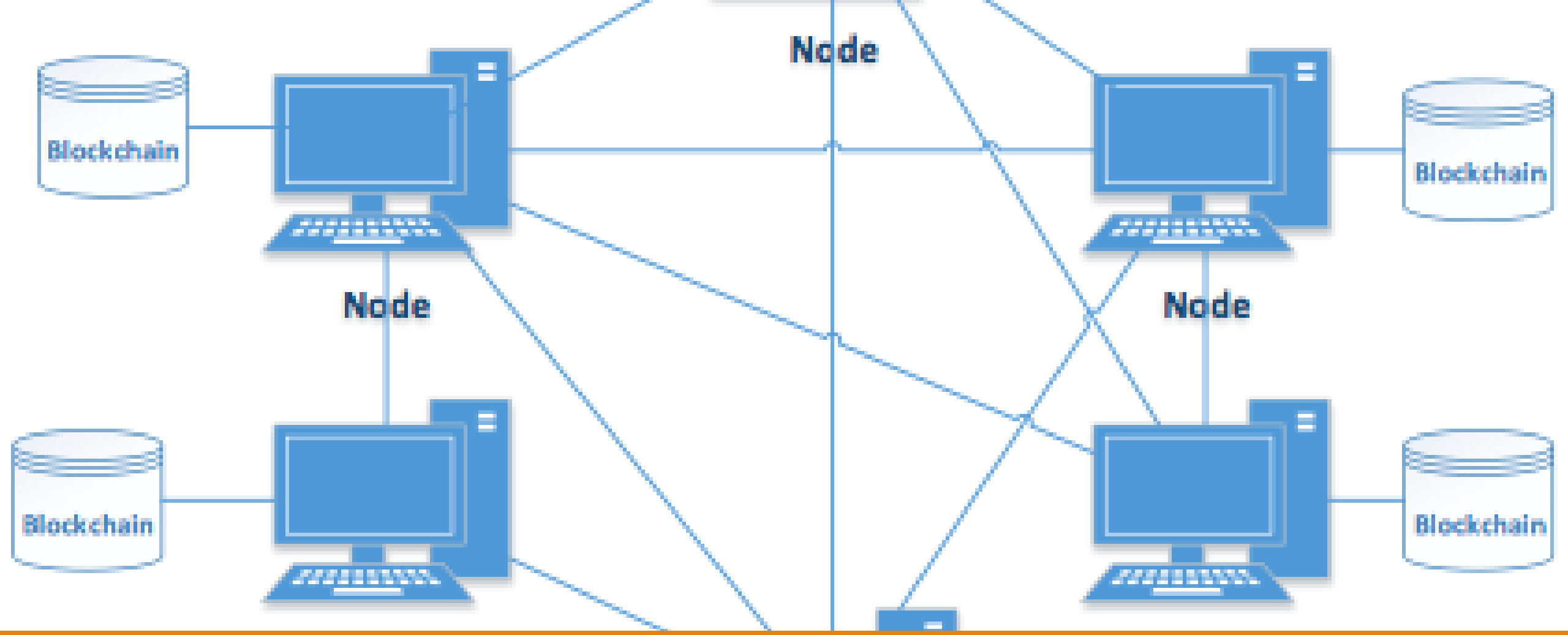


A Small Introduction to P2P systems

Slides from **Prof. Nalini Venkatasubramanian**, Distributed Systems

What is P2P (Peer-to-Peer)

Significantly autonomous from a centralized authority.

- Each node can act as a Client as well as a Server.

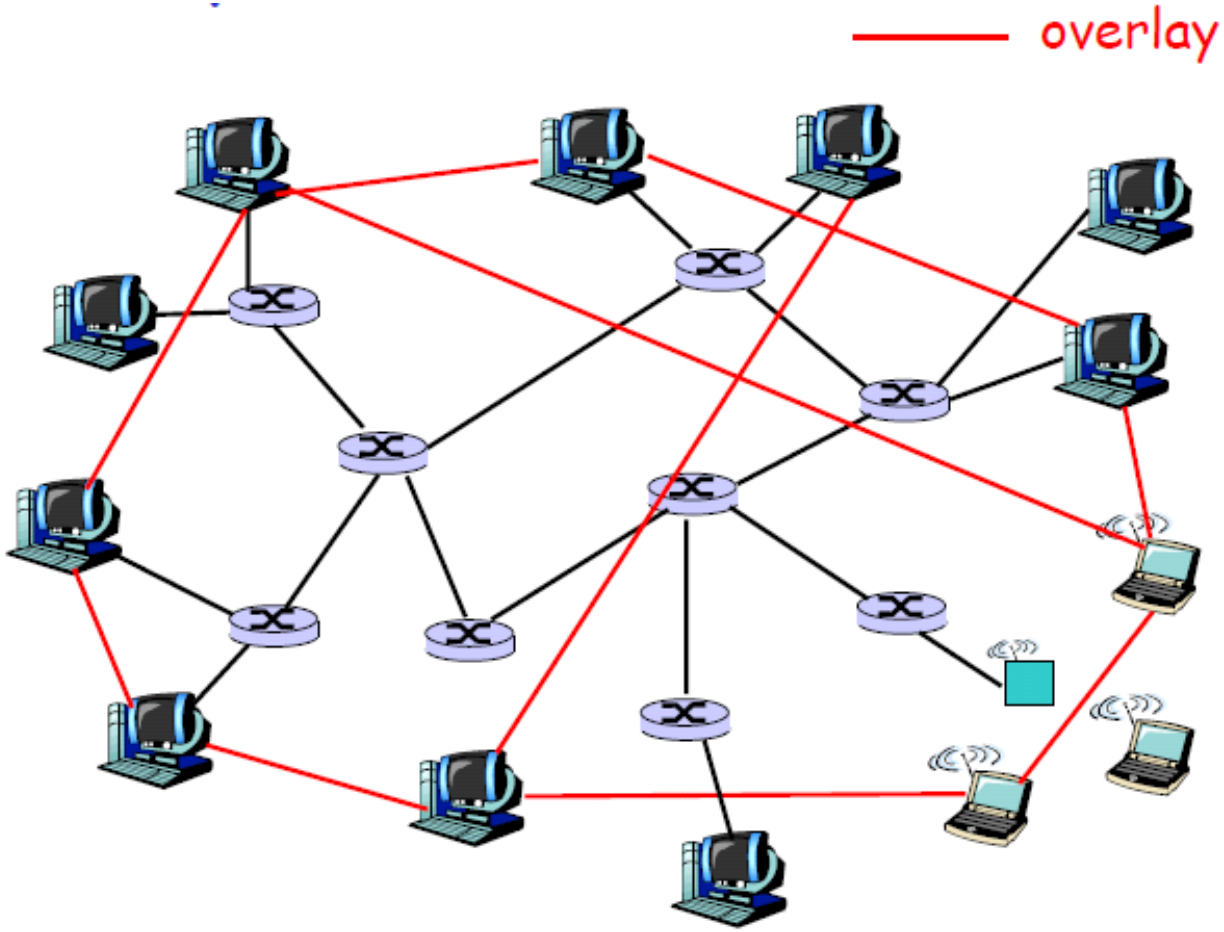
Use the vast resources of machines at the edge of the internet.

- Storage, content, CPU power, Human presence.

Resources at edge have intermittent connectivity, being added & removed.

- Infrastructure is untrusted and the components are unreliable.

Overlay Network



A P2P network is an overlay network. Each link between peers consists of one or more IP links.

