

Theory And Applications of Blockchain

Course Introduction

Department of Computer Science
and Engineering

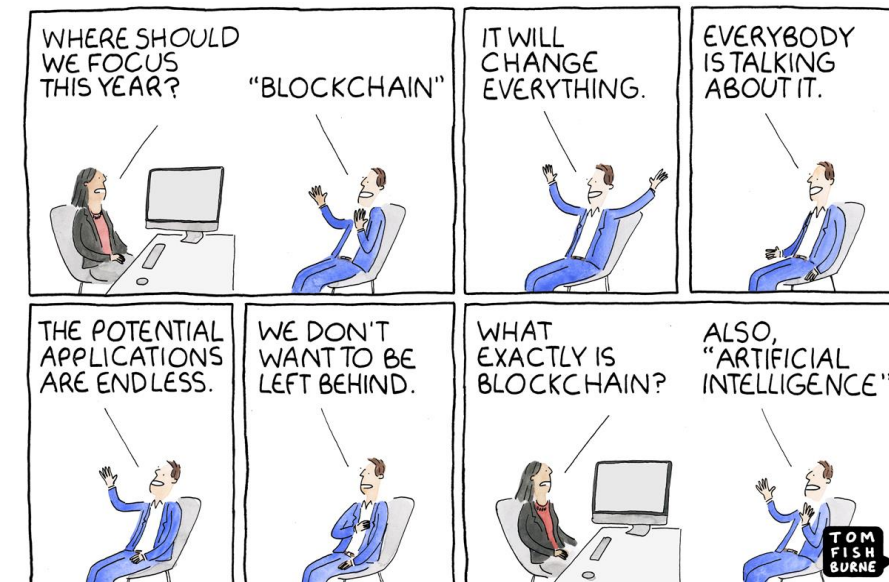


INDIAN INSTITUTE OF TECHNOLOGY
KHARAGPUR

Sandip Chakraborty
sandipc@cse.iitkgp.ac.in

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



Prerequisite for this Course

- Good programming skills
- Good grasp in Data Structures and Algorithms
- Concepts from operating systems
 - Process management
 - Inter-process communication
 - Memory management
 - Resource virtualization
- Concepts from computer networks
 - Network protocol stack
 - Peer to Peer networks
 - Network performance metrics

Then why should you take this course

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

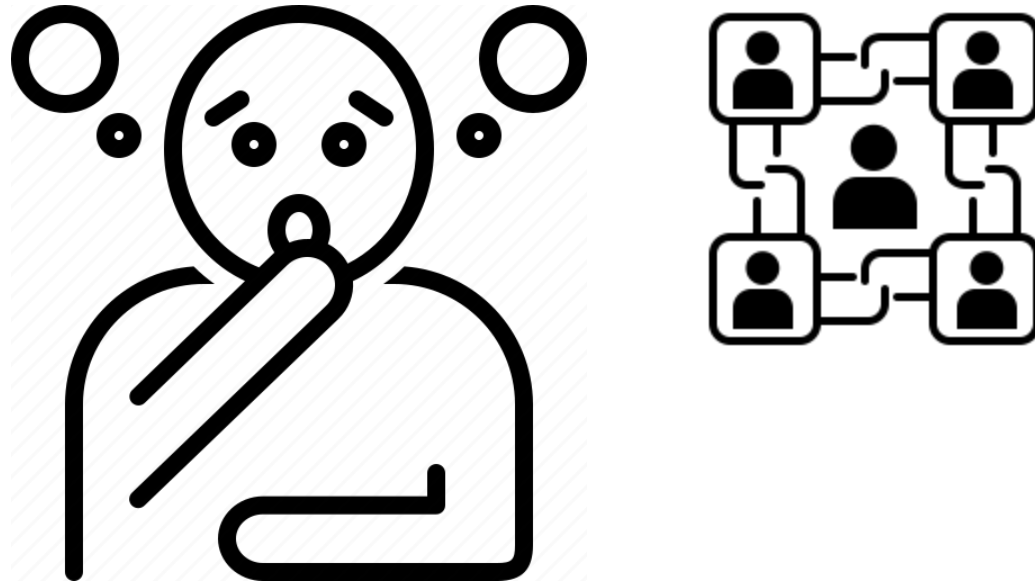
The Myth Busters

- 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
- You cannot replace a database with a blockchain
 - Blockchain is not a distributed database
 - Blockchain is not designed to securely store ANY data

Then why should you take this course

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

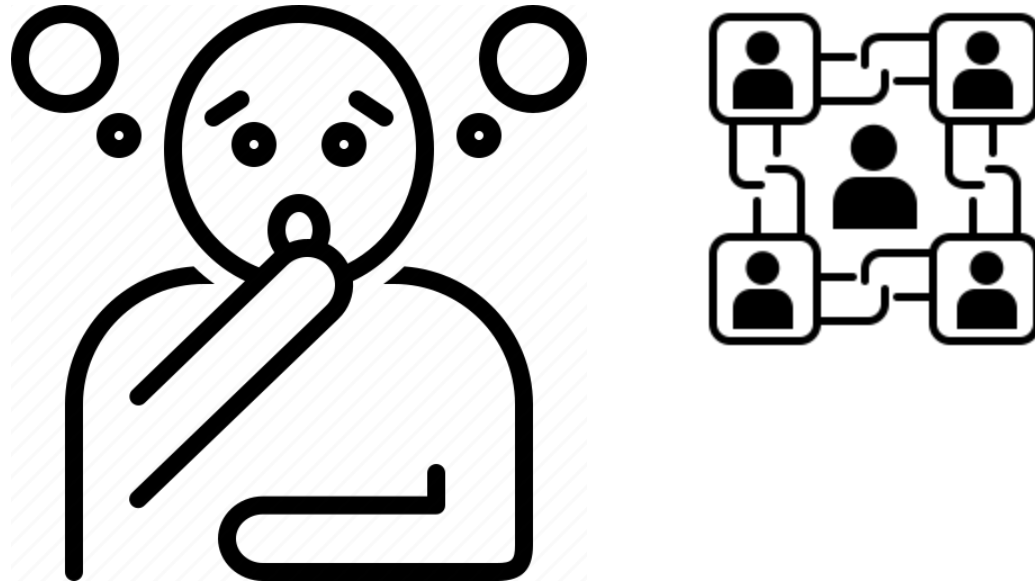
So, what is the right place?



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 !!

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?

What We'll Cover in This Course?

- Blockchain as a Networking Protocol
 - For what types of network architectures, can we design a blockchain-based solution?
 - What different networking protocols are used in blockchain?
 - How does the design of various network protocols impact blockchain performance?
 - How can we optimize the networking architecture to make a blockchain performant?

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?
- Blockchain as a Security Blackbox
 - How do we ensure the security of the data stored in a blockchain?
 - What are the attack models that can be applied on a Blockchain architecture?
 - What level of data security can be ensured with the help of a blockchain?
 - How can we optimize various cryptographic operations to make a Blockchain implementation performant?

What We'll Cover in This Course?

