Blockchain fundamentals

KBTU
Askar Aituov

Lecture 1 Distributed Ledger Technology (DLT)

About lecturer

Founding CTO at ClickLog.io

X MD at Techgarden Ventures (Delaware, USA)

XKPMG, XHuawei

Google developers group Astana Community manager

Singularity University Ambassador

Tasks

Activity

Students independent study (SIS)

Teachers supervised independent study of students (TSIS)

Syllabus

Week	Class work			SIS (students independent study	TSIS (teacher supervised independent study)
	Topic	Lectures	Practice		
1	Distributed Ledger Technology (DLT) Laboratory work #1	2	1	Distribution of tasks for SIS1	Distribution of tasks for TSIS1
2	Open Source ledgers Laboratory work #2	2	1		
3	Algorhitms and techniques Laboratory work #3	2	1		
4	Public Key cryptography & Hashes Laboratory work #4	2	1		
5	Decentralized systems Laboratory work #5	2	1		
6	Consensus protocols Laboratory work #6	2	1	SIS1 defense.	
7	Bitcoin and Etherium blockchains Laboratory work #7	2	1		TSIS1 defense
8	Bitcoin’s academic pedigree Laboratory work #8	2	1		Mid-term
9	Etherium Wallets Laboratory work #9	2	1		
10	Application in financial sector Laboratory work #10	2	1		
11	Application in supply chain sector Laboratory work #11	2	1		
12	Introduction to Hyperledger Laboratory work #12	2	1		
13	Hyperledger Fabric Laboratory work #13	2	1	SIS2 defense.	
14	Hyperledger Sawtooth Laboratory work #14	2	1		TSIS2 defense
15	Hyperledger Iroha Laboratory work #15	2	1		
16-17	Final Exam	2		(a quiz and an interview)	

Organizational aspects – information exchange with group

Askar Aituov

A_Aituov@kbtu.kz / aaituov@gmail.com

Telegram: @AskarAi

Phone: +7 771 585 11 00

Telegram chat?

If yes:

Block Chain Technology and applications Айтуов А. Т.

https://t.me/joinchat/H-dQbBk5h3W35h1bWlxZ5g

Lecture 1 - Intro

Larsen describes that a focus on 5G and AI should not overshadow the threat from China with digital currencies and blockchain technology. According to Larsen, the Chinese Government has subsidized vast amounts of energy needed to fuel cryptocurrency "miners".

According to Larsen, "...at least 65 percent of cryptocurrency mining is concentrated in China, which means the Chinese government has the majority needed to wield control over those protocols and can effectively block or reverse transactions".

Lecture 1 - Intro

eventbrite Search for events Browse Events Create Event

event ended

Washington Elite AI Blockchain Summit After Party Sponsored by BlokTech

View Details

Follow this organizer to stay informed on future events

BlokTech Network
Event creator

Follow

Events you might like:

MON, JAN 13 7:00 PM

Miami Blockchain Week

Miami Beach, Miami Beach

TUE, JAN 14 8:00 AM

Washington Elite A.I. Blockchain Summit - Autonomy & Robotics Edition

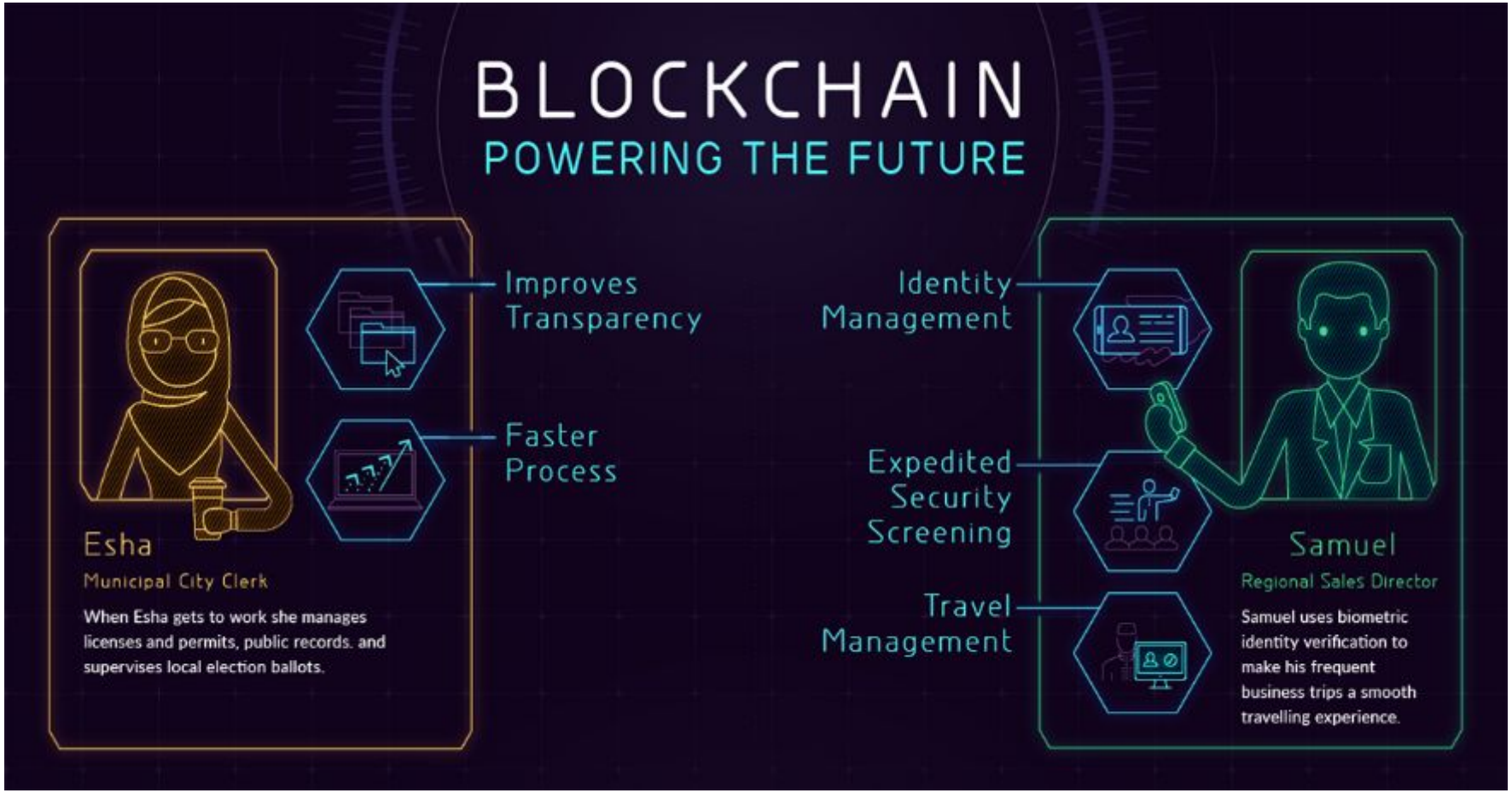
El Dorado 305, Miami

WED, JUL 22 8:00 AM

Mining Disrupt Conference 2020 | Bitcoin Blockchain Cryptocurrency Mining

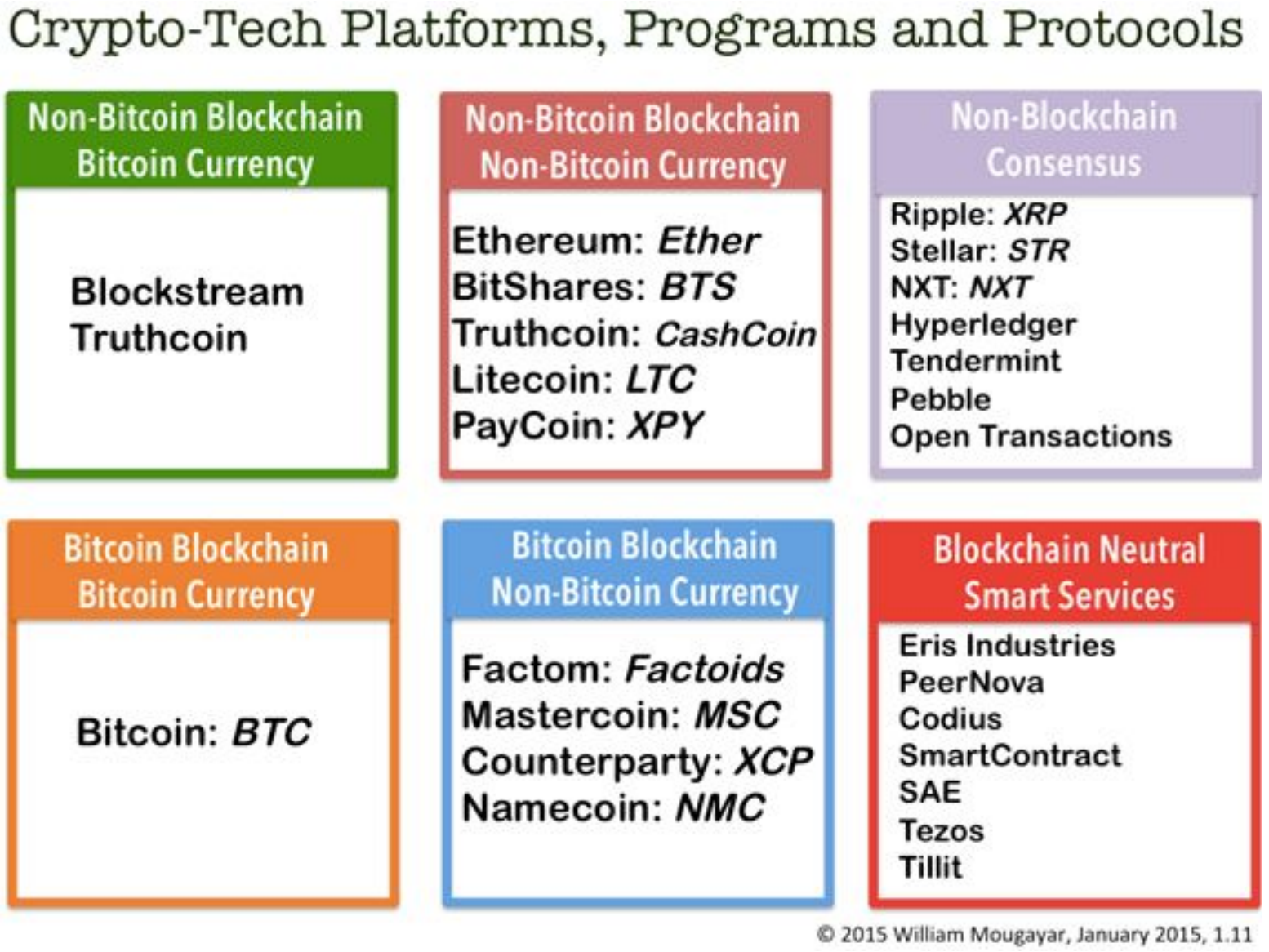
DoubleTree by Hilton Hotel Miami Airport & Con...

