Blockchain: Smart Contracts

Lecture 1

Please join course TEAMS: oob4snl

Grading

Laboratory activity :--**50%**

Final exam: **-- 50%**

- Final Written Exam (open books): **--50%**

- To pass the exam you have to obtain minim 5 at the final exam and the final grade is minimum 5

Rules

- laboratory activity will be done at the group level
- groups consist of max 2 students
- final exam is individual and is an open book exam (you can have access at the lecture notes and the lab notes)

Course Content

In this course we will discuss multiple blockchain related topics.
At the laboratory you are going to complete some small assignments.

.

Note

Our slides are based on different blockchain courses and tutorials freely available online.

What is a blockchain for?

Abstract answer: a blockchain provides coordination between many parties, when there is no single trusted party

if trusted party exists $\Rightarrow$ no need for a blockchain

What is a blockchain?

Abstract answer: a blockchain provides coordination between many parties, when there is no single trusted party

if trusted party exists $\Rightarrow$ no need for a blockchain

[financial systems: often no trusted party]

Blockchains: what is the new idea?

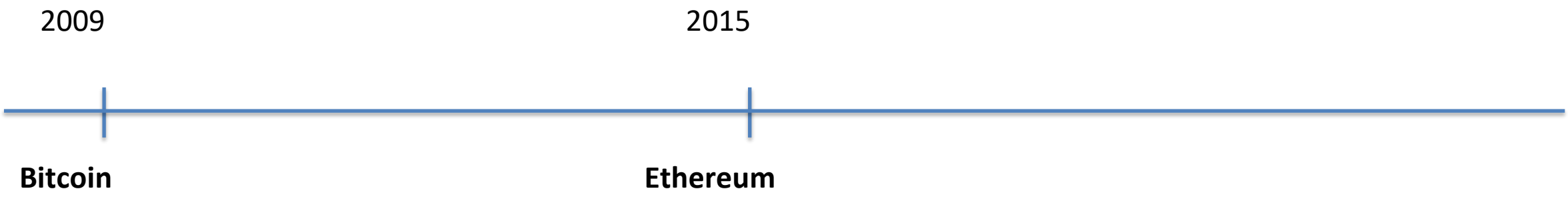
2009

Bitcoin

Several innovations:

- A practical **public append-only data structure**, secured by replication and incentives
- A fixed supply asset (BTC). Digital payments, and more.

Blockchains: what is the new idea?



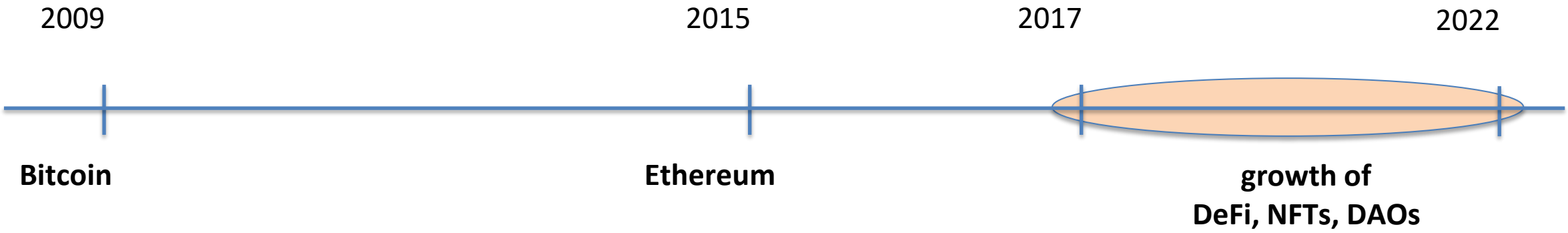
Several innovations:

- **Blockchain computer**: a fully programmable environment

  $\Longrightarrow$ public programs that manage digital and financial assets

- **Composability**: applications running on chain can call each other

Blockchains: what is the new idea?



So what is this good for?

(1) Basic application: a digital currency (stored value)
Current largest: Bitcoin (2009), Ethereum (2015)
Global: accessible to anyone with an Internet connection

Opinion

The New York Times

Bitcoin Has Saved My Family

"Borderless money" is more than a buzzword when you live in a collapsing economy and a collapsing dictatorship.

By Carlos Hernández
Mr. Hernández is a Venezuelan economist.

Feb. 23, 2019

What else is it good for?

(2) Decentralized applications (DAPPs)

DeFi: financial instruments managed by public programs

examples: stablecoins, lending, exchanges, ….

Asset management (NFTs)**:** art, game assets, domain names.

- A non-fungible token (**NFT**) is a unique digital identifier that is recorded on a blockchain and is used to certify ownership and authenticity.

•**Decentralized organizations** (DAOs): (decentralized governance)

- DAOs for investment, for donations, for collecting art, etc.

---

(3) New programming model: writing decentralized programs

Assets managed by DAPPs

MakerDAO	Ethereum	StableCoin	$4.5B
Curve	Ethereum	Exchange	$2.2B
Aave V3	Ethereum	Lending	$2.3B
Uniswap V3	Ethereum	Exchange	$3.1B
Compound	Ethereum	Lending	$1.8B

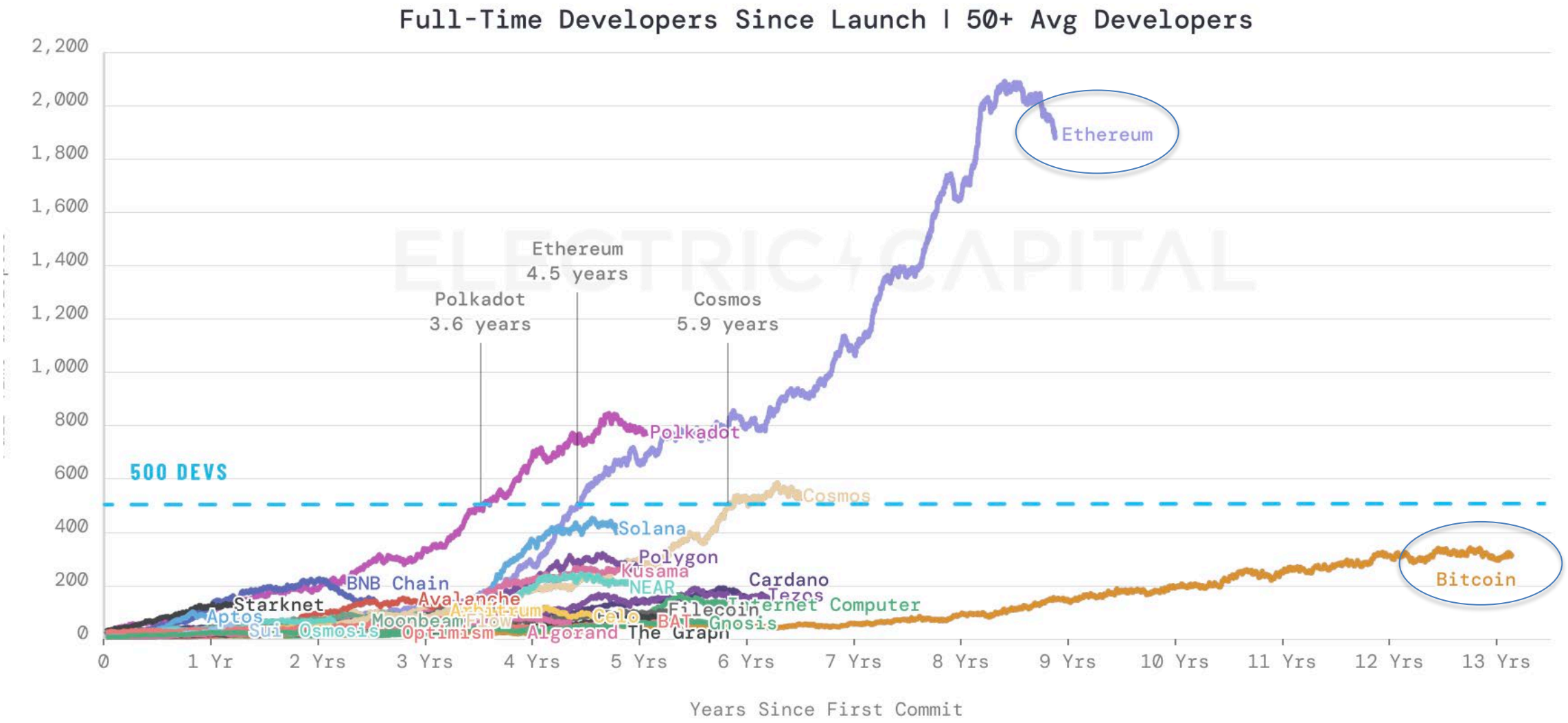
Sep. 2023

Transaction volume

Sep. 2023

	24h volume
Bitcoin • BTC	$9.9B
Ethereum • ETH	$3.4B
USDC USDC	$2.7B

Active developers since launch (as of 12/31/2022)



source: electric capital

Central Bank Digital Currency (CBDC)

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

Crude Purchase

Crude Transportation

Crude Storage

Refining

Distribution

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

Crude Storage

Refining

Distribution

Retail

Petroleum Supply Chain in India

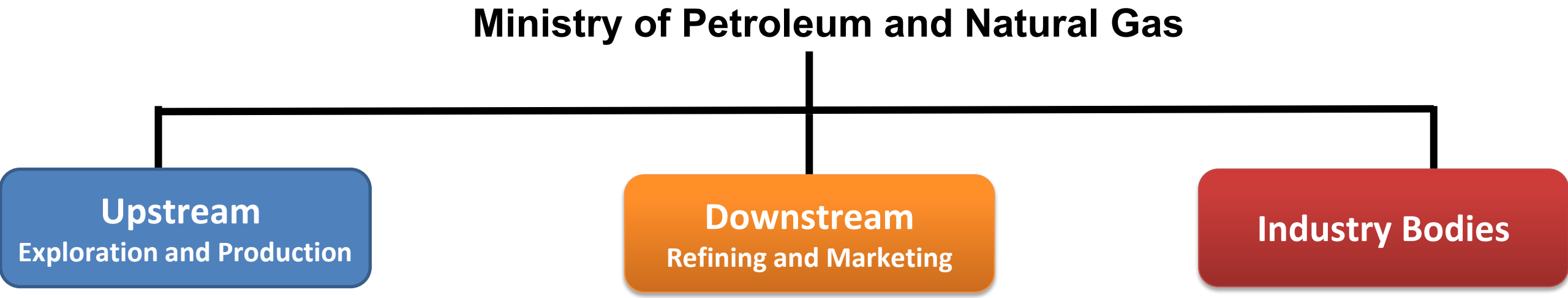
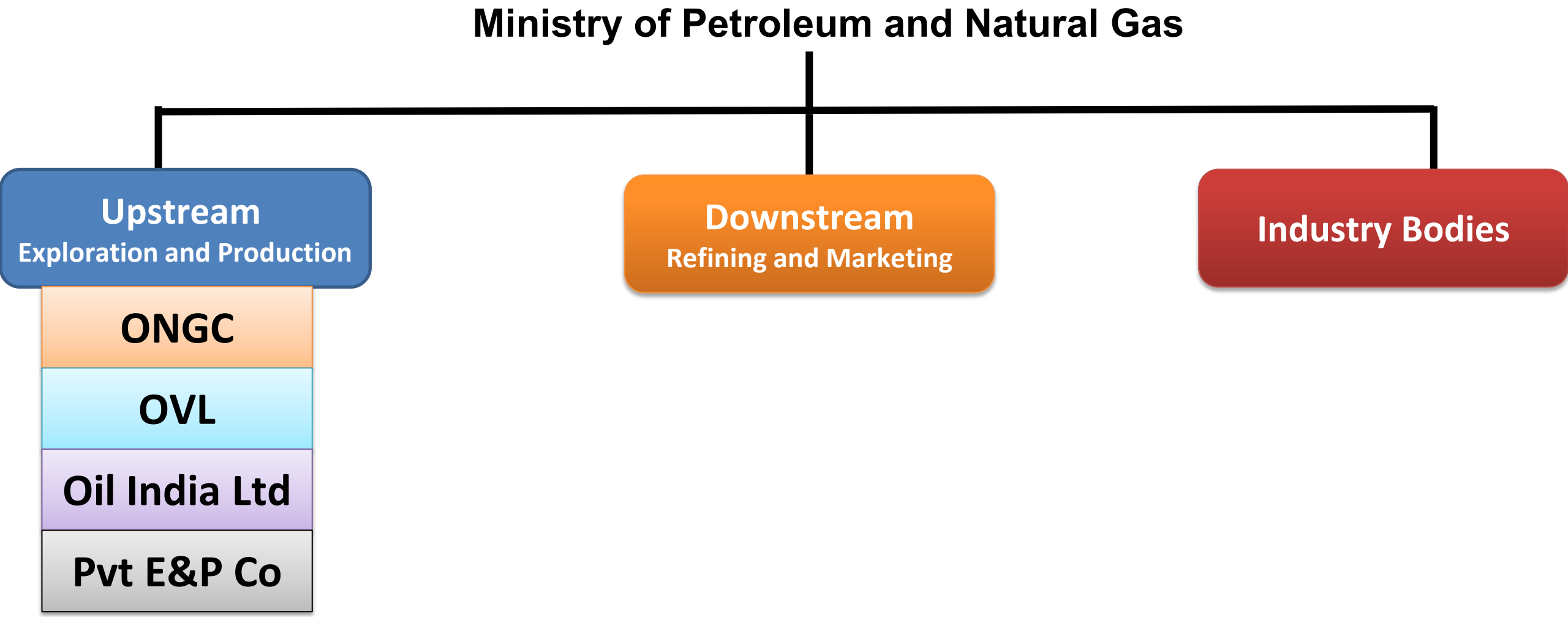
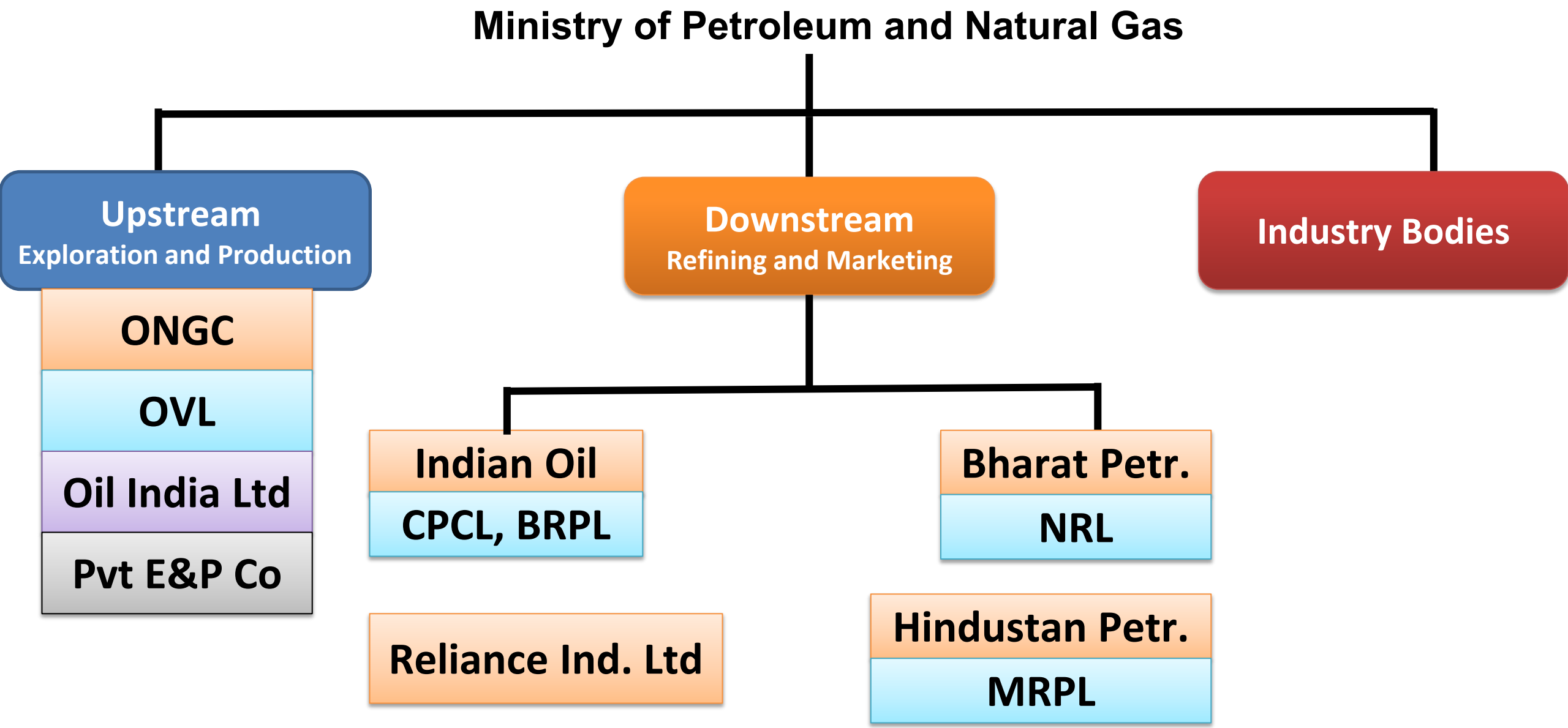


