BCDV 1001
Intro to Blockchain

(prev. Blockchain Architecture BCDV 1003)

[WEEK 01 - LESSON 02]

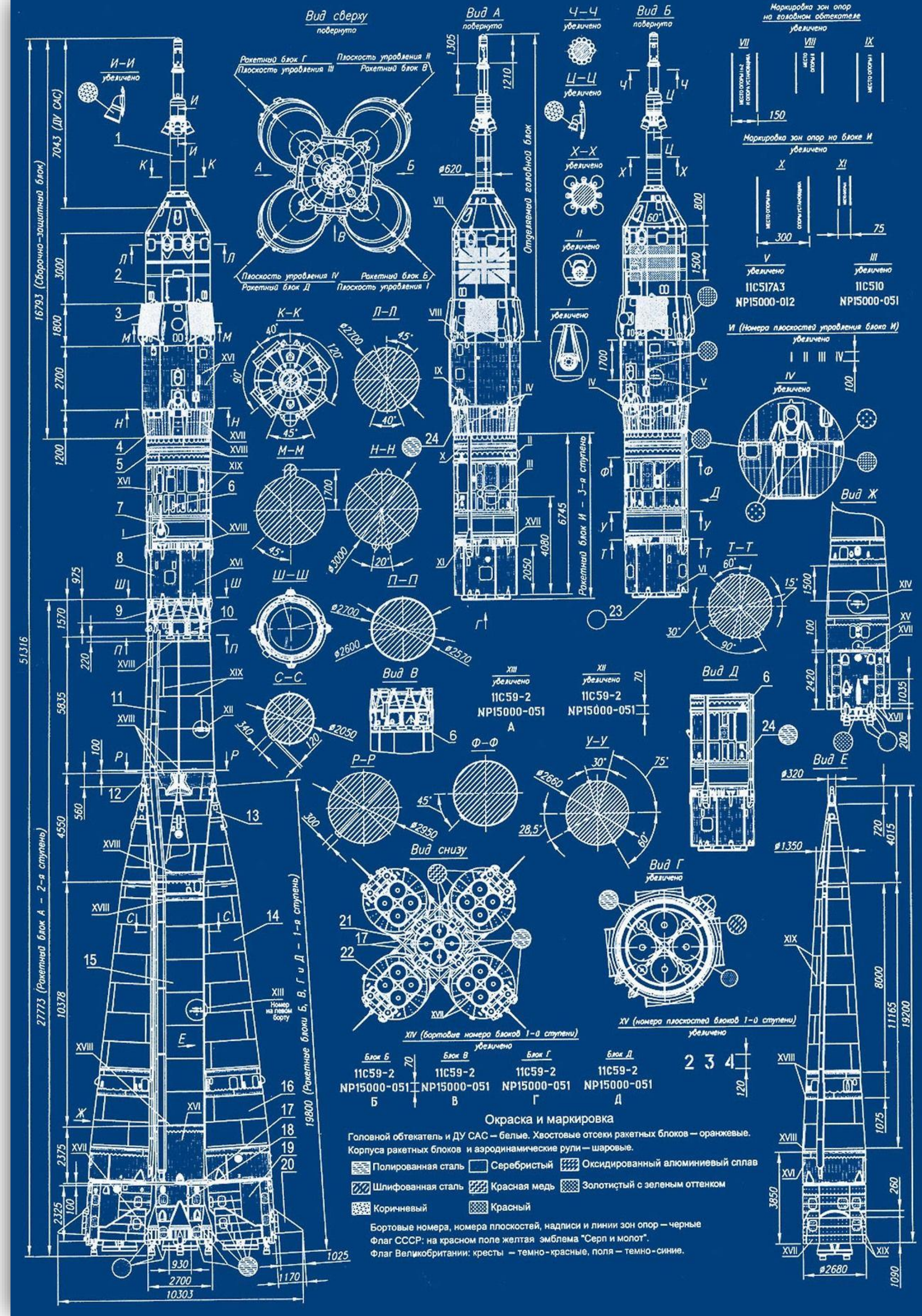
Prof: Djordje (George) Petrovic

djordje.petrovic@georgebrown.ca

Summary

- Lab Test 01
- Lab Exercise 01

- Blockchain Benefits
- Types of blockchains
- Blockchain Layers
- Consensus Mechanisms
- Data and blockchain
- Side chains / Off-chain
- Cost of data
- Oracles and Smart contracts
- Types of Oracles


Вид сверху
Вид А
Вид Б
Вид В
Вид Г
Вид Д
Вид Е
Вид Ж
Вид снизу
Окраска и маркировка
Головной обтекатель и ДУ САС – белые. Хвостовые отсеки ракетных блоков – оранжевые.
Корпуса ракетных блоков и аэродинамические рули – шаровые.
Полированная сталь
Серебристый
Оксидированный алюминиевый сплав
Шлифованная сталь
Красная медь
Золотистый с зеленым оттенком
Коричневый
Красный
Бортовые номера, номера плоскостей, надписи и линии зон опор – черные
Флаг СССР: на красном поле желтая эмблема "Серп и молот".
Флаг Великобритании: кресты – темно-красные, поля – темно-синие.
11С59-2
NP15000-051
11С517А3
NP15000-012
11С510

Course Outcomes

✓Describe the basic structure of a Blockchain Framework;

✓Compare and Contrast Permissioned and Permission-less Blockchain frameworks;

❑Evaluate applicability of a blockchain framework;

❑Assess blockchain consensus requirements for a given use case scenario;

Left overs from pervious class…

- How much time per day do you spend on studying/researching?
- What are good sources of information…
- Google blockchain, but google images (a picture is worth 1,000 words);
- How blockchain works? The process and the mining…
- OSI 7 layer model… how internet works…
- People wouldn't need nor do they have to know how blockchain works only to know that the application runs or uses blockchain…

Deloitte. EY accenture McKinsey & Company BCG experts in the industry…

Reminder from previous week…

- Mining and Creation of Blocks…
- Anders MIT video (video + 15 minutes demo to play with it) [LINK]

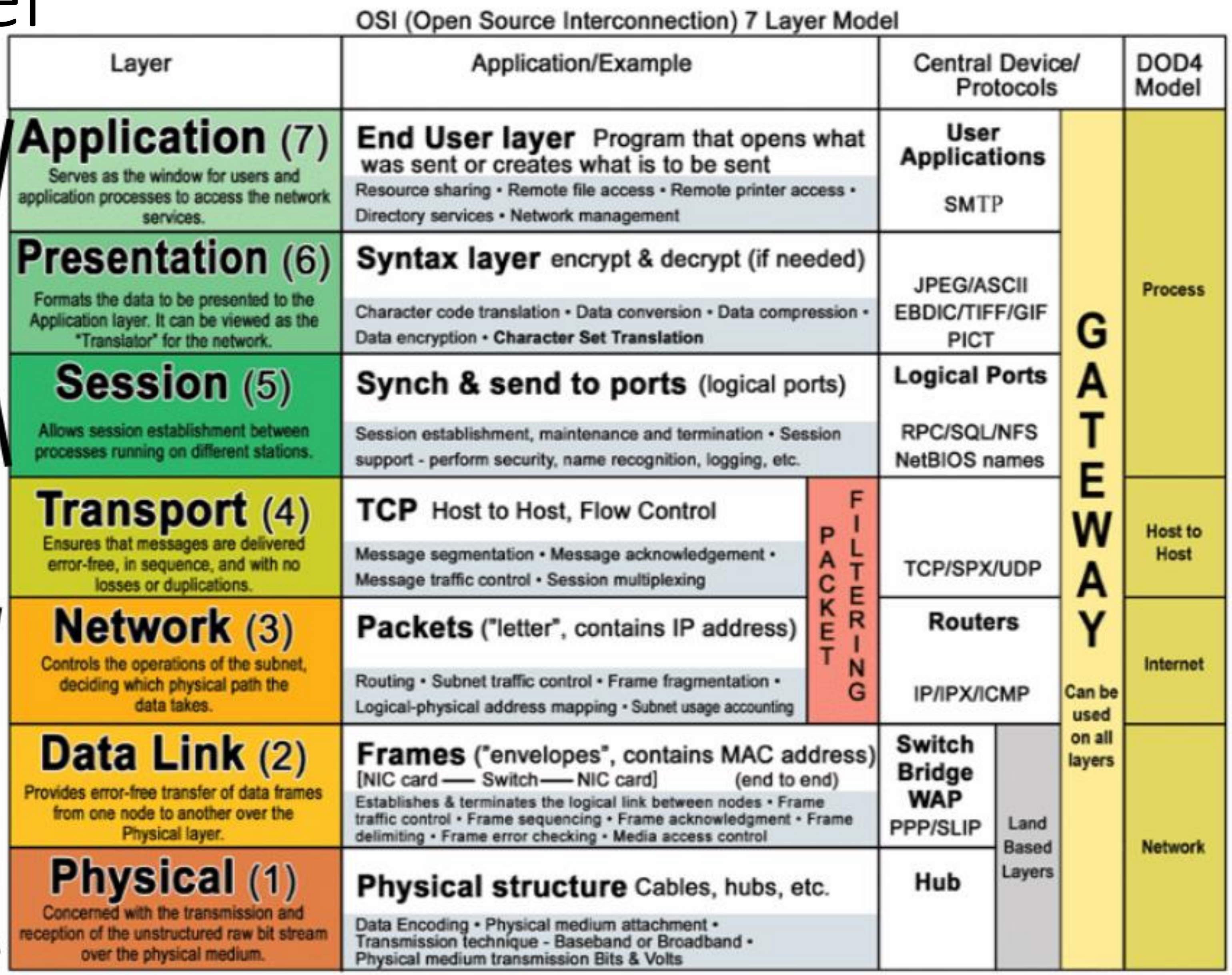
OSI 7 Layer Model

[how internet works]