Lecture 1 - Intro



Lecture 1 - Intro

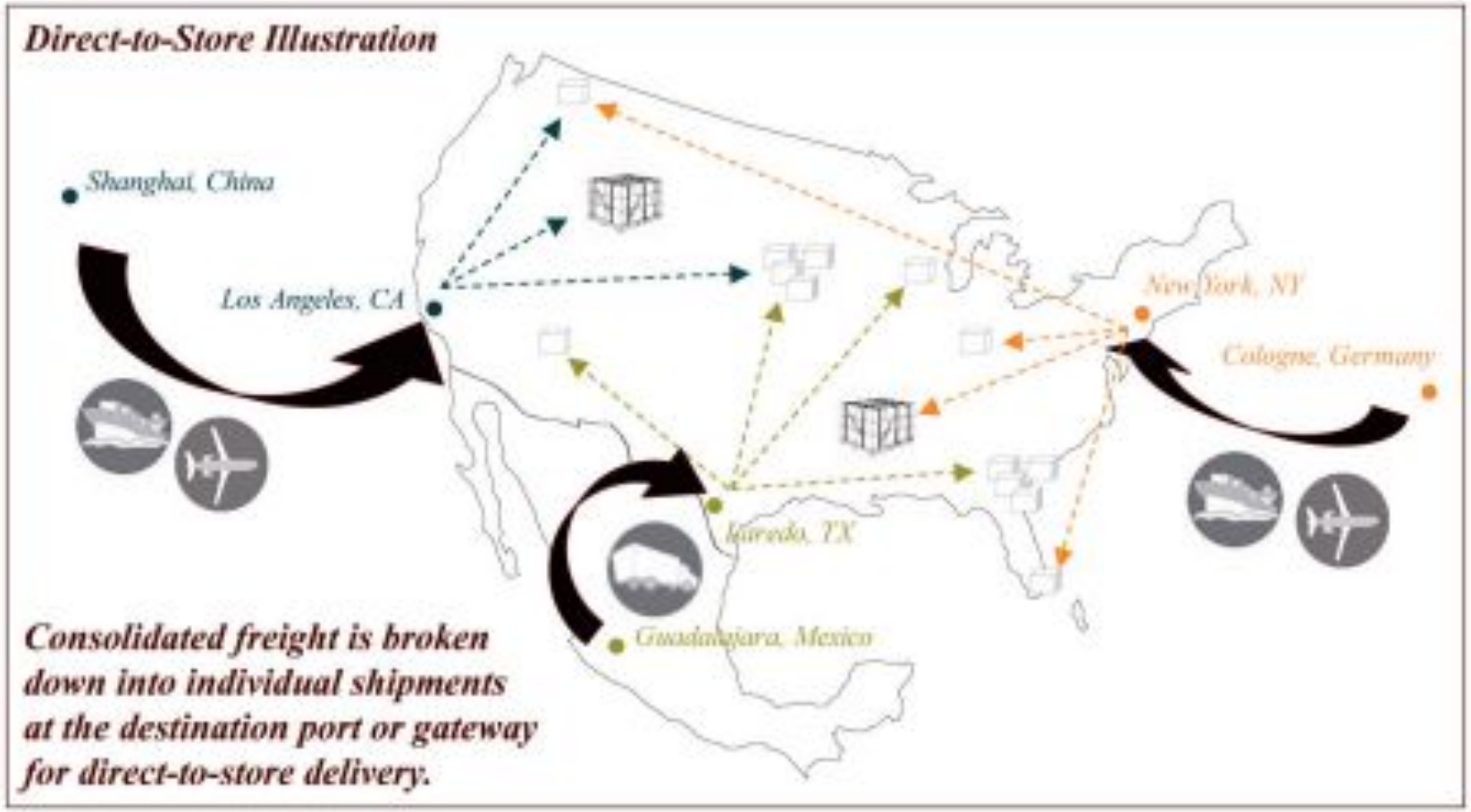
Lecture 1 - Intro



Lecture 1 – Intro. Experience in blockchain

BITA
BLOCKCHAIN
IN TRANSPORT ALLIANCE

Lecture 1 – Intro. Experience in blockchain

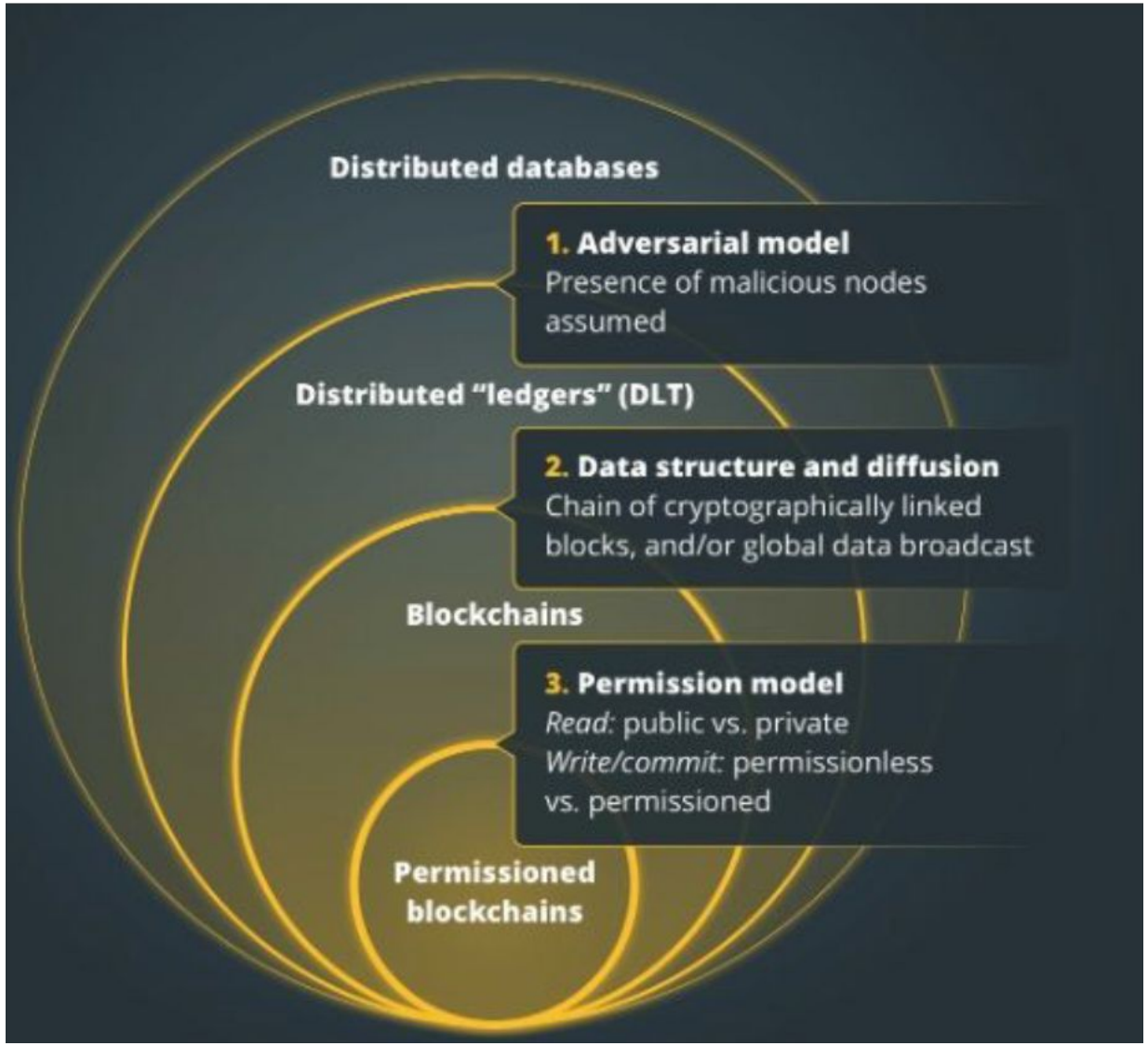


http://chain489.rssing.com/chan-9369409/all_p5.html

Lecture 1 - Contents

- **Blockchain**
- **Decentralization**