Overlay Graph

Virtual edge

- TCP connection
- or simply a pointer to an IP address

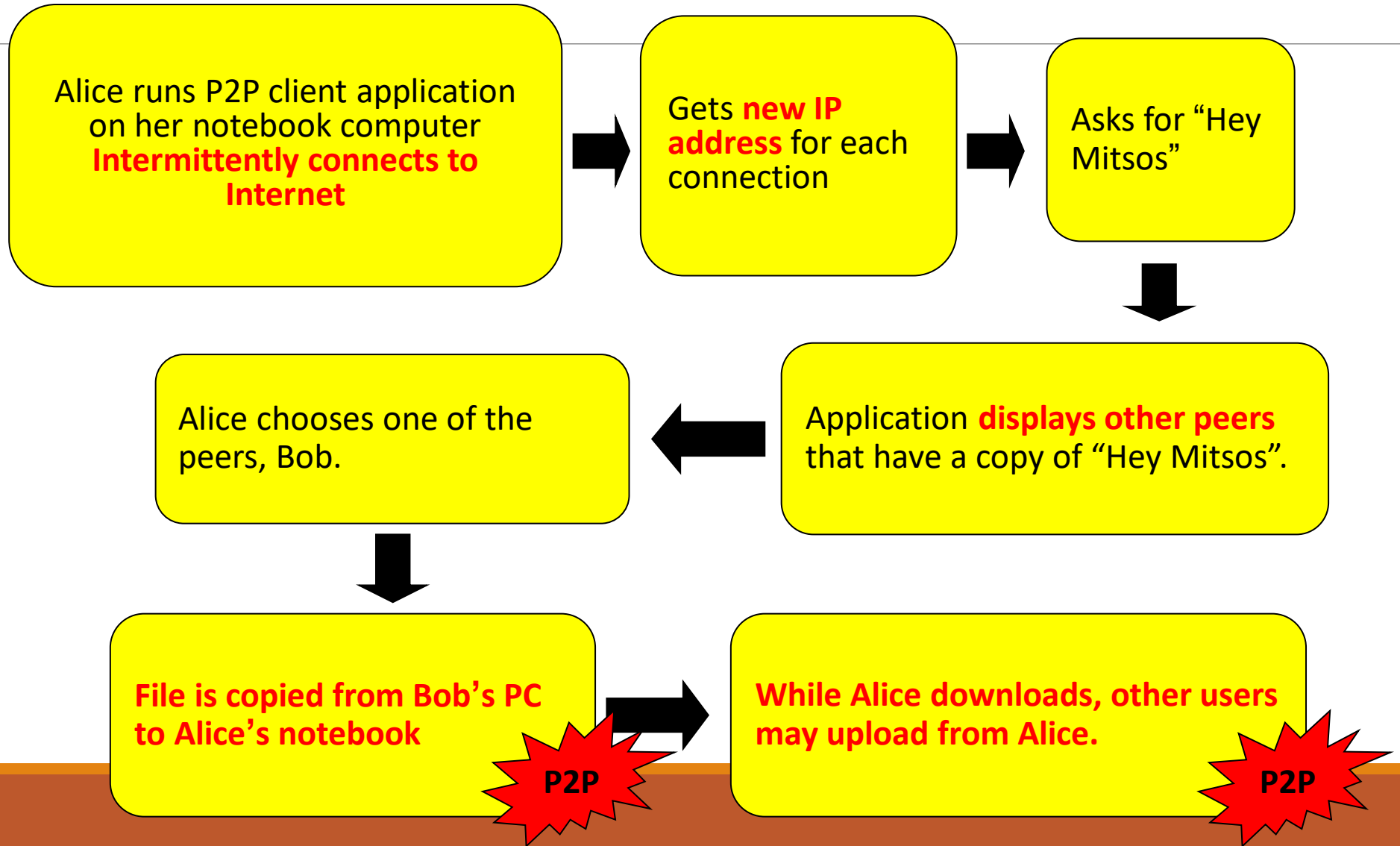
Overlay maintenance

- Periodically ping to make sure neighbor is still alive
- Or verify aliveness while messaging
- If neighbor goes down, may want to establish new edge
- New node needs to bootstrap
- **Could be a challenge under high churn rate**

Some P2P Applications

1. Blockchain (oh Yes…)
2. P2P File Sharing (some are dead)
   - Napster, Gnutella, Kazaa, eDonkey, BitTorrent
   - Chord, CAN, Pastry/Tapestry, Kademlia
3. P2P Communications
   - MSN, Skype, Social Networking Apps
4. P2P Distributed Computing
   - Seti@home (dead)
   - Folding@home (dead)

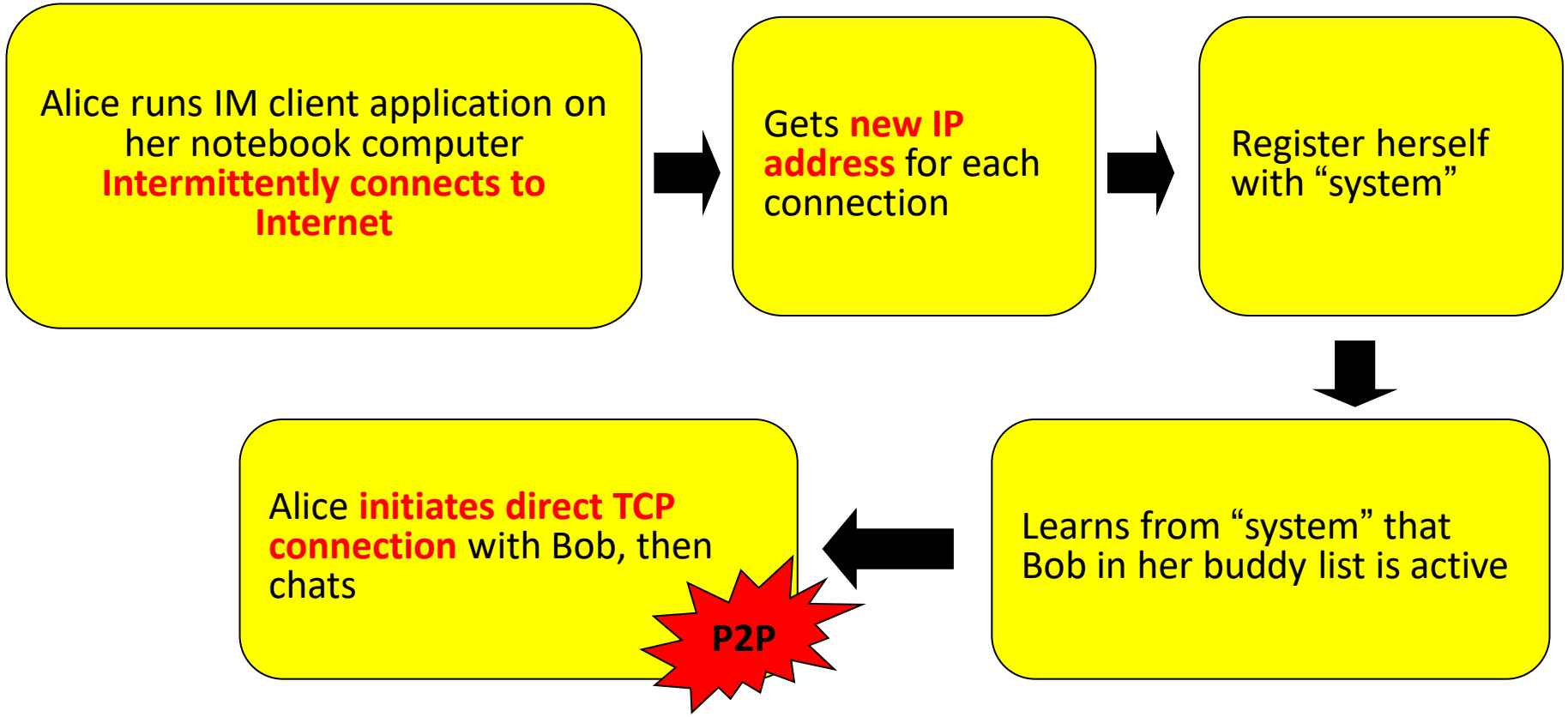
P2P File Sharing



P2P Communication

Instant Messaging

Skype is a VoIP P2P system



P2P Distributed Computing

seti@home

- Search for ET intelligence
- Central site collects radio telescope data
- Data is divided into work chunks of 300 Kbytes
- User obtains client, which runs in background
- Peer sets up TCP connection to central computer, downloads chunk
- Peer does FFT on chunk, uploads results, gets new chunk

Not P2P communication, but exploit Peer computing power

Promising properties of P2P

1. Massive scalability
2. Autonomy: there is no single point of failure
3. Resilience to Denial of Service
4. Load distribution
5. Resistance to censorship

Issues?

Management

- How to maintain the P2P system under high churn efficiently?

Lookup

- How to find out the appropriate content/resource that a user wants?

Throughput

- How to copy the content fast and efficiently?

Management Issue

A P2P network must be **self-organizing.**

- Join and leave operations must be self-managed.
- The infrastructure is untrusted and the components are unreliable.
- The number of faulty nodes grows linearly with system size.
- **Tolerance to failures and churn**

Efficient routing even if the structure of the network is unpredictable.

Dealing with **freeriders**

Load balancing

Napster (The Music Revolution)

Centralized Lookup

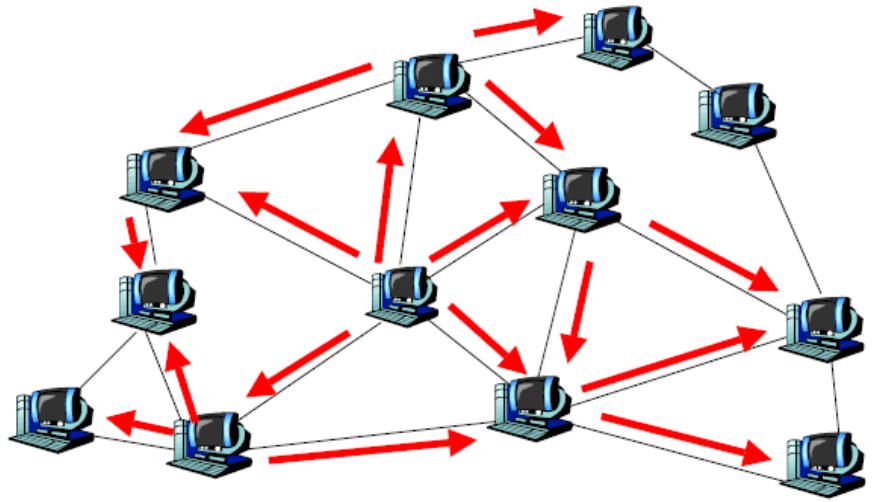
- Centralized directory services
- Step
  - Connect to Napster server.
  - Upload list of files to server.
  - Give server keywords to search the full list with.
  - Select “best” of correct answers. (ping)
- **Bottleneck of the performance**

Lookup is centralized, but files are copied in P2P manner

Gnutella (still alive)

Fully decentralized lookup for files

- Unstructured P2P
- Flooding based lookup
- **Inefficient** lookup in terms of scalability and bandwidth



Gnutella Scenario

Step 0: Join the network

Step 1: Determining who is on the network

- **"Ping"** packet is used to announce your presence on the network.
- Other peers respond with a **"Pong"** packet.
- Also forwards your Ping to other connected peers
- A Pong packet also contains:
  - an IP address
  - port number
  - amount of data that peer is sharing
  - Pong packets come back via same route

Step 2: Searching

- Gnutella "Query" ask other peers if they have the file you desire A Query packet might ask, ***"Do you have any content that matches the string 'Hey Jude"?***
- Peers check to see if they have matches & respond (if they have any matches) & send packet to connected peers
- Continues for TTL (how many hops a packet can go before it dies)

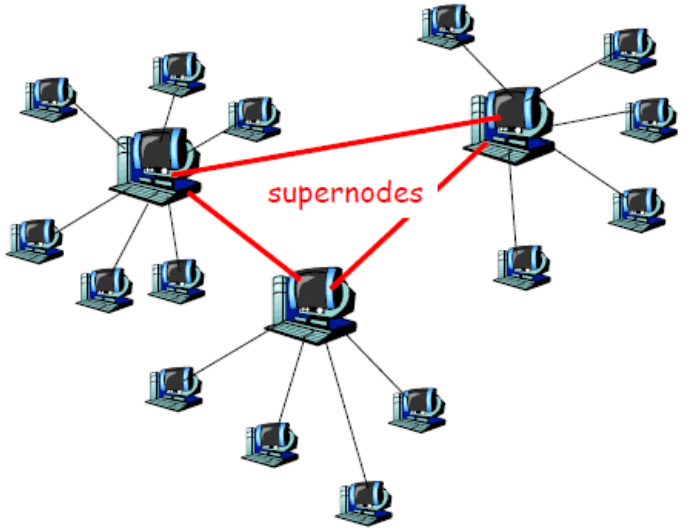
Step 3: Downloading

- Peers respond with a "QueryHit" (contains contact info)
- File transfers use direct connection using HTTP protocol's GET method