Not on exam!
Visualize the internet…
As we will do the same for blockchain…

Upper Layers

Lower Layers



OSI (Open Source Interconnection) 7 Layer Model

Layer	Application/Example		Central Device/ Protocols			DOD4 Model
Application (7) Serves as the window for users and application processes to access the network services.	**End User layer** Program that opens what was sent or creates what is to be sent Resource sharing • Remote file access • Remote printer access • Directory services • Network management		**User Applications** SMTP		**GATEWAY** Can be used on all layers	Process
Presentation (6) Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network.	**Syntax layer** encrypt & decrypt (if needed) Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation**		JPEG/ASCII EBDIC/TIFF/GIF PICT			
Session (5) Allows session establishment between processes running on different stations.	**Synch & send to ports** (logical ports) Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc.		**Logical Ports** RPC/SQL/NFS NetBIOS names			
Transport (4) Ensures that messages are delivered error-free, in sequence, and with no losses or duplications.	**TCP** Host to Host, Flow Control Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing	PACKET FILTERING	TCP/SPX/UDP			Host to Host
Network (3) Controls the operations of the subnet, deciding which physical path the data takes.	**Packets** ("letter", contains IP address) Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting		**Routers** IP/IPX/ICMP			Internet
Data Link (2) Provides error-free transfer of data frames from one node to another over the Physical layer.	**Frames** ("envelopes", contains MAC address) [NIC card — Switch — NIC card] (end to end) Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control		**Switch** **Bridge** **WAP** PPP/SLIP	Land Based Layers		Network
Physical (1) Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium.	**Physical structure** Cables, hubs, etc. Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts		**Hub**			

Types of Blockchain

- Public / Private / Consortium (Enterprise, Hybrid…)

- Main considerations when selecting a blockchain framework to develop your application on:
  - ❑PERMISSIONS
  - ❑PERFORMANCE
  - ❑PRIVACY
  - ❑CONSENSUS MECHANISMS

PUBLIC vs PRIVATE blockchain

- The major difference between public and private blockchain is **key generation**: can anyone generate a public and private key-pair to create an identity that can interact with the blockchain, or is there an **identification process** and permissioned access required?

- This impacts both **permissions** and **privacy**.

Permissionless (Open or Public)

1/2

- Permissionless/public blockchains are transparent and openly accessible. The entire transaction history is available for anyone to view or download; they can run the software and create nodes to participate in the consensus and validation process; and they can generate key-pairs and addresses, and submit transactions or develop and deploy smart contracts which alter the global state without the need to identify themselves.

- While this makes for a permisionless and decentralized system where you an interact with a degree of **privacy** in regards to identity, the transaction history associated with that identity is completely open due to the transparent nature of public blockchains.

Permissionless (Open or Public)

2/2

- Permissionless blockchains also tend to have a native token that is used to incentivize users and is tied to the **consensus mechanism**. The block **rewards for miners** in Proof-of-Work networks and the fees for executing transactions are distributed in this **token**.
- The **consensus** mechanism that a particular blockchain employs has a large impact on the **performance** of the framework and will affect the speed at which transactions are processed, and the functionality of your application.
- Governance in a permisionless model is generally implemented through the **consensus** layer with a 50% + 1 voting model.

Permissioned (Closed or Private)

1/3

- In a permissioned/private network you have the ability to decide which entities can participate in terms of clients, validators, and nodes, and define which operations they have access to by **controlling permissions** such as: reading transaction history, calling smart contract functions, or sending transactions.
- The ability to control the access to data allows for a higher degree of **privacy** for sensitive material while still ensuring transparency of less personal data records.
- Most private blockchain frameworks have the functionality to create tokenized digital assets, but few have an economically incentivized consensus model and therefore have no need for a native token.

Permissioned (Closed or Private)

2/3

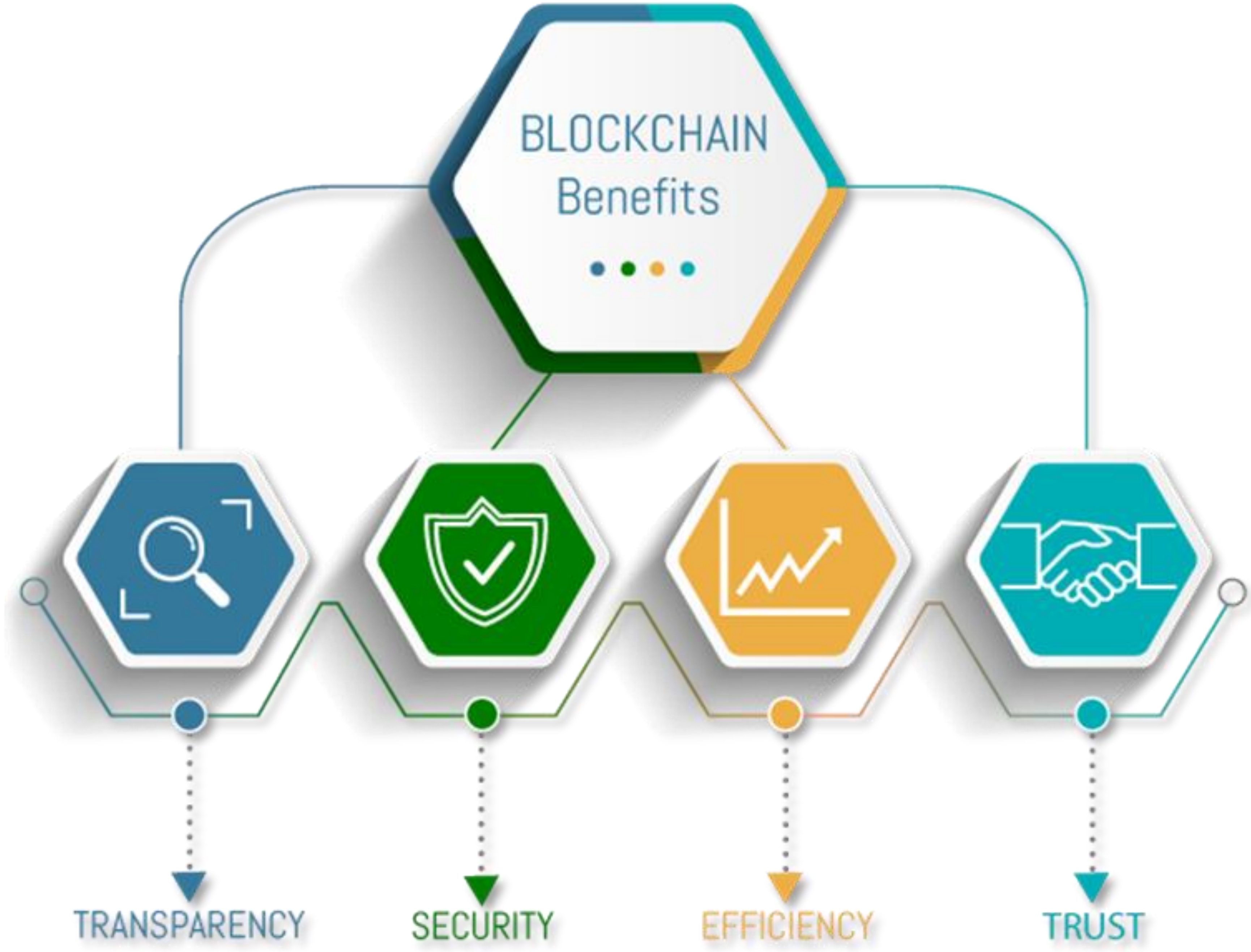
- Private blockchain frameworks offer a variety of different governance models when it comes to making administrative changes.
- **Hyperledger Sawtooth** can run as either a public or a private blockchain, and has two governance options that are implemented through the Settings Transaction Family. You can choose a single authorized key that is allowed to make changes to the network, or a list of authorized keys and a set minimum number of votes to approve proposed changes.

Permissioned (Closed or Private)

3/3

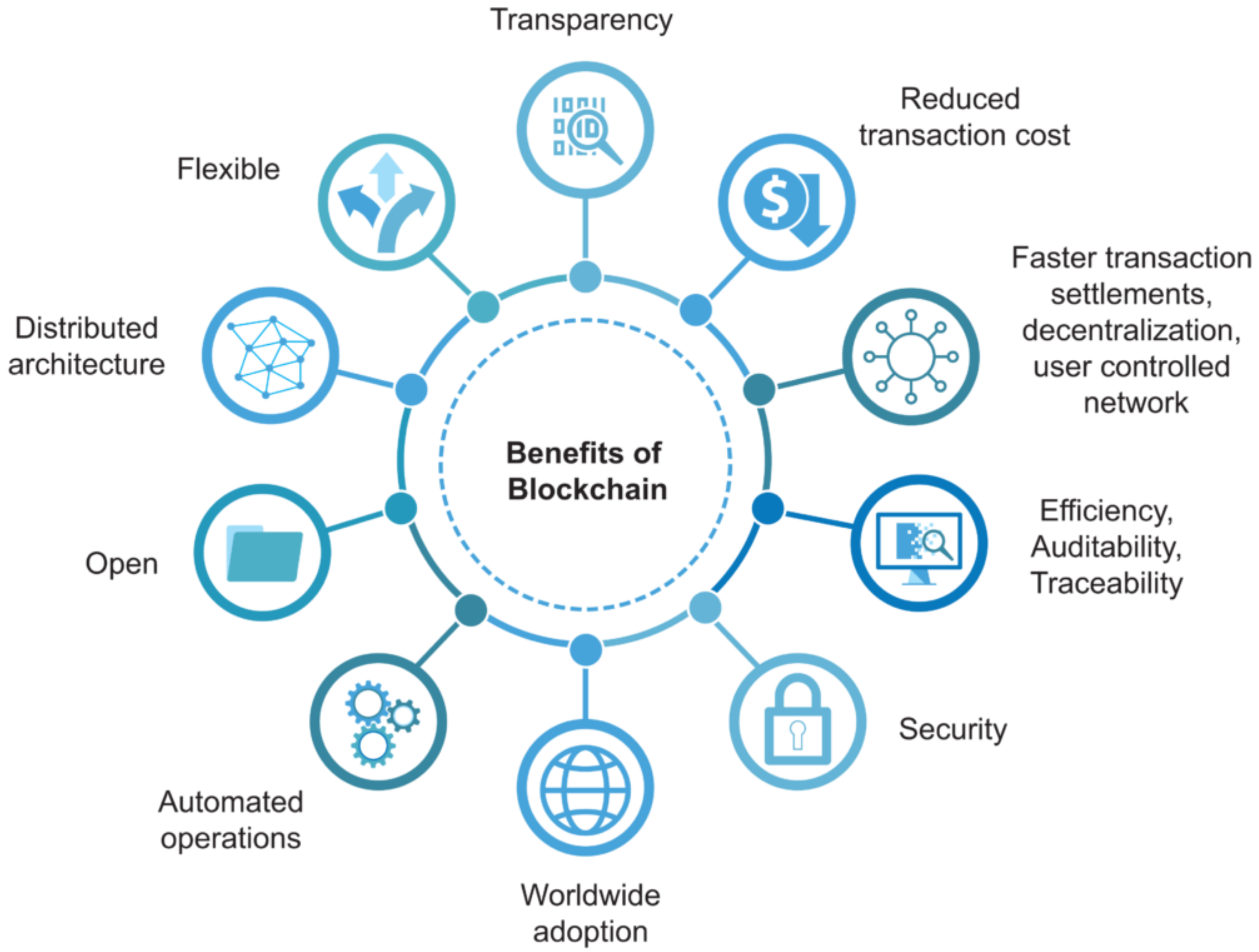
- Some of the changes contained in this transaction family are your chosen target wait time for Sawtooth's PoET lottery style consensus mechanism, and your preferred maximum number of transactions per block. The low-performance requirements of this consensus mechanism should allow for a very high transaction throughput and significant **performance** improvements over most existing **consensus** mechanisms.

