain

- Minimization of material procurement
- Maximization of manufacturing capacity and sales
- Meet demand numbers
- Respond quickly to market opportunity by purchasing the production shortfall from other players
- Objective of each production unit would be to maximize the throughput and its margin
- Procurement would purchase the feedstock with not the best yields at lowest cost

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



Needs Strong Coordination among the Players

- Procurement would purchase the feedstock with not the best yields at lowest cost

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



How do we obtain Real-time Information from the Stakeholders?

- Procurement would purchase the feedstock with not the best yields at lowest cost

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



How do we obtain Real-time Information from the Stakeholders?

A web-based portal?

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



**How do we obtain Real-time Information from the Stakeholders?
What is the guarantee that the information submitted is correct?**

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

**We need a decentralized solution where no one
trust each other but they should co-operate**

Information Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

Requirements of a Successful Supply Chain

- Minimization of material procurement



How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

We need a decentralized solution where no one trust each other but they should co-operate

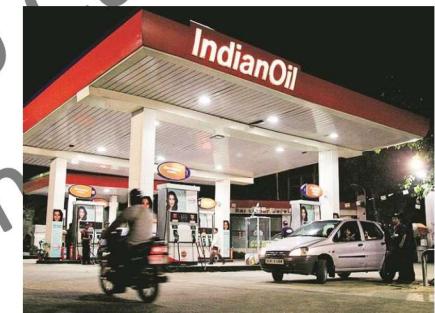
Blockchain is the answer !!

Conclusion

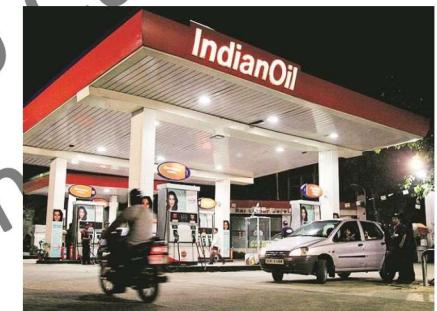
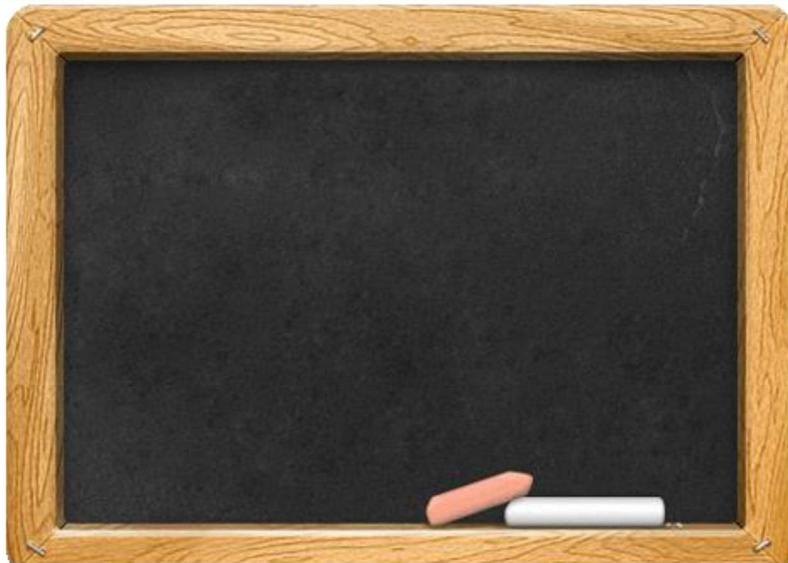
- You have a network of different players) businesses, enterprises, commercial establishments, government or private bodies or even individuals)
- Everyone has their own interest they want to fulfill their goal
- They do not trust each other
- If they cooperate, the society will get benefited
- Trustless Decentralization: Blockchain

Block chain and Crypto Currencies
Dr. Ahlad Kumar

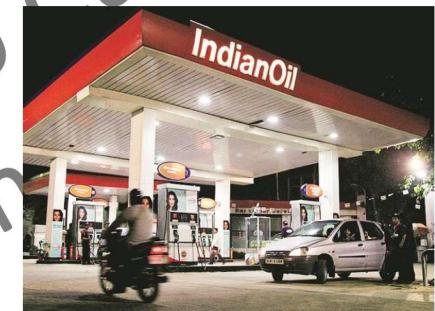
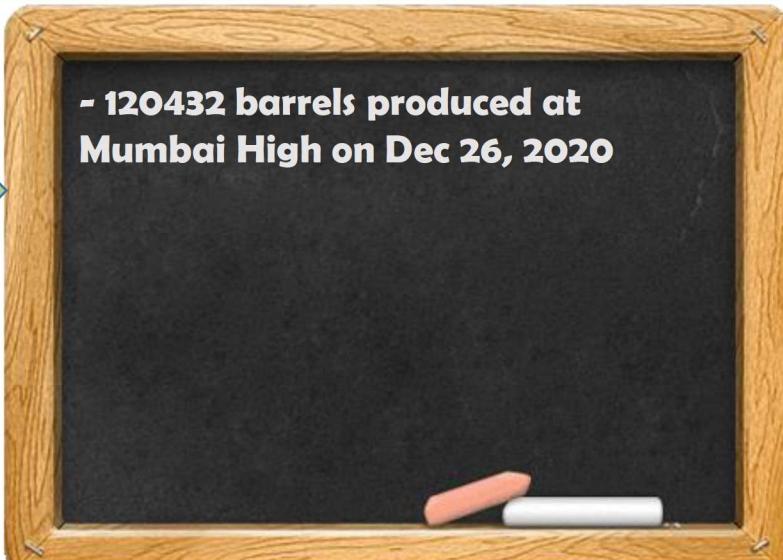
How Can We Obtain Real Time Information?



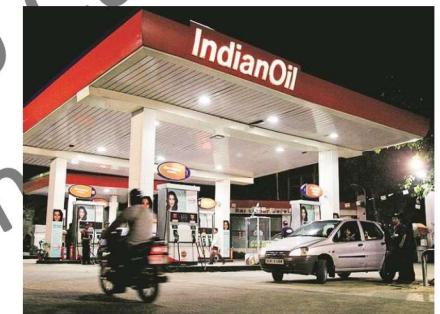
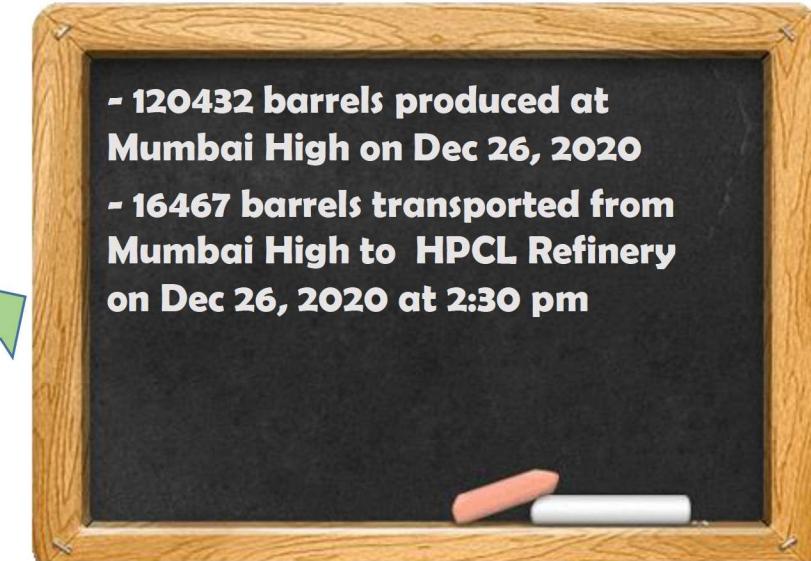
Use a Public Bulletin Board