Diagram Source: https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india

Petroleum Supply Chain in India



Petroleum Supply Chain in India

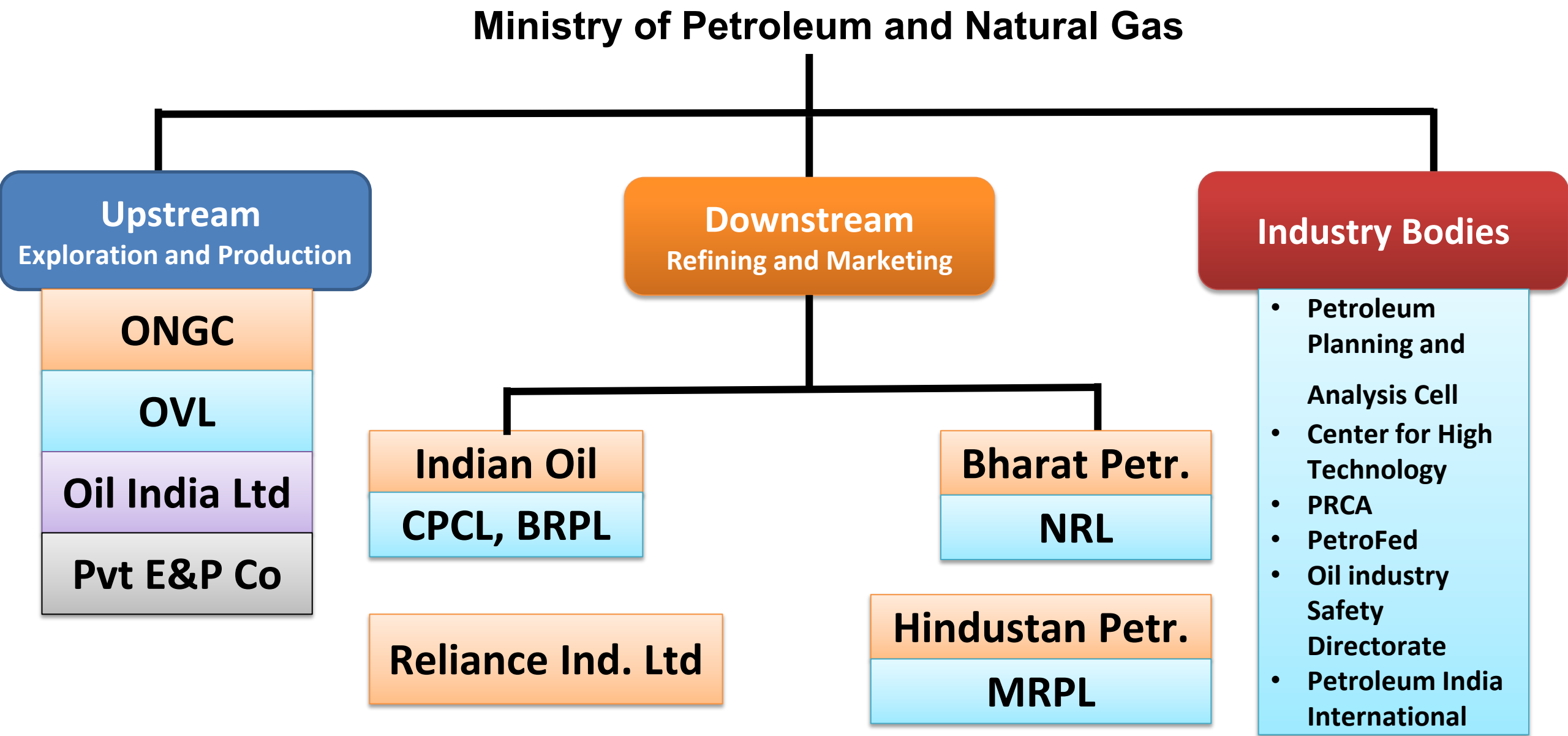


Requirements of a Successful Supply Chain

- 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

Petroleum Supply Chain in India



Requirements of a Successful Supply Chain

Needs Strong Coordination among the Players

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

Requirements of a Successful Supply Chain

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

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

Requirements of a Successful Supply Chain

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

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

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

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

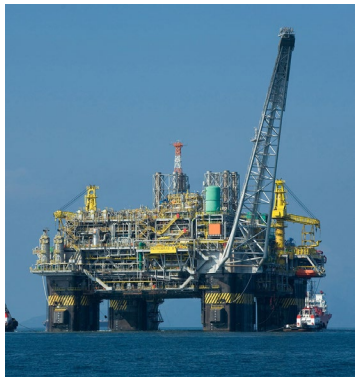
What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

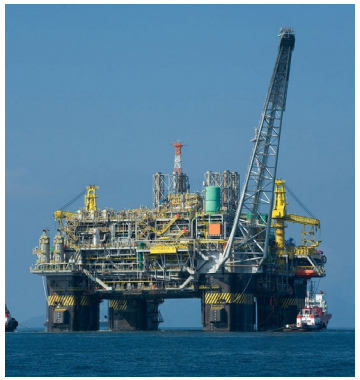
Blockchain is the answer !!

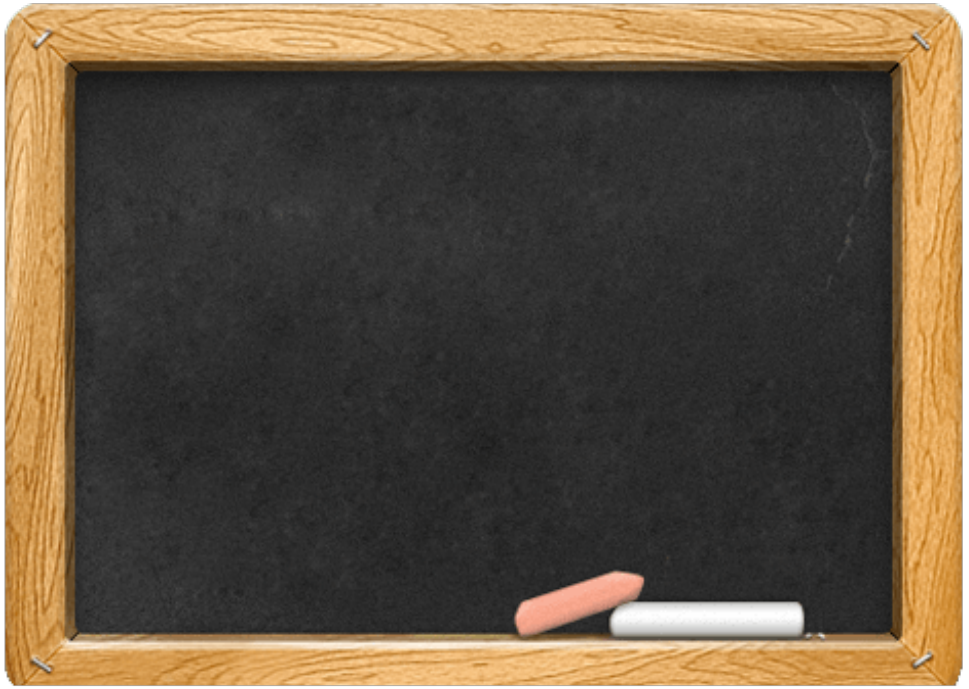
Information Source: https://www.slideshare.net/naseer9848/supply-chain-and-logistics-issues-of-crude-oil-in-india

How Can We Obtain Real Time Information?

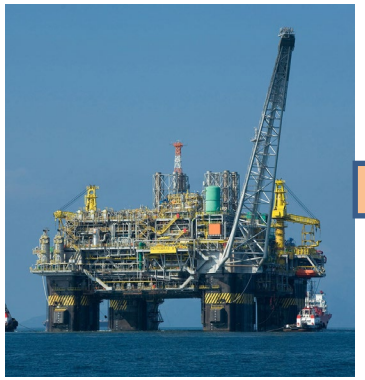


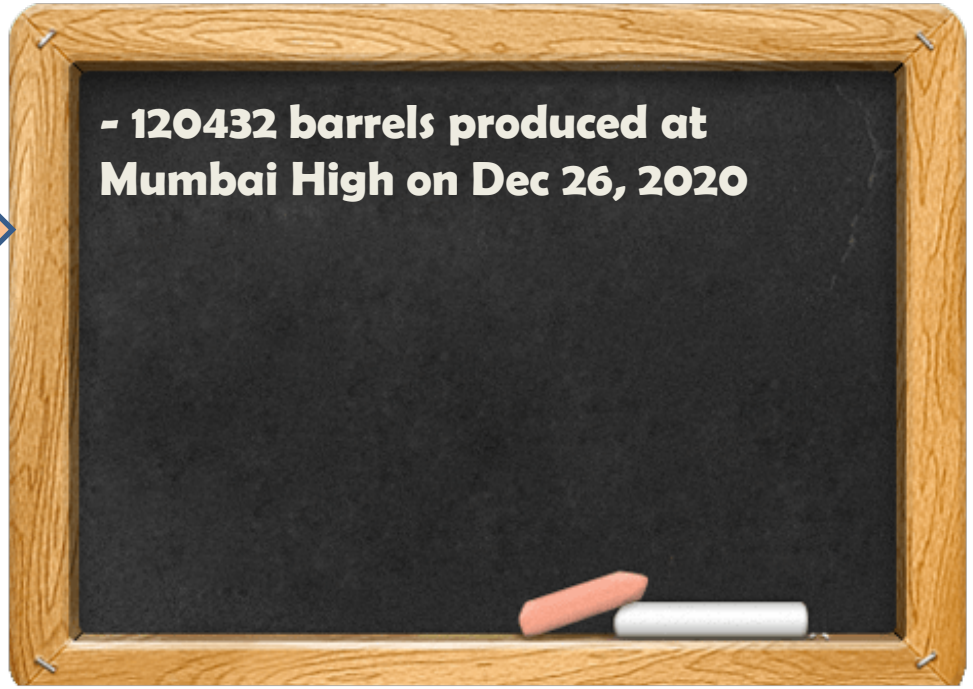
Use a Public Bulletin Board



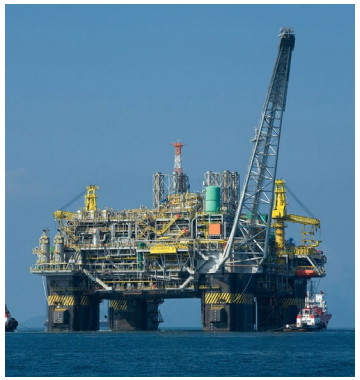


Use a Public Bulletin Board



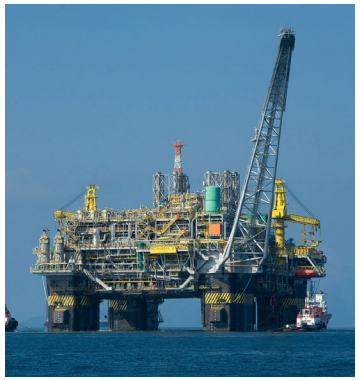


Use a Public Bulletin Board

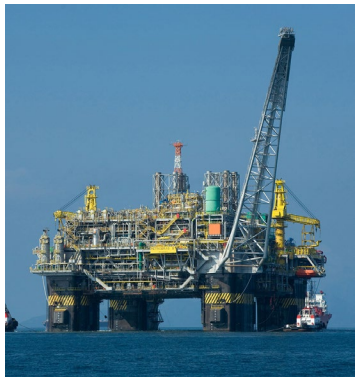


- 120432 barrels produced at Mumbai High on Dec 26, 2020
- 16467 barrels transported from Mumbai High to HPCL Refinery on Dec 26, 2020 at 2:30 pm

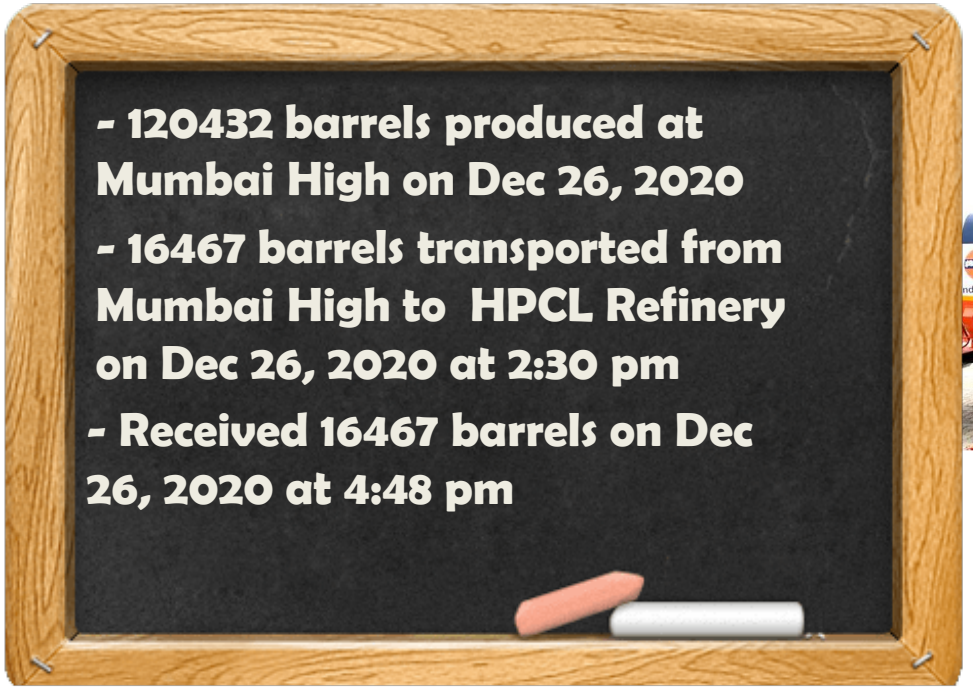
Use a Public Bulletin Board



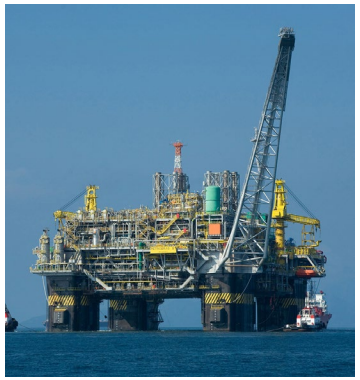
Use a Public Bulletin Board -- Advantages



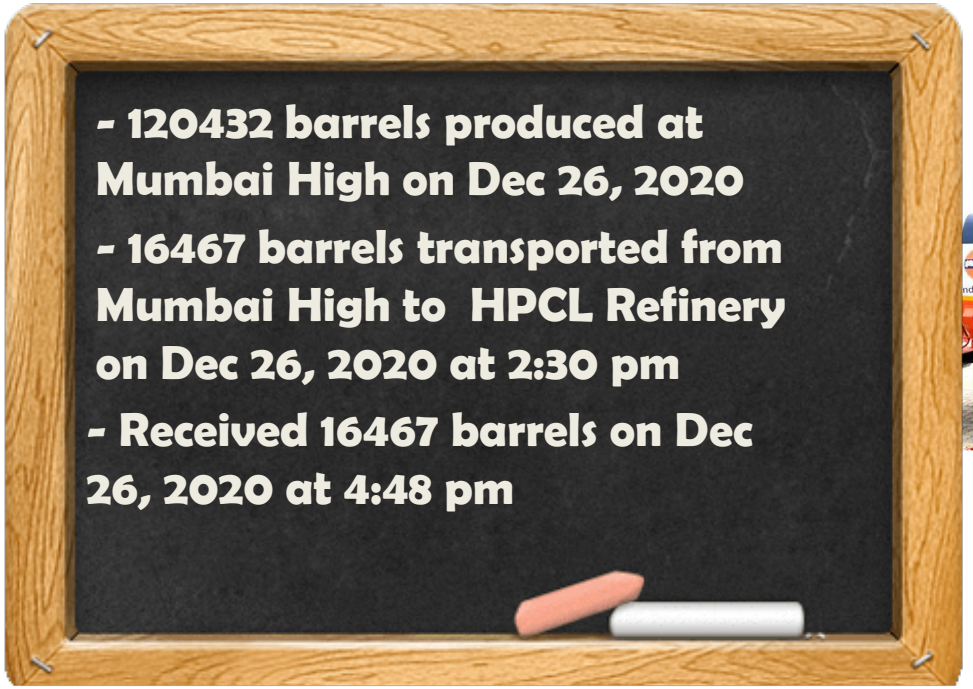
- **Everyone can see all the logs and verify**