- **DLT components**
- Consensus
- Tokens

Distributed ledgers

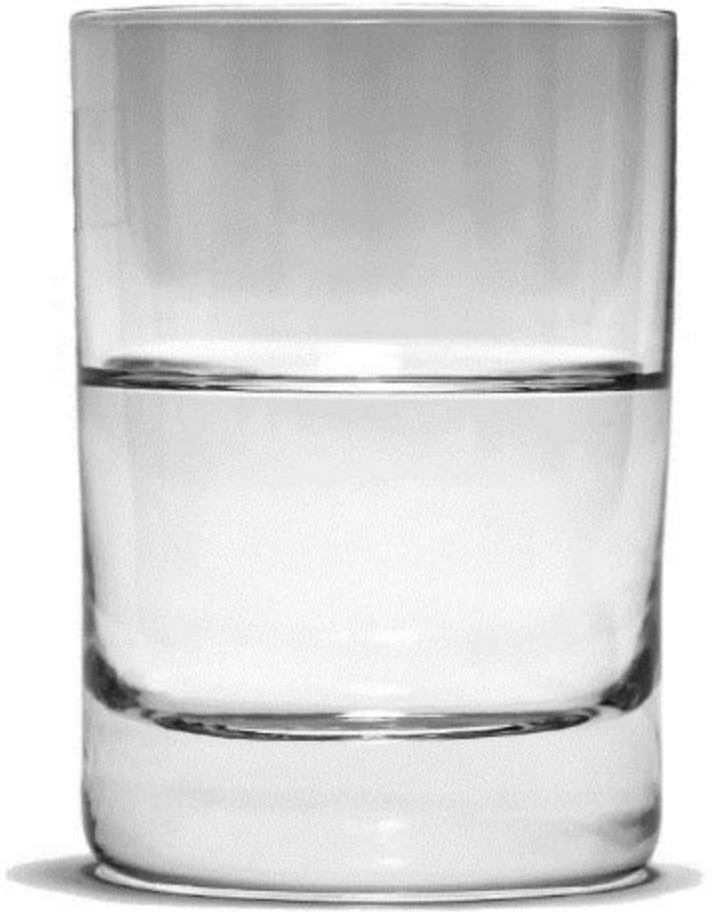


Distributed Ledgers – base technology for distributed databases, while blockchain – is a subspecy of **Distributed Ledger Technology (DLT)**

Main difference between general DLT and blockchain is in **decentralization**, which is not mandatory in DLT, but mandatory for **public blockchain**