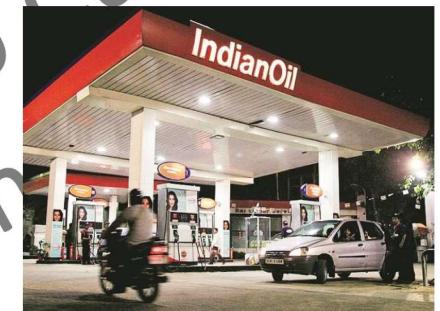
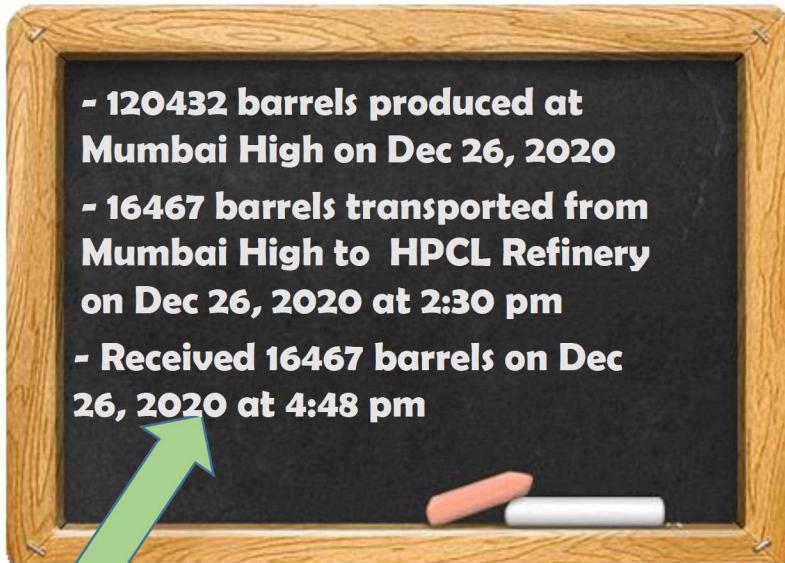
Use a Public Bulletin Board



Use a Public Bulletin Board



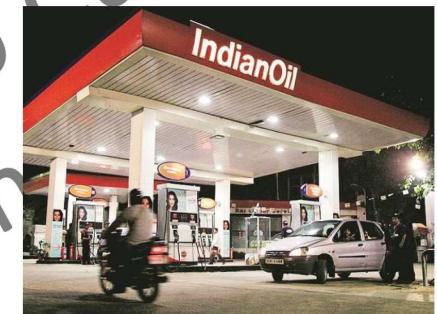
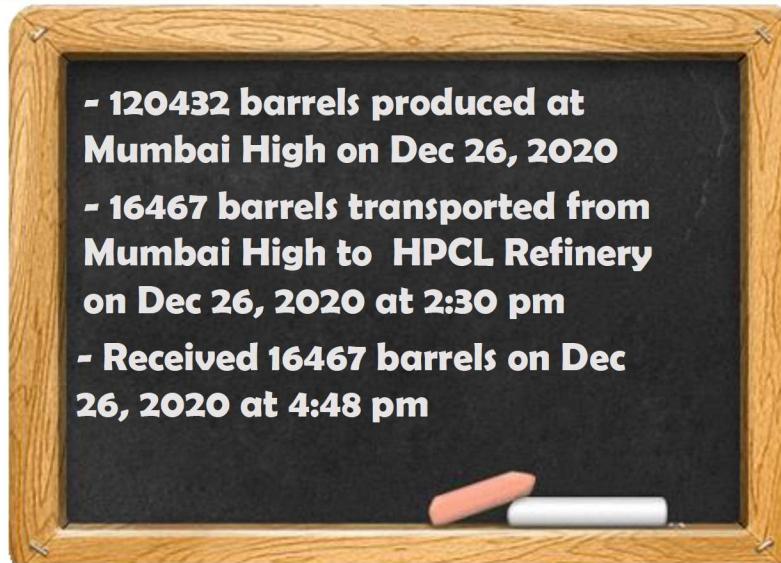
Use a Public Bulletin Board



Use a Public Bulletin Board -- Advantages



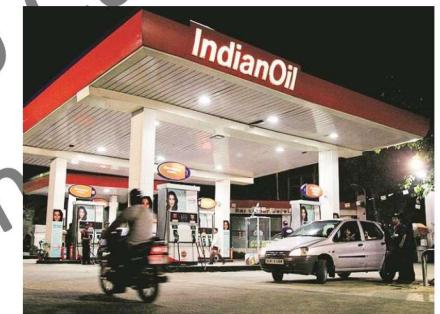
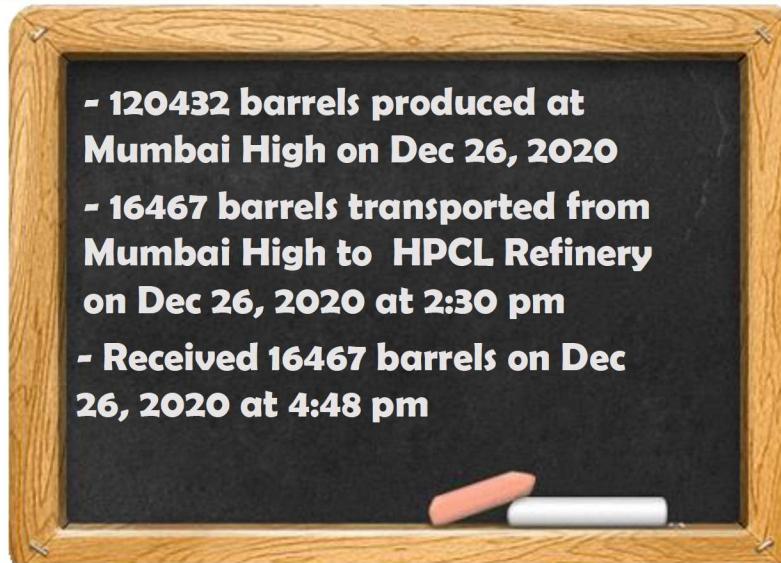
- **Everyone can see all the logs and verify**
- **Infinite space to write**