KaZaA (dead)

Hierarchical approach between Gnutella and Napster

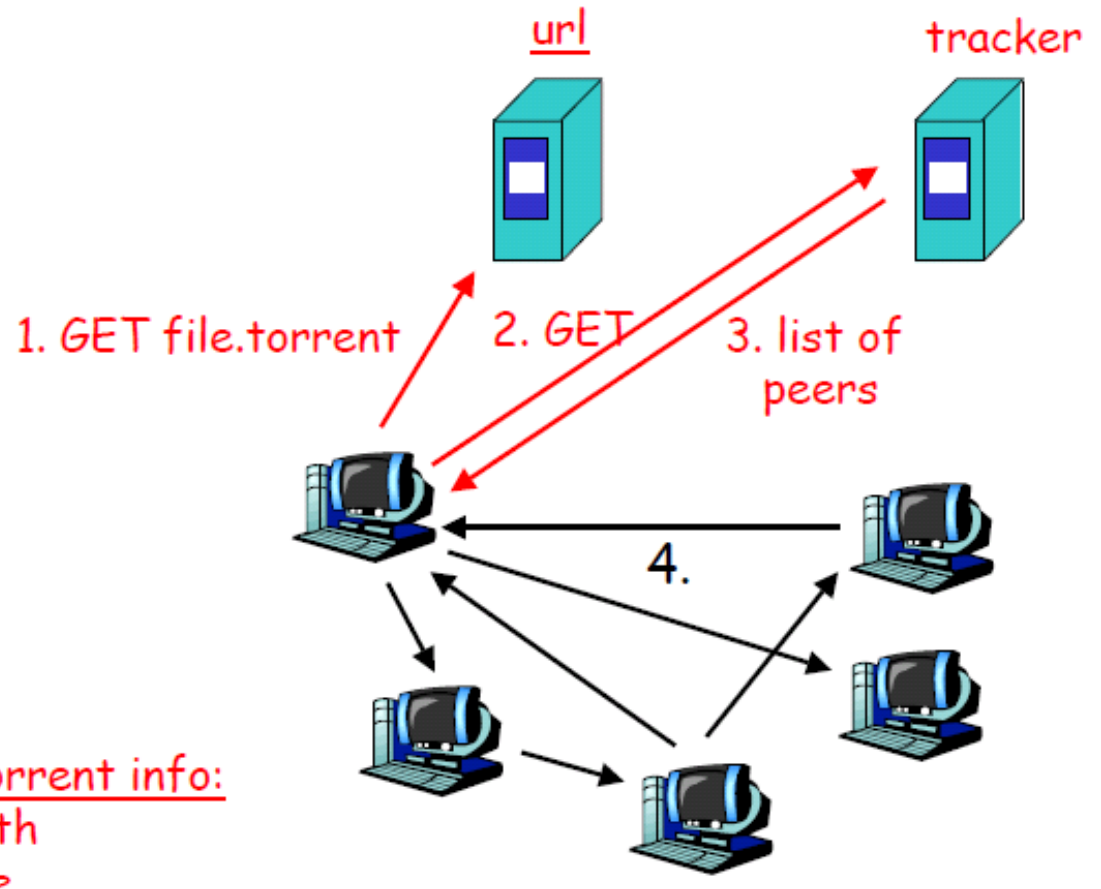
- Powerful nodes (supernodes) act as local index servers, and client queries are propagated to other supernodes. Two-layered architecture.
- Each supernode manages around 30-50 nodes
- More efficient lookup than Gnutella and more scalable than Napster



BitTorrent

Sharing large volume of files faster and more efficiently

Maximizing the utilization of bandwidth



file.torrent info:
- length
- name
- hash
- url of tracker

BitTorrent : Pieces

File is broken into pieces

- Typically, each piece is 256 KBytes
- Upload pieces while downloading pieces

Piece selection

- Select **rarest piece**
- Except at beginning, select random pieces

Tit-for-tat

- Bit-torrent uploads to at most four peers
- Among the uploaders, upload to the four that are downloading to you at the highest rates
- A little randomness too, for probing

Structured P2P

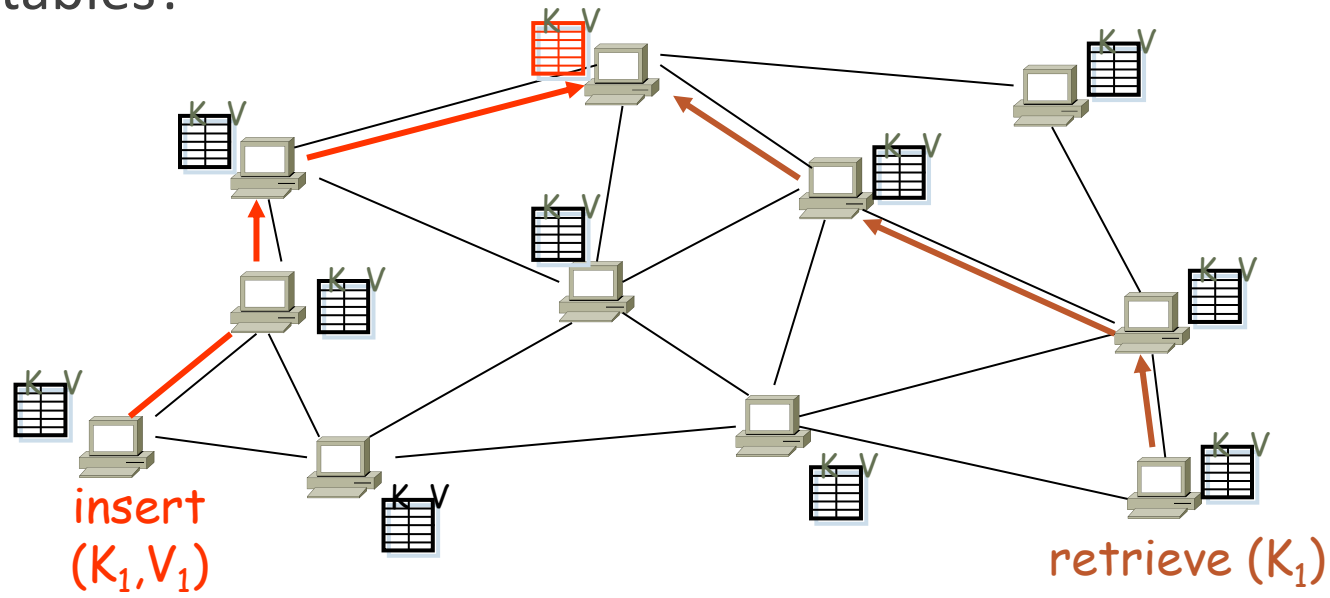
Peer-to-peer hash lookup:

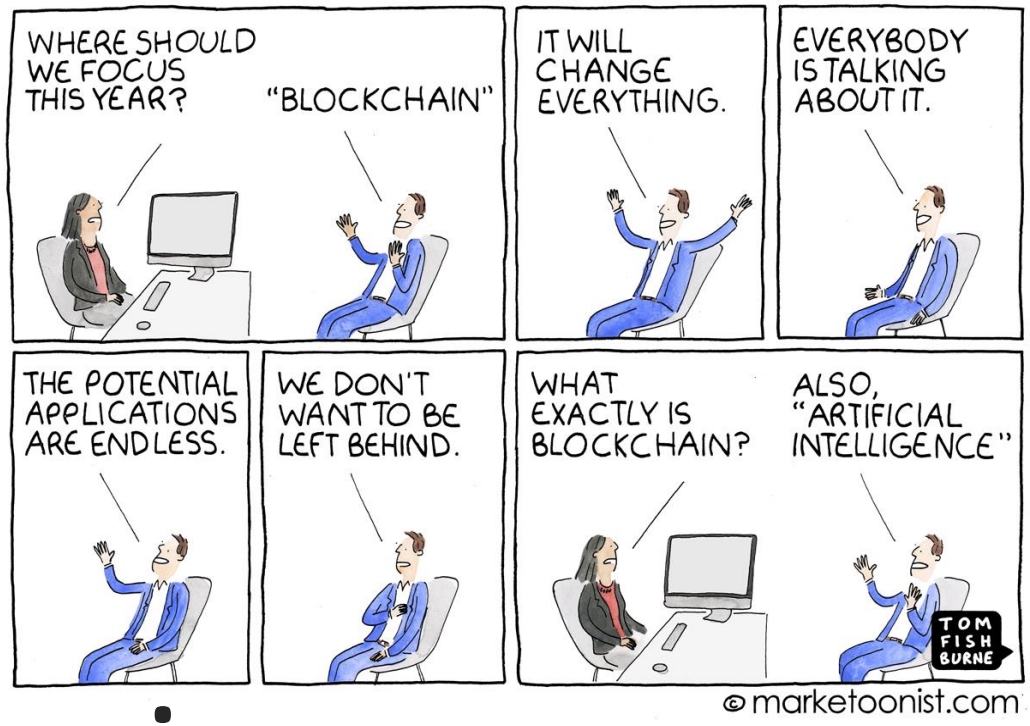
- Node ID(Key) , Object ID(Key)
- Lookup(key) → IP address

How does these route lookups?

How does these maintain routing tables?

Chord,
Pastry,
Tepastry,
Can,
Kademlia,
etc.