- Because of the separation of the network and the application layer, and the modular design which defines these rules in one place and the rest of the framework references them, it means that on an approved vote changes can be dynamically updated without negatively impacting the applications running on the network.

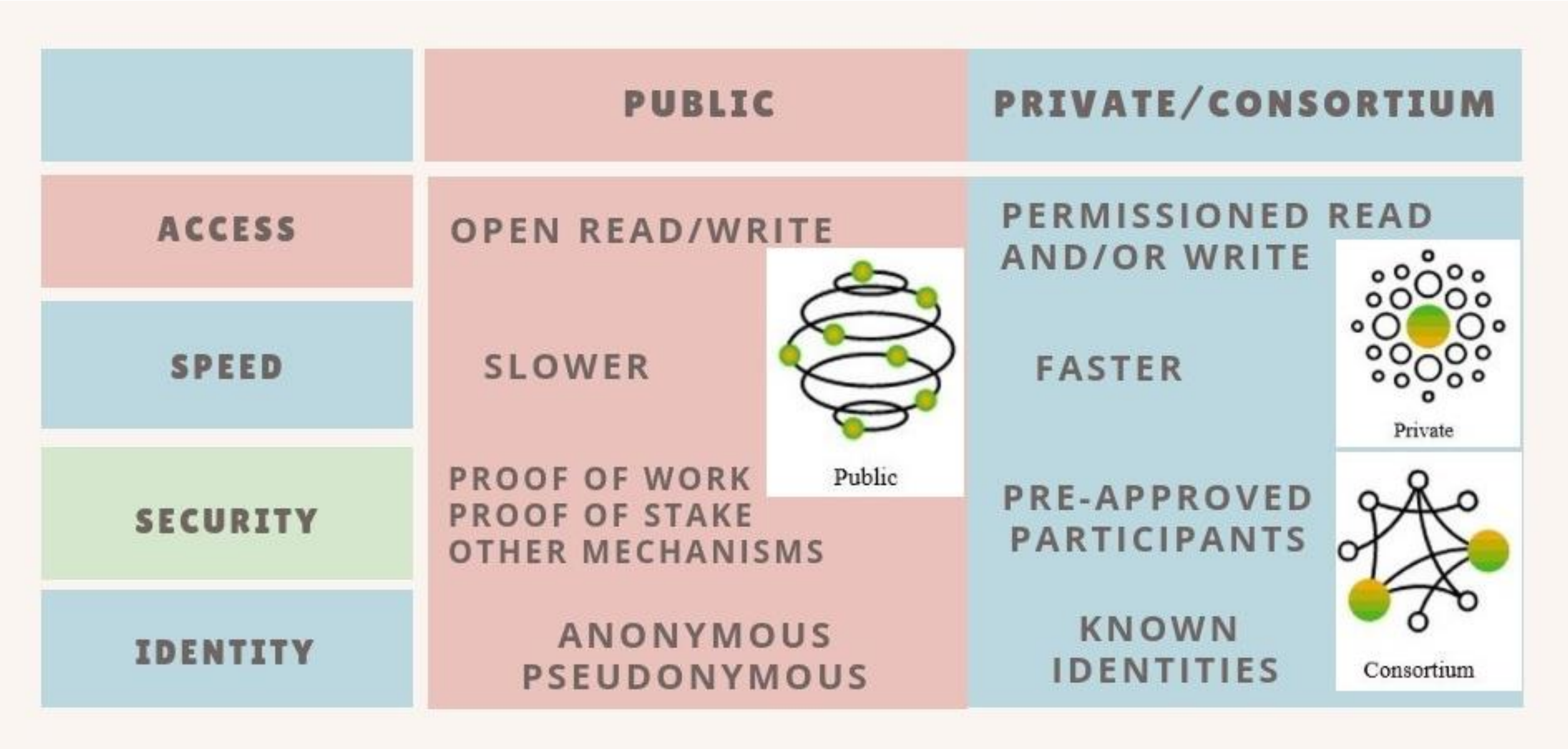

BLOCKCHAIN
Benefits
TRANSPARENCY
SECURITY
EFFICIENCY
TRUST

Blockchain Benefits

[more]



Types of blockchains



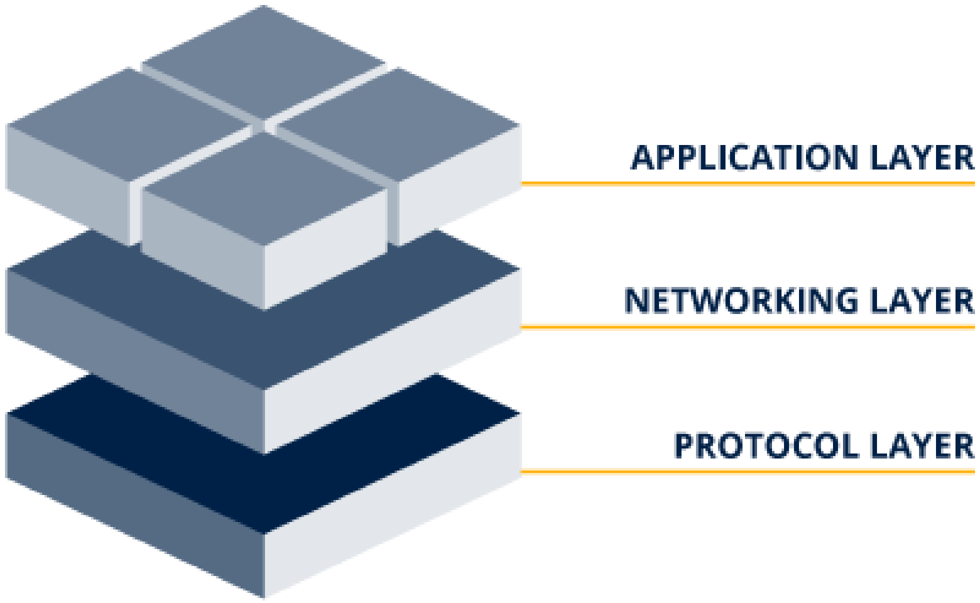
	PUBLIC	PRIVATE/CONSORTIUM
ACCESS	OPEN READ/WRITE	PERMISSIONED READ AND/OR WRITE
SPEED	SLOWER	FASTER
SECURITY	PROOF OF WORK PROOF OF STAKE OTHER MECHANISMS	PRE-APPROVED PARTICIPANTS
IDENTITY	ANONYMOUS PSEUDONYMOUS	KNOWN IDENTITIES

Public
Private
Consortium

Blockchain Layers

[the blockchain Development Stack]