Use a Public Bulletin Board -- Advantages



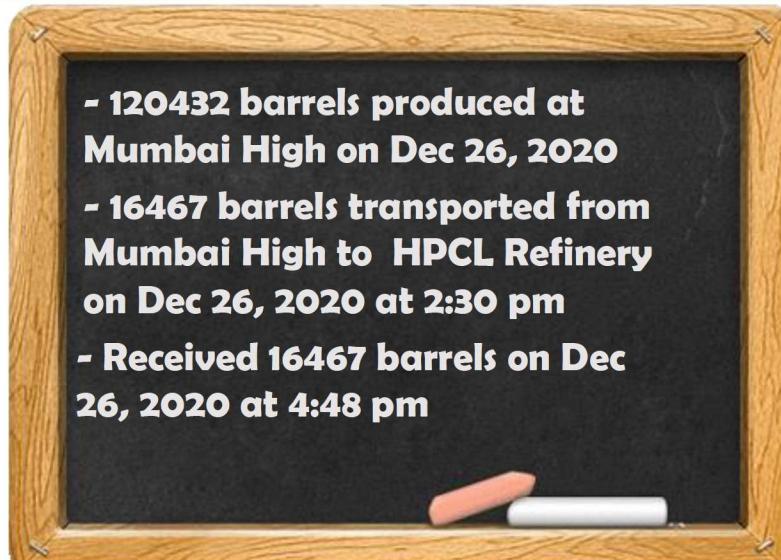
- Any change in information is visible to everyone



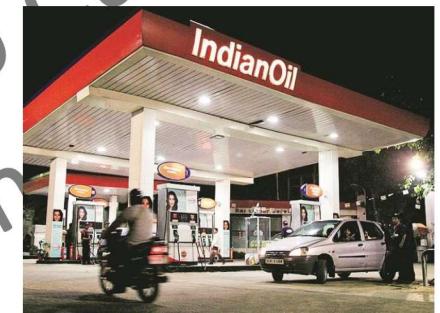
Use a Public Bulletin Board -- Advantages



- **The board is not erasable, no one can deny later**



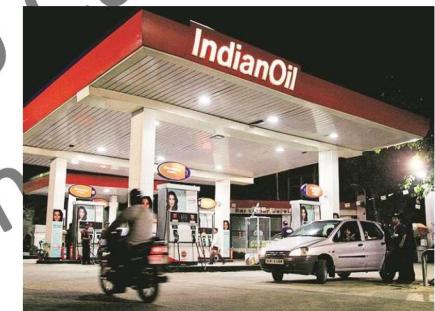
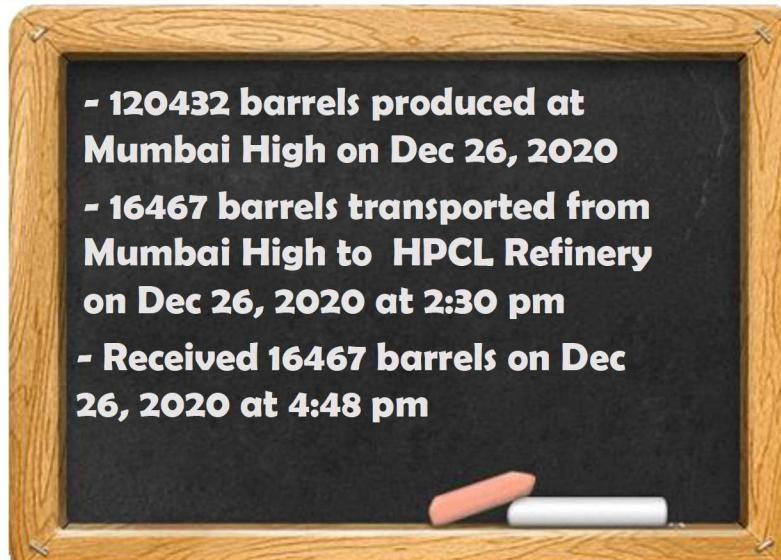
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm
- Received 16467 barrels on Dec 26, 2020 at 4:48 pm



Use a Public Bulletin Board -- Advantages



- **Simple one-step auditing**



Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

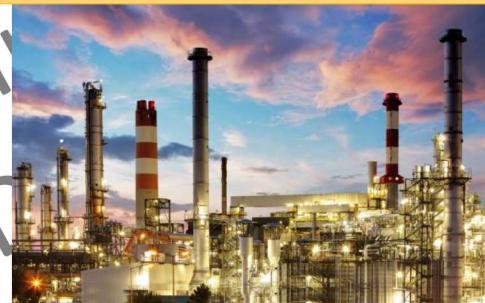


Use a Public Bulletin Board -- Challenges

- 120432 barrels produced at Mumbai High on Dec 26, 2020
16457 barrels transported from

Who will maintain this bulletin board?

- Buy Cloud from amazon



Block chain
D

Use a Public Bulletin Board -- Challenges

- 120432 barrels produced at Mumbai High on Dec 26, 2020
16457 barrels transported from

Who will maintain this bulletin board?

- Buy Cloud from amazon

Who will manage it and provide the cost?



Use a Public Bulletin Board -- Challenges

- 120432 barrels produced at Mumbai High on Dec 26, 2020
16457 barrels transported from

Who will maintain this bulletin board?

- Buy Cloud from amazon
- One of the enterprises maintain a private cloud

Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
What is the guarantee that it is not a fraud?



Blockchain



Use a Public Bulletin Board -- Challenges

- 120432 barrels produced at Mumbai High on Dec 26, 2020

16457 barrels transported from

Who will maintain this bulletin board?

- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
- Let everyone maintain the same copy of the board individually and independently



Blockchain

Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
- Let everyone maintain the same copy of the board individually and independently – **BUT HOW?**



Blockchain

Use a Public Bulletin Board -- Challenges



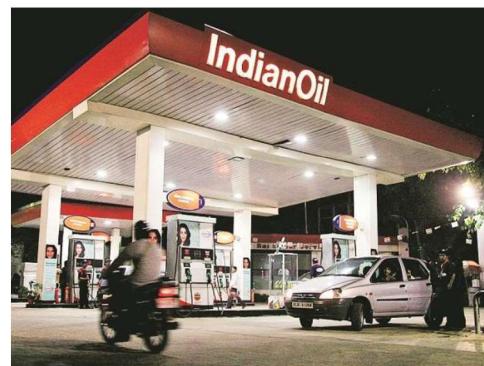
Who will maintain this bulletin board?

- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
- Let everyone maintain the same copy of the board individually and independently



Block chain
D

What is this “Blockchain”?



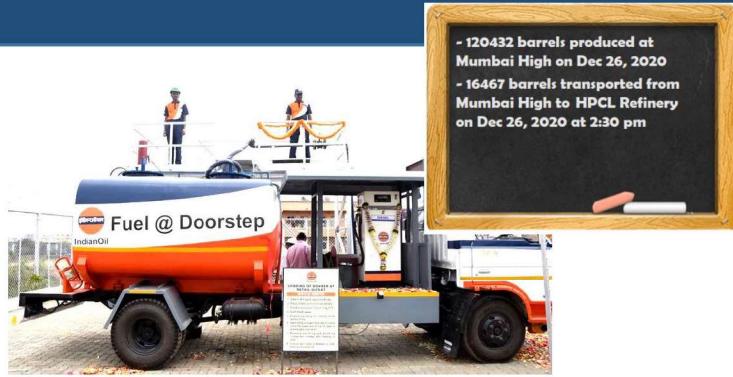
A decentralized and multi-authority networked information data storage and access system

BIO
and Cryptocurrencies
. Ahlad Kumar

What is this “Blockchain”?