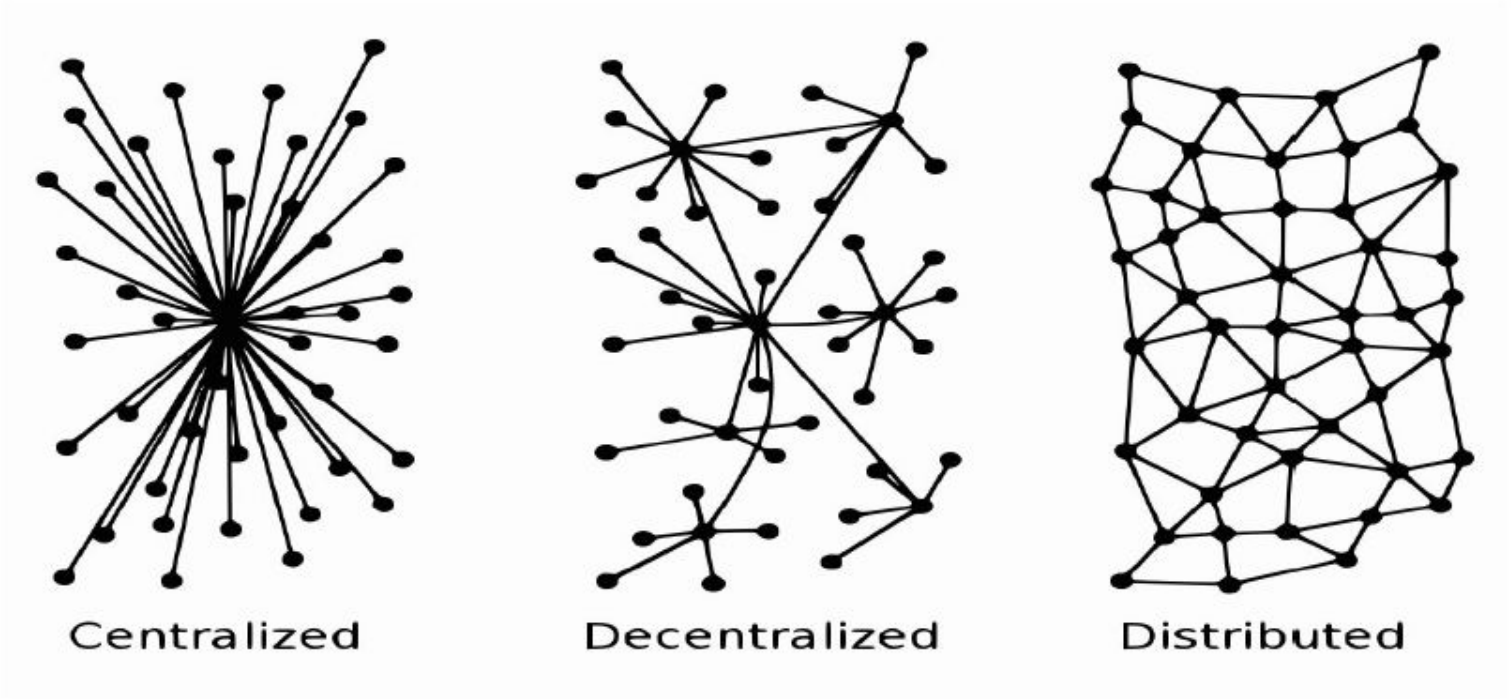
Technically «**private blockchain**» should not exist, it is created by marketing guys.

Decentralized or distributed?



Distributed communication network

In 1962 Paul Baran one of founders of Internet proposed three models of network organization



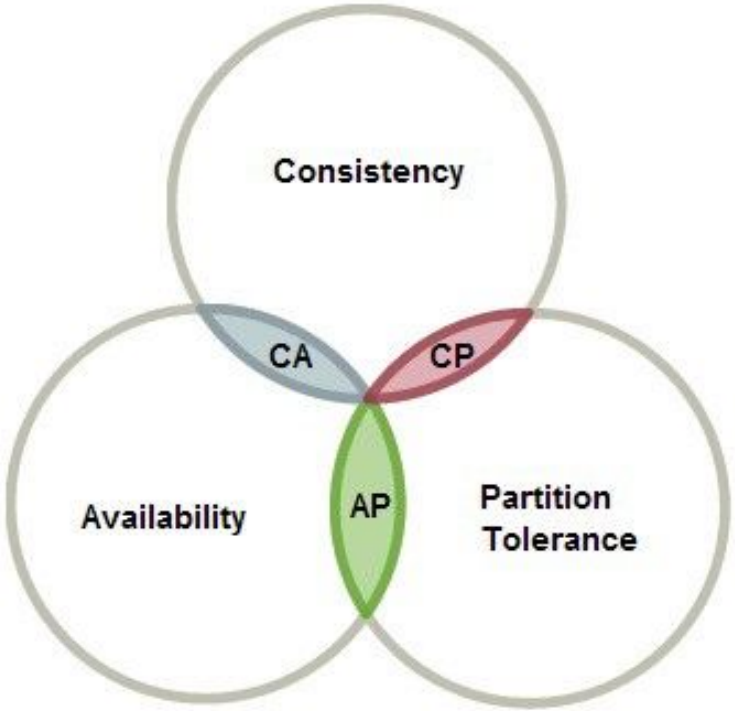
http://pages.cs.wisc.edu/~akella/CS740/F08/740-Papers/Bar64.pdf

Term **Distributed** is actively used in IT and considered from several points:

- Number of network nodes (P-2-P)
- Data Integrity (CAP theorem)
- Remoteness of nodes from each other
- Complexity of tasks

CAP theorem

A distributed database system can only have 2 of the 3: Consistency, Availability and Partition Tolerance. **CAP Theorem** is very important in the Big Data world, especially when we need to make trade off's between the three, based on our unique use case



Consistency and availability

Consistency: Every read receives the most recent write or an error
Availability: Every request receives a (non-error) response, without the guarantee that it contains the most recent write

When choosing availability over consistency, the system will always process the query and try to return the most recent available version of the information, even if it cannot guarantee it is up to date due to network partitioning.

In the absence of network failure – that is, when the distributed system is running normally – both availability and consistency can be satisfied.