- Blockchain as a Networking Protocol
 - For what types of network architectures, can we design a blockchain-based solution?
 - What different networking protocols are used in blockchain?
 - How does the design of various network protocols impact blockchain performance?
 - How can we optimize the networking architecture to make a blockchain performant?
- Blockchain as a Distributed System
 - What happens when some participants in a blockchain-based system starts behaving maliciously?
 - How do we ensure the correctness of blockchain protocols?
 - How do we ensure "safety" and "liveness" of blockchain operations?

What We'll Cover in This Course?

- Blockchain as a Programming Framework
 - How can you write a "smart" distributed application on top of blockchain?
 - What are the supported features for such a programming framework?
 - What can and cannot be done with such a programming framework?

What We'll Cover in This Course?

- Blockchain as a Programming Framework
 - How can you write a "smart" distributed application on top of blockchain?
 - What are the supported features for such a programming framework?
 - What can and cannot be done with such a programming framework?
- Finally, the Blockchain Applications
 - What are the different types of applications that can be realized with blockchain?
 - What are the different types of applications that cannot be realized with blockchain?

The Different Blockchain Frameworks That We'll Explore



Ethereum



**Hyperledger
FABRIC**

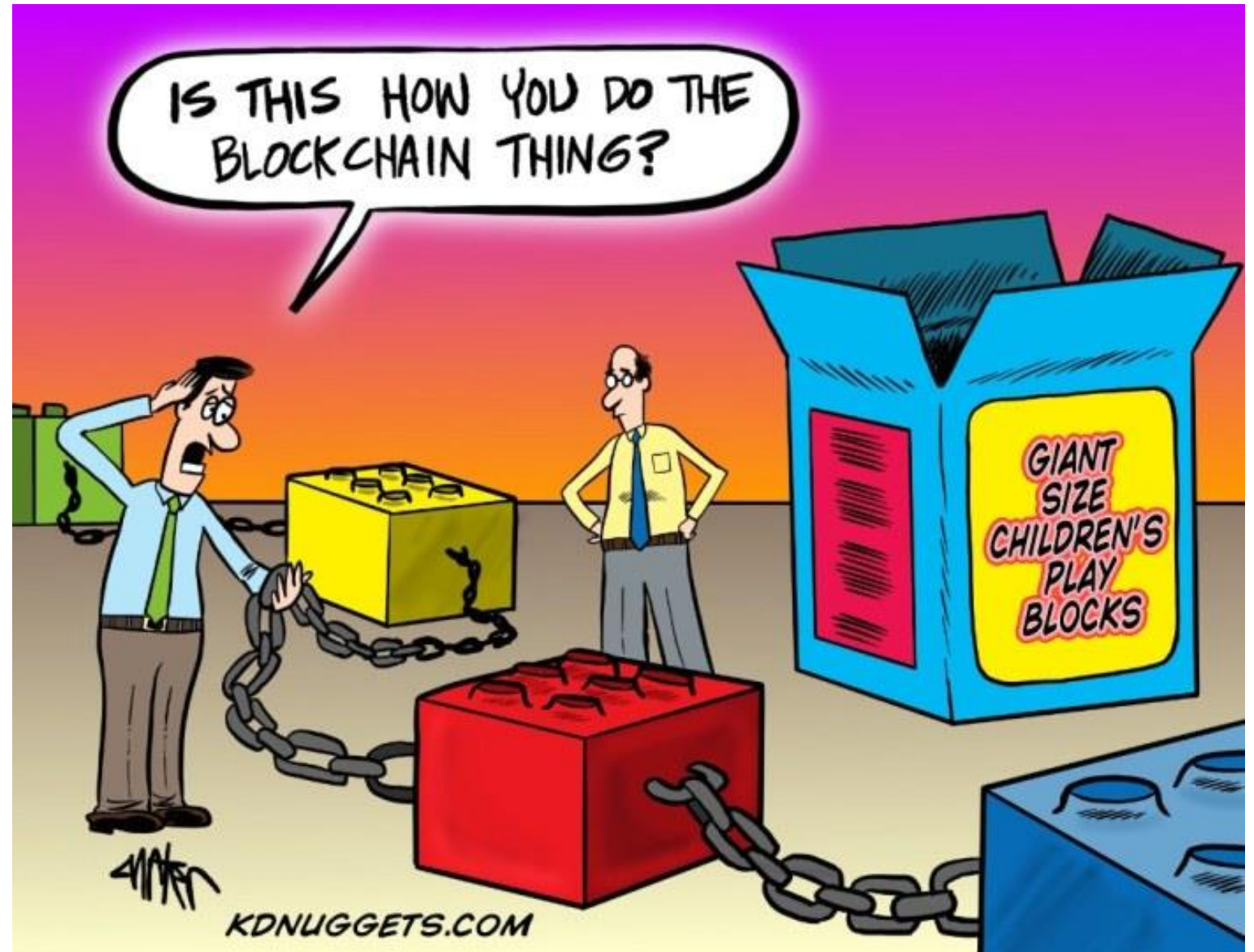


**Hyperledger
INDY**

Grading

- 5 Programming Assignments (Covers Tutorials): 50 Marks
 - All the assignments have equal weightage
- Mid-Sem: 30
- End-Sem: 30

So, What is a
Blockchain?



A vibrant, stylized illustration representing Supply Chain Management. The background is white, populated with various icons and shapes. At the top, a grey speech bubble contains a white box icon with the number '11'. To its right, a green speech bubble contains the letters 'SCM'. Below these, a blue cloud contains a white barcode with the number '1715' and a magnifying glass icon. To the right of the barcode, a green cloud contains a white airplane icon. Further right, a blue cloud contains a white calendar icon with the number '17'. At the bottom left, a blue cloud contains a white bar chart and a gear icon. In the center, a green cloud contains a white train icon. To the right of the train, a green cloud contains a white shopping cart icon. At the bottom right, a green cloud contains a white warehouse icon. In the background, there are green industrial buildings, a green truck, and a green cloud containing a white gear and a speech bubble with a gear icon. The text 'Supply Chain Management: The Players and the Game' is overlaid in the center in a black, sans-serif font.