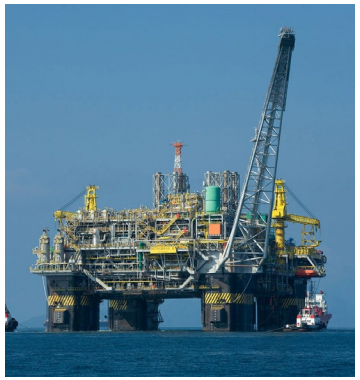
Use a Public Bulletin Board -- Advantages



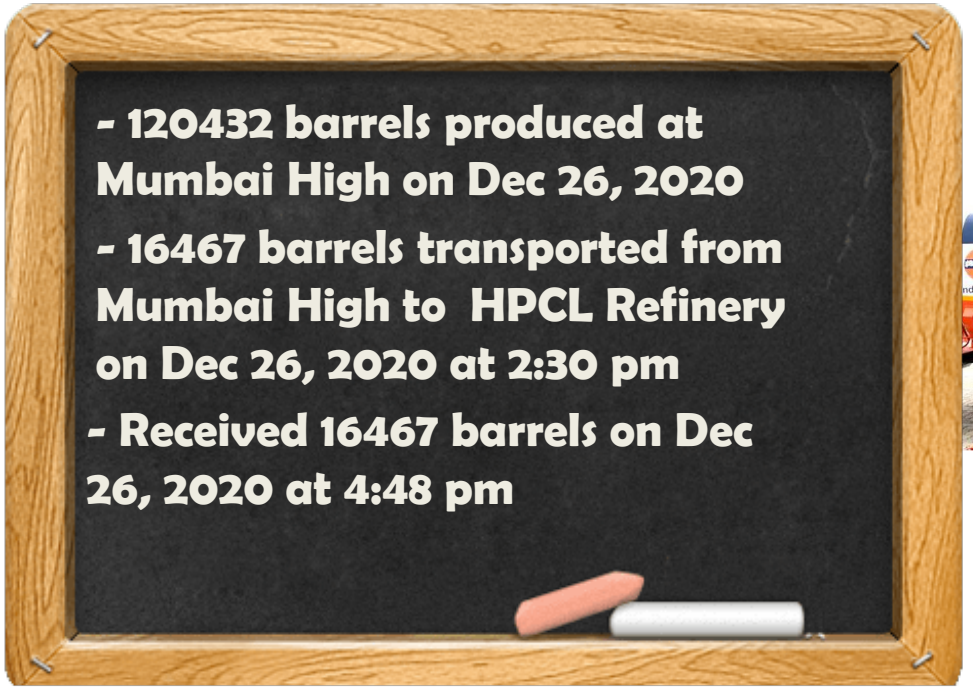
- Any change in information is visible to everyone



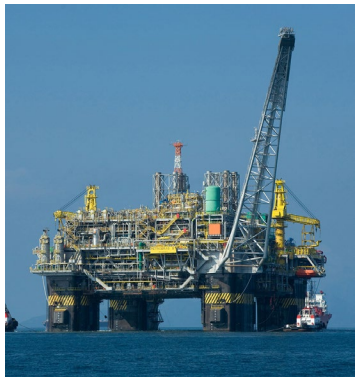
Use a Public Bulletin Board -- Advantages



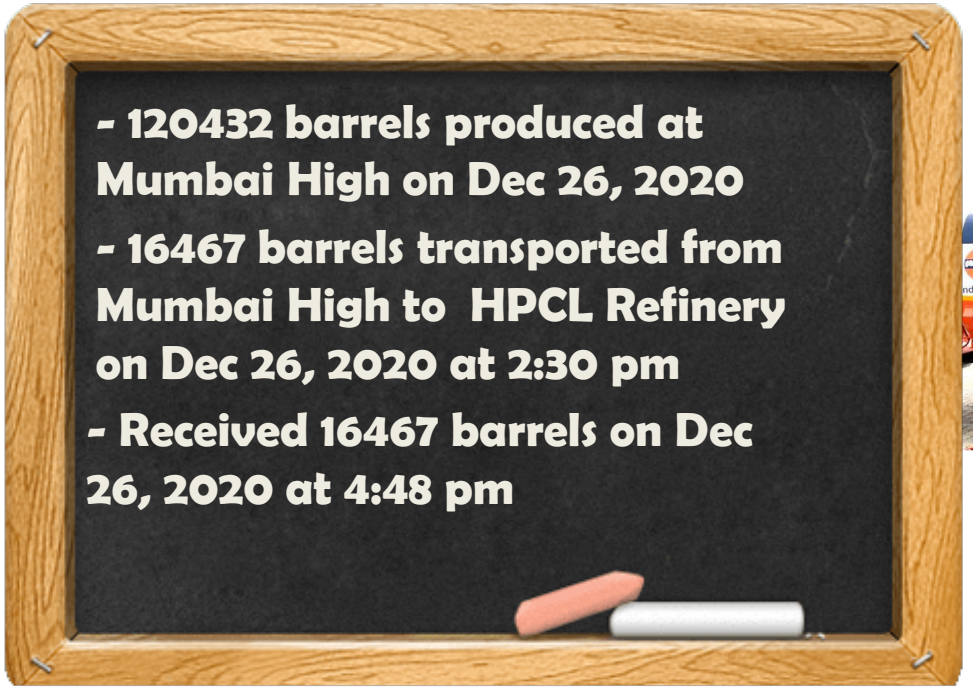
- The board is not erasable, no one can deny later



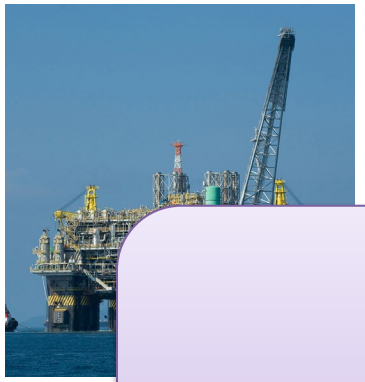
Use a Public Bulletin Board -- Advantages

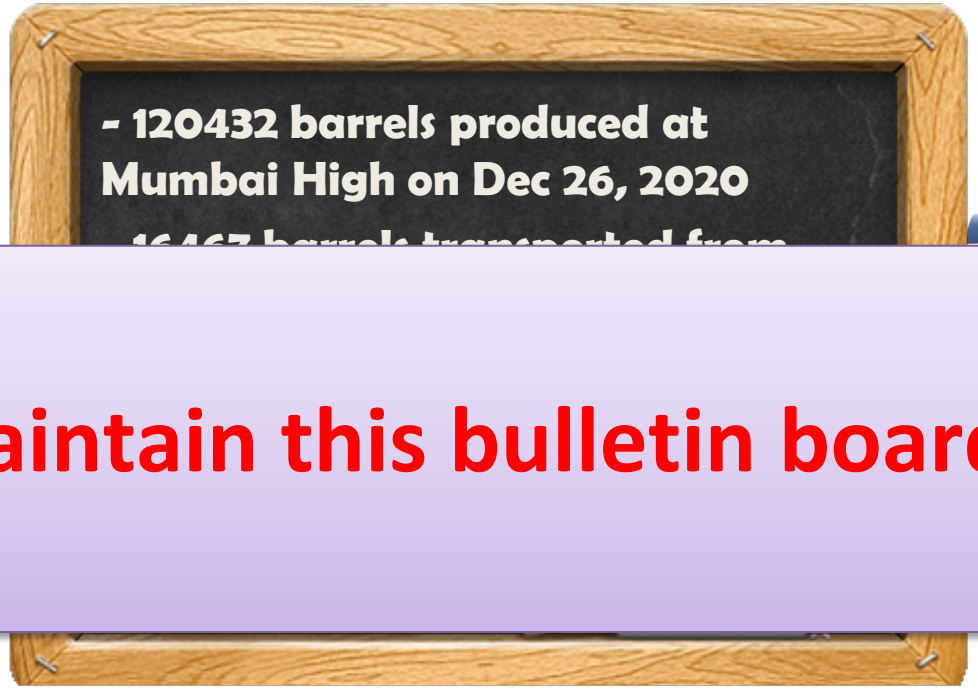


- **Simple one-step auditing**



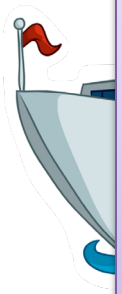
Use a Public Bulletin Board -- Challenges





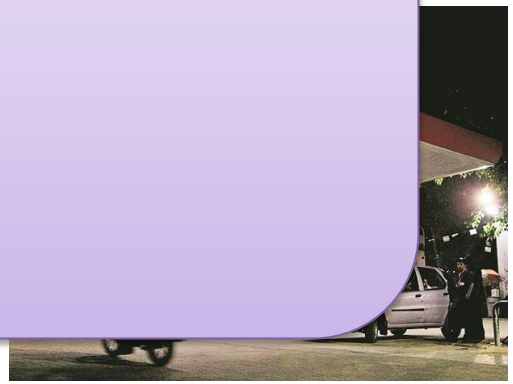
Who will maintain this bulletin board?

Use a Public Bulletin Board -- Challenges

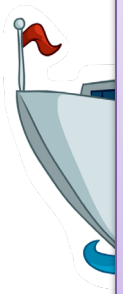


Who will maintain this bulletin board?

- Buy Cloud from amazon



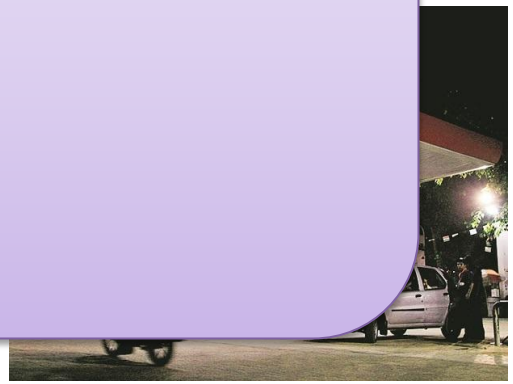
Use a Public Bulletin Board -- Challenges



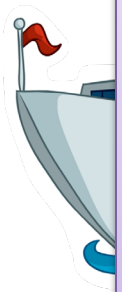
Who will maintain this bulletin board?

- Buy Cloud from amazon

Who will manage it and provide the cost?



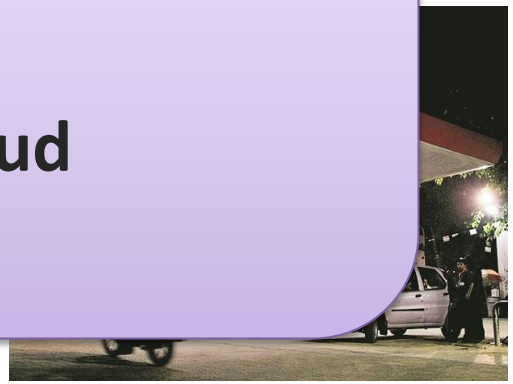
Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

- Buy Cloud from amazon

- One of the enterprises maintain a private cloud



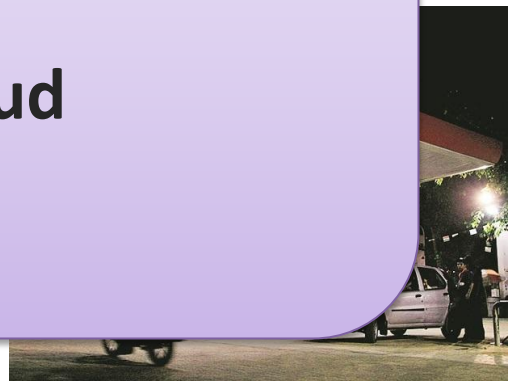
Use a Public Bulletin Board -- Challenges

Who will maintain this bulletin board?

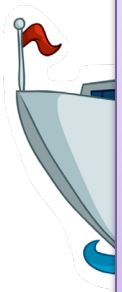
- Buy Cloud from amazon

- One of the enterprises maintain a private cloud

What is the guarantee that it is not a fraud?

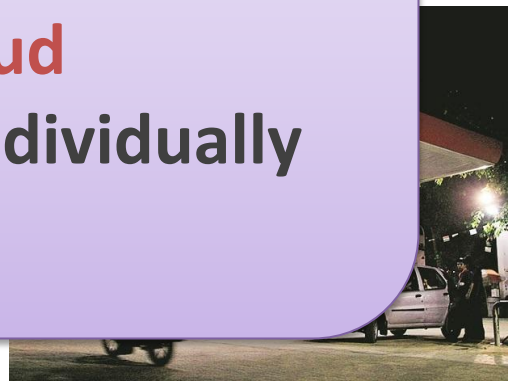


Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

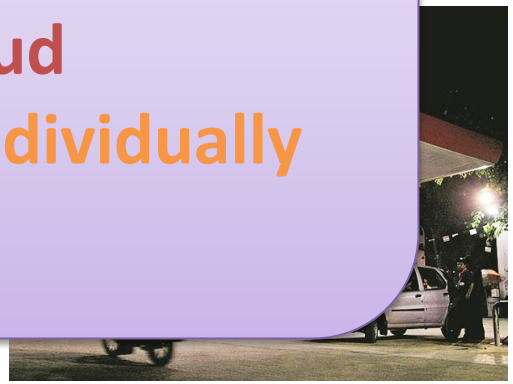
- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
- Let everyone maintain the same copy of the board individually and independently



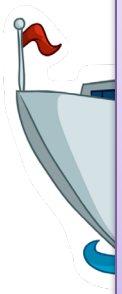
Use a Public Bulletin Board -- Challenges

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?**

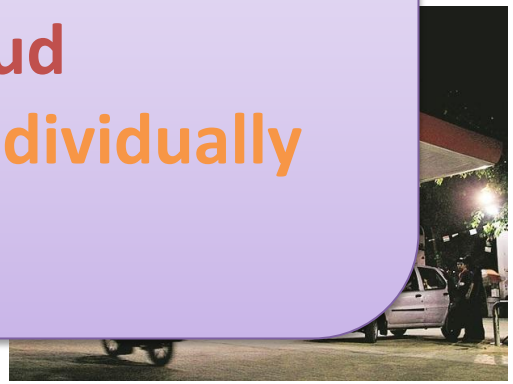


Use a Public Bulletin Board -- Challenges



Who will maintain this bulletin board?