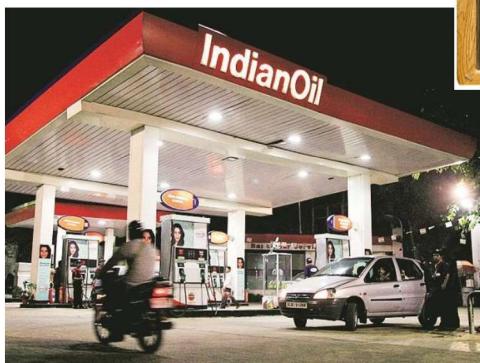
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm



- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm



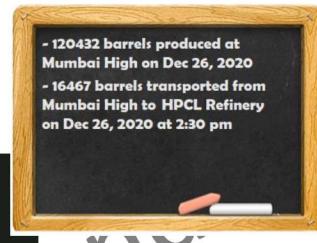
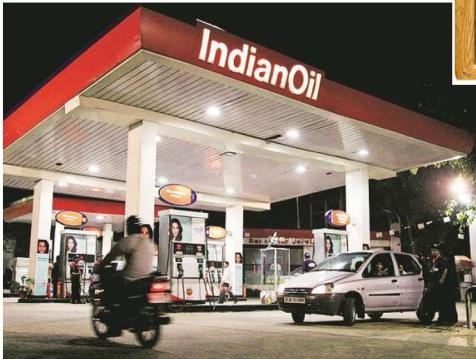
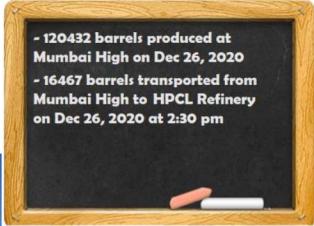
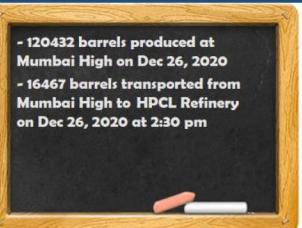
- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm



- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

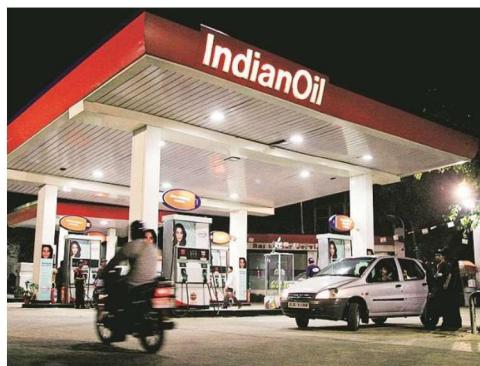
No one is the sole-owner of the data, but everyone has a copy of the data - there is no central database

What is this “Blockchain”?



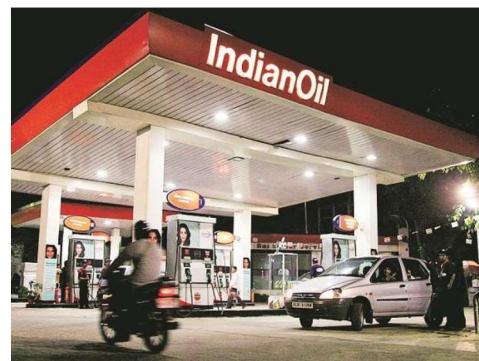
Everyone holds exactly the same copy of the data at the same instance of the time

What is this “Blockchain”?



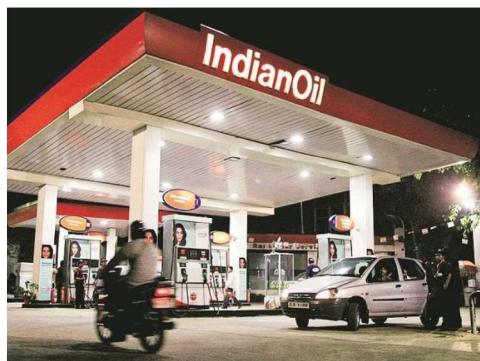
An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later

What is this “Blockchain”?



An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later

What is this “Blockchain”?



An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later

Once something is added in the blockchain, it cannot be denied later

What is this “Blockchain”?

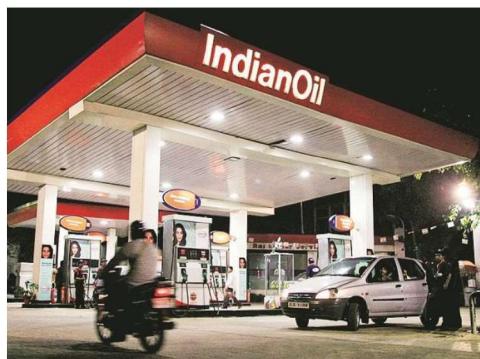
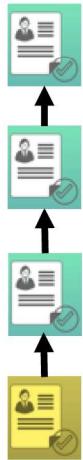


The information is transparent to all - everyone can see what is going on in the system

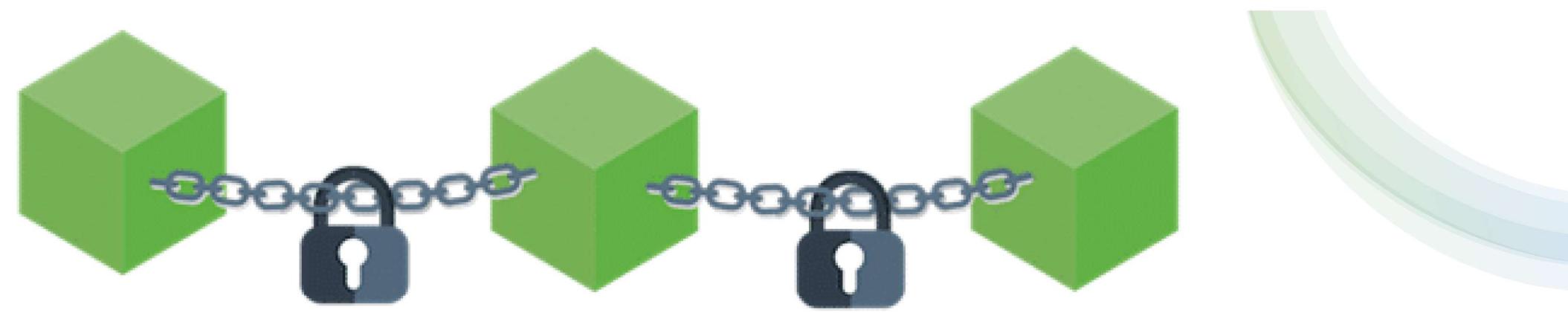
What is this “Blockchain”?