THE BLOCKCHAIN DEVELOPMENT STACK



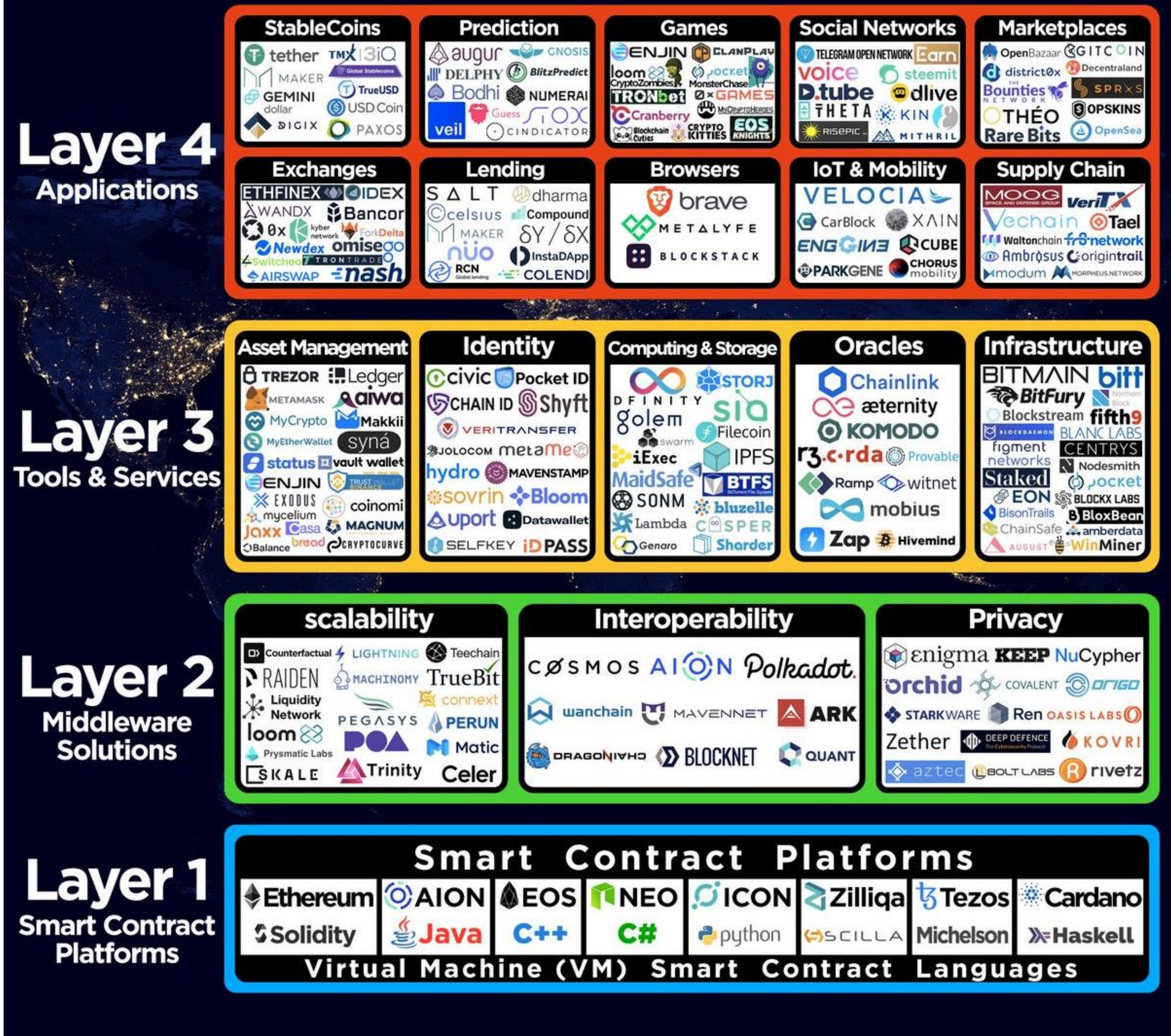
APPLICATION LAYER

NETWORKING LAYER

PROTOCOL LAYER

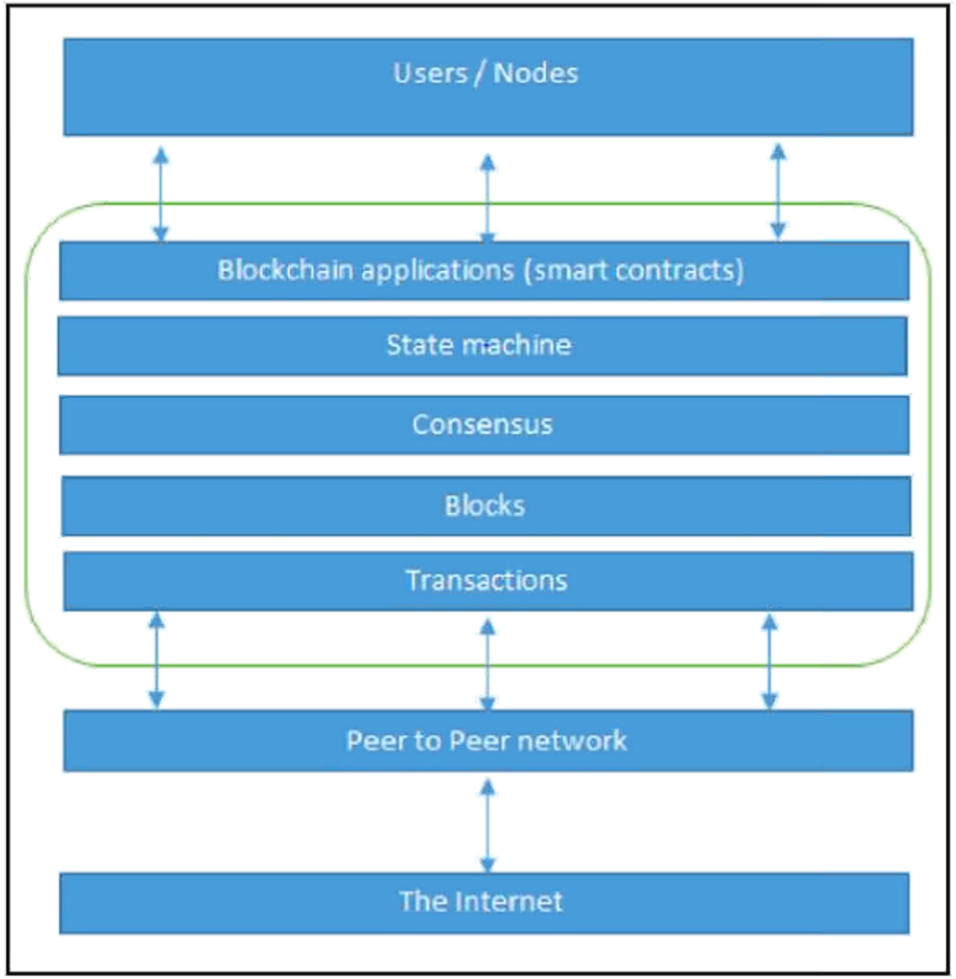
Blockchain ecosystem

[blockchain technology stack]



Blockchain Layers

Network view of a Blockchain

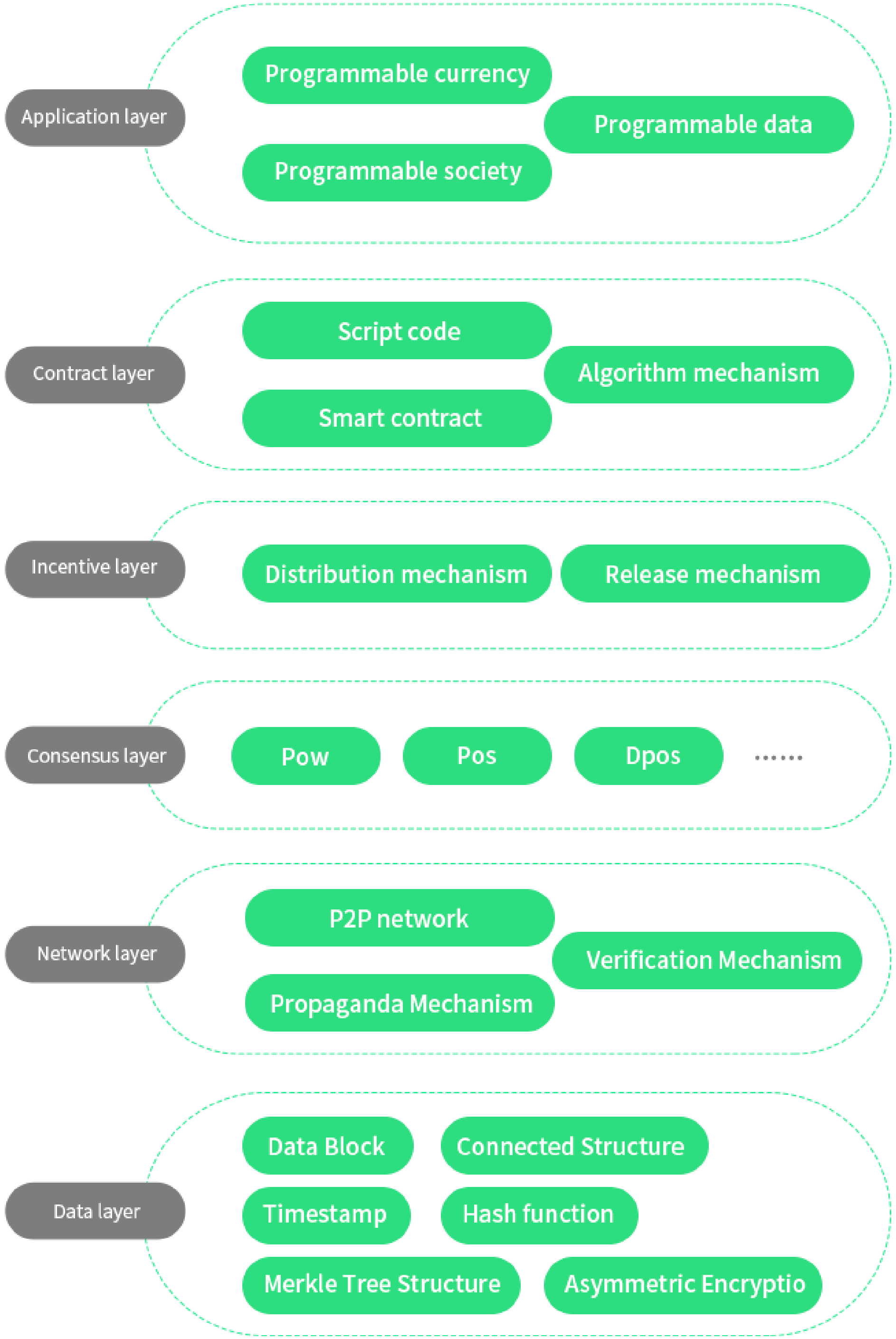


Bashir, I., 2017. *Mastering blockchain*. Packt Publishing Ltd.