Supply Chain Management: The Players and the Game

Supply Chain in Petroleum Industry



Crude Purchase

Supply Chain in Petroleum Industry



Crude Purchase



Crude Transportation

Supply Chain in Petroleum Industry



Crude Purchase



Crude Transportation



Crude Storage

Supply Chain in Petroleum Industry



Crude Purchase



Crude Transportation

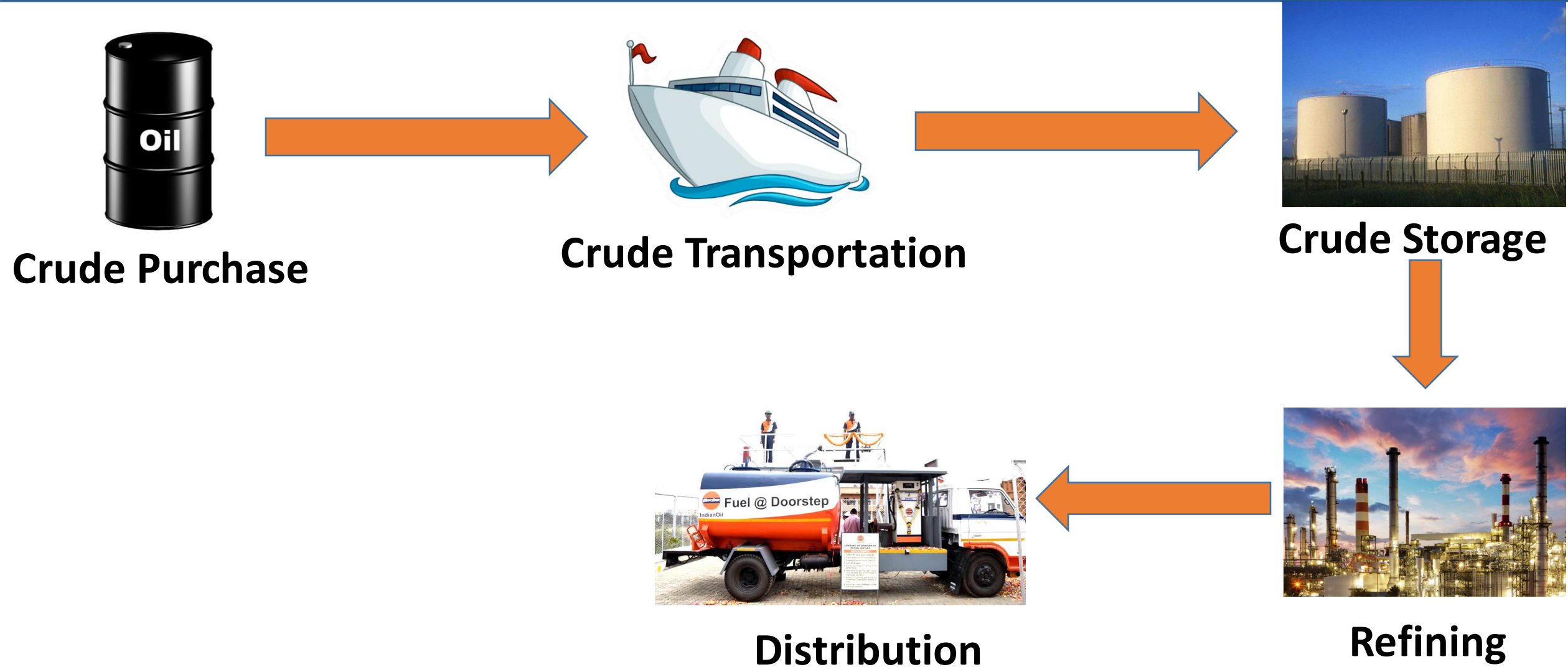


Crude Storage



Refining

Supply Chain in Petroleum Industry



Supply Chain in Petroleum Industry



Crude Purchase



Crude Transportation



Crude Storage



Retail



Distribution



Refining

Petroleum Supply Chain in India

Ministry of Petroleum and Natural Gas

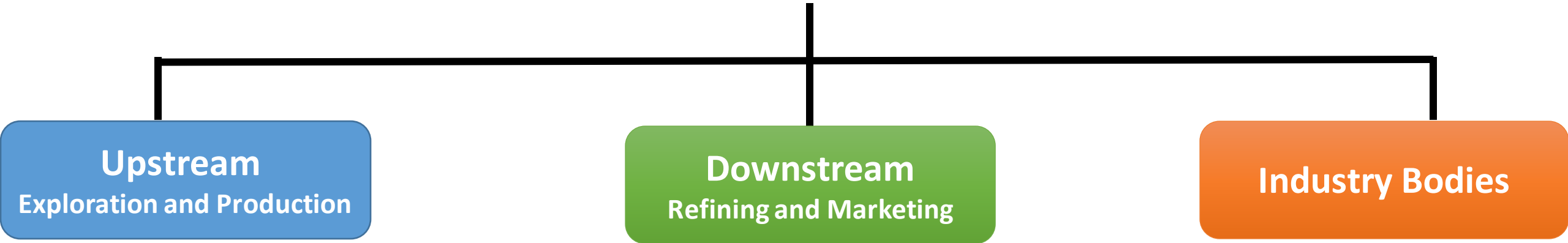
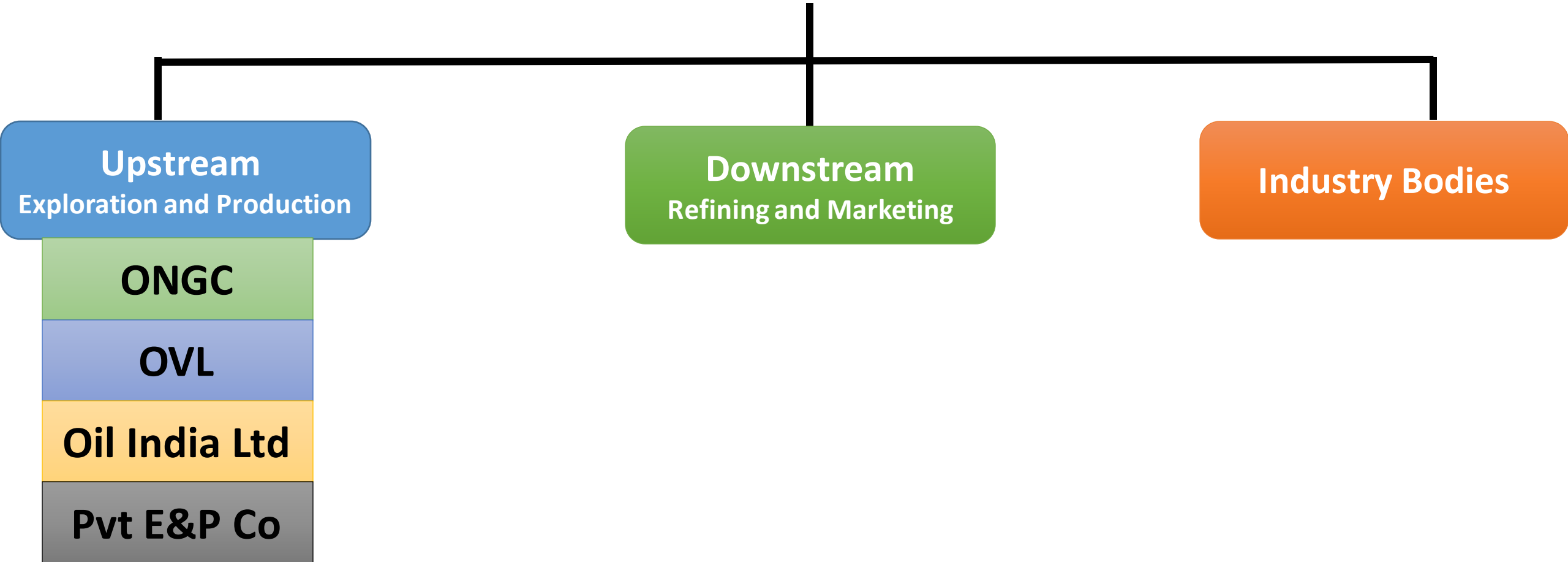


Diagram Source: <https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india>