Organizational aspect

Terms **centralized**, **decentralized** and **distributed** should be viewed from the following points of view:

- Trust
- Control
- Decision making
- Management
- Economics

Coffee break 20 mins

Lecture 1 - Announcement

UNITY 3D developer

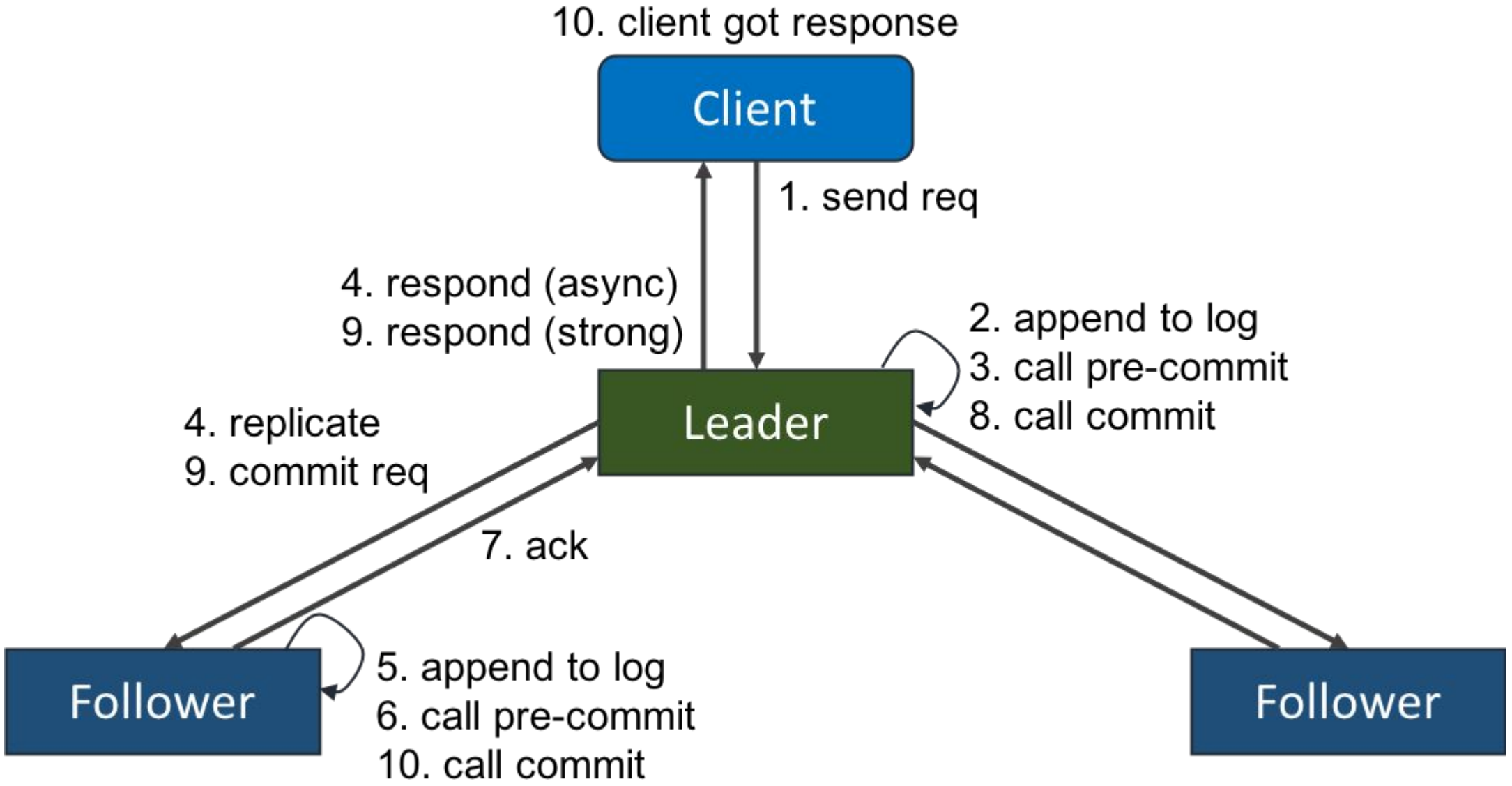
Distributed ledger technology

1. If we create **organizationally centralized business**, i.e. distributed base in the network of one organization and there is complete trust between nodes. Then it is enough to use Raft or Paxos consensus protocol

The need for such systems arises when increased load and / or to increase fault tolerance and service availability.
Examples of distributed databases:

- BigTable on Google,
- DynamoDB in AWS, or
- open source analogue of Cassandra

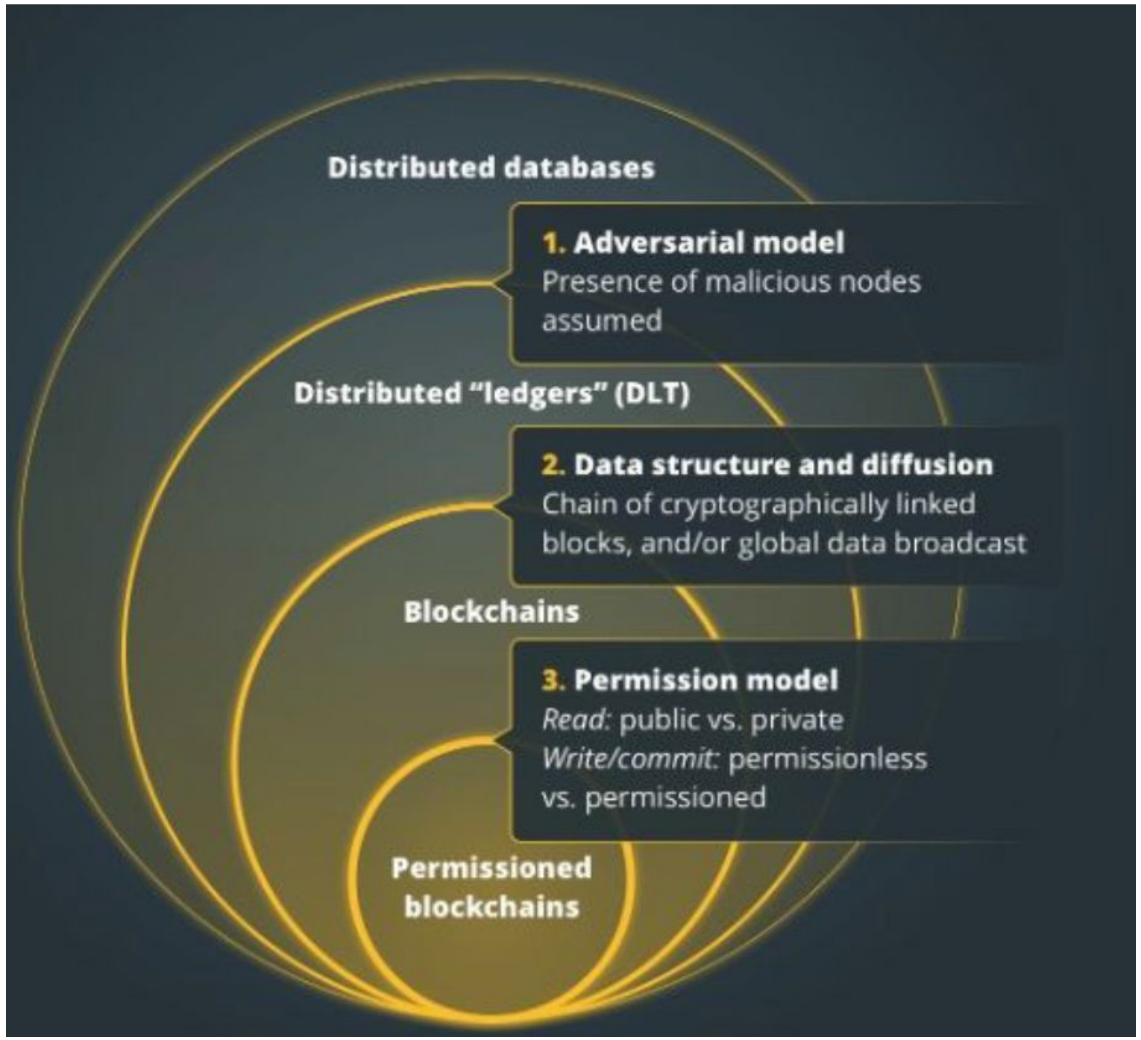
Raft consensus protocol



Raft consensus protocol

- Raft achieves consensus via an elected leader. A server in a raft cluster is either a *leader* or a *follower*, and can be a *candidate* in the precise case of an election (leader unavailable).
- The leader is responsible for log replication to the followers. It regularly informs the followers of its existence by sending a heartbeat message.
- Each follower has a timeout (typically between 150 and 300 ms) in which it expects the heartbeat from the leader. The timeout is reset on receiving the heartbeat. If no heartbeat is received the follower changes its status to candidate and starts a leader election.

Distributed ledger technology



2. In the event that we create organizationally decentralized or distributed business, that is, as soon as the trust between nodes / malicious nodes appear the need to use Distributed Ledger Technology, including blockchain

DLT components

1. A data model that captures the current state

2. A transaction language that changes state

3. Consensus Protocol

Two main properties of DLT:

- Data does not change after recording

- There is no central node to discreetly change the state

DLT: state model

- Blockchain - Chain of blocks (UTX0, etc.)
- HashGraph - HashGraph
- Directed Acyclic Graph (DAG) - Directional Acyclic Graph
- HOLOCHAIN