Blockchain Layers

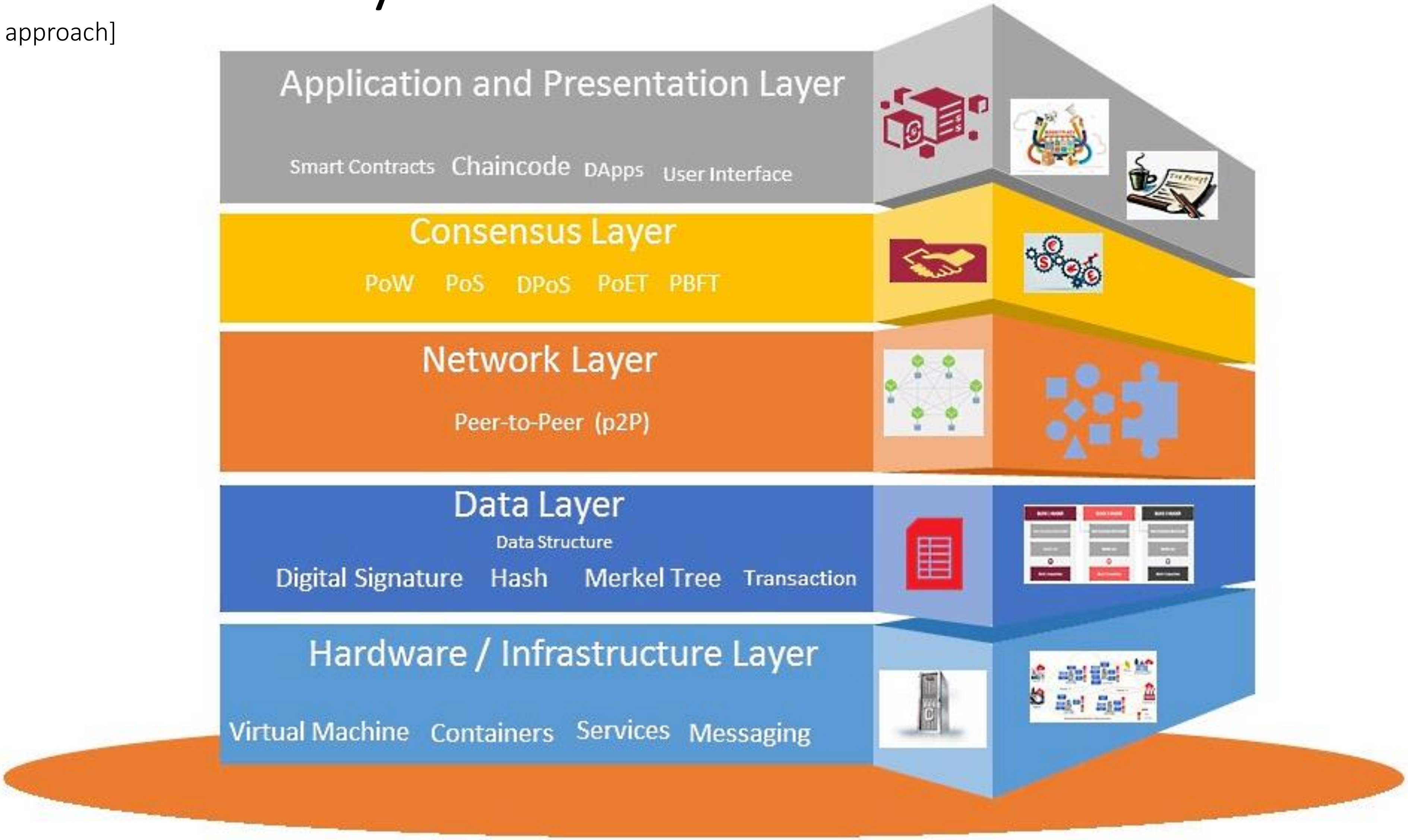
[different approach]

- The blockchain infrastructure is divided into 6 layers, including data layer, network layer, consensus layer, incentive layer, contract layer, and application layer. Each layer completes a core function, and each layer cooperates to achieve a decentralized trust mechanism.



Blockchain Layers

[different approach]



Application and Presentation Layer

Smart Contracts Chaincode DApps User Interface

Consensus Layer

PoW PoS DPoS PoET PBFT

Network Layer

Peer-to-Peer (p2P)

Data Layer

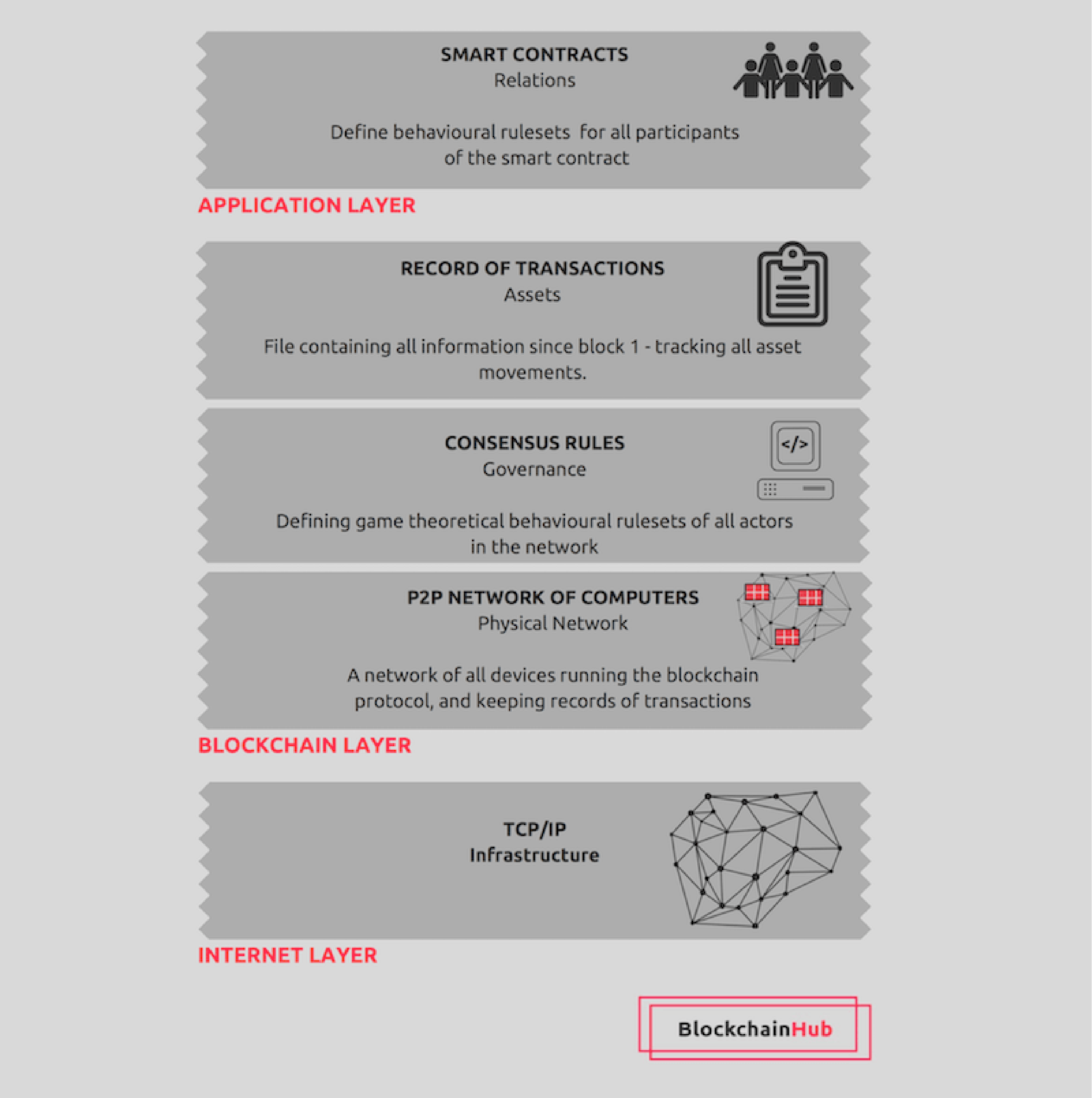
Data Structure

Digital Signature Hash Merkel Tree Transaction

Hardware / Infrastructure Layer

Virtual Machine Containers Services Messaging

More Layers…



SMART CONTRACTS
Relations

Define behavioural rulesets for all participants of the smart contract

APPLICATION LAYER

RECORD OF TRANSACTIONS
Assets

File containing all information since block 1 - tracking all asset movements.

CONSENSUS RULES
Governance

Defining game theoretical behavioural rulesets of all actors in the network

P2P NETWORK OF COMPUTERS
Physical Network

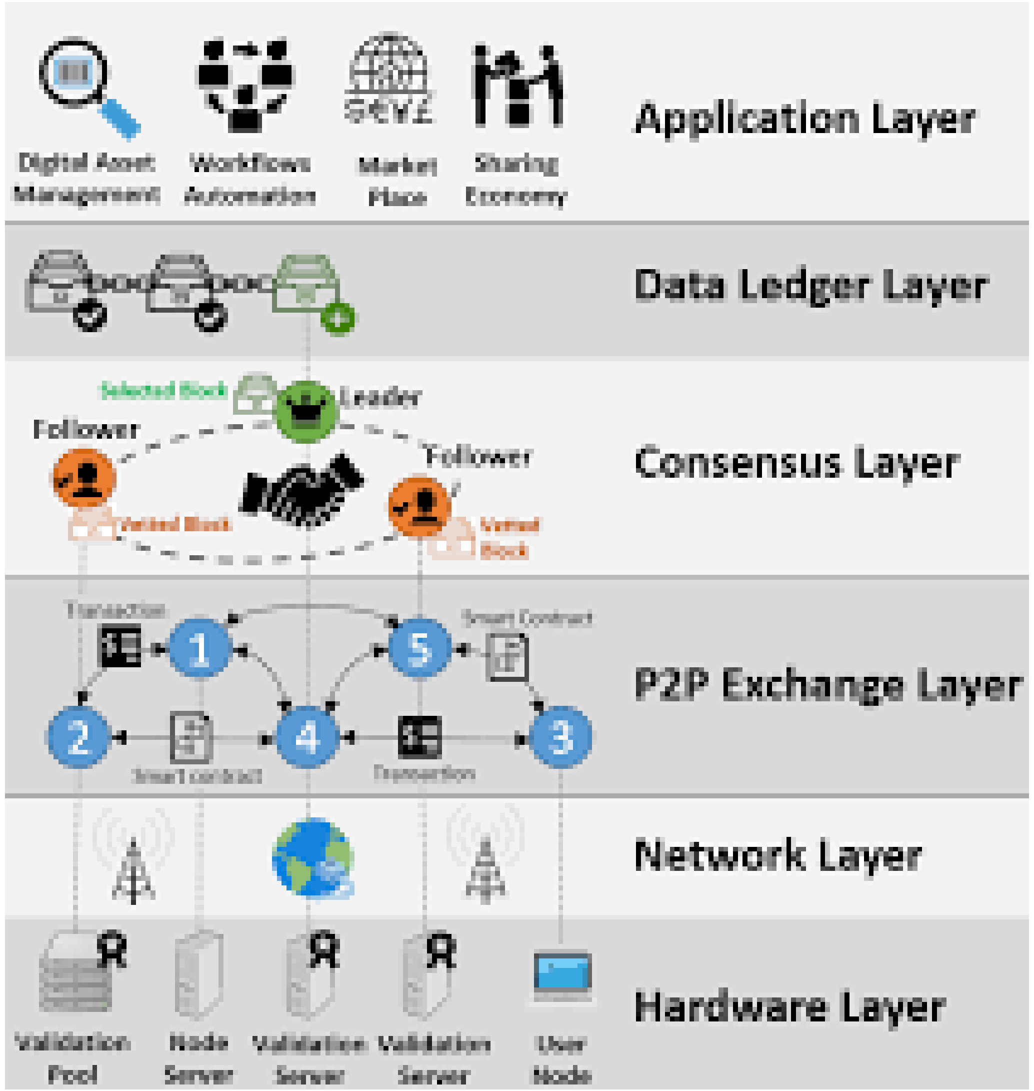
A network of all devices running the blockchain protocol, and keeping records of transactions

BLOCKCHAIN LAYER

TCP/IP
Infrastructure

INTERNET LAYER

More Layers…



Digital Asset Management
Workflows Automation
Market Place
Sharing Economy
Application Layer
Data Ledger Layer
Selected Block
Leader
Follower
Follower
Vetted Block
Vetted Block
Consensus Layer
Transaction
Smart Contract
1
5
2
4
3
Smart contract
Transaction
P2P Exchange Layer
Network Layer
Validation Pool
Node Server
Validation Server
Validation Server
User Node
Hardware Layer

Recap from last class…

- What are the types of blockchains?
- What makes different types of blockchain different?
- Permission vs Permission-less // Open vs Closed
- Biggest problem with blockchain… scalability!
- Your labs are milestones towards your assignment!