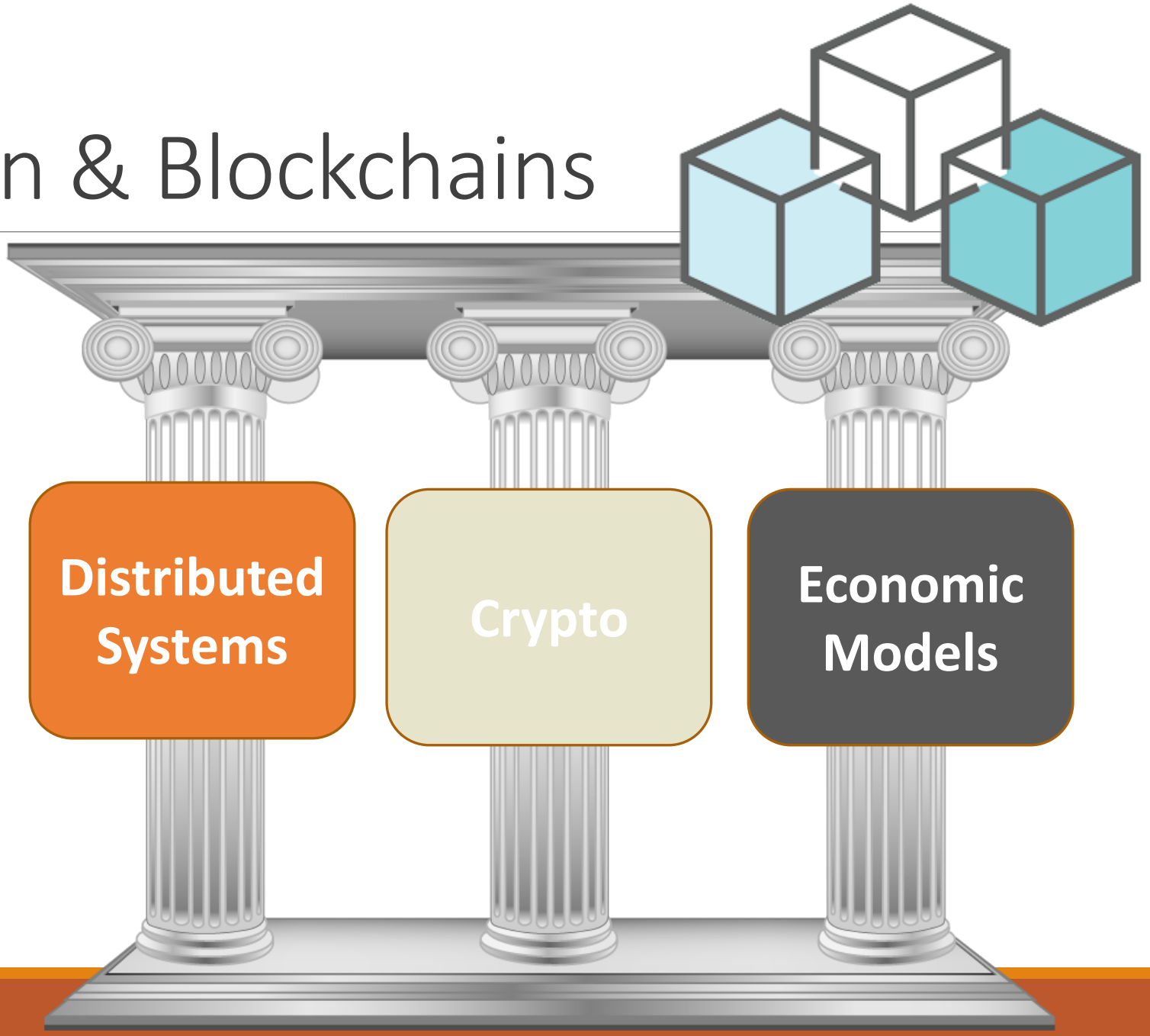
Intro to Blockchains

BASED ON SLIDES FROM:

1. S. CHAKRABORTY, S. SURAL
2. P. VISWANATH

Decentralization & Blockchains

The Three Pillars



The Myth Busters

Blockchain ≠ Bitcoin (or any other cryptocurrencies)

- I am not going to talk about trading of cryptocurrencies!
- I will try to make no 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

What is a BlockChain?

(or what will I talk about in a blockchain 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 is a BlockChain?

(or what should I talk about in a blockchain 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 is a BlockChain?

(or, what should I talk about in a blockchain 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?

What are Blockchains?

Blockchains are decentralized digital trust platforms

Evolution of Trust

Human success is based on flexible cooperation in large numbers.
This requires trust