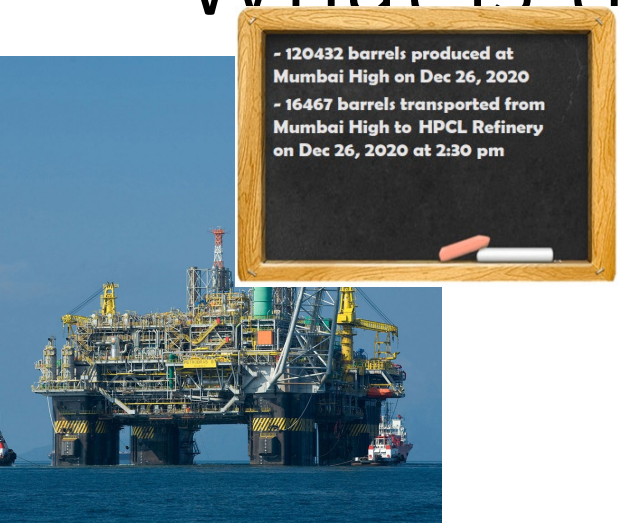
- Buy Cloud from amazon
- One of the enterprises maintain a private cloud
- Let everyone maintain the same copy of the board individually and independently

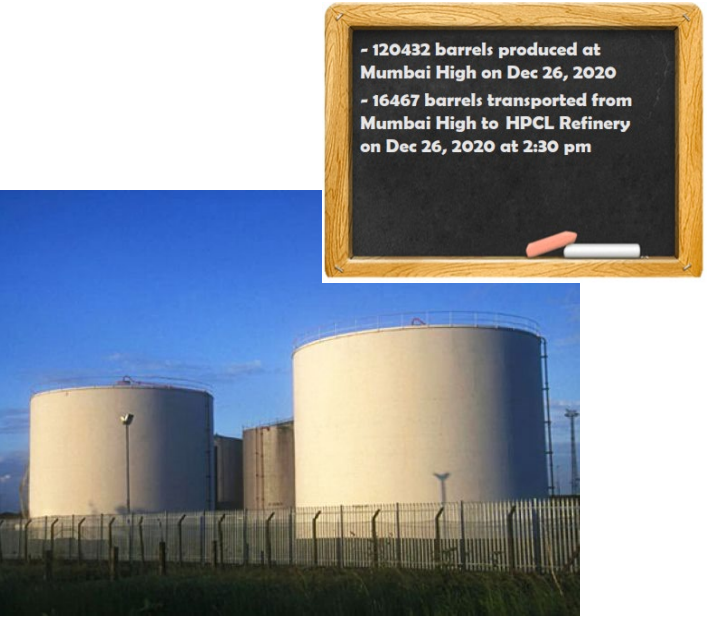


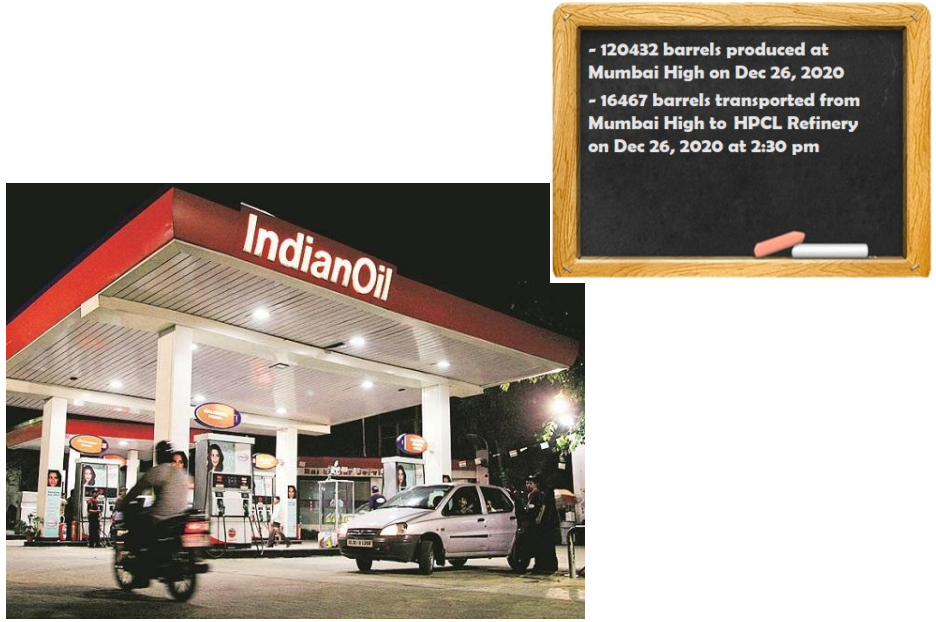
What is this “Blockchain”?

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

What is this “Blockchain”?

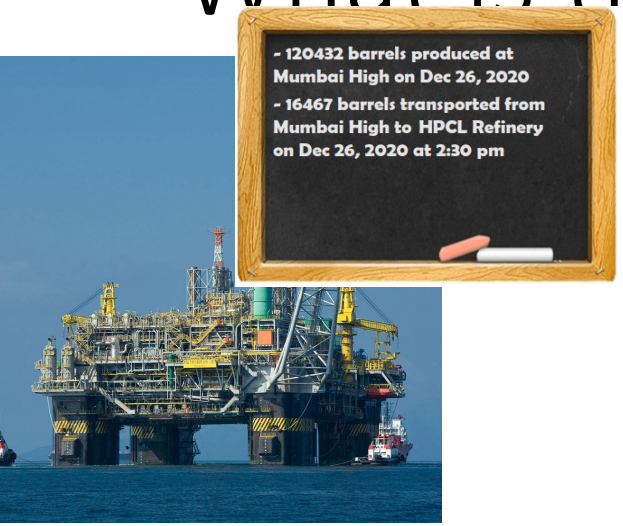


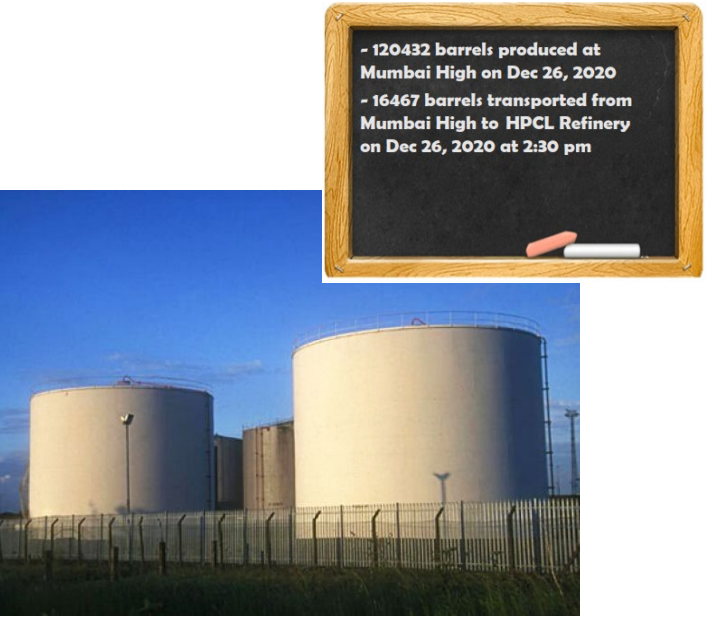


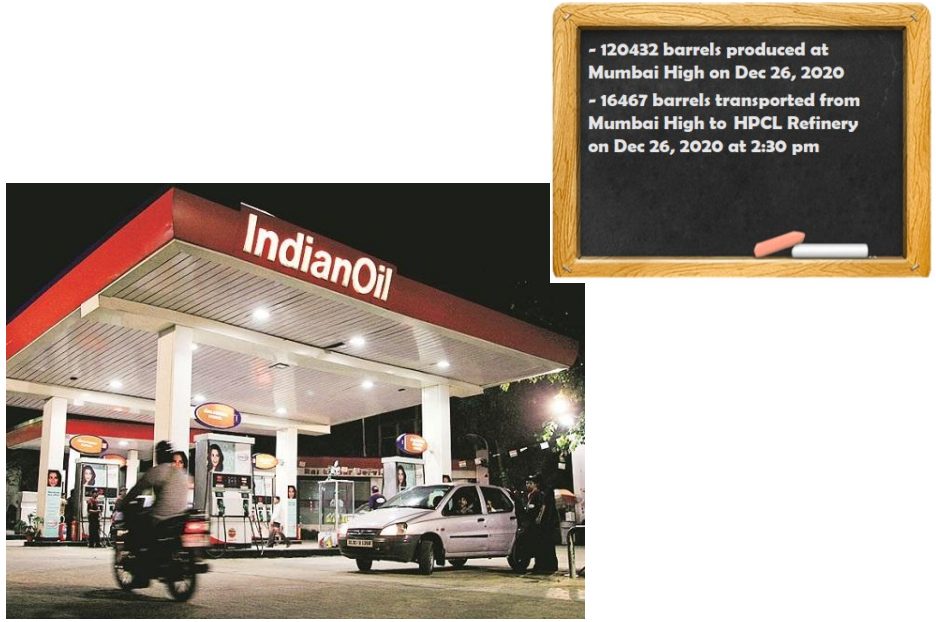


No one is the sole-owner of the data, but everyone has a copy of the data - there is no central database

What is this “Blockchain”?

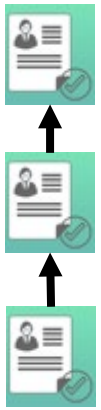


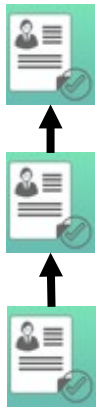




Everyone holds exactly the same copy of the data at the same instance of the time

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

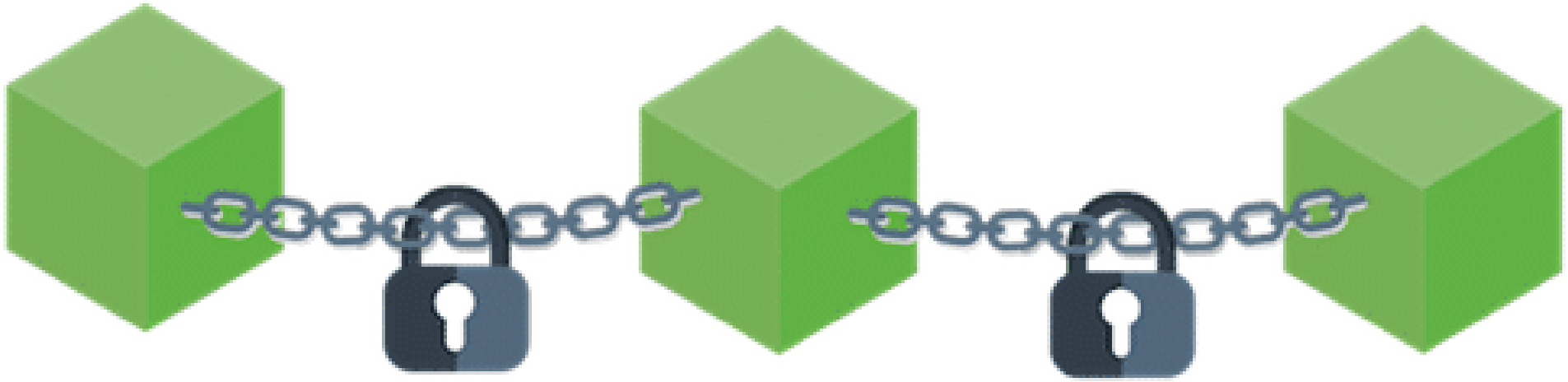
What is this “Blockchain”?

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

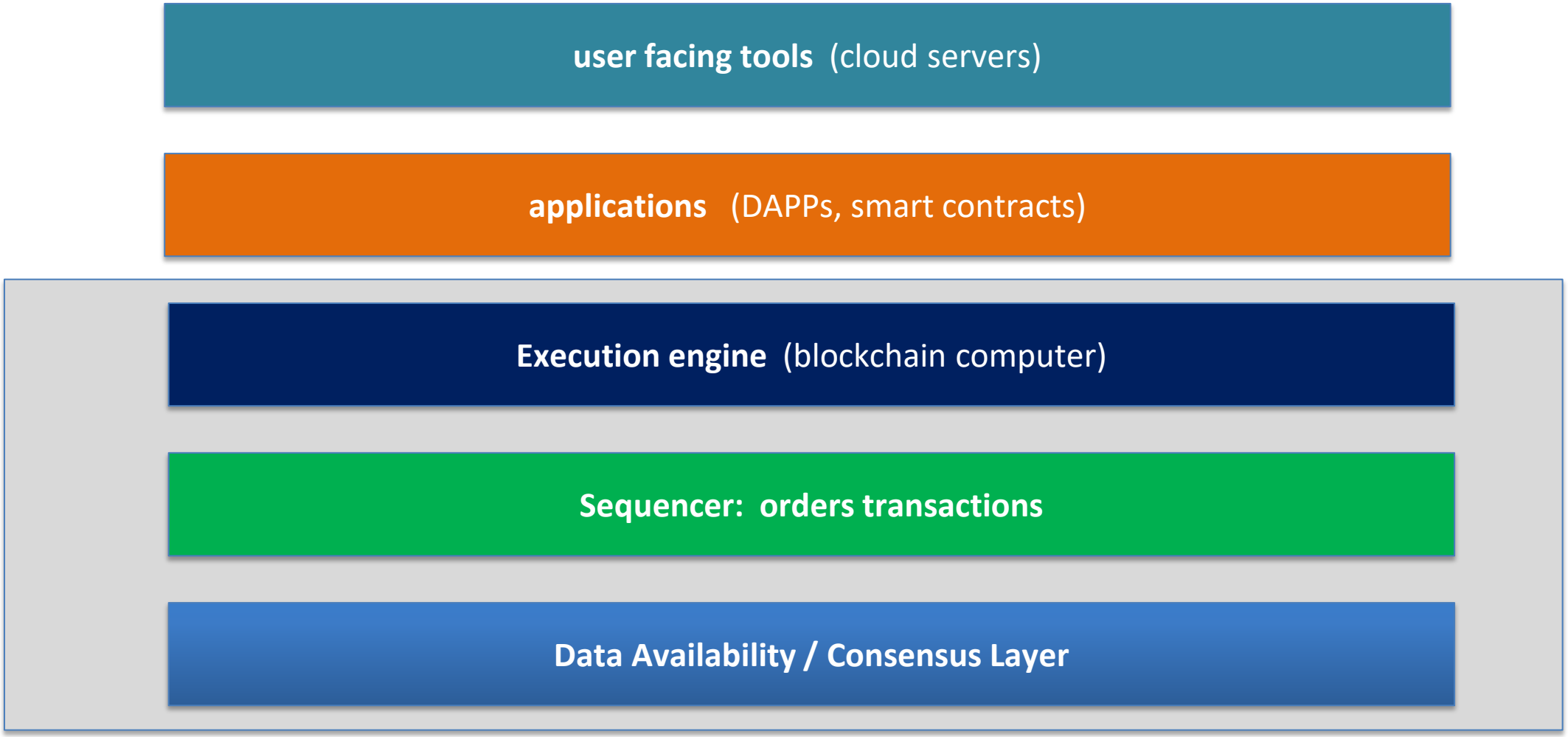
No-one can make any change without others to notice it



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

A decentralized immutable append-only public ledger

What is a blockchain?



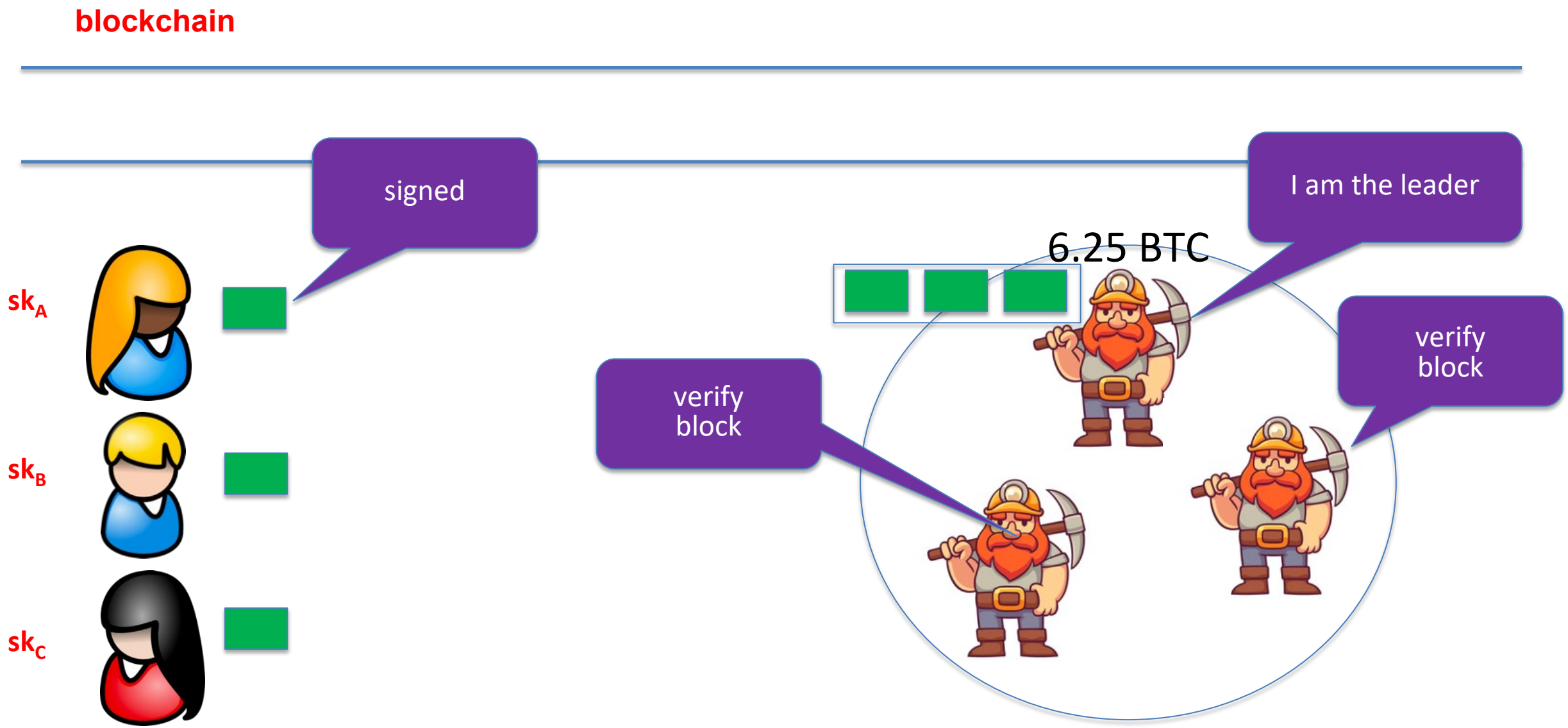
Consensus layer (informal)