The information is transparent to all - everyone can see what is going on in the system



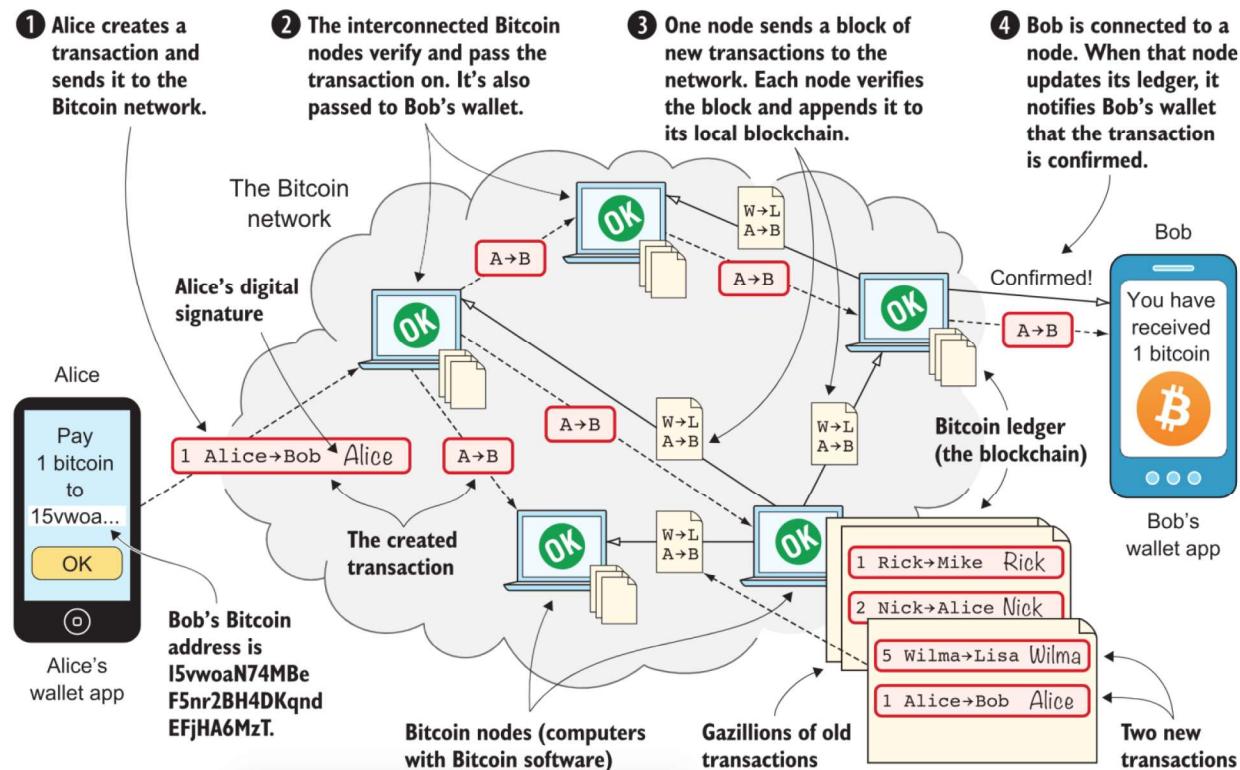
No-one can make any change without others to notice it



So, What Can be the Definition of a "Blockchain"

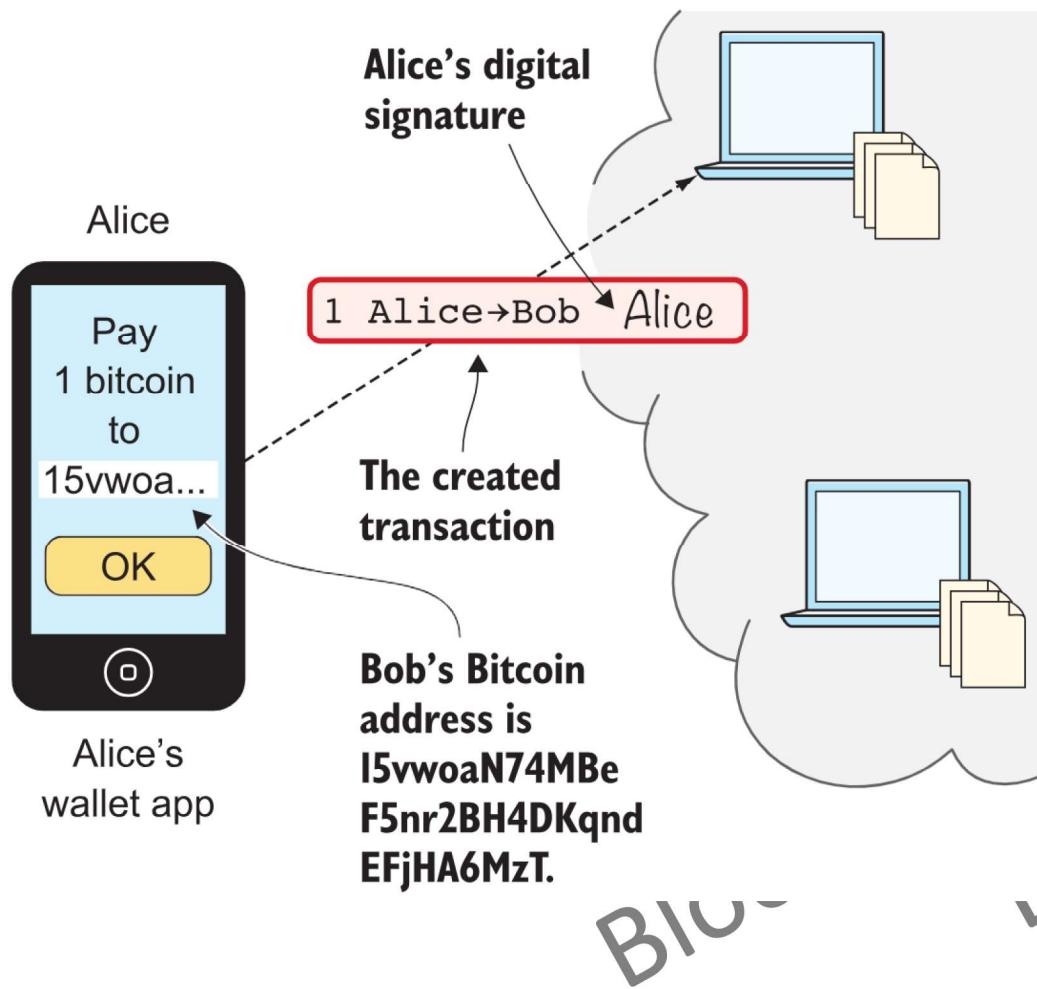
A decentralized immutable append-only public ledger

Big Picture



- (1) Alice creates and signs a transaction that moves 1 bitcoin from her to Bob. She then sends the transaction to the Bitcoin network.
- (2) The computers in the network check that Alice actually has the money to spend and that the transaction is authentic. They then pass the transaction to their neighbours, called *peers*.
- (3) Each computer updates its own copy of the *Bitcoin blockchain*, or the *ledger*, with the new payment information.
- (4) The network notifies Bob that he has received 1 bitcoin.