Bitcoin is the Original BlockChain

BITCOIN IS A CRYPTOCURRENCY

LAUNCHED IN JANUARY 2009

VERY SECURE: SAFETY AND LIVENESS

Bitcoin

Cryptocurrency

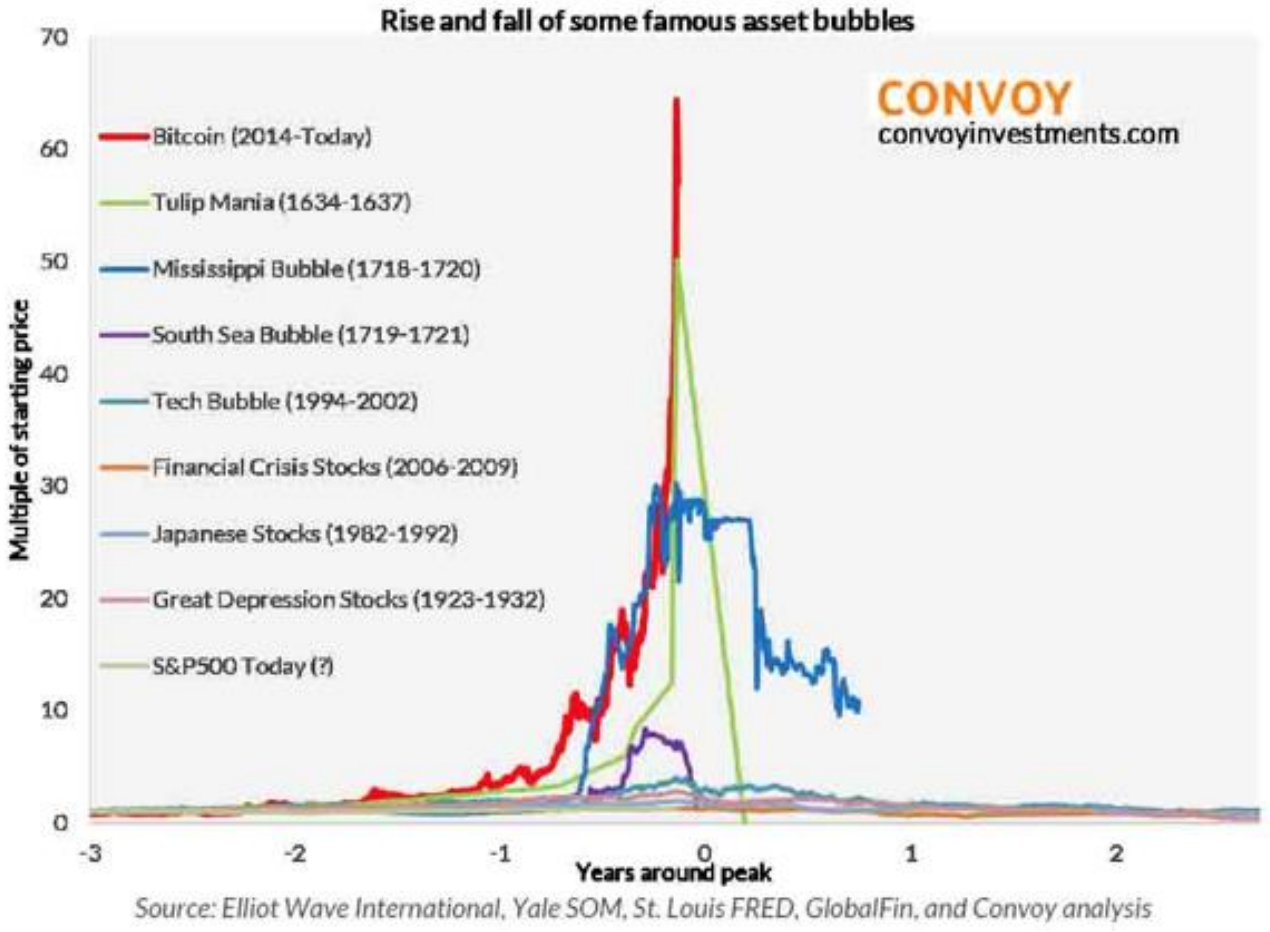
medium of exchange and store of value

Born during the 2008 Financial Crisis

Anonymous inventor

pseudonym: Satoshi Nakamoto

Bitcoin is THE bubble of all time

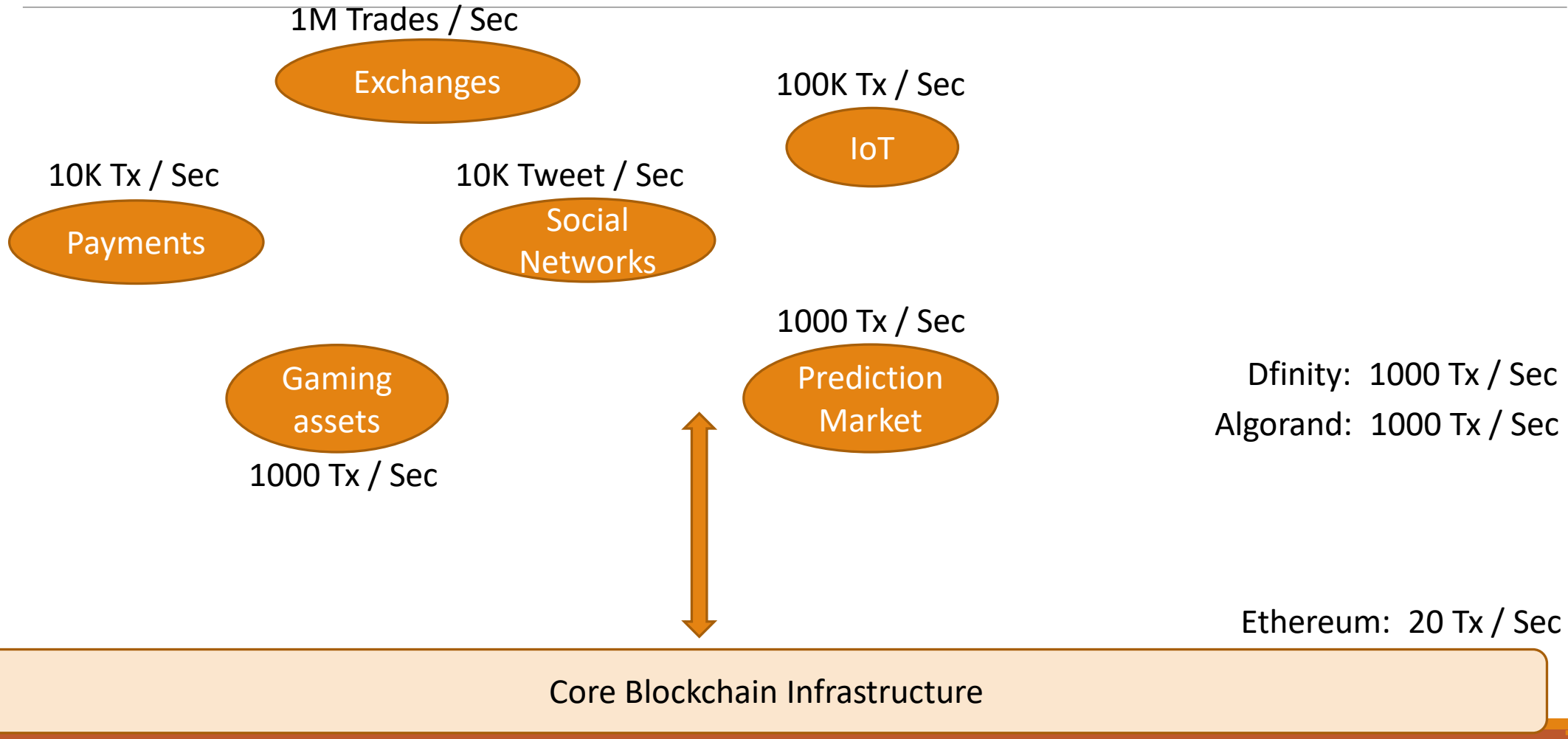


Source: Elliot Wave International, Yale SOM, St. Louis FRED, GlobalFin, and Convoy analysis

Bitcoin Performance

1. Security	50% adversary
2. Transaction throughput	7 tx/s
3. Confirmation Latency	hours
4. Energy consumption	medium-size country
5. Compute	specialized mining hardware
6. Storage	everyone stores everything
7. Communication	everyone tx/rx everything

The Promise and the Gap



Supply Chain Management: The Players and the Game

Supply Chain in Petroleum Industry

Crude Purchase

Crude Transportation

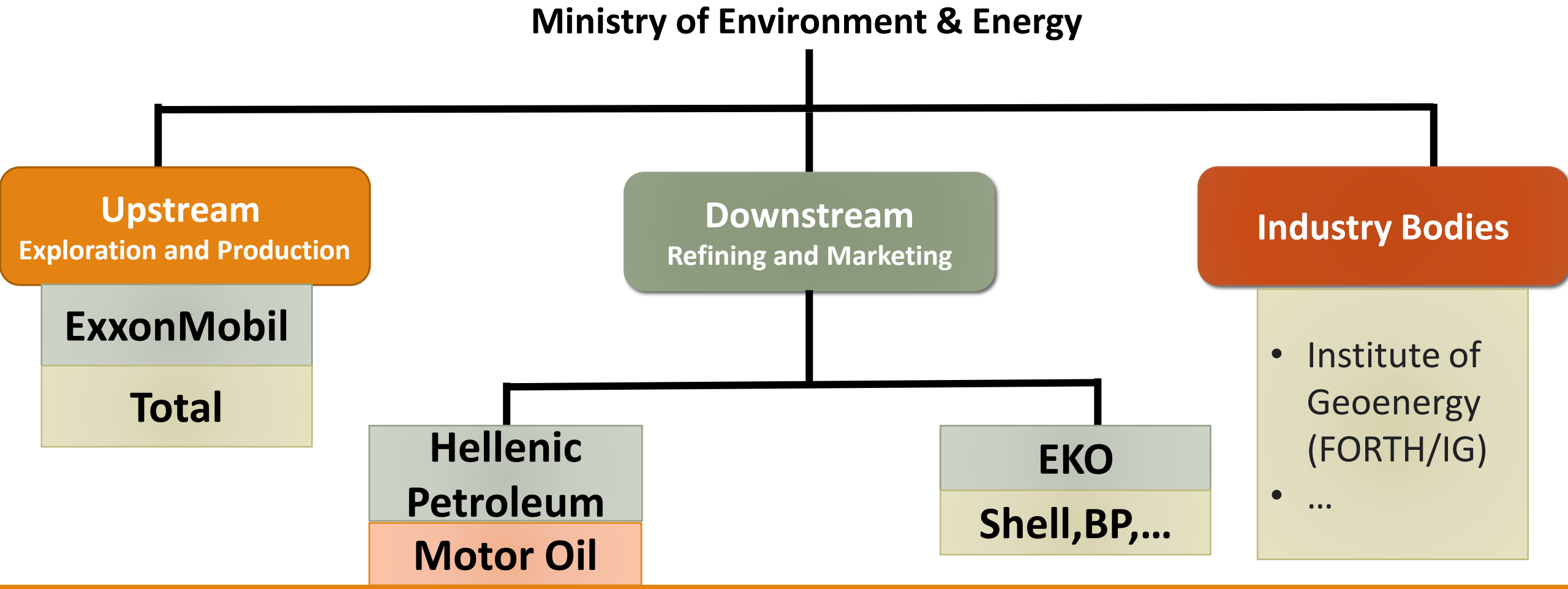
Crude Storage

Refining

Distribution

Retail

Petroleum Supply Chain



Requirements of a Successful Supply Chain






Needs Strong Coordination among the Players

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

A web-based portal?

Requirements of a Successful Supply Chain





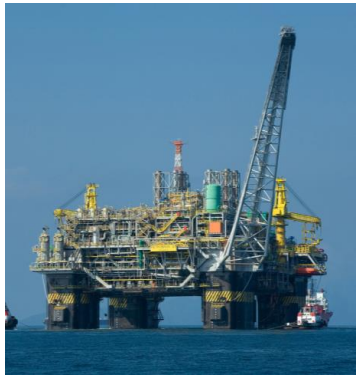

How do we obtain Real-time Information from the Stakeholders?

What is the guarantee that the information submitted is correct?

What if someone denies the information later on?

Blockchain is the answer !!

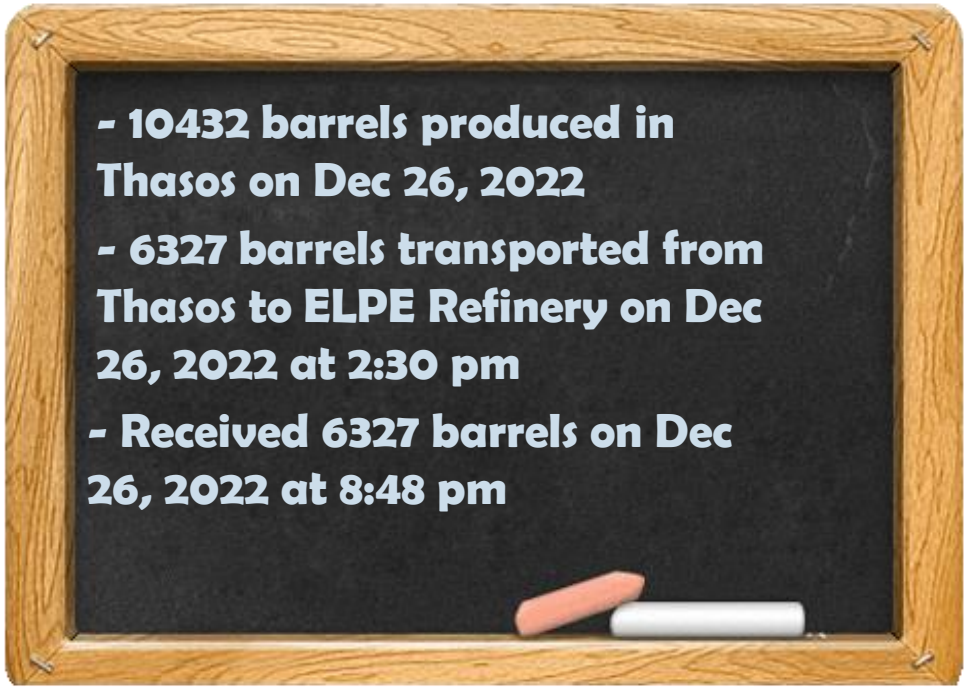
How Can We Obtain Real Time Information?



Use a Public Bulletin Board

Advantages:

- Everyone can see all the logs and verify
- Any change in information is visible to everyone
- The board is not erasable, no one can deny later
- Simple one-step auditing



Use a Public Bulletin Board - Challenges

Who will maintain this bulletin board?

- **Buy Cloud from amazon**

Who will manage it and provide the cost?

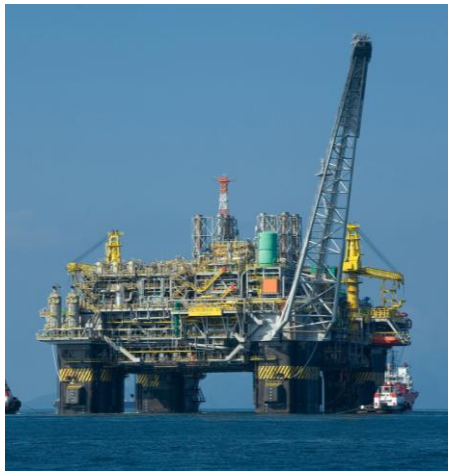
- **One of the enterprises maintains a private cloud**

What is the guarantee that it is not a fraud?