achieved by replication

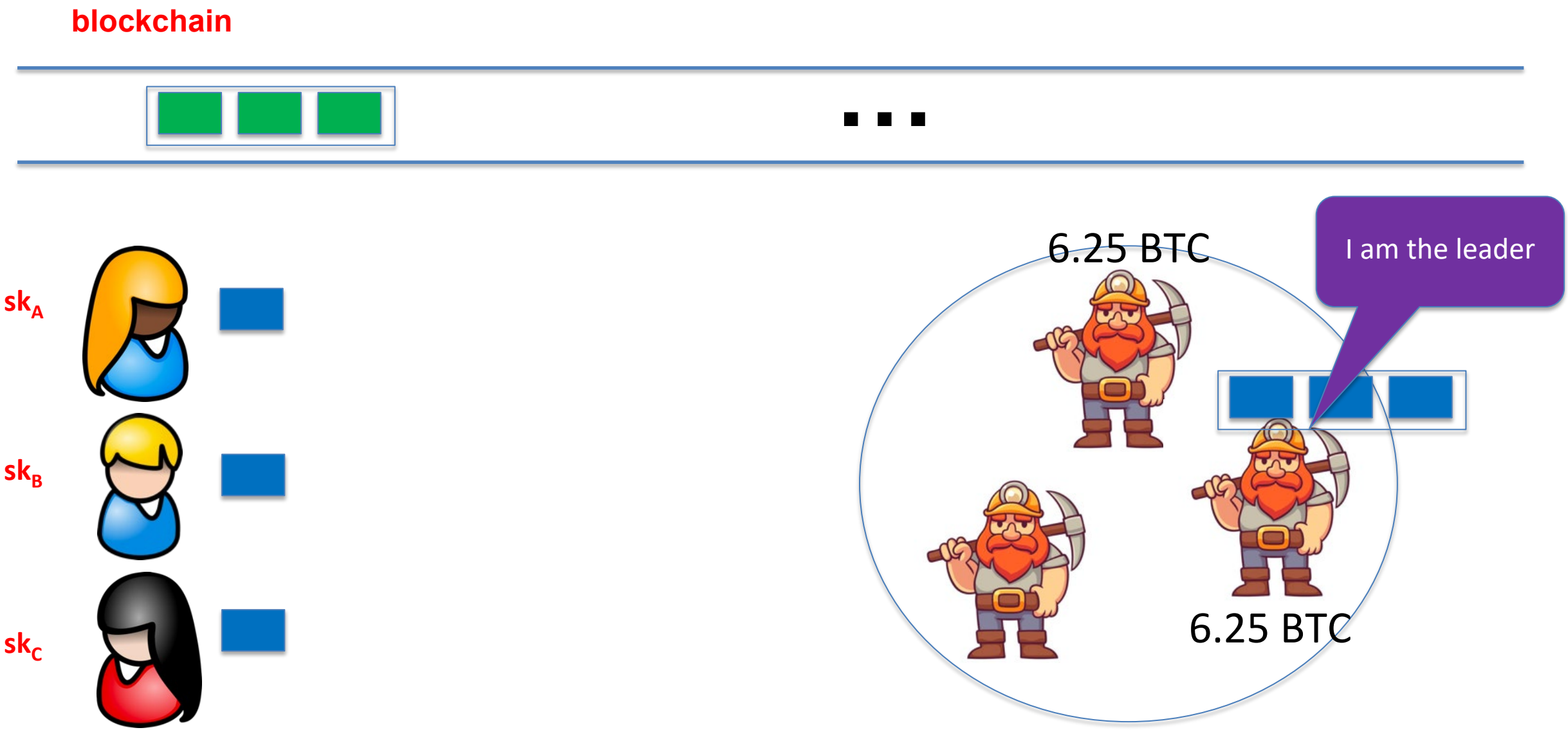
A **public** <u>append-only data structure</u>:

- **Persistence**: once added, data can never be removed*
- **Safety**: all honest participants have the same data**
- **Liveness:** honest participants can add new transactions
- **Open(?)**: anyone can add data (no authentication)

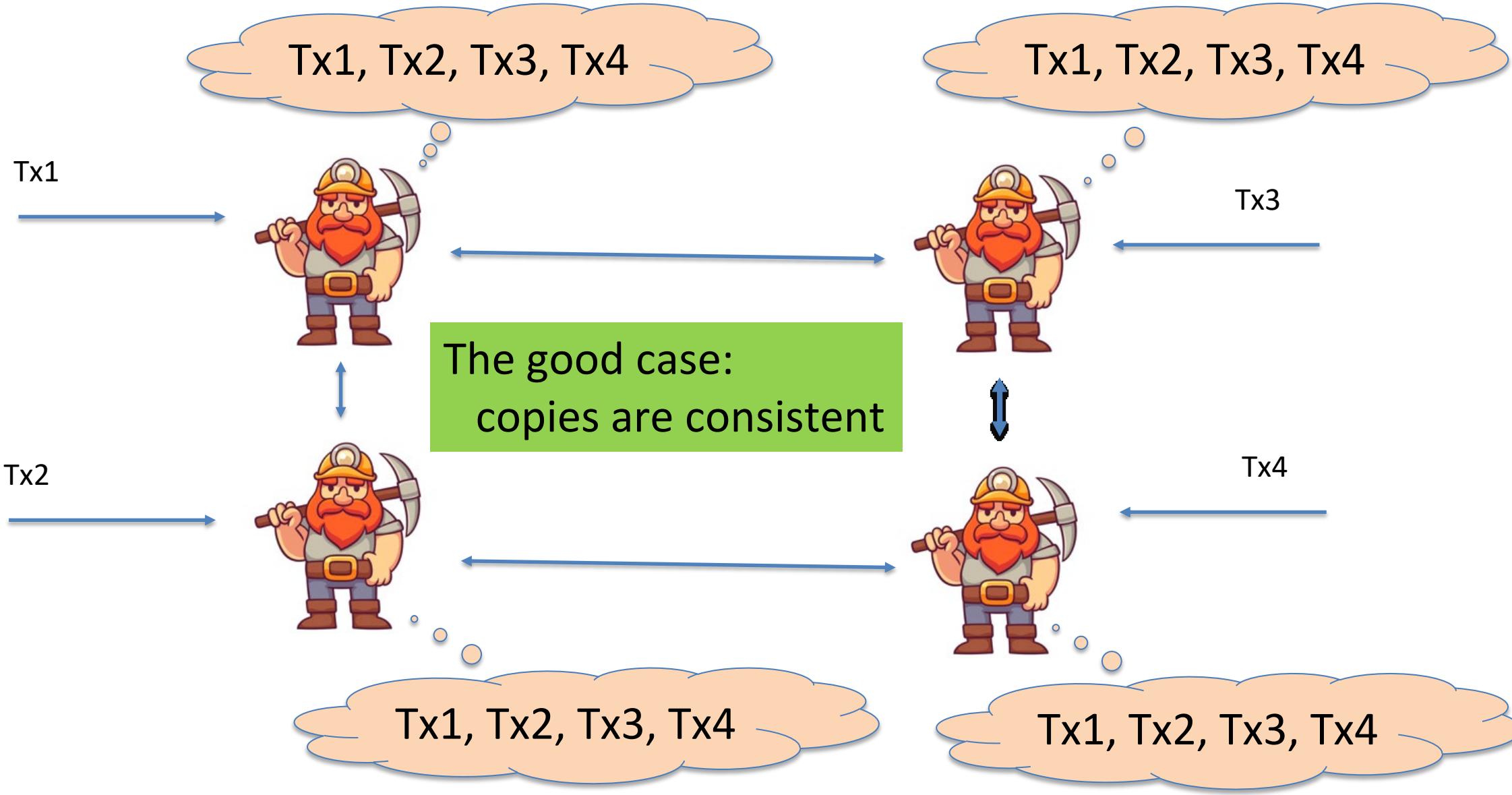
How are blocks added to chain?



How are blocks added to chain?



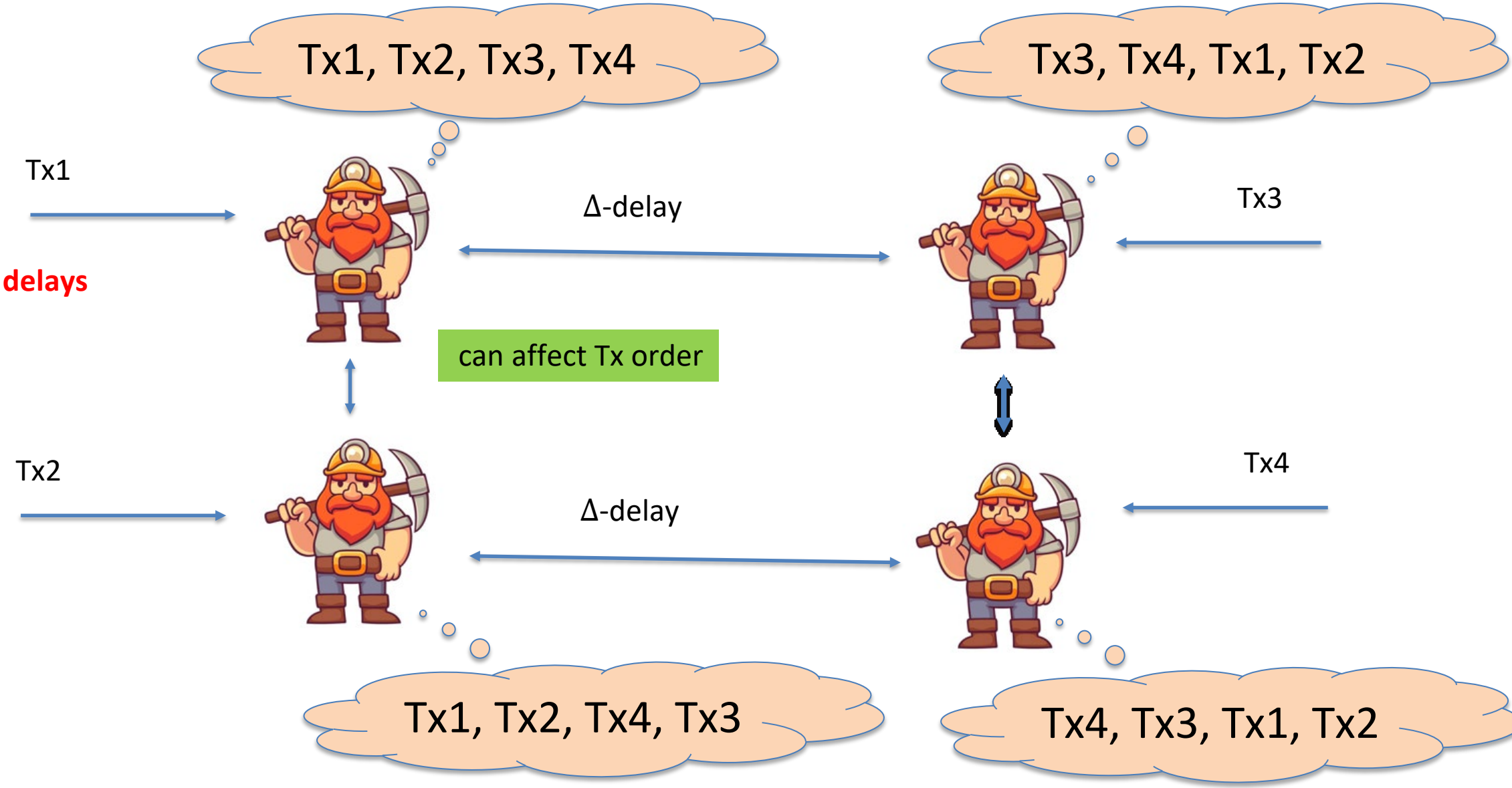
Why is consensus a hard problem?



Why is consensus a hard problem?

Problems:

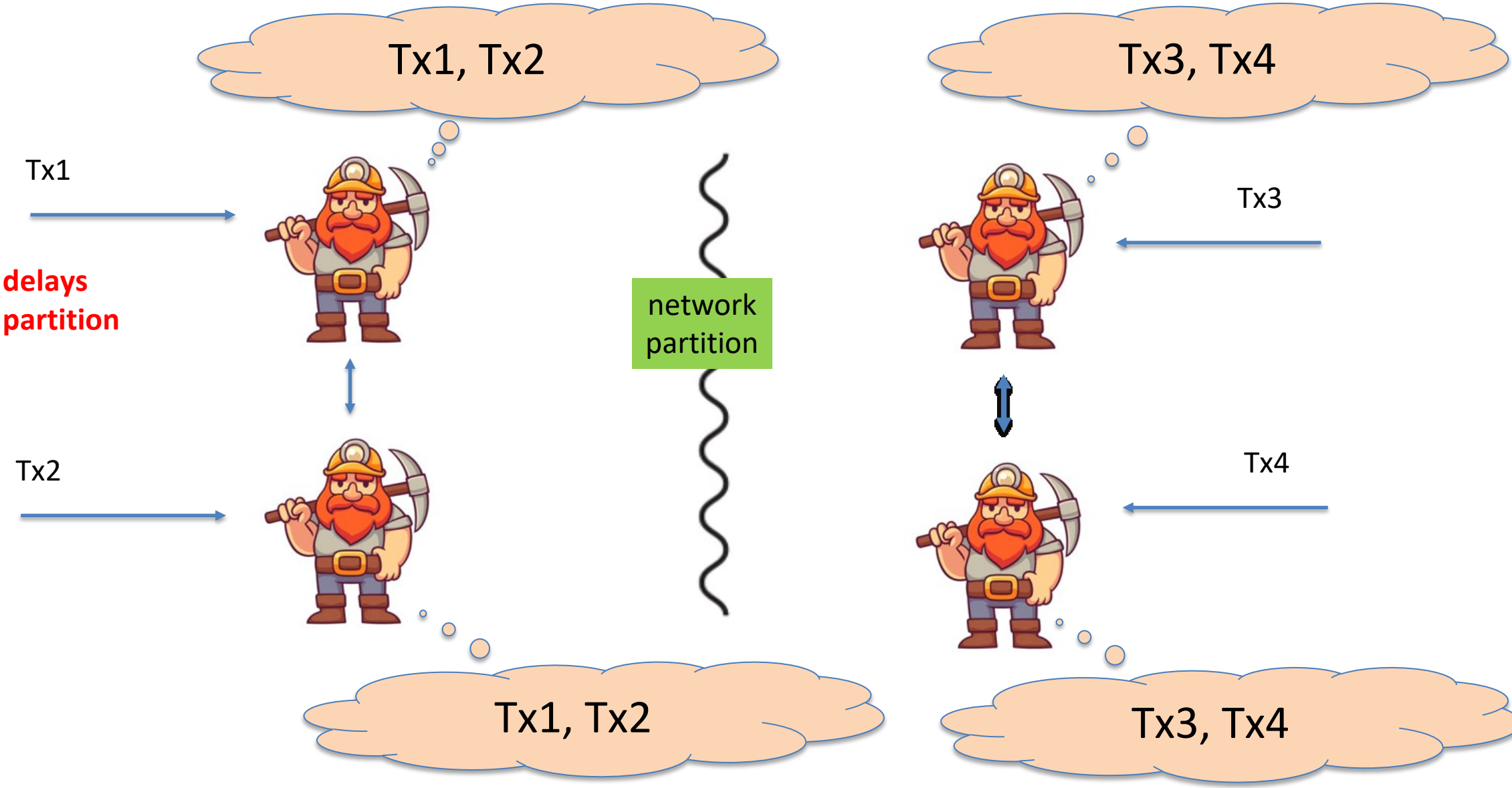
- **Network delays**



Why is consensus a hard problem?