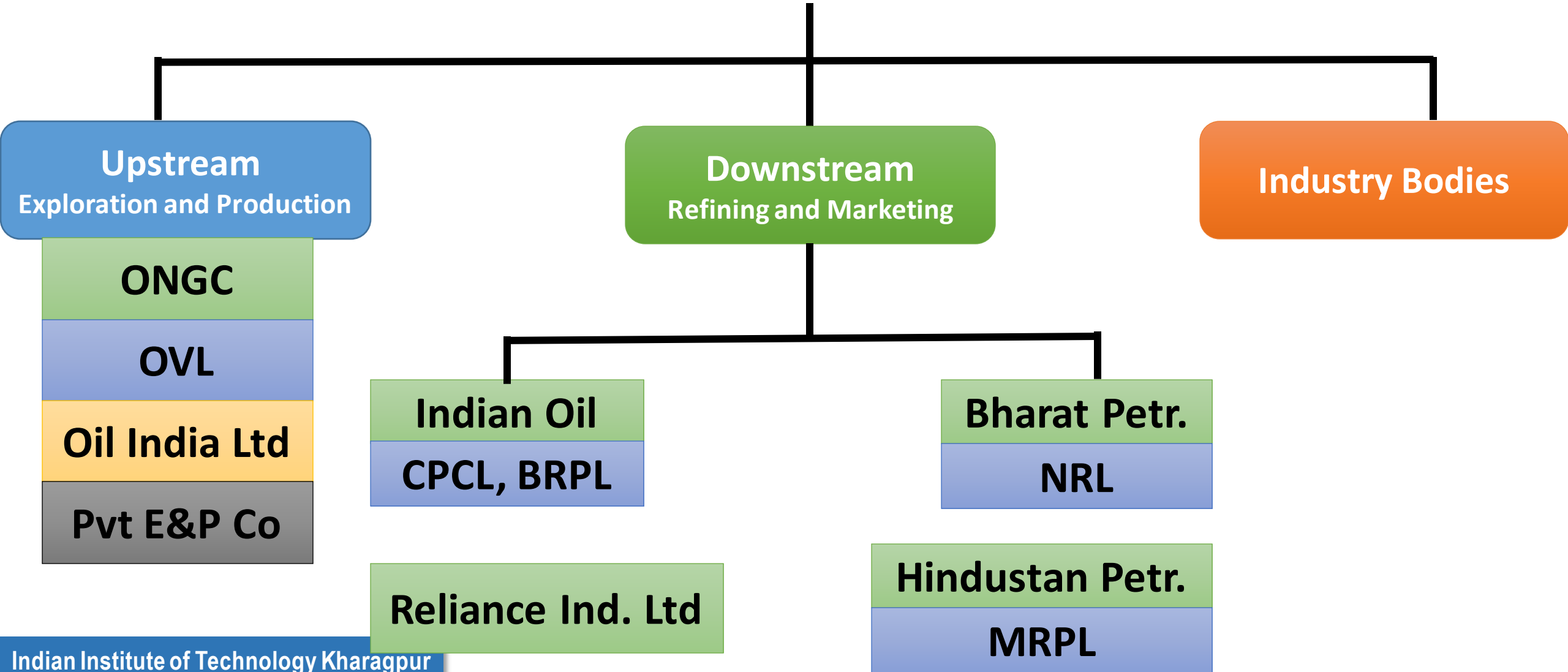
Petroleum Supply Chain in India

Ministry of Petroleum and Natural Gas



Petroleum Supply Chain in India

Ministry of Petroleum and Natural Gas

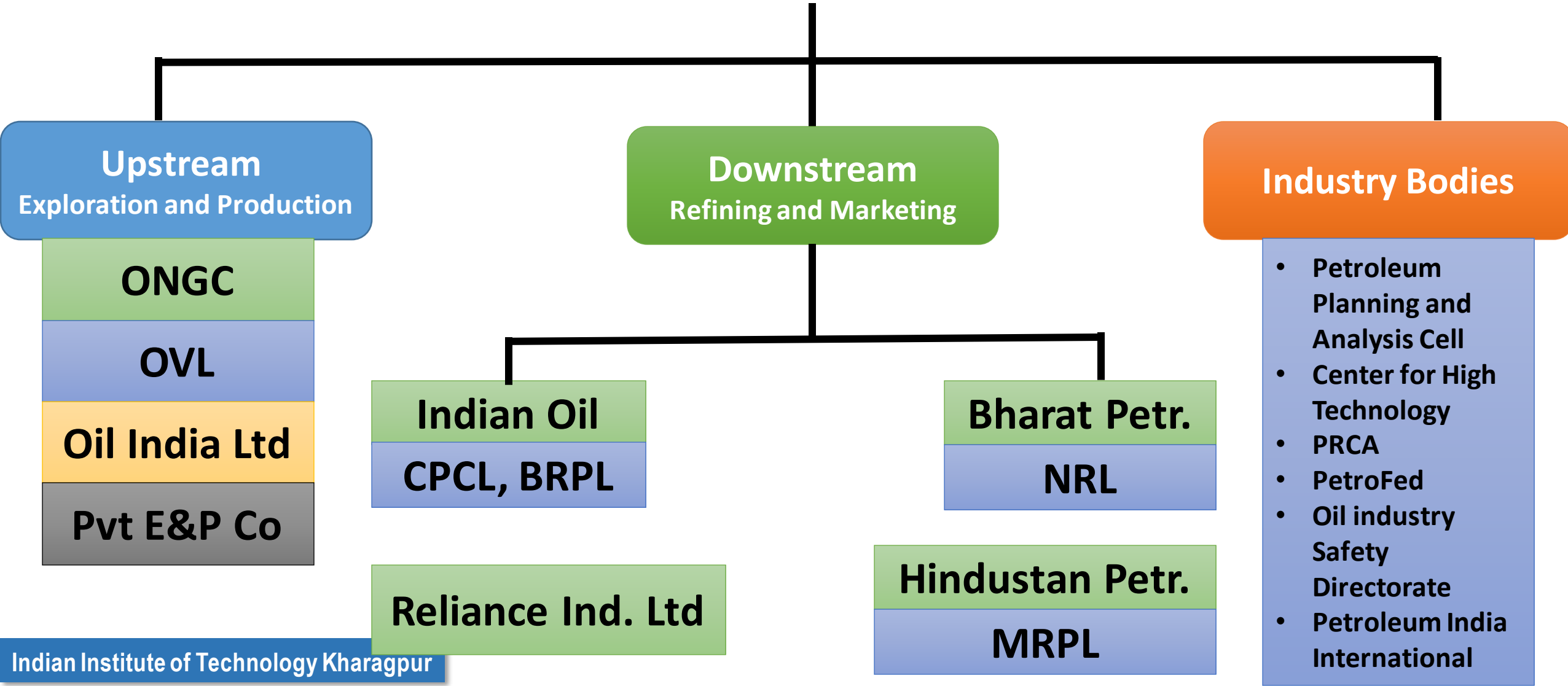


Requirements of a Successful Supply Chain

- 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

Petroleum Supply Chain in India

Ministry of Petroleum and Natural Gas



Requirements of a Successful Supply Chain

- Minimization of material procurement



Needs Strong Coordination among the Players

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



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

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



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?