Let everyone maintain the same copy of the board individually and independently

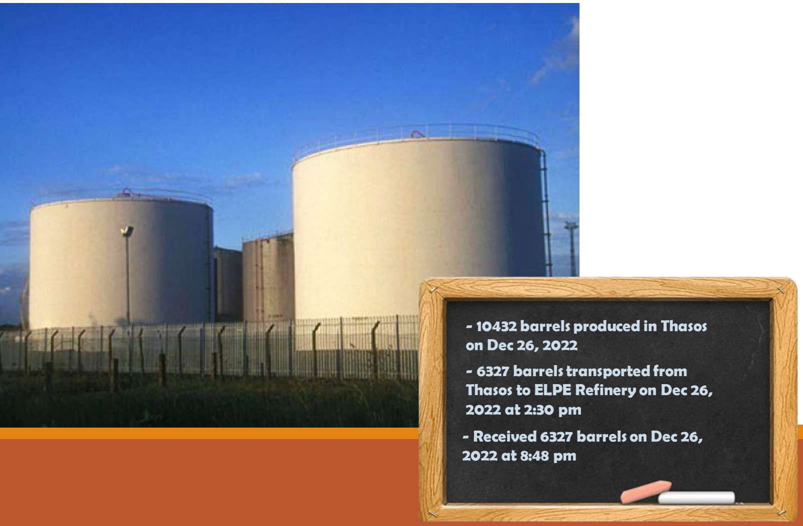
– BUT HOW?

What is this “Blockchain”?



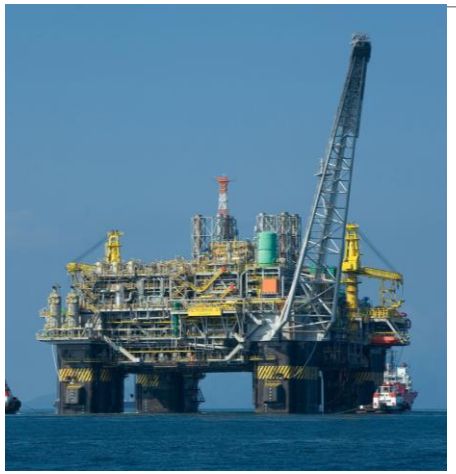
A decentralized and multi-authority networked information data storage and access system

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

What is this “Blockchain”?

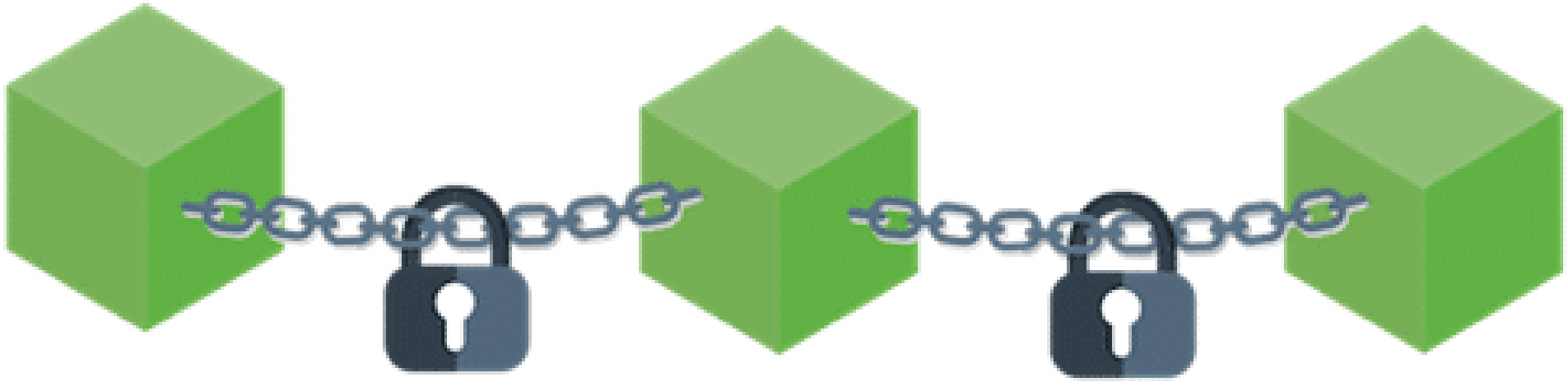


An immutable append-only ever-growing chain of data. Data once added cannot be deleted or modified later

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

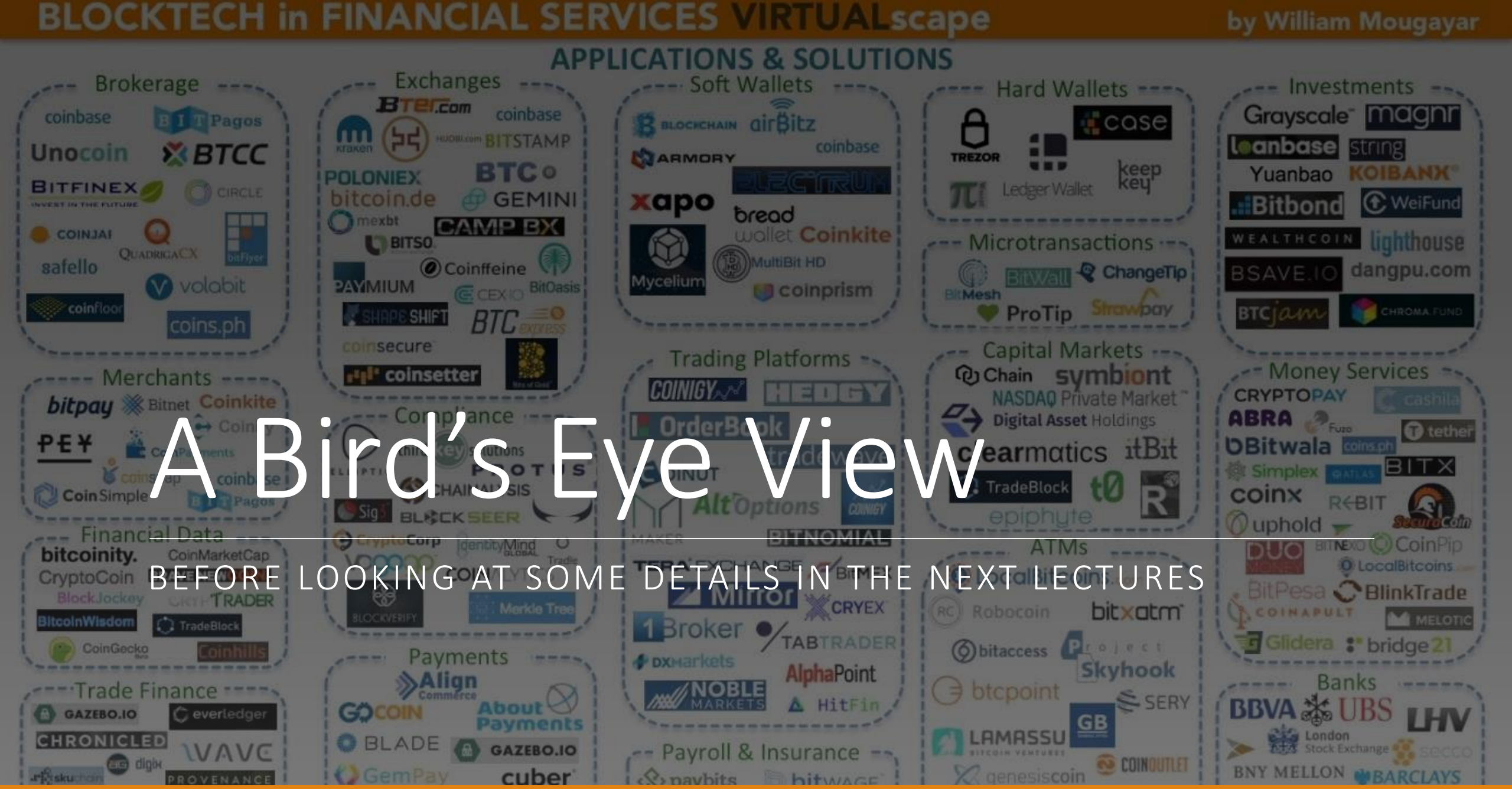
The information is transparent to all - everyone can see what is going on in the system

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



So, What is the Definition of a "Blockchain"

A decentralized immutable append-only public ledger



A Bird's Eye View

BEFORE LOOKING AT SOME DETAILS IN THE NEXT LECTURES

Tasks for Designing a P2P System for Managing Ownership

Goal	Major Concept
Describing Ownership	History of Transaction Data
Prtotecting Ownership	Digital Signature
Storing Transaction Data	Blockchain Data Structure
Preparing Ledgers for being Distributed	Immutability
Distributing Ledgers	Information Forwarding in Networks
Adding New Transactions	Blockchain Algorithm
Deciding which Ledger Represents the Truth	Distributed Consensus

Technical Concepts of the Blockchain and their Purpose (1)

Technical Concept	Purpose
Transaction Data	Describing Transfer of Ownership
Transaction History	Proving the Current State of Ownership
Cryptographic Hash Value	Identifying any kind of Data Uniquely
Asymmetric Cryptography	Encrypting and Decrypting Data
Digital Signature	Stating Agreement with the Content of Transaction Data
Hash Reference	A Reference that becomes Invalid once the Data being Referred are Changed
Change-Sensitive Data Structures	Storing Data in a way that Makes any Manipulation Stand out Immediately

Technical Concepts of the Blockchain and their Purpose (2)

Technical Concept	Purpose
Hash Puzzle	Imposing a Computational Expensive Task
Blockchain Data Structure	Storing Transaction Data in a Change-Sensitive way and Maintaining their Order
Immutability	Making it impossible to Change the History of Transaction Data
P2P Network	Sharing the Transaction History Among all Nodes in Network
Message Passing	Ensure that all Nodes of the System Eventually Receive all Information
BlockChain Algorithm	Ensure that only Valid Transaction Data are added to the Blockchain Data Structure
Distributed Consensus	Ensure that all Nodes of the System use the Identical History of Transaction Data
Compensation	Giving Nodes and Incentive to Maintain Integrity