Problems:

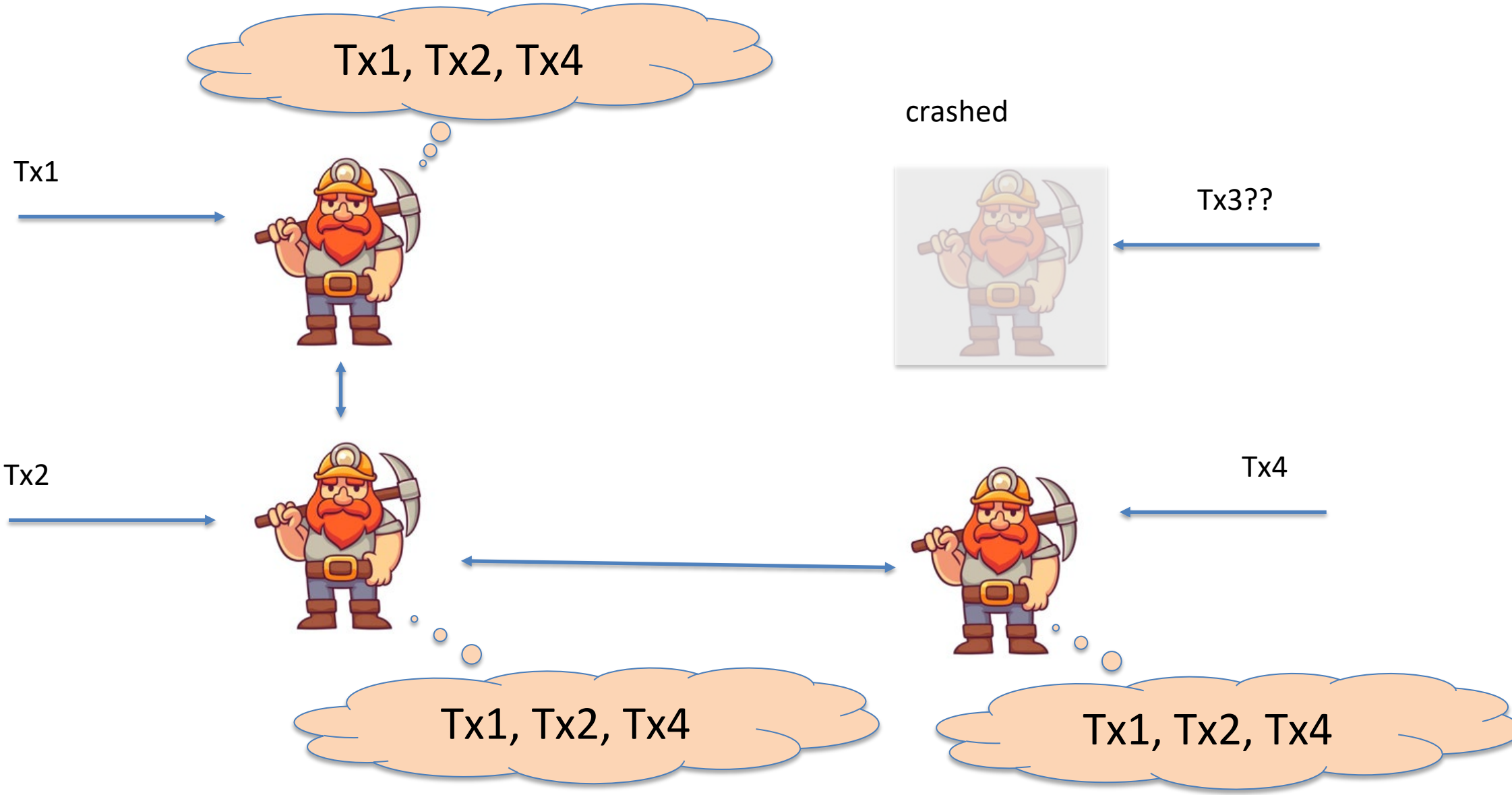
- **Network delays**
- **Network partition**



Why is consensus a hard problem?

Problems:

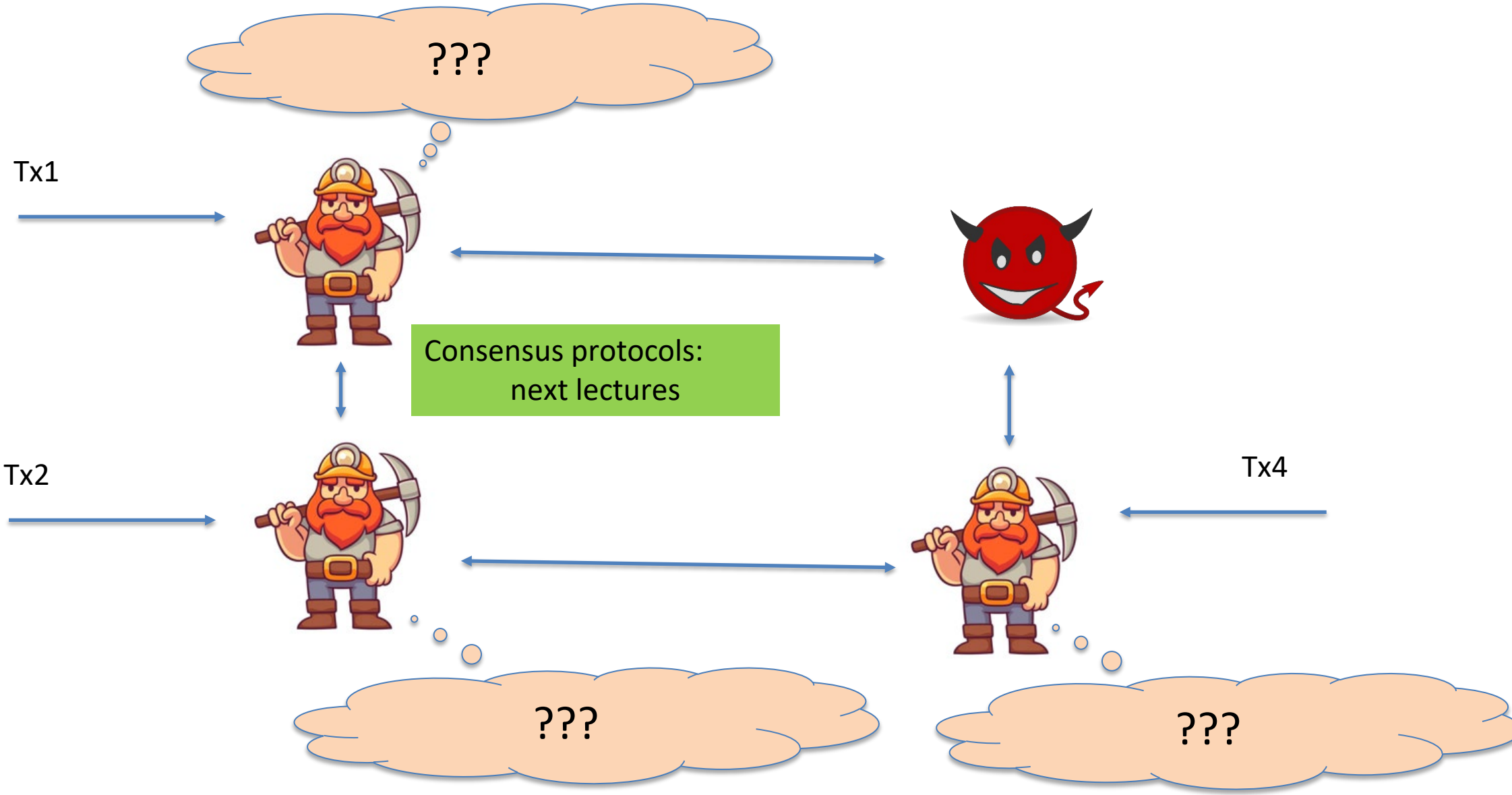
- **crash**



Why is consensus a hard problem?

Problems:

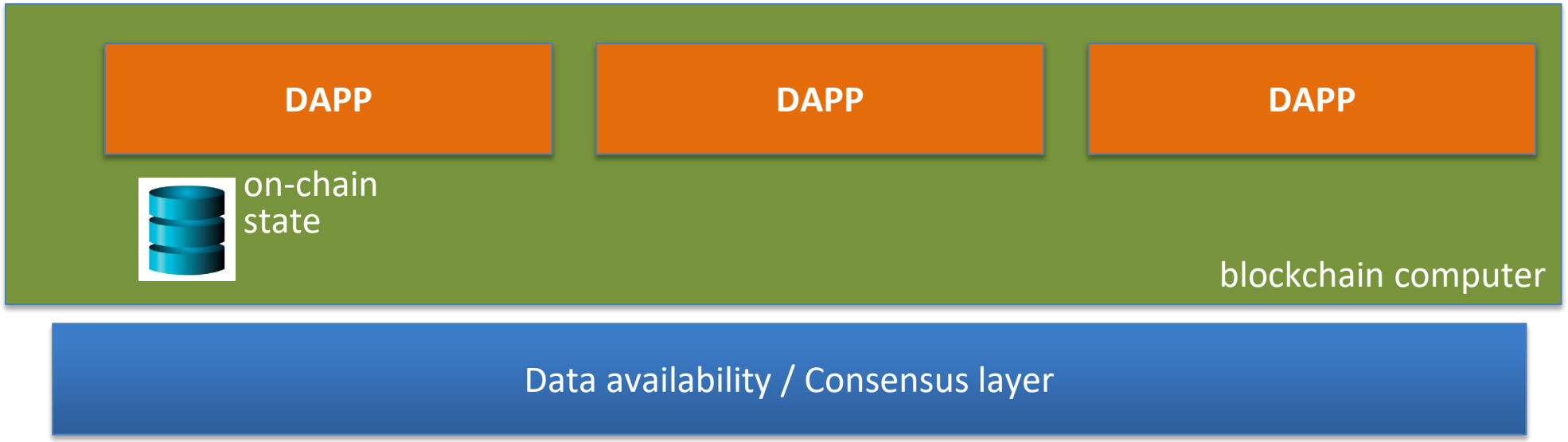
- **crash**
- **malice**



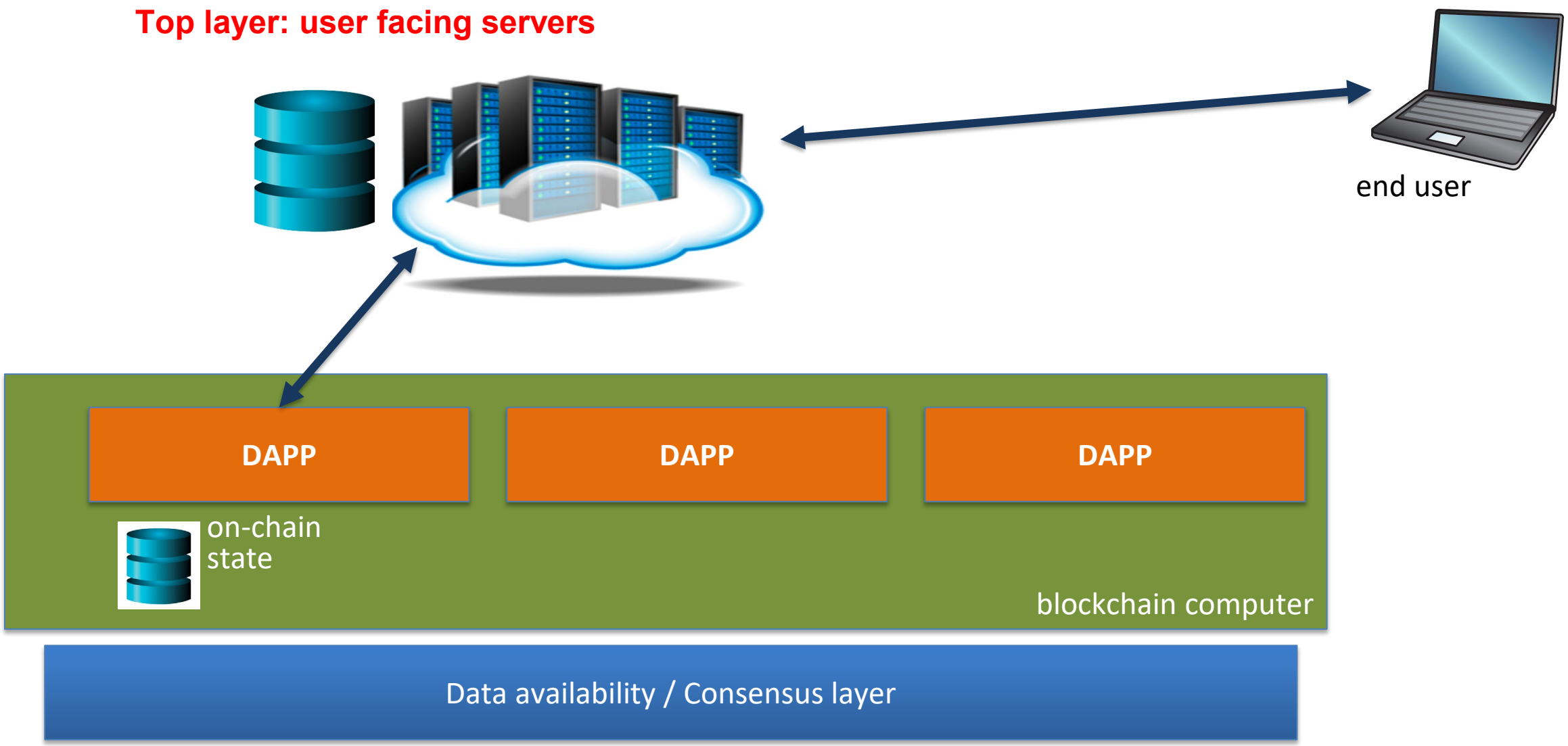
Next layer: the blockchain computer

Decentralized applications (DAPPs):

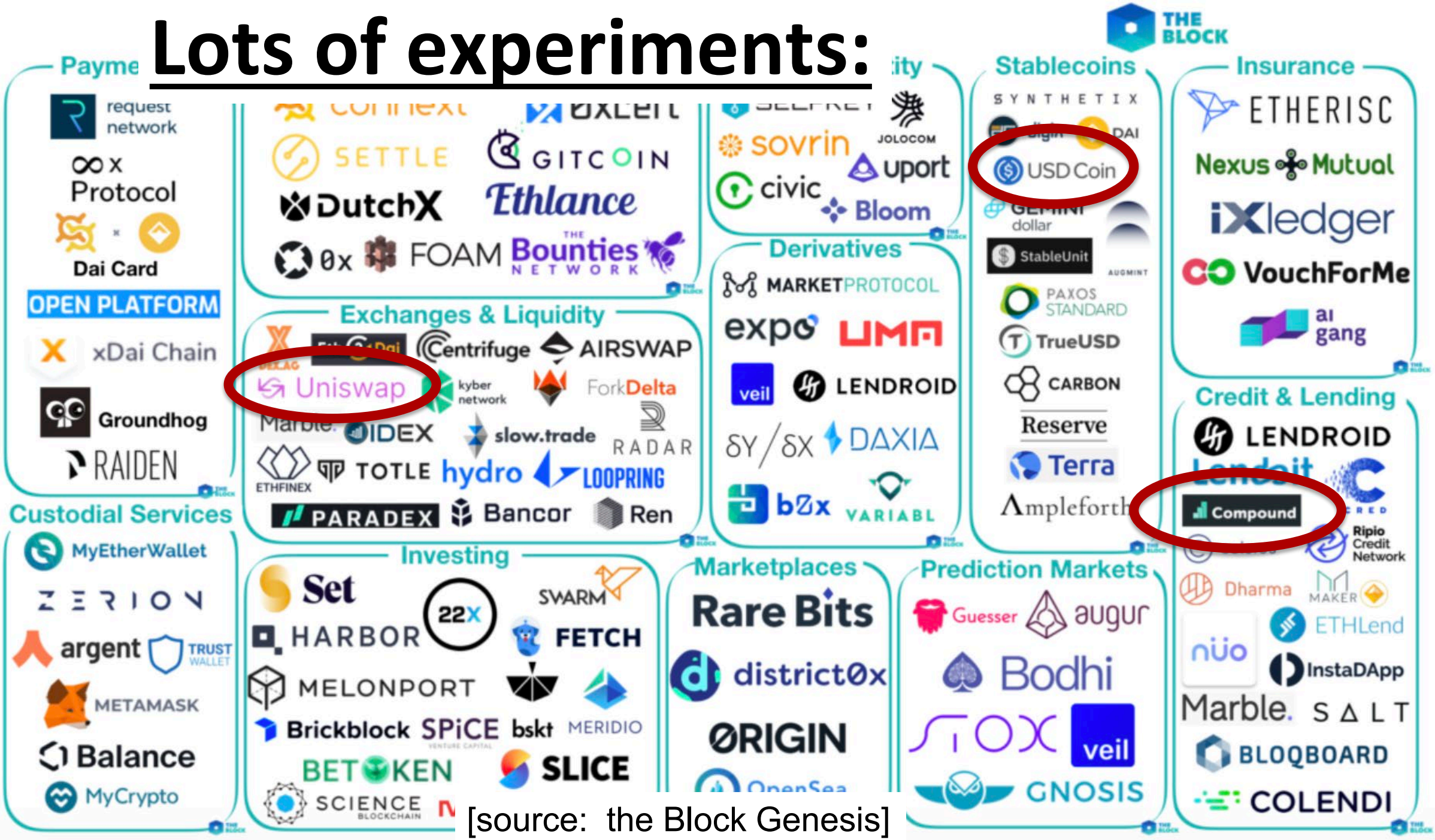
- Run on blockchain: code and state are written on chain
- Accept Tx from users ⇒ state transitions are recorded on chain