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?
What is the guarantee that the information submitted is correct?
What if someone denies the information later on?

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?
What is the guarantee that the information submitted is correct?
What if someone denies the information later on?

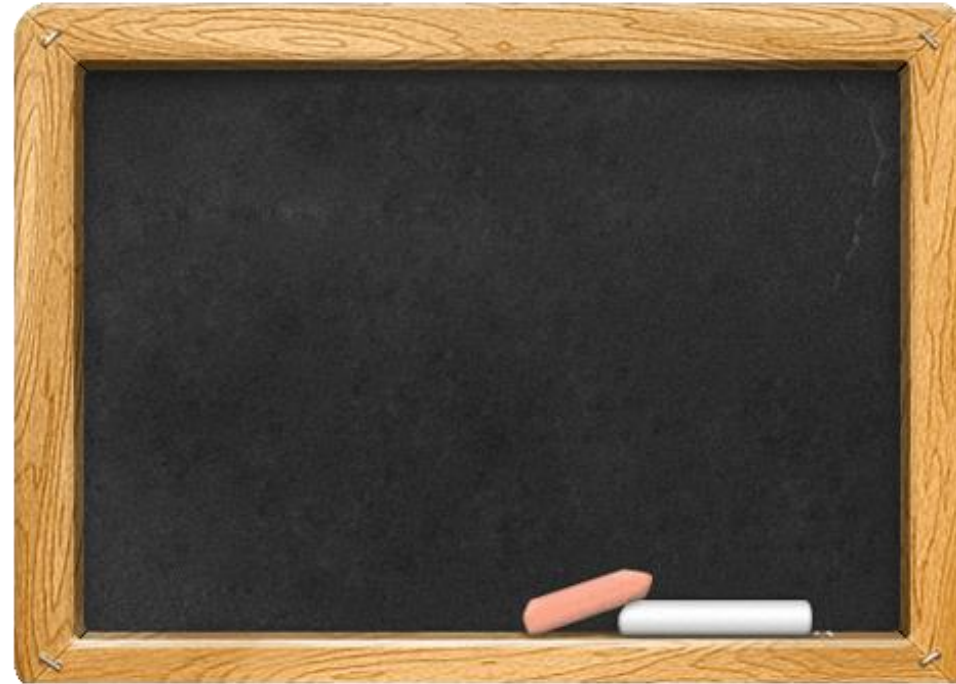
Blockchain is the answer !!

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

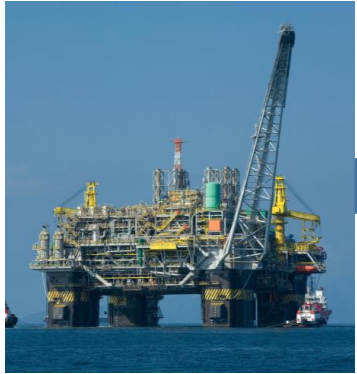
How Can We Obtain Real Time Information?



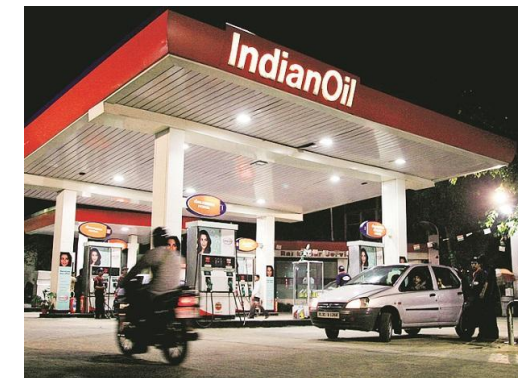
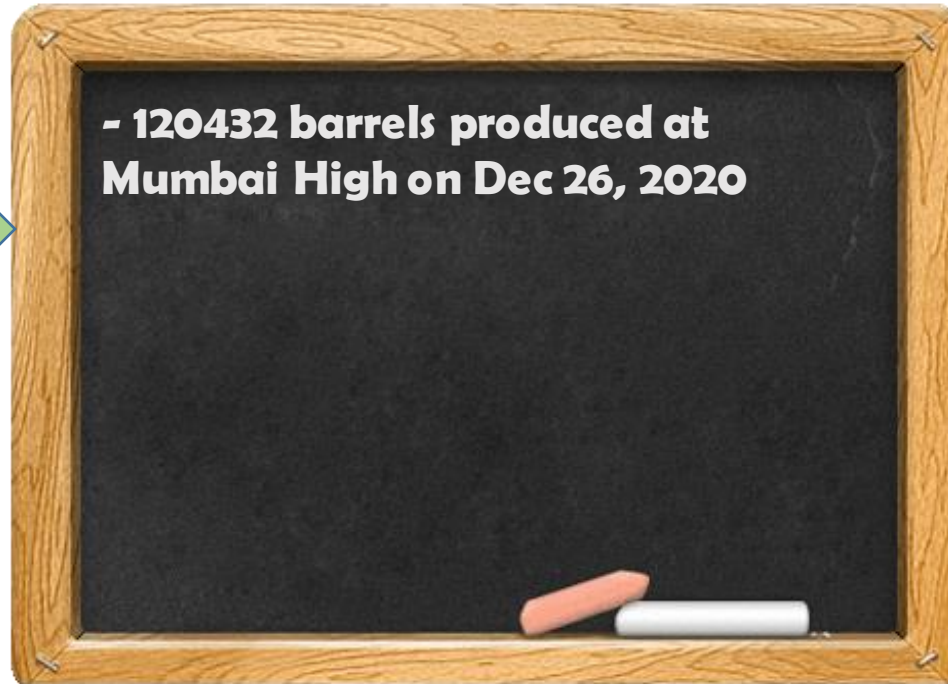
Use a Public Bulletin Board