Short video clips…

- What is blockchain? (6min) [LINK]

❖USE CASES…

  - Walmart & IBM (3min) [LINK]
  - Money/crypto (3min) [LINK]
  - Financial Institutions/Business+ (6min) [LINK]
  - Estonia Government: e-residency [LINK]; e-health (5min) [LINK]
  - Dimond's (1.5min) [LINK]
  - Royal Mint (2min) [LINK]

Reminder: Blockchain Architecture Terms

[reminder to create and update your list]

Permissioned | Permission-less | Private | Public | Consortium/Hybrid | Consensus Mechanisms| PoW | PoS | PoET | Centralized | Distributed | Decentralized | Hyperledger | Ethereum | Bitcoin | Hash | Merkel Tree/Root | P2P | 51% Attack | Blockchain 1.0 2.0 3.0 | Sidechains | Oracle | Smart contract | Data storage | Off-chain |

Agenda for today

❑Consensus Mechanisms

❑Data & Blockchain

❑Side chains /Off-chain

❑Oracles

Consensus Mechanisms

Blockchain are not a truth machine!

So, how do blockchains networks make and agree on decisions?

Consensus Mechanisms

- One of the **primary selling points of blockchains networks is decentralization** – they can **function even in the absence of a central authority.**

- However, since decisions about future development and maintenance of the projects still have to be made, a **consensus algorithm allows network participants to arrive at a common decision.**

Consensus Mechanisms

"The purpose of a consensus algorithm is to allow for the secure updating of a state according to some specific state transition rules, where the right to perform the state transitions is distributed among the users of a particular economic set"

- Vitalik Buterin, Ethereum -

Consensus Mechanisms

- This proliferation of consensus algorithms can be attributed to the **blockchain scalability trilemma**, a term that refers to the technology’s various bottlenecks.
- While an ideal distributed network would excel at security, decentralization, and throughput, most digital currencies today have only managed to obtain one or two of those characteristics.
- As a result, **developers are constantly working on new consensus algorithms** to build a close-to-perfect blockchain network.

At which stage is the consensus used

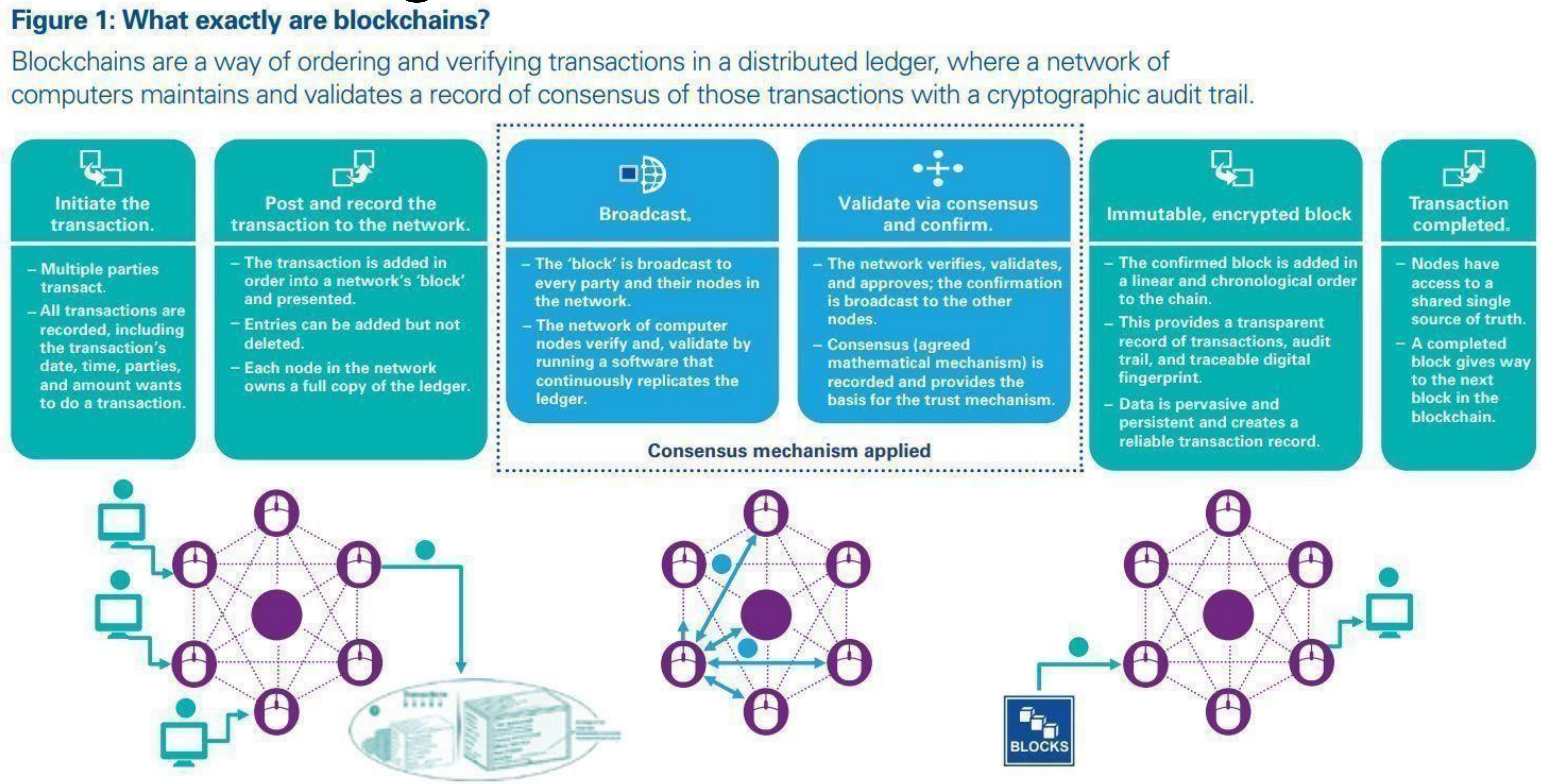


Figure 1: What exactly are blockchains?

Blockchains are a way of ordering and verifying transactions in a distributed ledger, where a network of computers maintains and validates a record of consensus of those transactions with a cryptographic audit trail.

Initiate the transaction.

- Multiple parties transact.
- All transactions are recorded, including the transaction's date, time, parties, and amount wants to do a transaction.

Post and record the transaction to the network.

- The transaction is added in order into a network's 'block' and presented.
- Entries can be added but not deleted.
- Each node in the network owns a full copy of the ledger.

Broadcast.

- The 'block' is broadcast to every party and their nodes in the network.
- The network of computer nodes verify and, validate by running a software that continuously replicates the ledger.

Validate via consensus and confirm.

- The network verifies, validates, and approves; the confirmation is broadcast to the other nodes.
- Consensus (agreed mathematical mechanism) is recorded and provides the basis for the trust mechanism.

Consensus mechanism applied

Immutable, encrypted block

- The confirmed block is added in a linear and chronological order to the chain.
- This provides a transparent record of transactions, audit trail, and traceable digital fingerprint.
- Data is pervasive and persistent and creates a reliable transaction record.

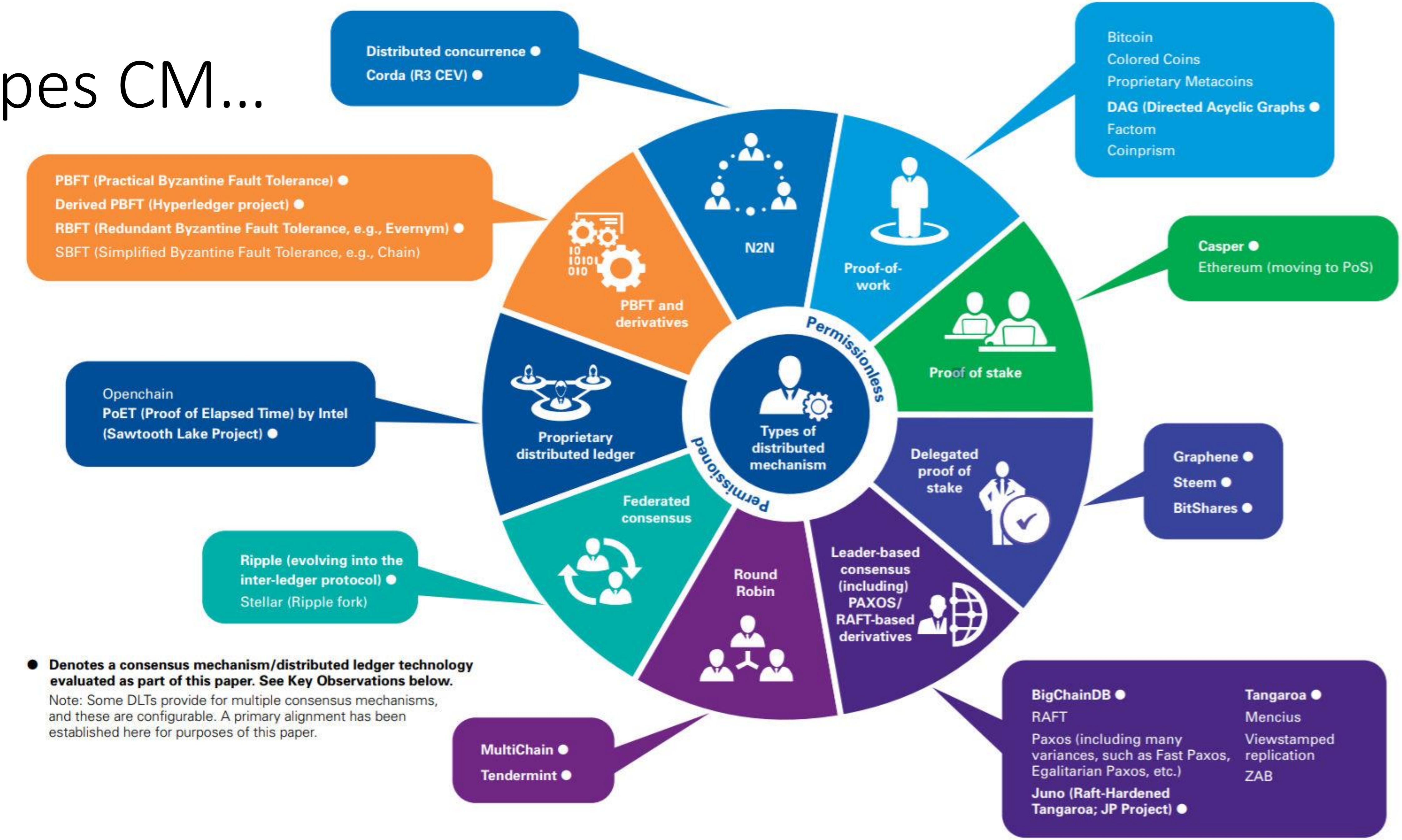
Transaction completed.