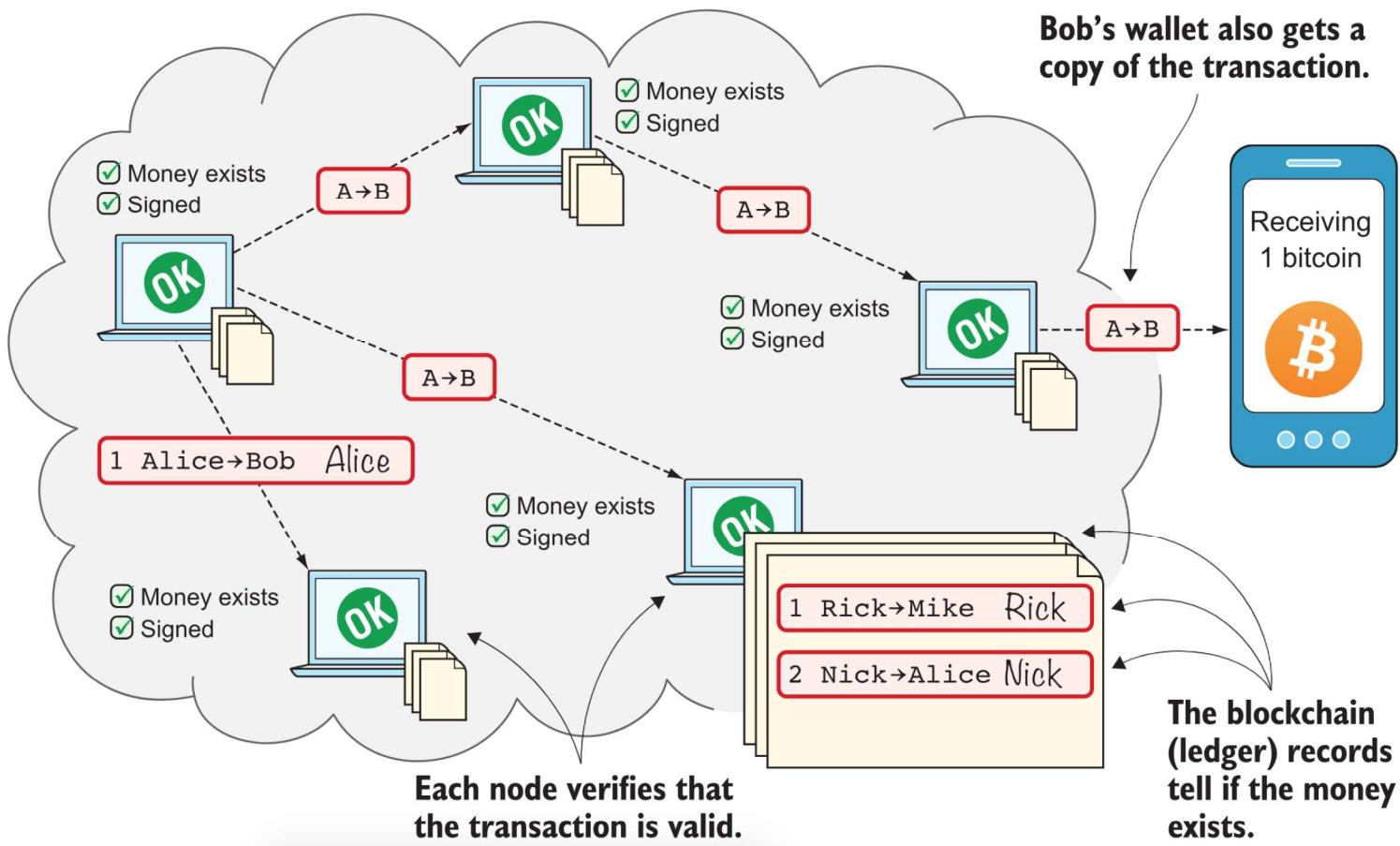
(1) Transactions



The Bitcoin *transaction* is a piece of data specifying

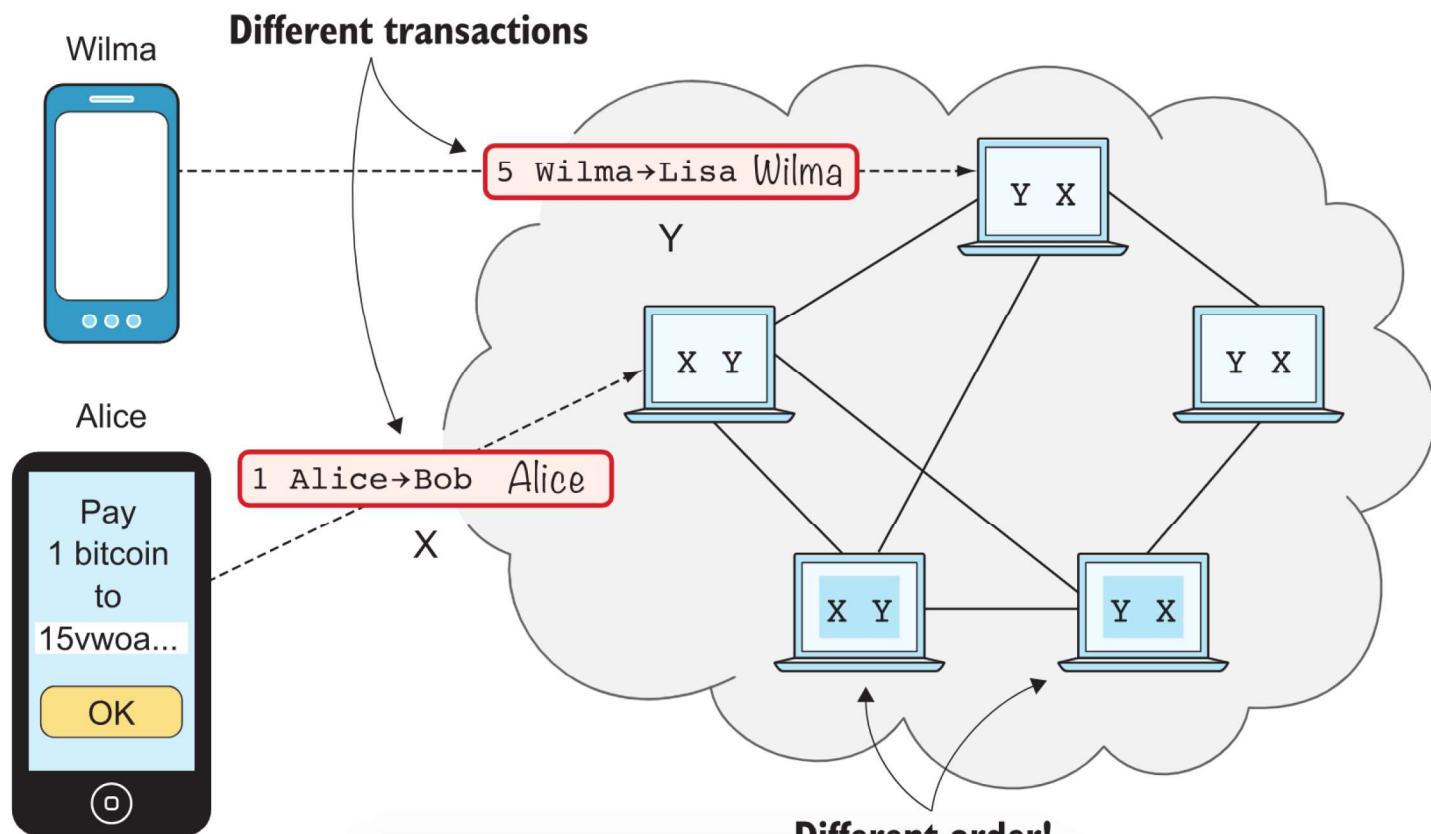
- (1) The amount to move (1 bitcoin)
- (2) The Bitcoin address to move the money to (Bob's Bitcoin address)
15vwoaN74MBe F5nr2BH4DKqnd EFjHA6MzT
- (3) A *digital signature* (made with Alice's private key)