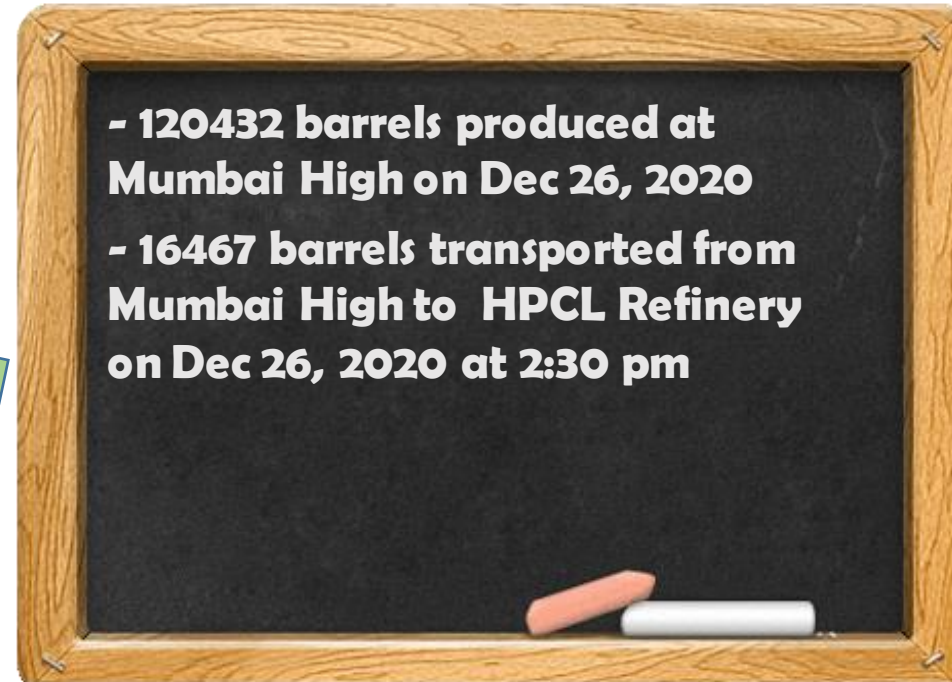
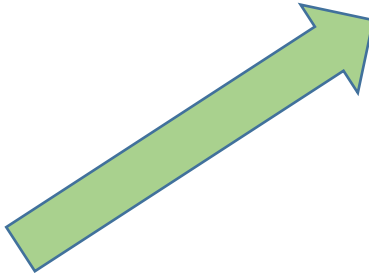
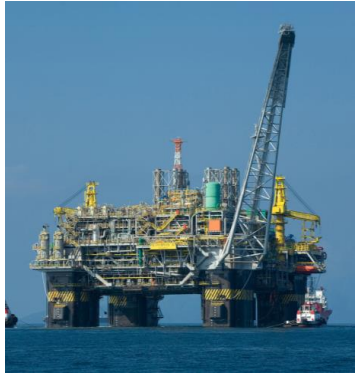
Use a Public Bulletin Board



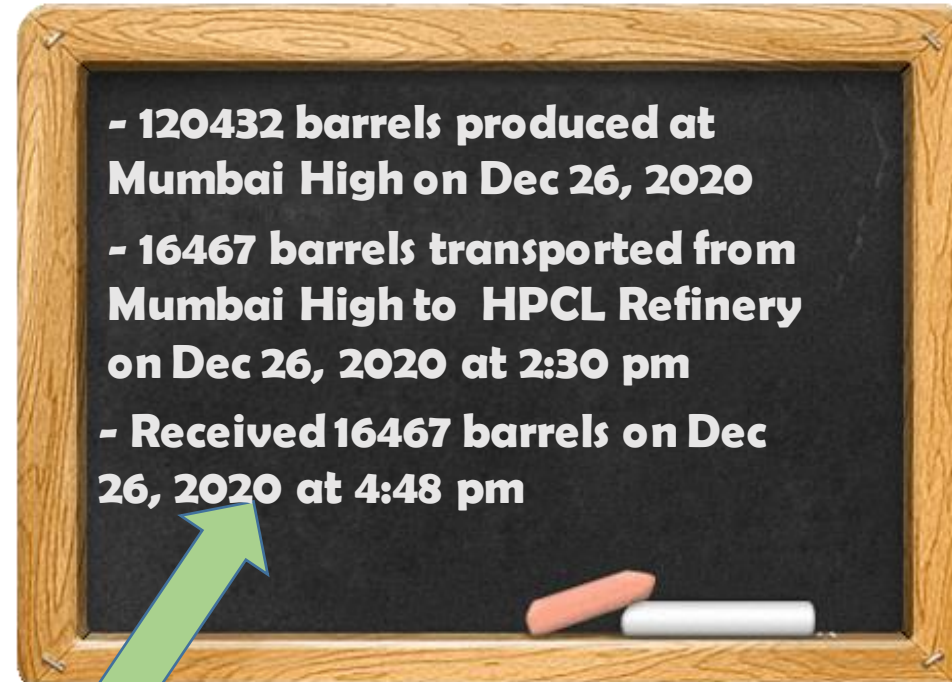
**- 120432 barrels produced at
Mumbai High on Dec 26, 2020**