- Nodes have access to a shared single source of truth.
- A completed block gives way to the next block in the blockchain.

Consensus are the Core to Blockchain

- Without central authority, participants **have to agree on rules and how to apply them.**
- Consensus mechanism is a **set of rules and procedures** that maintains a coherent set of facts among the participating nodes.
- The consensus mechanism is at the **core of Blockchain design** and selection.
- There are **many consensus** mechanisms.

Types CM…



Types of distributed mechanism

Permissionless

Permissioned

N2N

- Distributed concurrence ●
- Corda (R3 CEV) ●

Proof-of-work

- Bitcoin
- Colored Coins
- Proprietary Metacoins
- **DAG (Directed Acyclic Graphs ●**
- Factom
- Coinprism

Proof of stake

- **Casper ●**
- Ethereum (moving to PoS)

Delegated proof of stake

- **Graphene ●**
- **Steem ●**
- **BitShares ●**

Leader-based consensus (including) PAXOS/ RAFT-based derivatives

- **BigChainDB ●**
- RAFT
- Paxos (including many variances, such as Fast Paxos, Egalitarian Paxos, etc.)
- **Juno (Raft-Hardened Tangaroa; JP Project) ●**
- **Tangaroa ●**
- Mencius
- Viewstamped replication
- ZAB

Round Robin

- **MultiChain ●**
- **Tendermint ●**

Federated consensus

- **Ripple (evolving into the inter-ledger protocol) ●**
- Stellar (Ripple fork)

Proprietary distributed ledger

- Openchain
- **PoET (Proof of Elapsed Time) by Intel (Sawtooth Lake Project) ●**

PBFT and derivatives

- **PBFT (Practical Byzantine Fault Tolerance) ●**
- **Derived PBFT (Hyperledger project) ●**
- **RBFT (Redundant Byzantine Fault Tolerance, e.g., Evernym) ●**
- SBFT (Simplified Byzantine Fault Tolerance, e.g., Chain)

● Denotes a consensus mechanism/distributed ledger technology evaluated as part of this paper. See Key Observations below.

Note: Some DLTs provide for multiple consensus mechanisms, and these are configurable. A primary alignment has been established here for purposes of this paper.

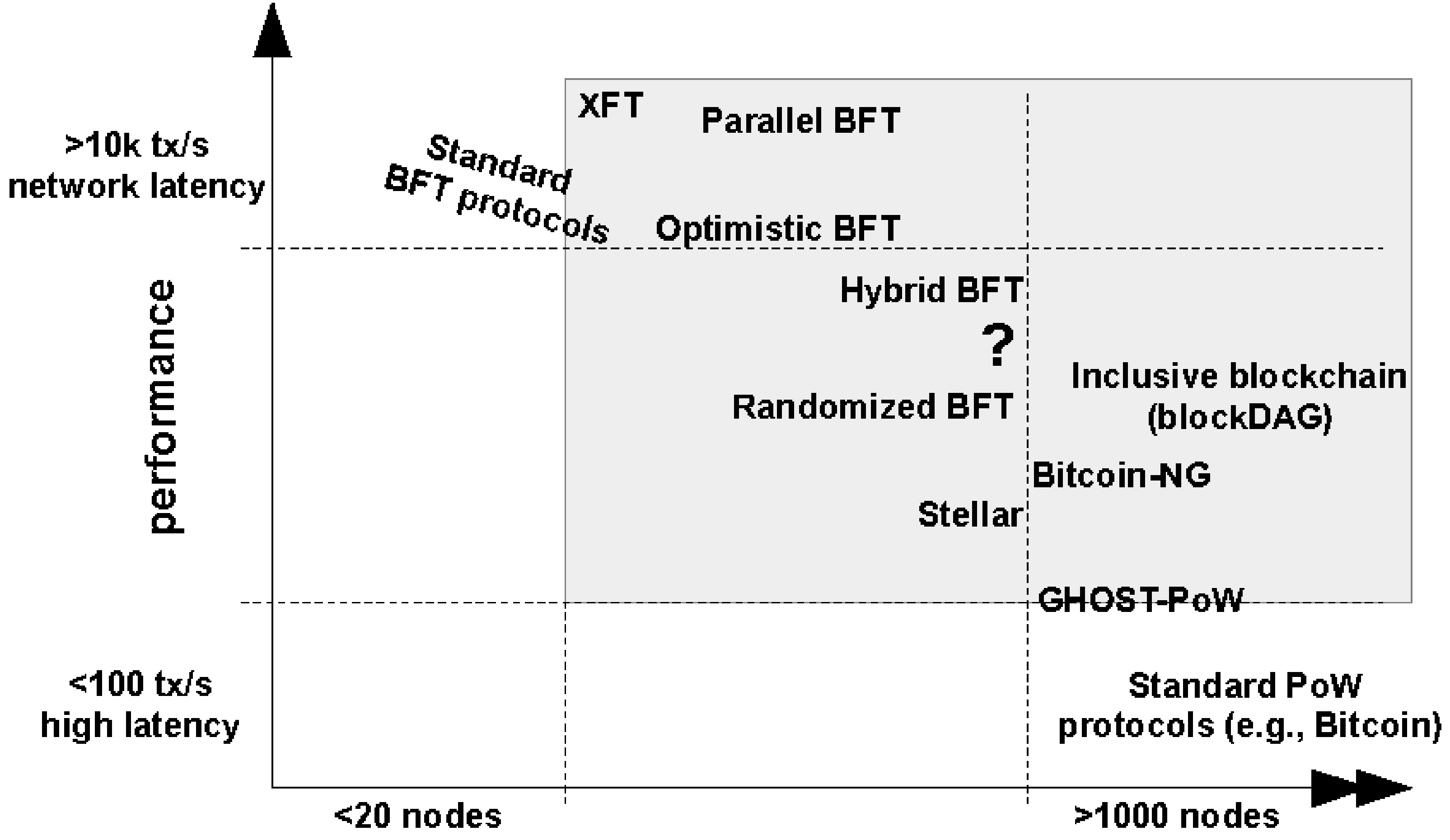
Consensus Mechanisms

	PoW (Bitcoin)	PoS (Ethereum)	PoET (Intel SawTooth)	BFT & Variants (Hyperledger)	Federated BFT (Ripple, Stellar)
Blockchain Type	Permisionless	Both	Both	Permissioned	Permissioned
Transaction Finality	Probabilistic	Probabilistic	Probabilistic	Immediate	Immediate
Transaction Rate	Low	High	Medium	High	High
Token Needed?	Yes	Yes	No	No	No
Cost of Participation	Yes	Yes	No	No	No
Number of Peer Nodes	High	High	High	Low	High
Trust Model	Untrusted	Untrusted	Untrusted	Semi-trusted	Semi-trusted

Source: Whitepaper Understanding Blockchain Consensus Models

Split into groups

Scalability



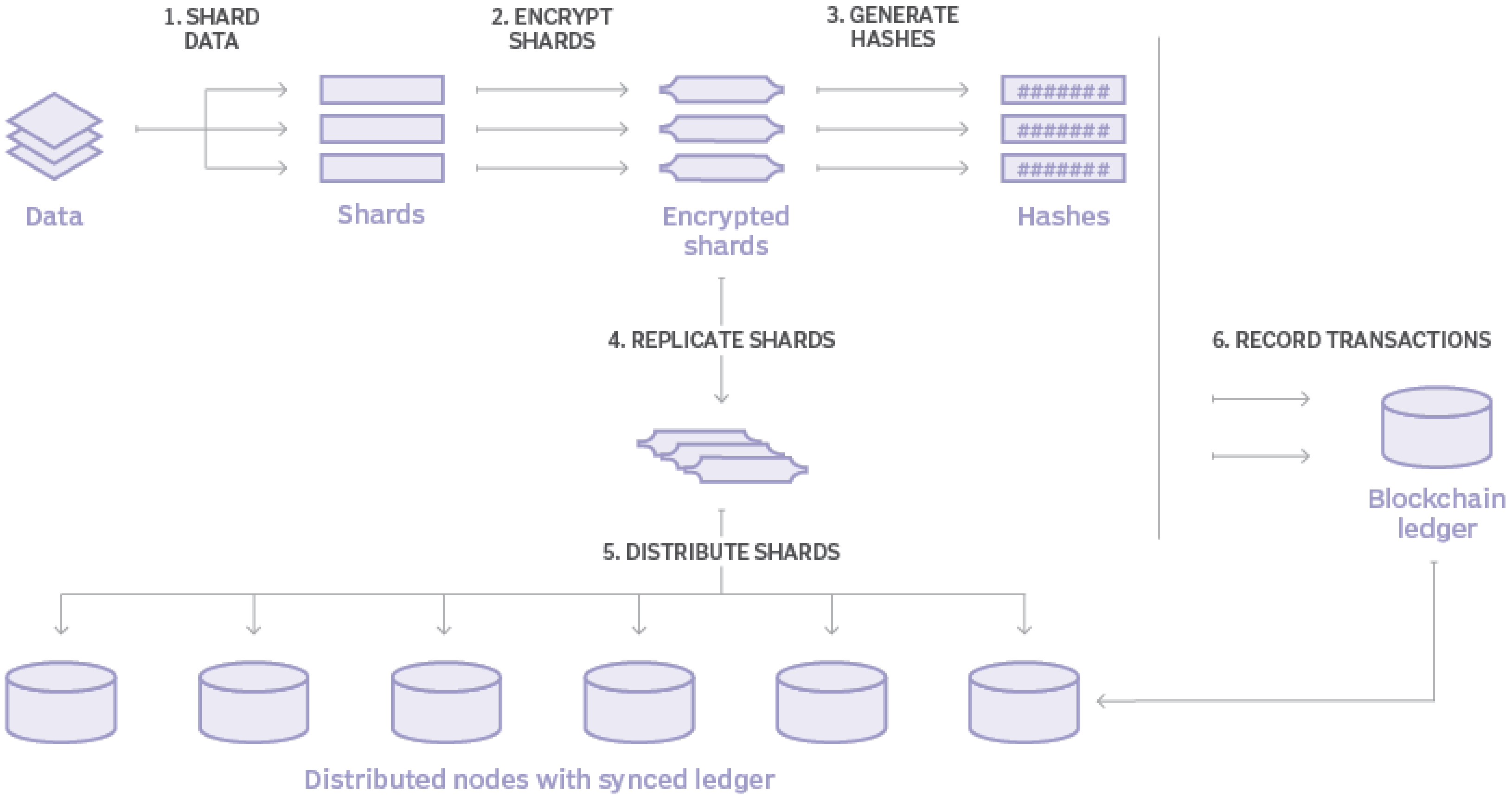
Marko Vukolic, IBM research in Switzerland (excellent paper to read - link)