The Blockchain network



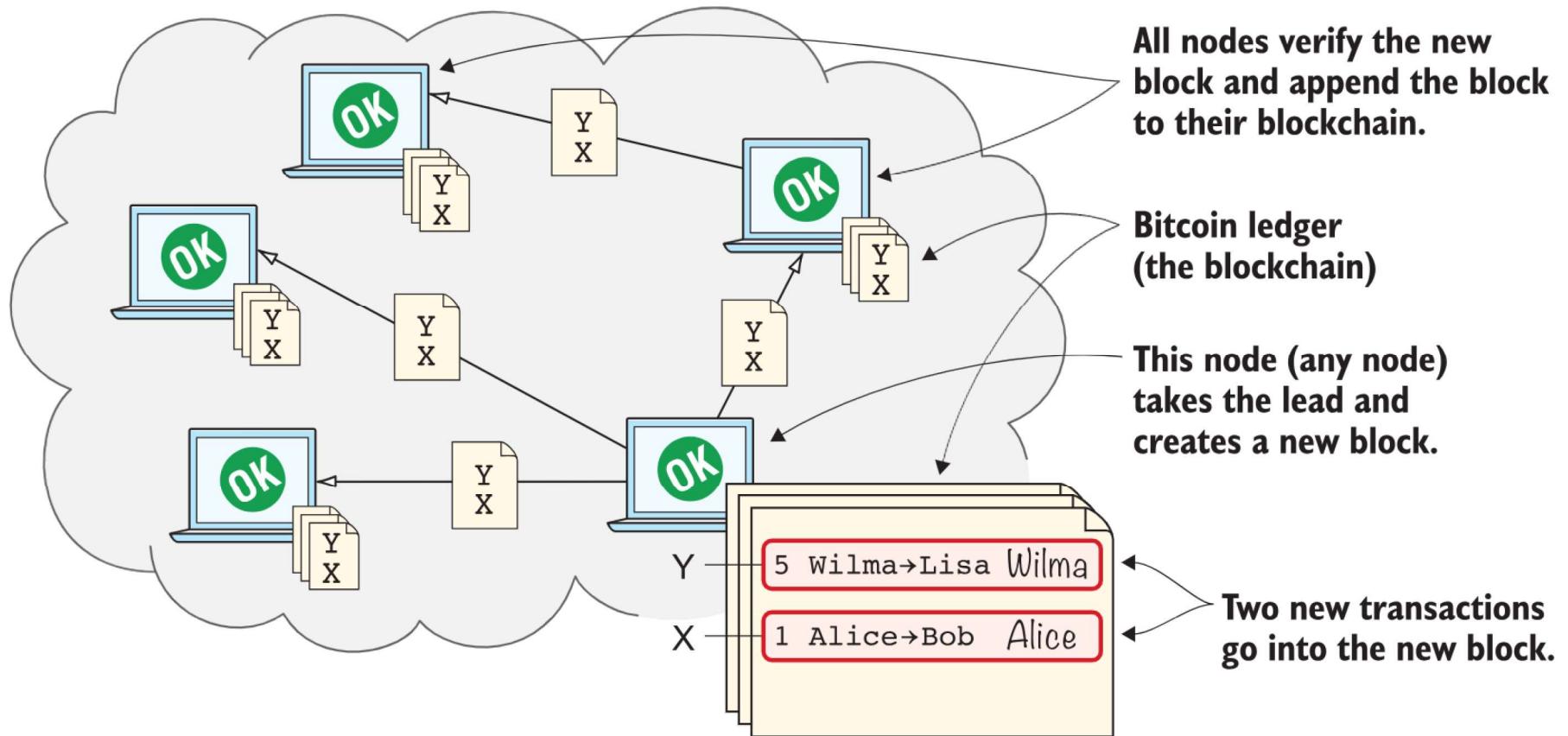
Alice has sent her transaction to a node in the network. The node verifies the transaction and forwards it to other nodes. Eventually, the transaction will reach all nodes in the network.