Use a Public Bulletin Board



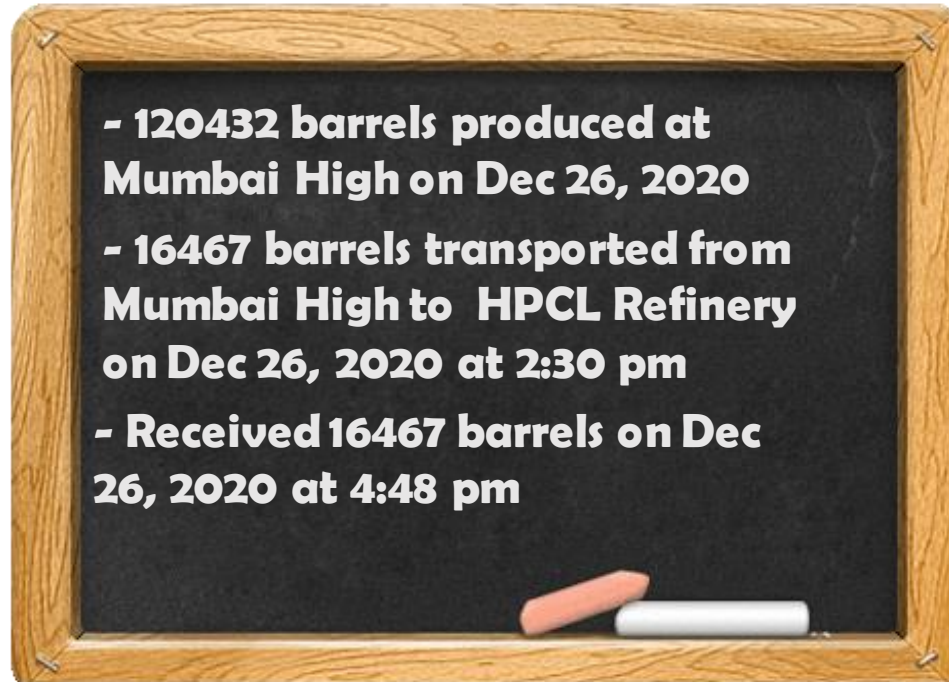
Use a Public Bulletin Board



Use a Public Bulletin Board -- Advantages



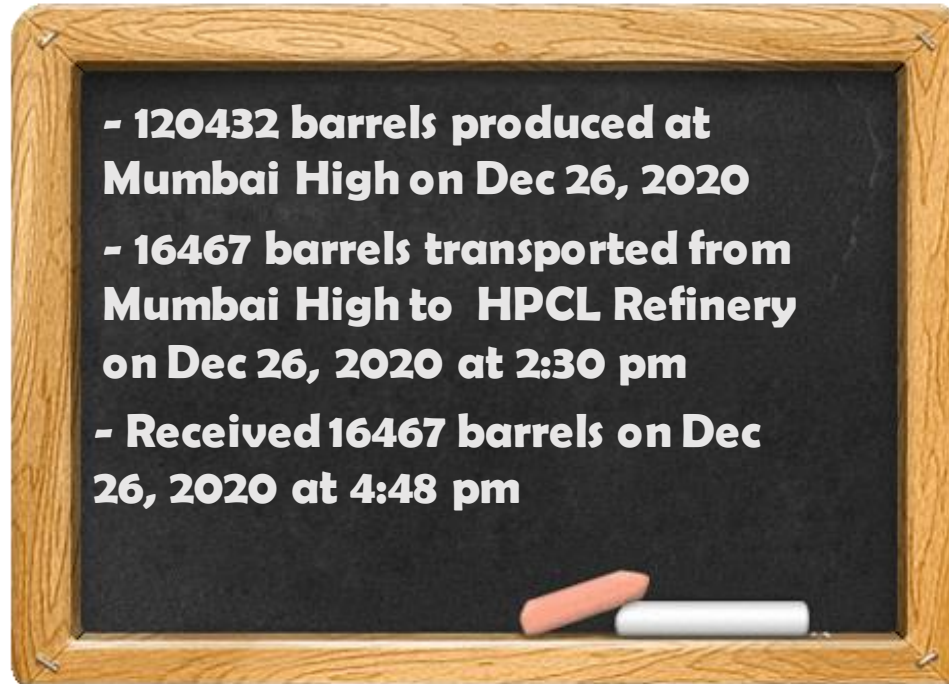
- **Everyone can see all the logs and verify**



Use a Public Bulletin Board -- Advantages



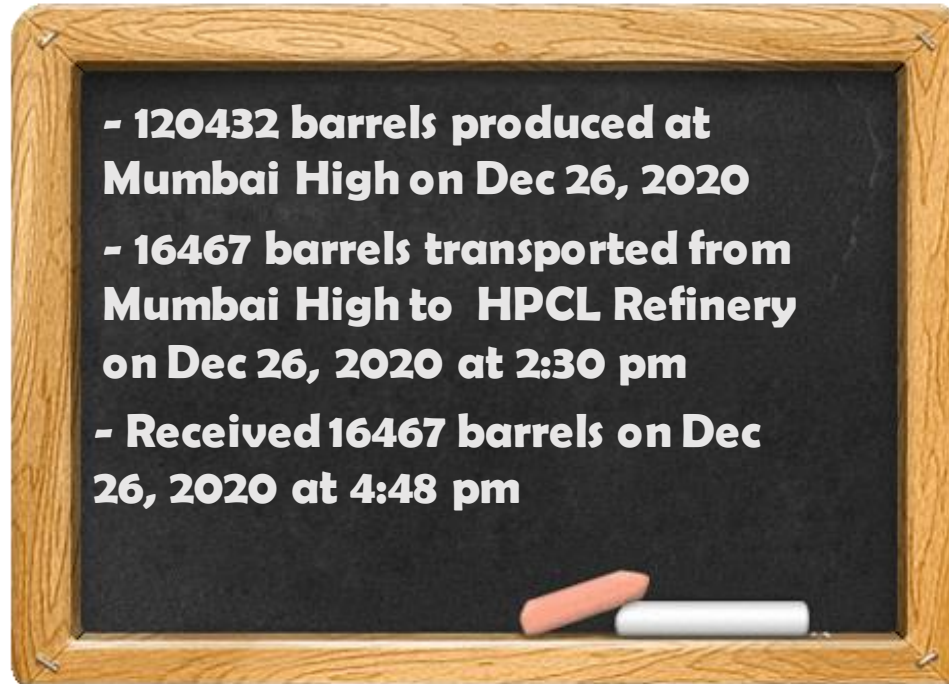
- **Any change in information is visible to everyone**



Use a Public Bulletin Board -- Advantages



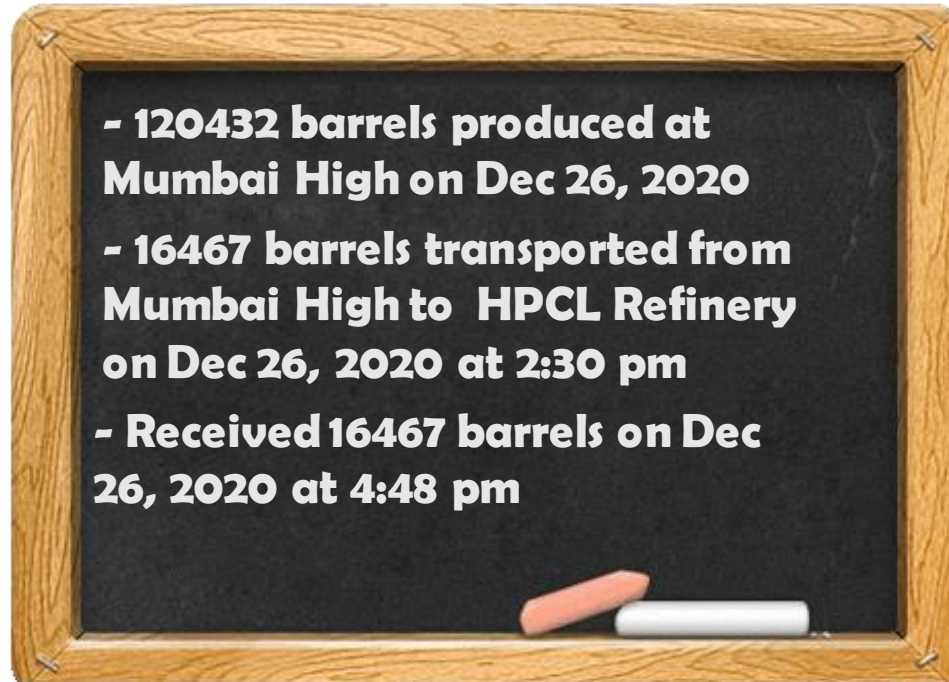
- The board is not erasable, no one can deny later



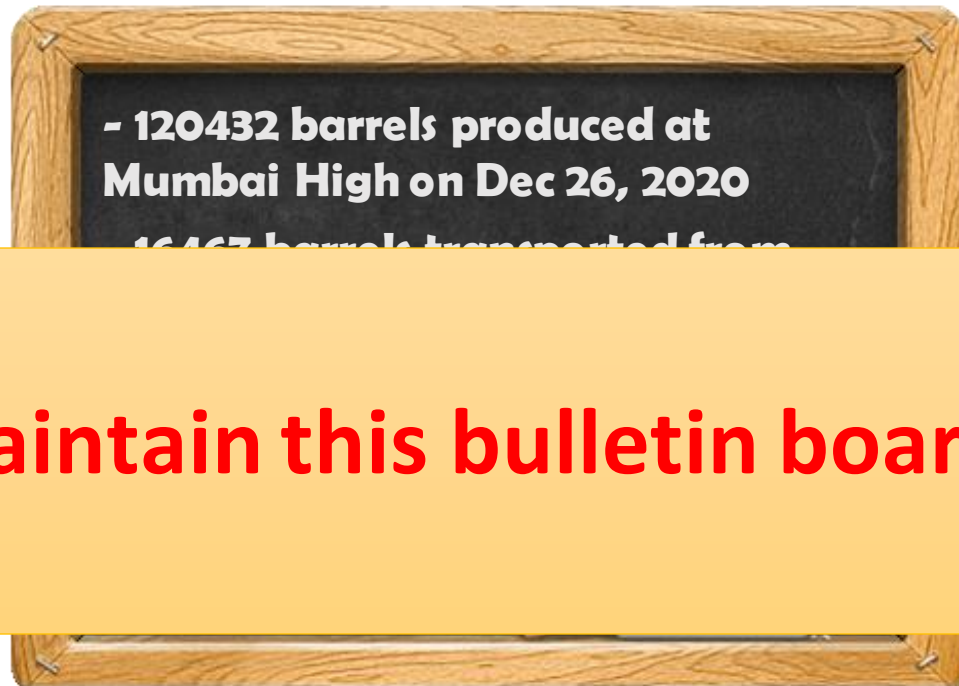
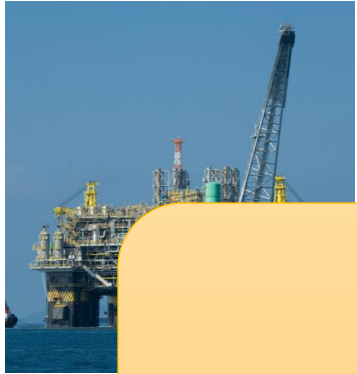
Use a Public Bulletin Board -- Advantages