Purpose of BlockChain

1. Clarifying Ownership

2. Transferring Ownership

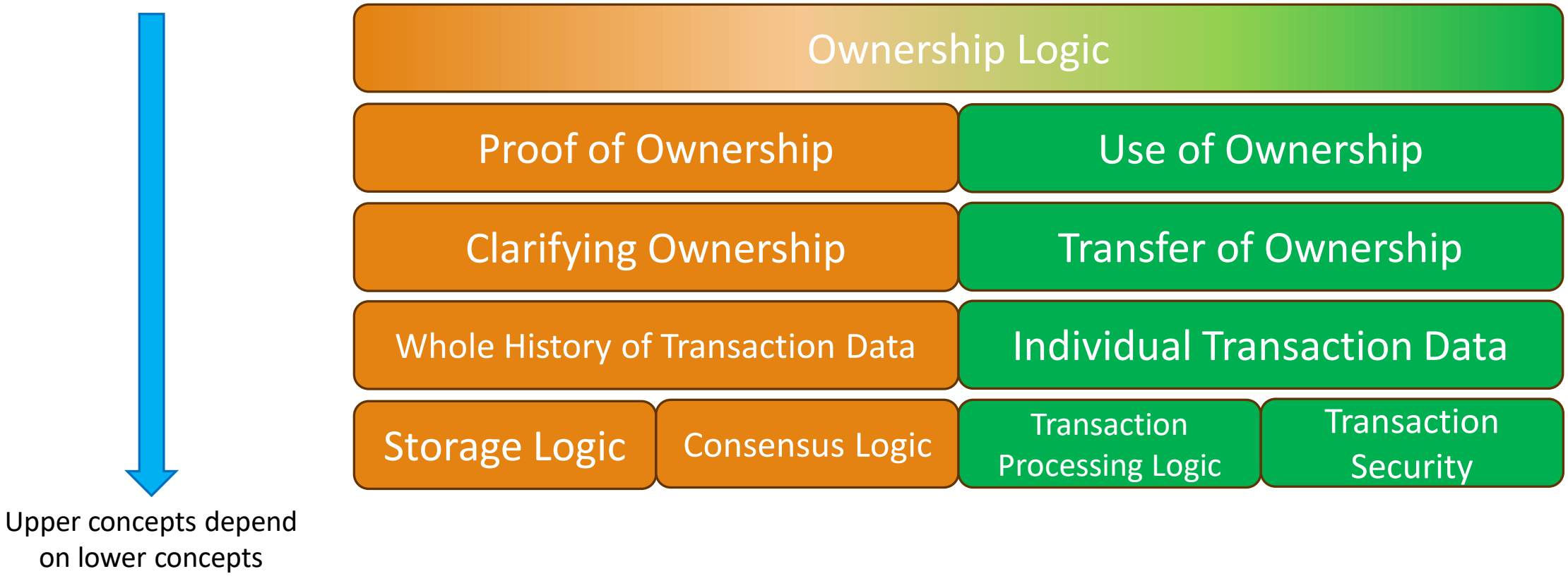
Properties of BlockChain

- Highly Available
- Censorship Proof
- Reliable
- Open
- Pseudoanonymous
- Secure
- Resilient
- Eventually Consistent
- Keeping Integrity

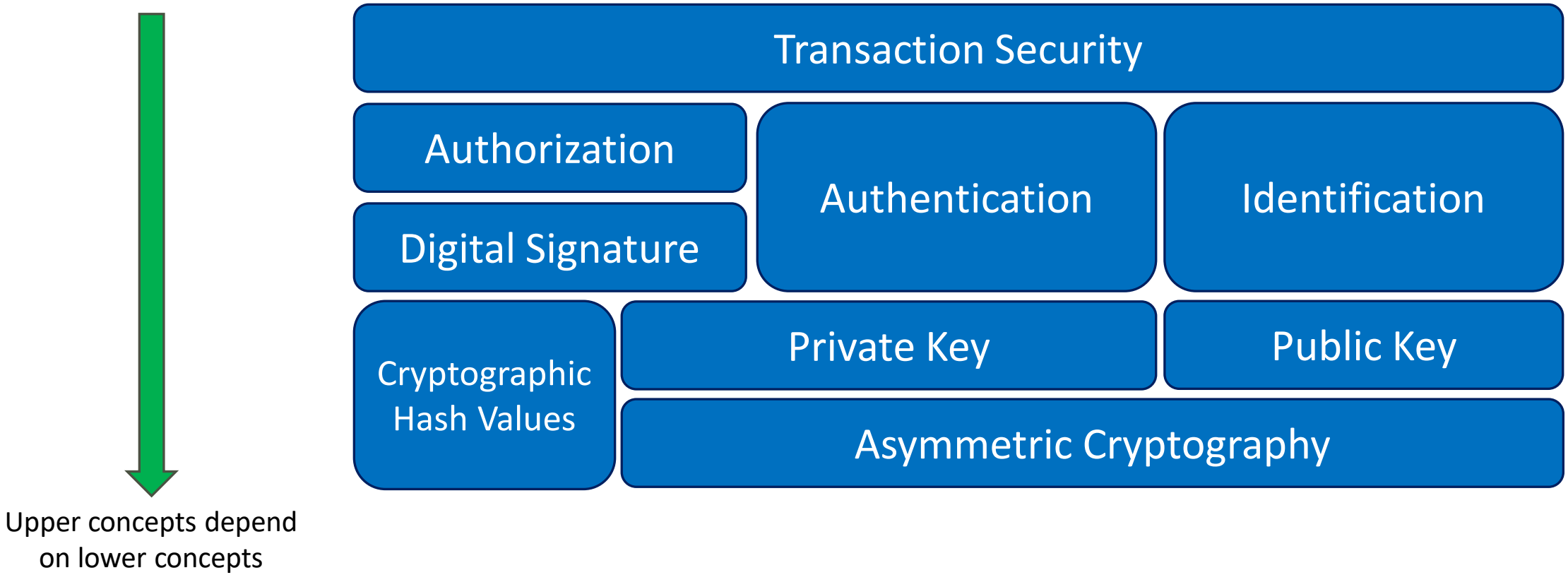
Internal Functioning of BlockChain

- Ownership Logic
- Transaction Security
- Transaction Processing Logic
- Storage Logic
- P2P Architecture
- Consensus Logic