Next layer: the blockchain computer

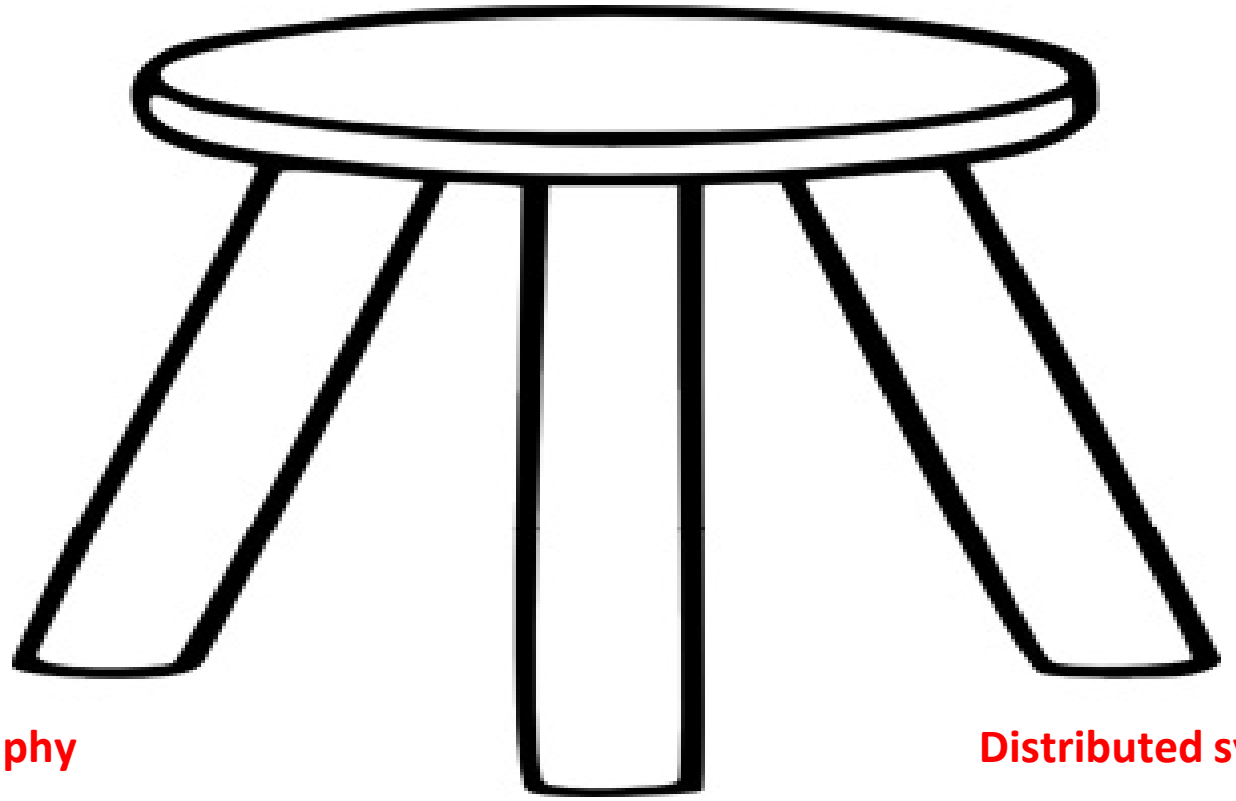


Lots of experiments:



[source: the Block Genesis]

This course



Cryptography

Distributed systems

Economics

Course organization

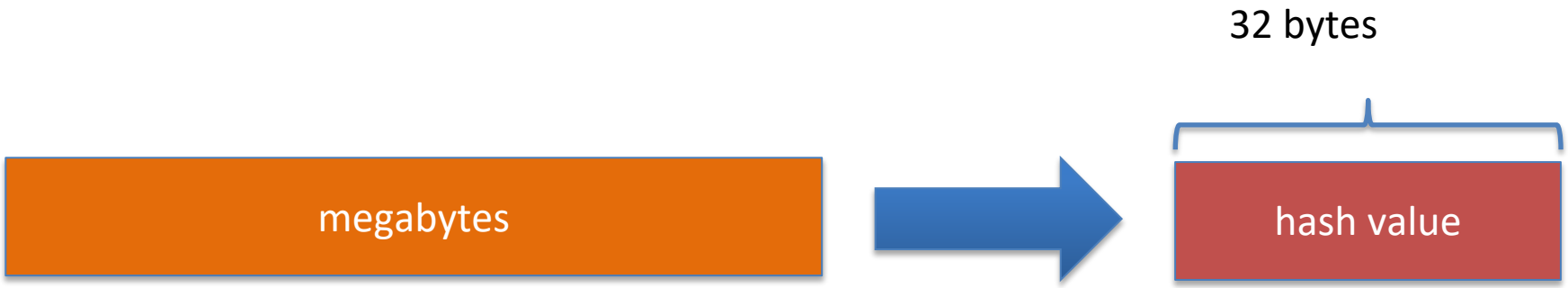
1. The starting point: Bitcoin mechanics
2. Consensus protocols
3. Ethereum and decentralized applications
4. DeFi: decentralized applications in finance
5. Private transactions on a public blockchain
   (SNARKs and zero knowledge proofs)
6. Scaling the blockchain: getting to 10K Tx/sec
7. Interoperability among chains: bridges and wrapped coins

Let’s get started …

Cryptography Background

(1) cryptographic hash functions

An efficiently computable function $H: M \to T$
where $|M| \gg |T|$



$T = \{0,1\}^{256}$

Collision resistance

Def: a **collision** for $H: M \to T$ is pair $x \neq y \in M$ s.t. $\boxed{H(x) = H(y)}$

$|M| \gg |T|$ implies that many collisions exist

Def: a function $H: M \to T$ is **collision resistant** if it is "hard" to find even a single collision for H (we say H is a CRF)

Example: **SHA256**: $\{x : \text{len}(x) < 2^{64} \text{ bytes}\} \to \{0,1\}^{256}$

(output is 32 bytes)

Application: committing to data on a blockchain

Alice has a large file m. She posts $h = H(m)$ (32 bytes)

Bob reads h. Later he learns m' s.t. $H(m') = h$

H is a CRF $\Rightarrow$ Bob is convinced that $m' = m$
(otherwise, m and m' are a collision for H)

We say that $h = H(m)$ is a **binding commitment** to m

(note: not hiding, h may leak information about m)

Committing to a list (of transactions)

Alice has $S = (m_1, m_2, \ldots, m_n)$

32 bytes

Goal:

- Alice posts a <u>short</u> binding commitment to S, $h = \text{commit}(S)$

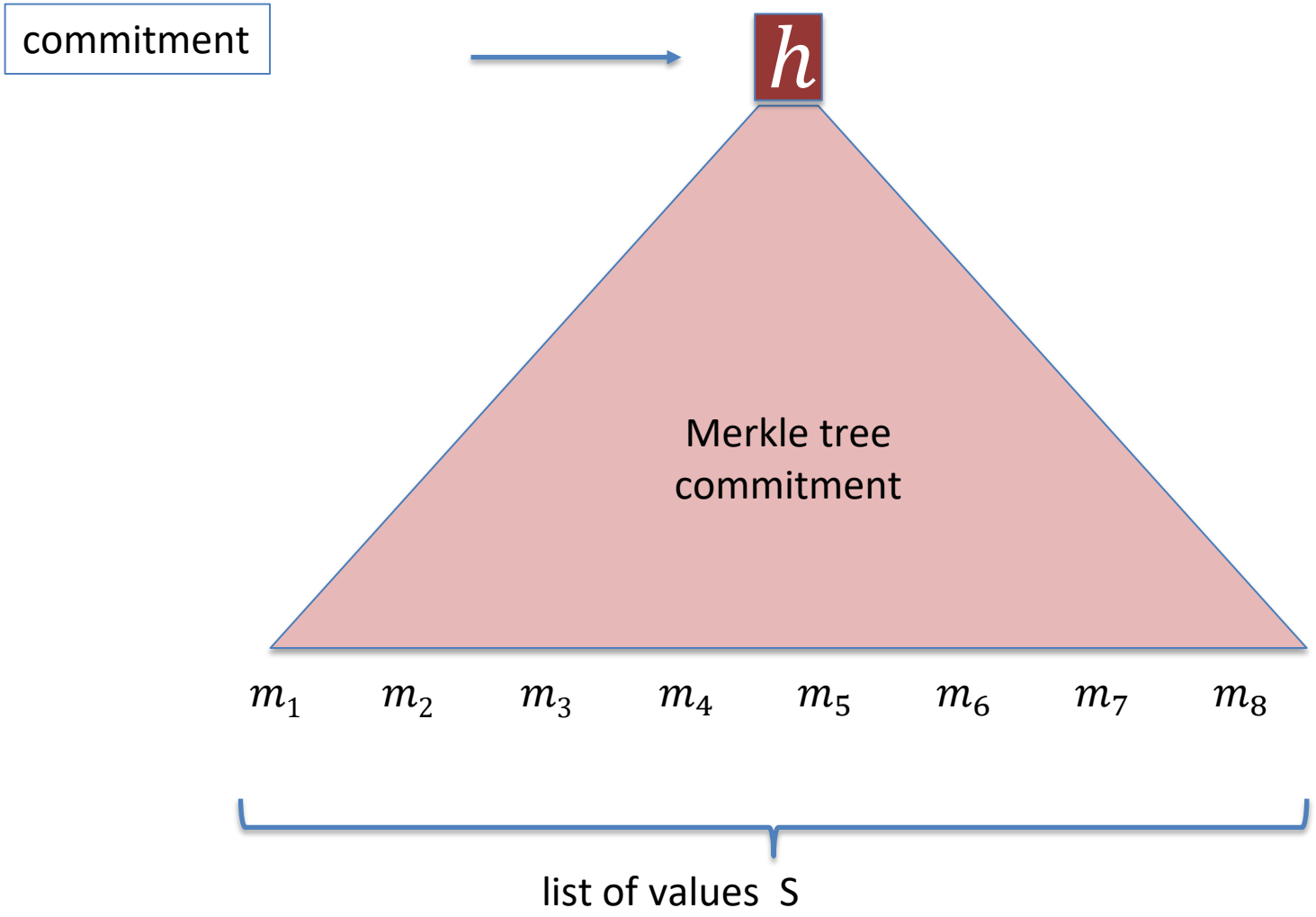
-Bob reads h. Given $(m_i,\ \text{proof}\ \pi_i)$ can check that $S[i] = m_i$

Bob runs $\text{verify}(h, i, mi, \pi_i) \rightarrow$ accept/reject

security: adv. cannot find (S, i, m, π) s.t. $m \neq S[i]$ and

$\text{verify}(h, i, m, \pi) = \text{accept}$ where $h = \text{commit}(S)$

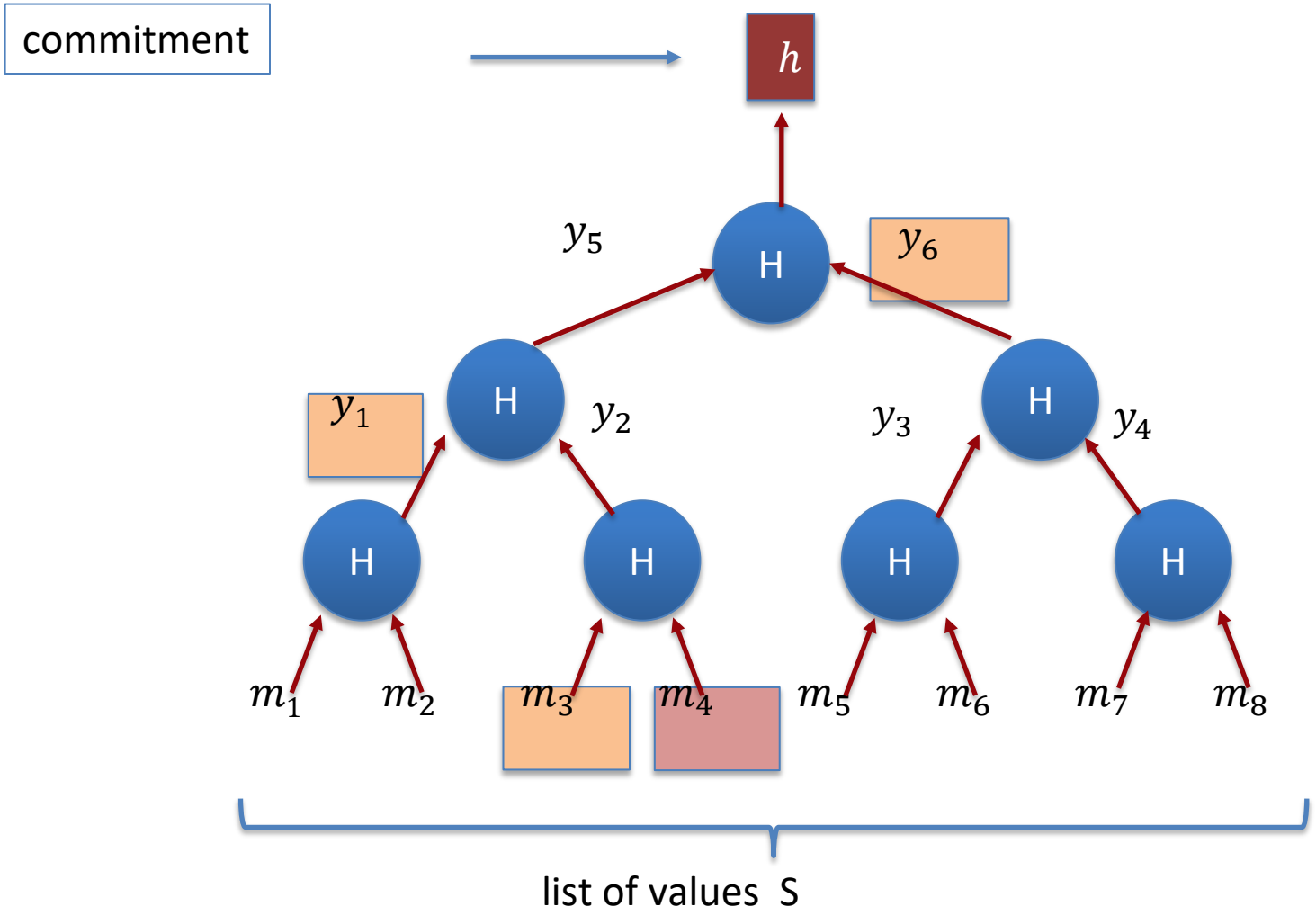
Merkle tree (Merkle 1989)



Goal:

- commit to list S of size n
- Later prove $S[i] = m_i$

Merkle tree (Merkle 1989) [simplified]



Goal:

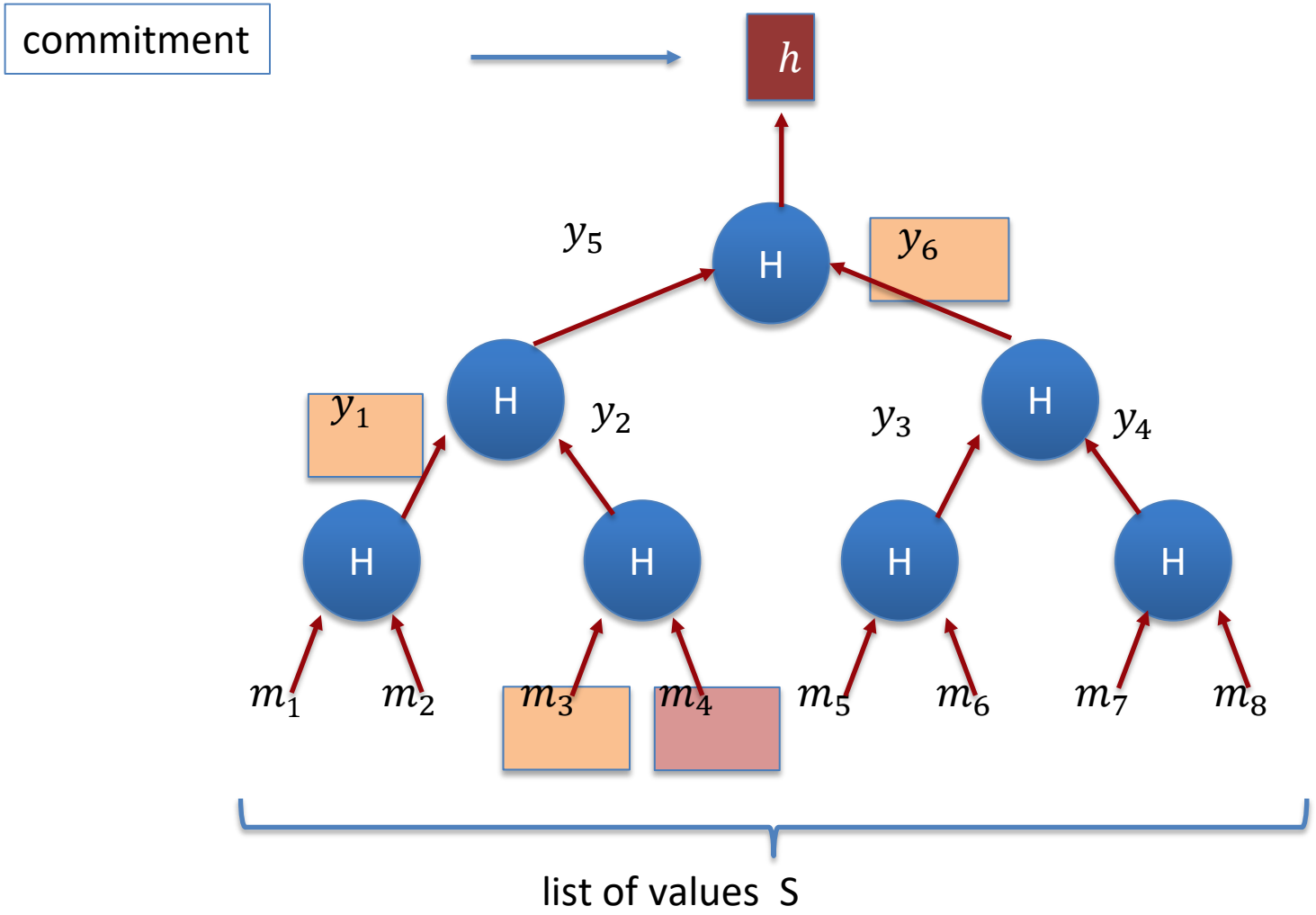
- commit to list S of size n
- Later prove $S[i] = m_i$

To prove $S[4] = m_4$,

proof $\pi = (m_3, y_1, y_6)$

length of proof: $\log_2 n$

Merkle tree (Merkle 1989) [simplified]



To prove $S[4] = m_4$,

proof $\pi = (m_3, y_1, y_6)$

Bob does:

$y_2 \leftarrow H(m_3, m_4)$

$y_5 \leftarrow H(y_1, y_2)$

$h' \leftarrow H(y_5, y_6)$

accept if $h = h'$

Merkle tree (Merkle 1989)

Thm: For a given n: if H is a CRF then

adv. cannot find (S, i, m, π) s.t. $|S| = n$, $m \neq S[i]$,

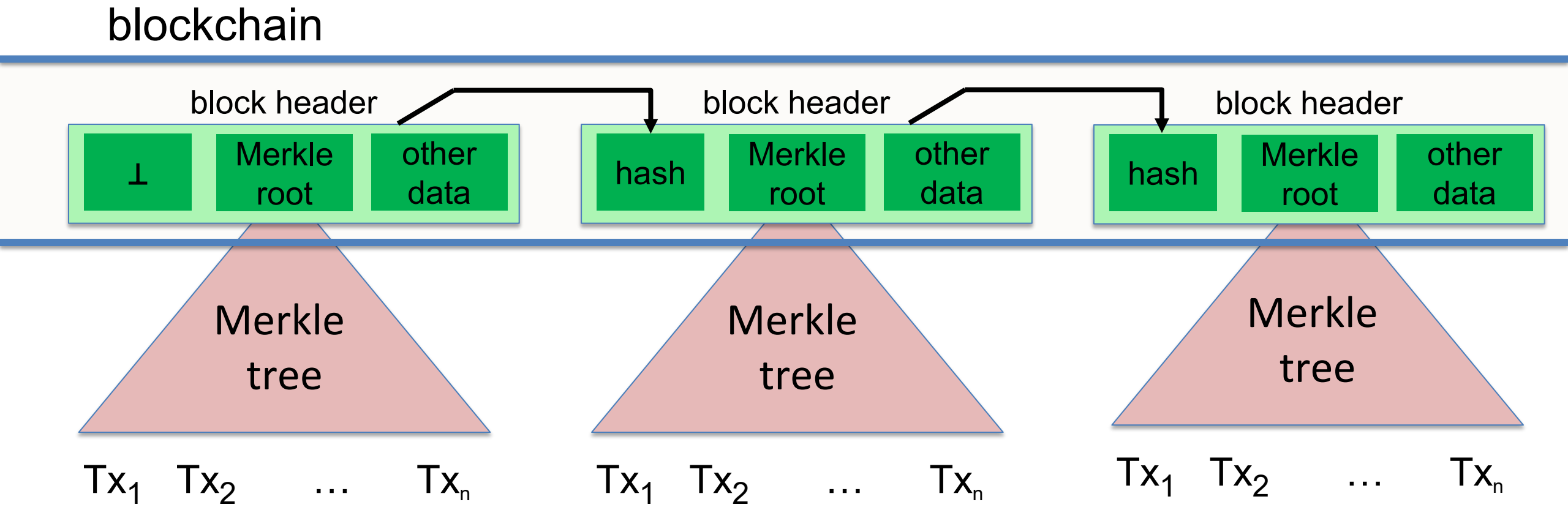
$h = \text{commit}(S)$, and $\text{verify}(h, i, m, \pi) = \text{accept}$

(to prove, prove the contra-positive)

How is this useful? To post a block of transactions S on chain suffices to only write commit(S) to chain. Keeps chain small.

$\Rightarrow$ Later, can prove contents of every Tx.

Abstract block chain



Merkle proofs are used to prove that a Tx is “on the block chain”

Another application: proof of work

<u>Goal</u>: computational problem that
takes time $\Omega(D)$ to solve, but(D is called the **difficulty**)
solution takes time O(1) to verify

How? $H: X \times Y \to \{0,1,2,\ldots,2^n - 1\}$ e.g. $n = 256$

puzzle: input $x \in X$, output $y \in Y$ s.t. $H(x,y) < 2^n/D$

verify(x,y): accept if $\boxed{H(x,y) < 2^n/D}$

Another application: proof of work

<u>Thm</u>: if H is a "random function" then the best algorithm requires D evaluations of H in expectation.

Note: this is a parallel algorithm

$\Rightarrow$ the more machines I have, the faster I solve the puzzle.

Proof of work is used in some consensus protocols (e.g., Bitcoin)

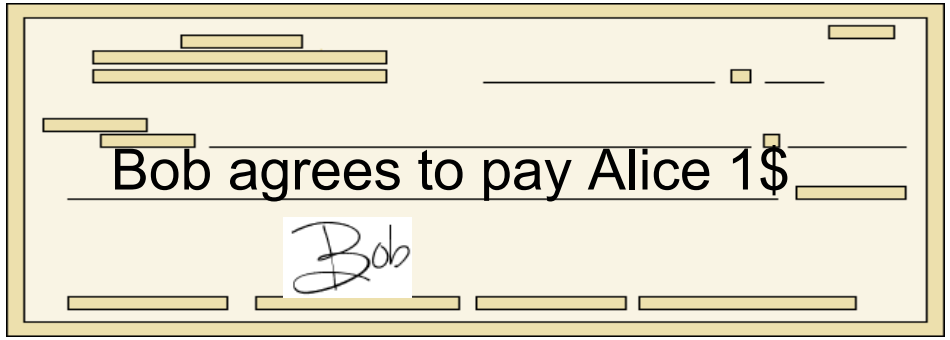
Bitcoin uses $H(x, y) = \mathrm{SHA256}(\mathrm{SHA256}(x.y))$

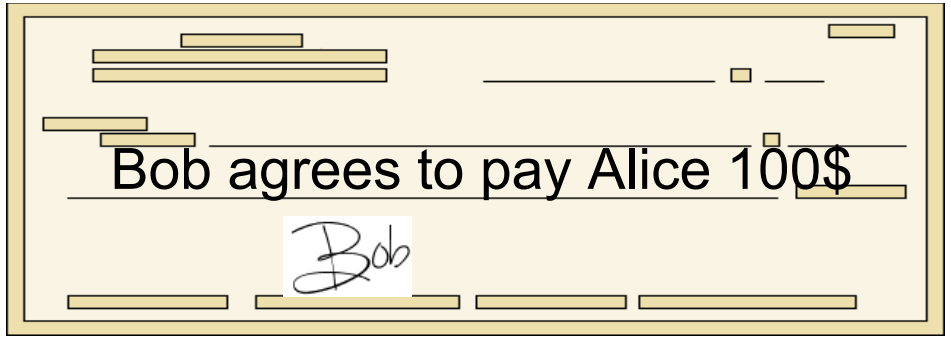
Cryptography background: Digital Signatures

How to authorize a transaction

Signatures

Physical signatures: bind transaction to author



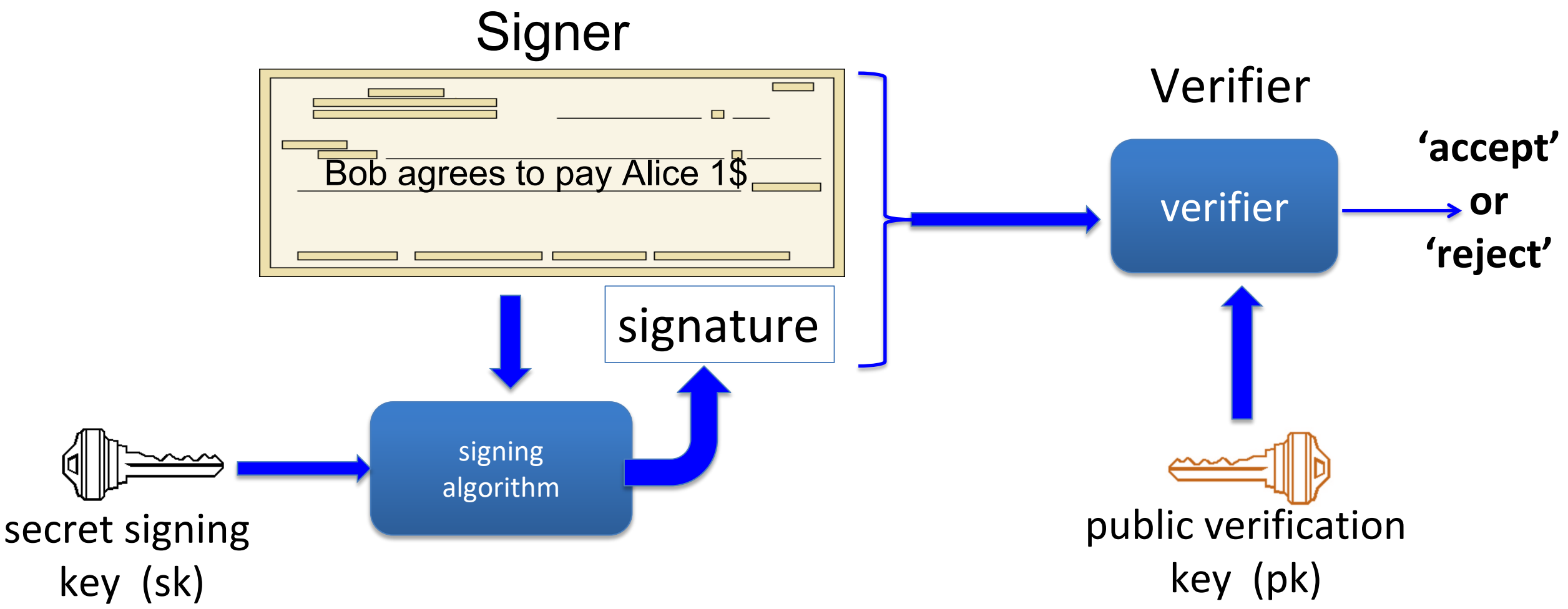


Problem in the digital world:

anyone can copy Bob's signature from one doc to another

Digital signatures

Solution: make signature depend on document



Digital signatures: syntax

<u>Def</u>: a signature scheme is a triple of algorithms:

Gen(): outputs a key pair (pk, sk)

Sign(sk, msg) outputs sig. σ

Verify(pk, msg, σ) outputs 'accept' or 'reject'

<u>Secure signatures</u>: (informal)

Adversary who sees signatures **on many messages** of his choice, cannot forge a signature on a new message.

Families of signature schemes

1. <u>RSA signatures (old … not used in blockchains)</u>:
   long sigs and public keys (≥256 bytes), fast to verify

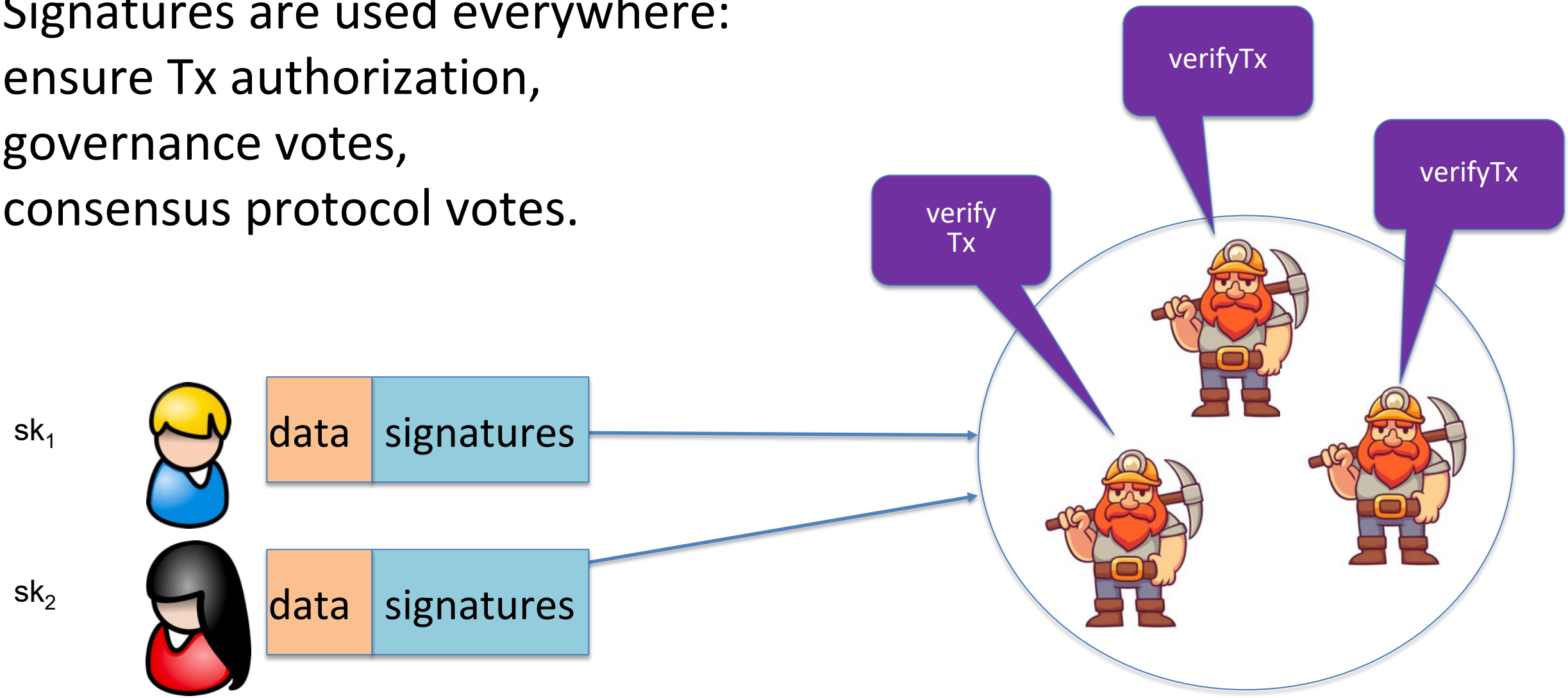
2. <u>Discrete-log signatures</u>: Schnorr and ECDSA (Bitcoin, Ethereum)
   short sigs (48 or 64 bytes) and public key (32 bytes)

3. <u>BLS signatures</u>: 48 bytes, aggregatable, easy threshold

   (Ethereum 2.0, Chia, Dfinity)

---

4. <u>Post-quantum</u> signatures: long (≥600 bytes)

Signatures on the blockchain

Signatures are used everywhere:
ensure Tx authorization,
governance votes,
consensus protocol votes.