- **Simple one-step auditing**



Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?



Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

- Buy Cloud from amazon



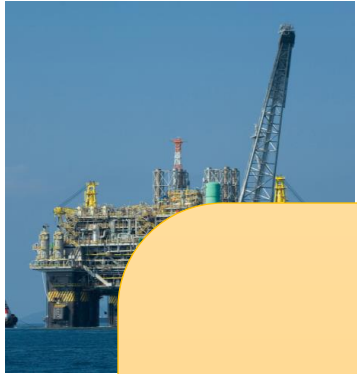
Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

- Buy Cloud from amazon

Who will manage it and provide the cost?



Use a Public Bulletin Board -- Challenges



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?**



Use a Public Bulletin Board -- Challenges

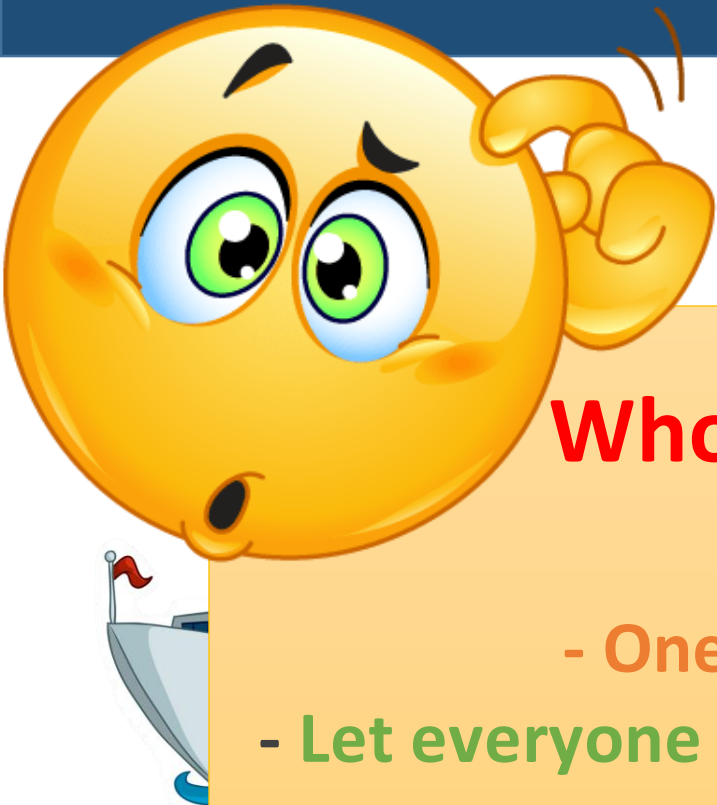


Who will maintain this bulletin board?

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



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?**



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



What is this “Blockchain”?



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



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

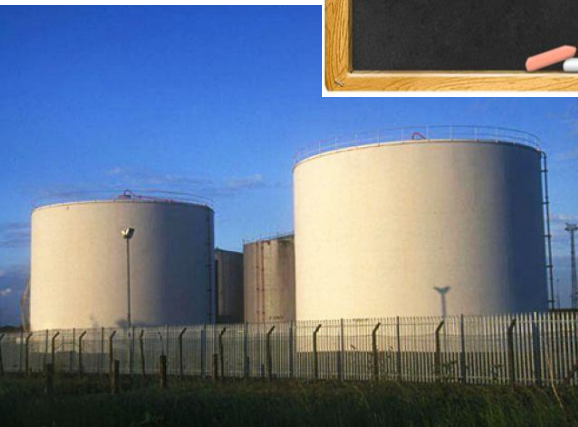


- 120432 barrels produced at
Mumbai High on Dec 26, 2020
- 16467 barrels transported from
Mumbai High to HPCL Refinery
on Dec 26, 2020 at 2:30 pm

- 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”?




- 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

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



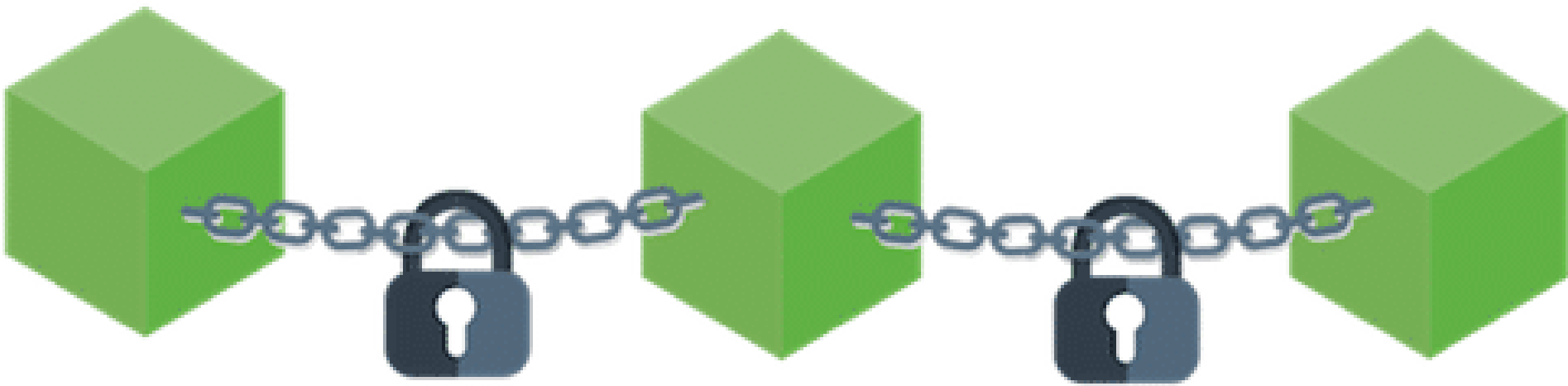
What is this “Blockchain”?



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**

What's Next?

- Some basics of various crypto techniques
 - Cryptographic Hash
 - Public key cryptography
 - Digital Signature