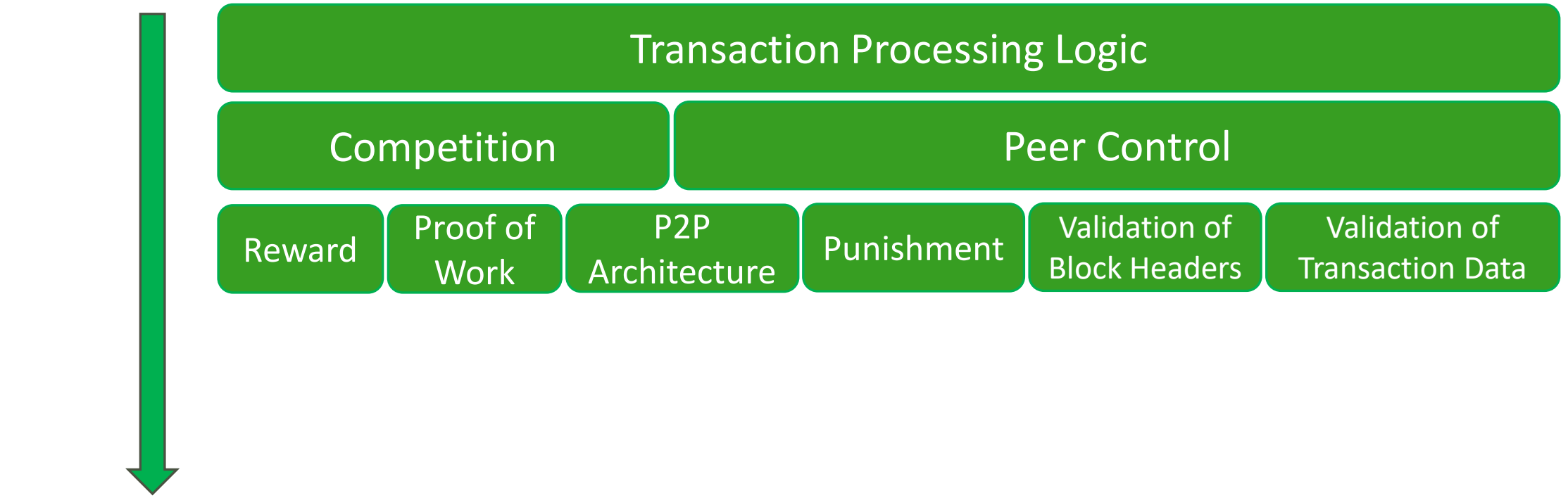
Ownership Logic



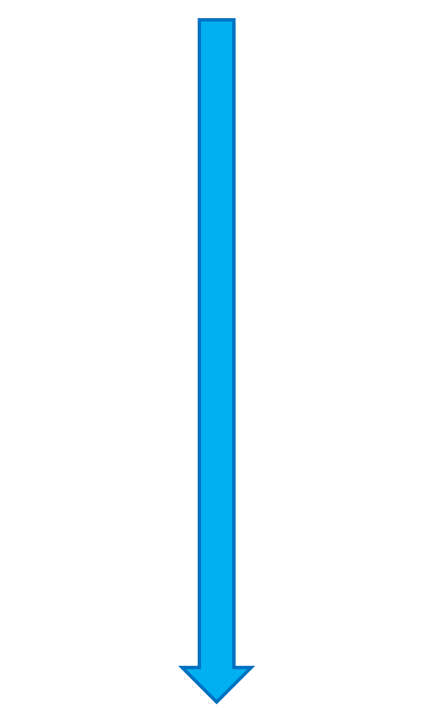
Transaction Security

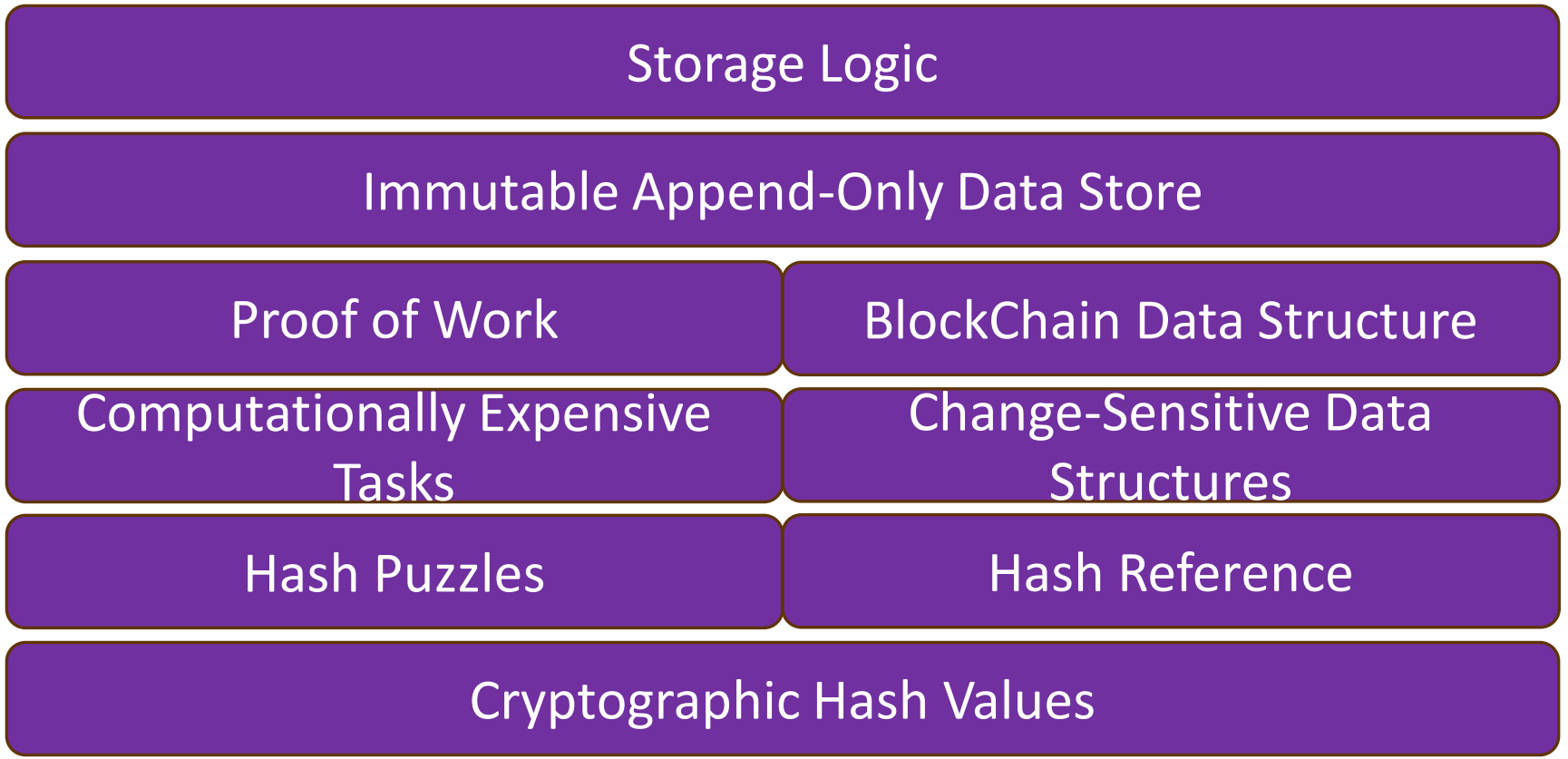


Transaction Processing Logic

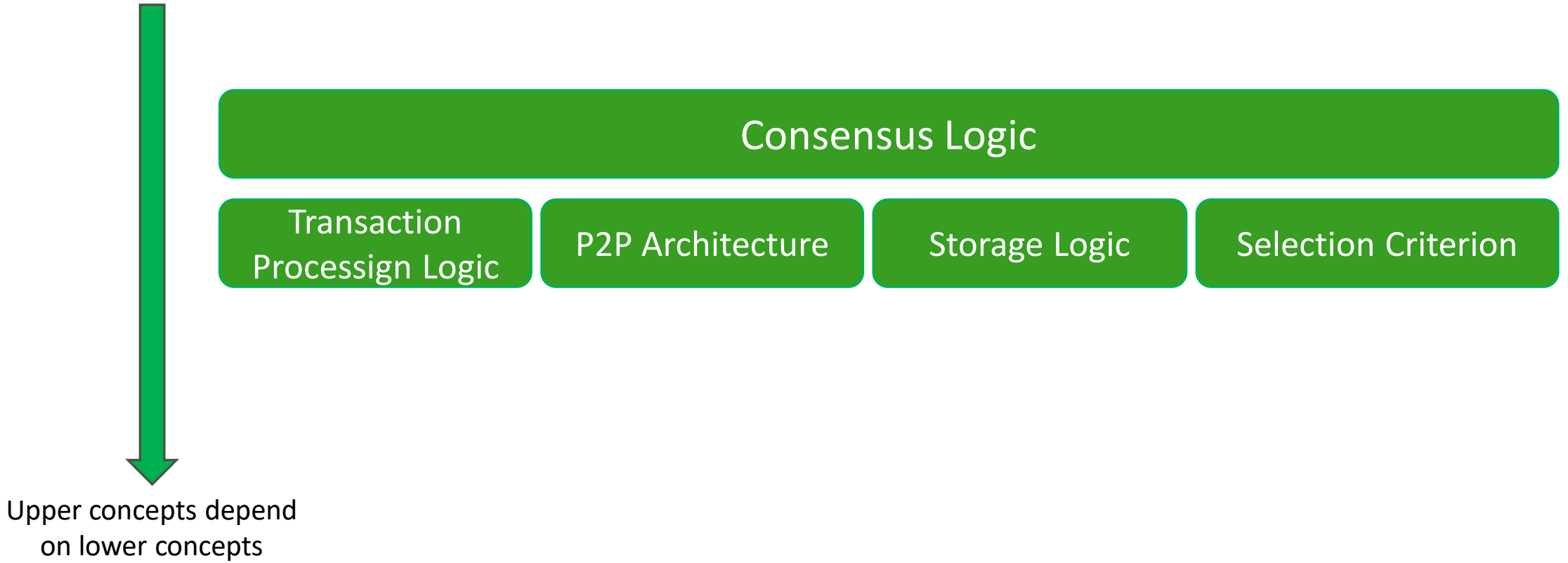


Storage Logic

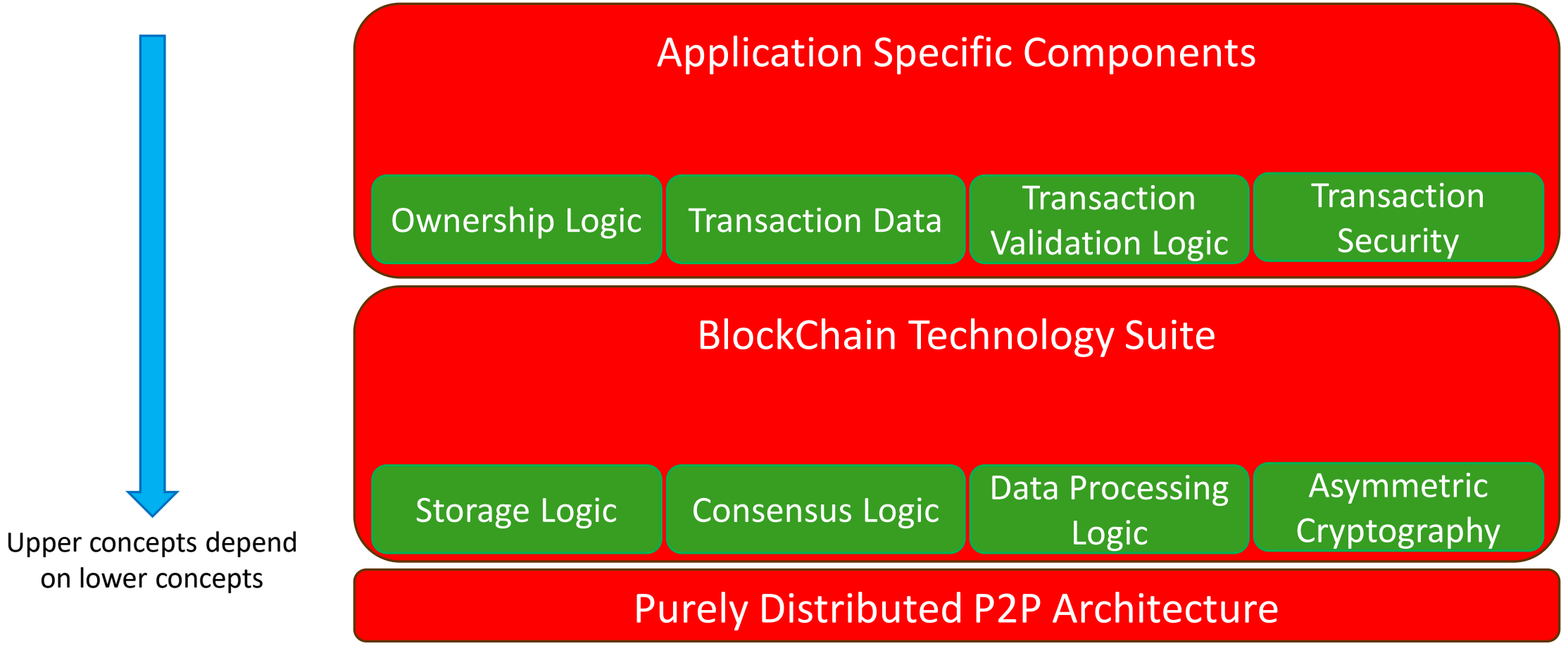




Consensus Logic



Abstraction



Βιβλιογραφία

Blockchain Basics
A Non-Technical Introduction in 25 Steps