Data and blockchains

- Blockchains are not designed or meant for data storage and storing large documents would be very expensive.
- What blockchain hold is the hash of the data, and uses it as a reference to the data (fingerprint).
- Blockchains might be used to maintain a Distributed Hash Table (DHT), which contains hashes of data files stored off-chain.
- Blockchain-like solutions designed just to store data were developed recently:
  - ❖STORJ.IO
  - ❖SIA-coin
  - ❖FILECOIN
  - ❖IPFS
  - ❖MaidSafe
  - ❖Sharder
  - ❖BigchainDB

Split into groups

How blockchain storage works



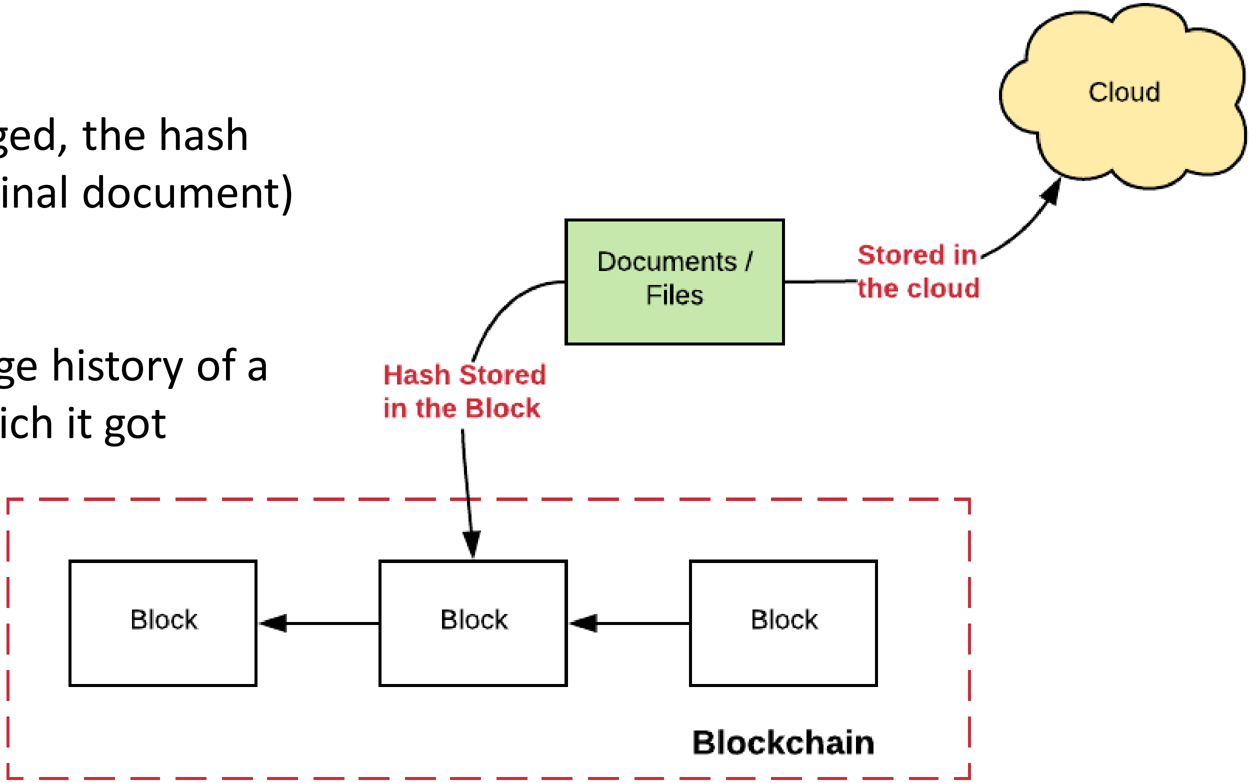
Benefits of storing hashes on blockchain

- Brings the general benefit of the Blockchain in relation to the document, such as **integrity, non-repudiation, authentication** etc.

- Store Document related information: As part of the transaction, information such as **who created the document, version, timestamp** etc. also gets recorded.

- **Minimize the fraud**: In case the document is changed, the hash value won't match with the hash value (of the original document) stored in the blockchain.

- **Document history using the timestamp**: The change history of a particular document vis-a-vis the date/time on which it got changed gets recorded as the digital timestamp.



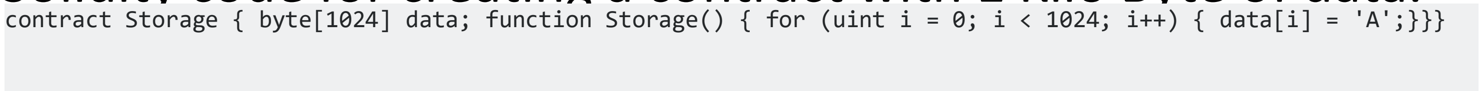
Side-Chains/Off-Chain

- Emerging mechanism that allow tokens and other digital assets to **move from one blockchain (main chain) and to be securely used in a separate blockchain** and then moved back to the original blockchain if needed.
- A side chain is a **separate similar to blockchain** tech that is attached to its parent blockchain using a **two-way peg**. The two-way peg enables interchangeability of assets at a predetermined rate between the parent blockchain and the sidechain.

Cost of Data

Year 2016:

- <u>Storage costs:</u>
  - This is Solidity code for creating a contract with 1 Kilo Byte of data.



```
contract Storage { byte[1024] data; function Storage() { for (uint i = 0; i < 1024; i++) { data[i] = 'A';}}}
```

  - If we run this code in the online compiler, we get an estimated transaction cost of 5925085 gas. The gas price today is 23731285772 Wei (10^18 Wei = 1 Ether = **$15**). So, **storing 1 Kilo Byte of data in the public blockchain**, as per conversion rates on is approximately **$2.11**.
- <u>Reading costs:</u>
  - Similarly, r**eading 1 Kilo Byte** of data costs 284396 gas, which is approximately **$0.1**.
  - This **price might increase if there is an increase in the Gas value or Ether value**.

Smart Contracts

- A smart contract is software code that **runs on a blockchain** network such as Ethereum and **performs actions** or tasks **based on certain events.**
- Such an example is sending Ether; If everything checks out, the network will 'transfer' the funds to the receiver.
- But what if I wanted to **create a decentralized application** that **needed external data** such as the current weather temperature, the price of a stock or even the results of the NBA, NHL, FIFA World Cup finals? How does a smart contract, or, in other words, a piece of code on a blockchain, get this information?

Oracles and Blockchain

So where does the blockchain get the ‘truth’ from the **outside world**?

Smart Contracts and Oracles

- Oracles are **trusted data sources** or entities that provide information or sign claims about the **state of the world** for smart contracts. They are the **link between real world events and the digital world** of blockchain platforms. They **don’t make predictions** about the future but **report events from the past**.
- The **most powerful oracle architecture offers a decentralized network of oracles that connects directly to smart contracts**, and **feeds the data back in a secure manner**. With both **software and hardware security measures**, this ensures **security and tamper-proof data that can be trusted.**

Smart Contracts, Oracles and Trust

- The whole point of the blockchain and its decentralized network was to **remove the need to trust any intermediary and remove any single point of failure so obviously a smart contract that requires trusting a single outside data source is a bit of a contradiction but this can be mitigated by having multiple independent oracles to form a consensus.**

Types of Oracle

SOFTWARE	Handles data sourced online
HARDWARE	Replays offline data from physical world
INBOUND	Passes external data to smart contrast
OUTBOUND	Communicates smart contracts data to outside world
CONSENSUS OF ORACLES	Increased data validity confirmation from several oracles

Blockchain-Oracle projects

AUGUR

GNOSIS

Chain Link

æternity

BLOCKCHAIN

Lab Exercise

[60 minutes]

- Form groups and select a use case from the list…
- Your lab for today will be to research your choice and write a brief draft proposal.
- Your paper should describe the problem that you’re looking to solve as well as any current issues or challenges faced in that particular field, and why you feel that a blockchain solution would be the best option for resolving these things.
- Your write-up should be at minimum a two page draft and includes any relevant links to research resources.
- This will form the basis of your Individual Assignment, so be thorough, think things through, and delegate tasks among your group members.
- Due date for the following class. Present at the begging of the next class minutes each.

- Next week… more one
- Process of Building a block chain
- PoW
- Ethereum & Smart Contracts
- Hyperledger

- Blockchain-as-a-Service