The Blockchain



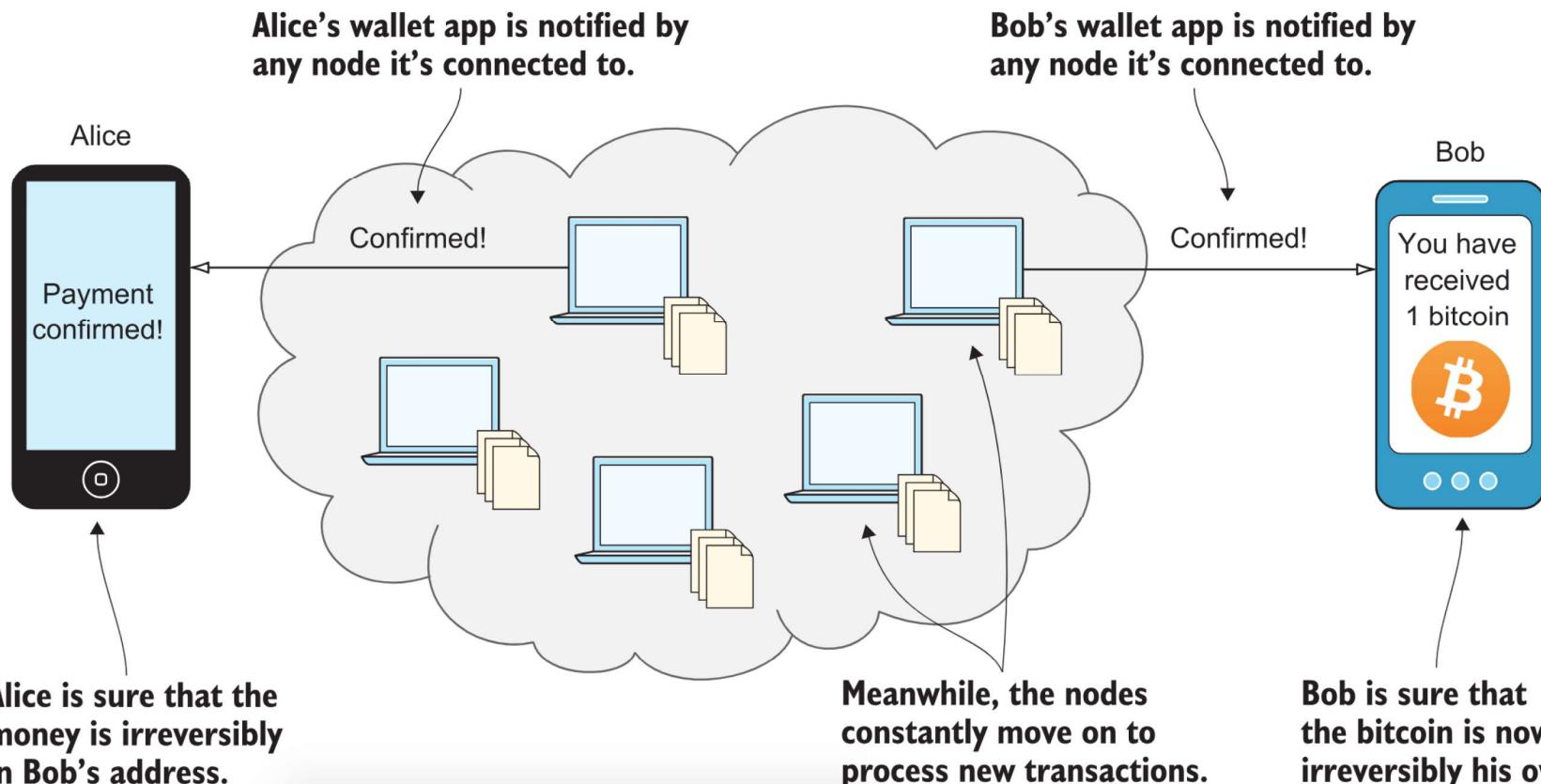
Transactions arrive in different orders at different nodes. If all nodes wrote their transactions to the blockchain in order of arrival, the different nodes blockchains would differ.

The Blockchain network



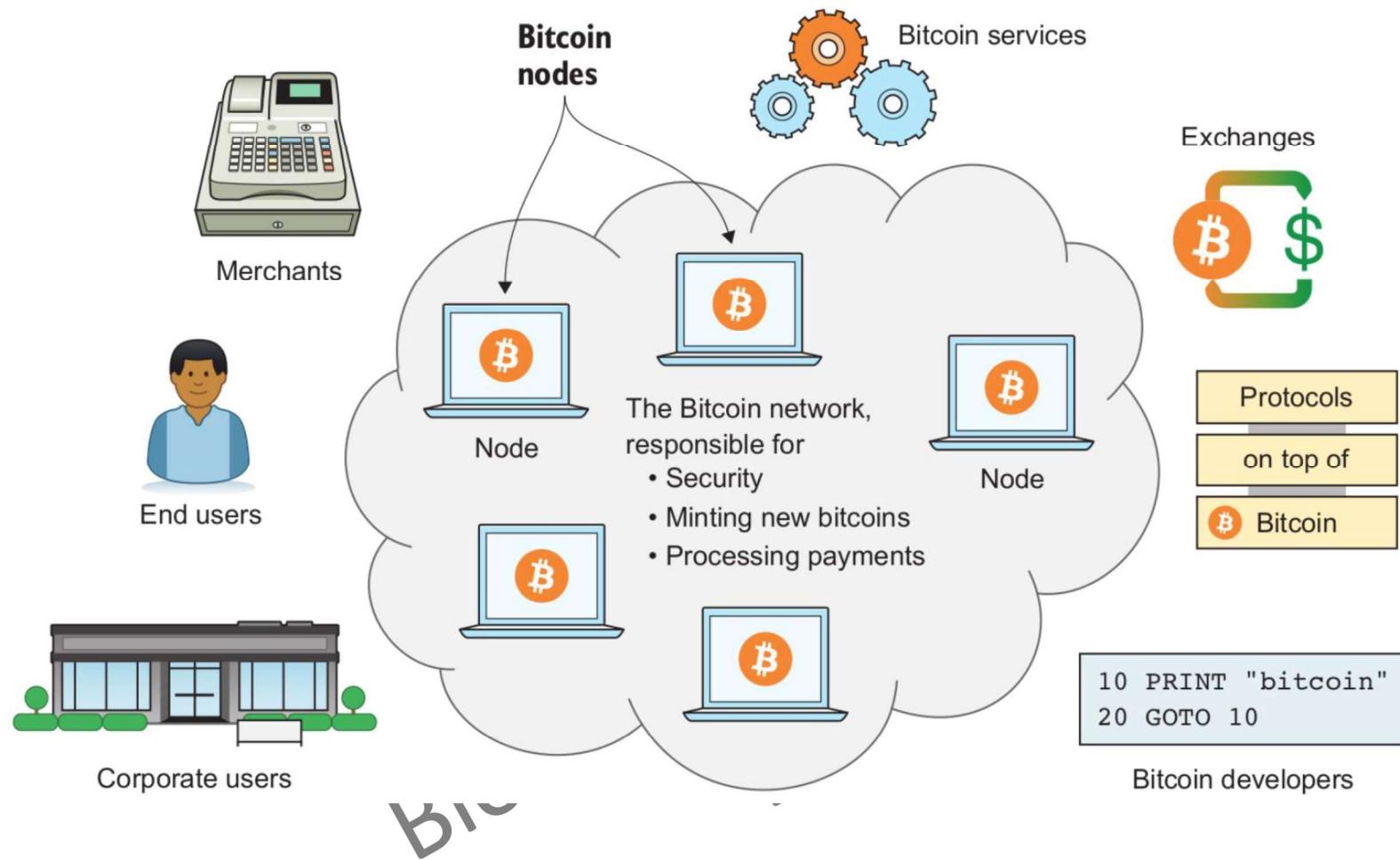
One node takes the lead and tells the others in what order to add transactions. The other nodes verify the block and update their blockchain copies accordingly.

Wallets



Bob's wallet has asked a node to notify the wallet upon activity at Bob's Bitcoin address. Alice pays to Bob's address, and the node has just written the transaction to the blockchain, so it notifies Bob's wallet.

Customers



- **End users:** People using Bitcoin for their day-to-day needs, such as savings, shopping, speculation, or salaries
- **Corporate users :** Companies using Bitcoin to solve their business needs, such as paying wages internationally, or use cases similar to those of end users
- **Merchants:** For example, a restaurant or a bookstore accepting Bitcoin payments
- **Bitcoin services:** Companies providing Bitcoin-related services to customers, such as topping up mobile phones, anonymization services, remittance services, or tipping services
- **Exchanges :** Commercial services people can use to exchange their local currency to and from bitcoins
- **Protocols on top:** Systems that operate “on top” of Bitcoin to perform certain tasks, such as payment network protocols, specialized tokens, and decentralized exchanges
- **Bitcoin developers:** People working, often for free, with the open source computer programs that participants of the Bitcoin network use