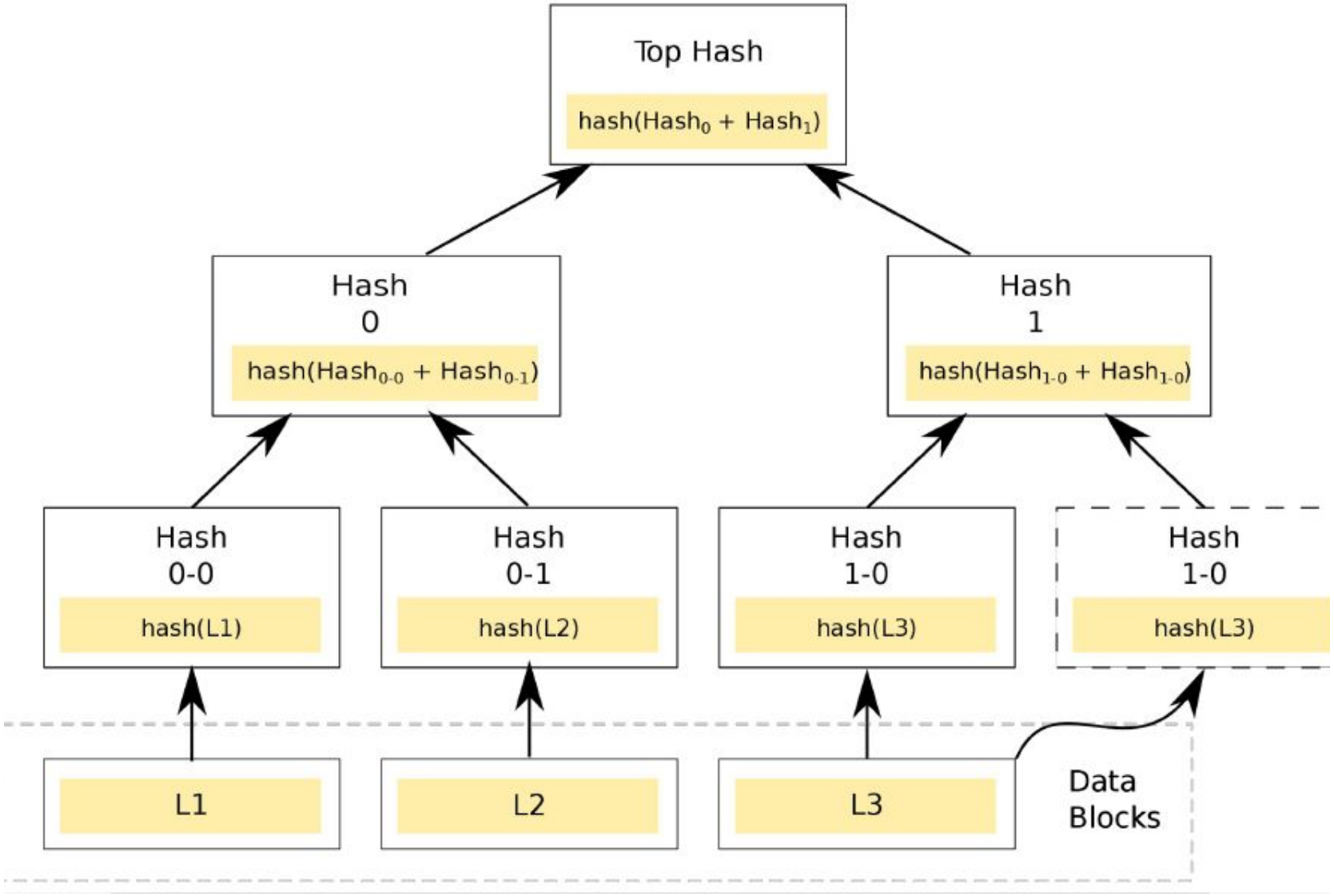
DATA model - blockchain

- Hash Tree or Merkle Tree
- Assumes change history linear in strict sequence
- Cannot be used if possible side events
- Low extensibility due to high Transaction validation “costs”
- Low performance ~ 3+ TPS

DATA model - blockchain

- Hash Tree or Merkle Tree
- Assumes change history linear in strict sequence
- Cannot be used if possible side events
- Low extensibility due to high Transaction validation “costs”
- Low performance ~ 3+ TPS

DATA model - blockchain



DATA model – hashgraph (1/2)

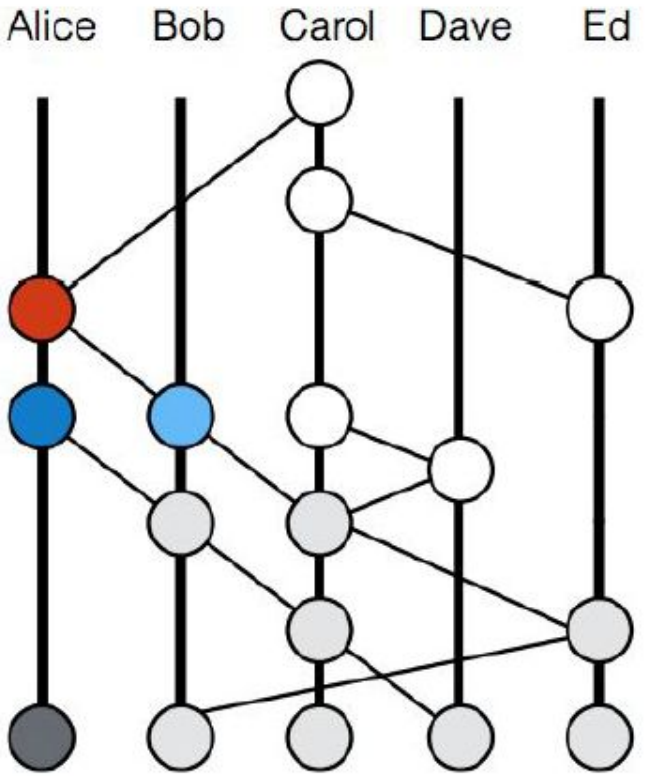
- Hash Graph as the main structure
- relies solely on the consensus

mechanism for checking transactions

on your network

- consensus is achieved through

virtual voting methods and gossip



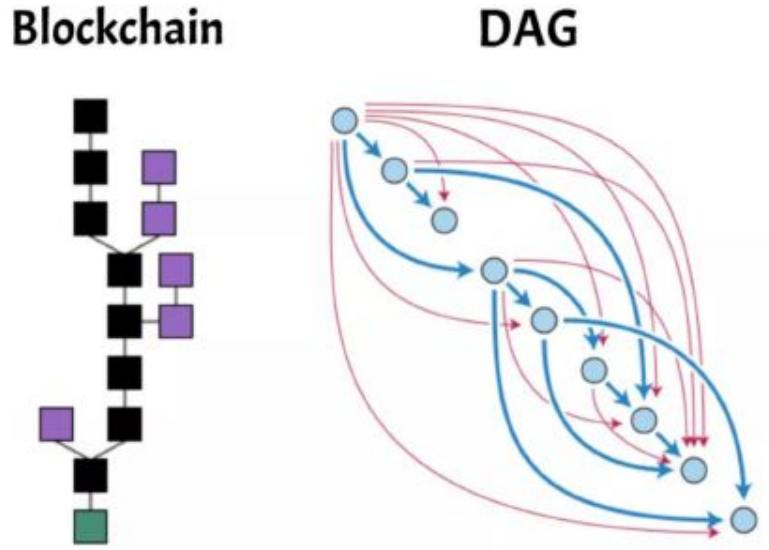
DATA model – hashgraph (2/2)

- Provide higher scalability and softer storage requirements
- Declares a performance of 10,000 + TPS by Compared to Bitcoin

3+ TPS

DATA model – DAG (1/2)

- Directional acyclic graph
- The ability to conduct nano transactions, for which no commission is charged
- The more transactions on the network, the faster it becomes



DATA model – DAG (1/2)

- Any node can initiate a transaction, but

to check he must check two previous transactions in the registry

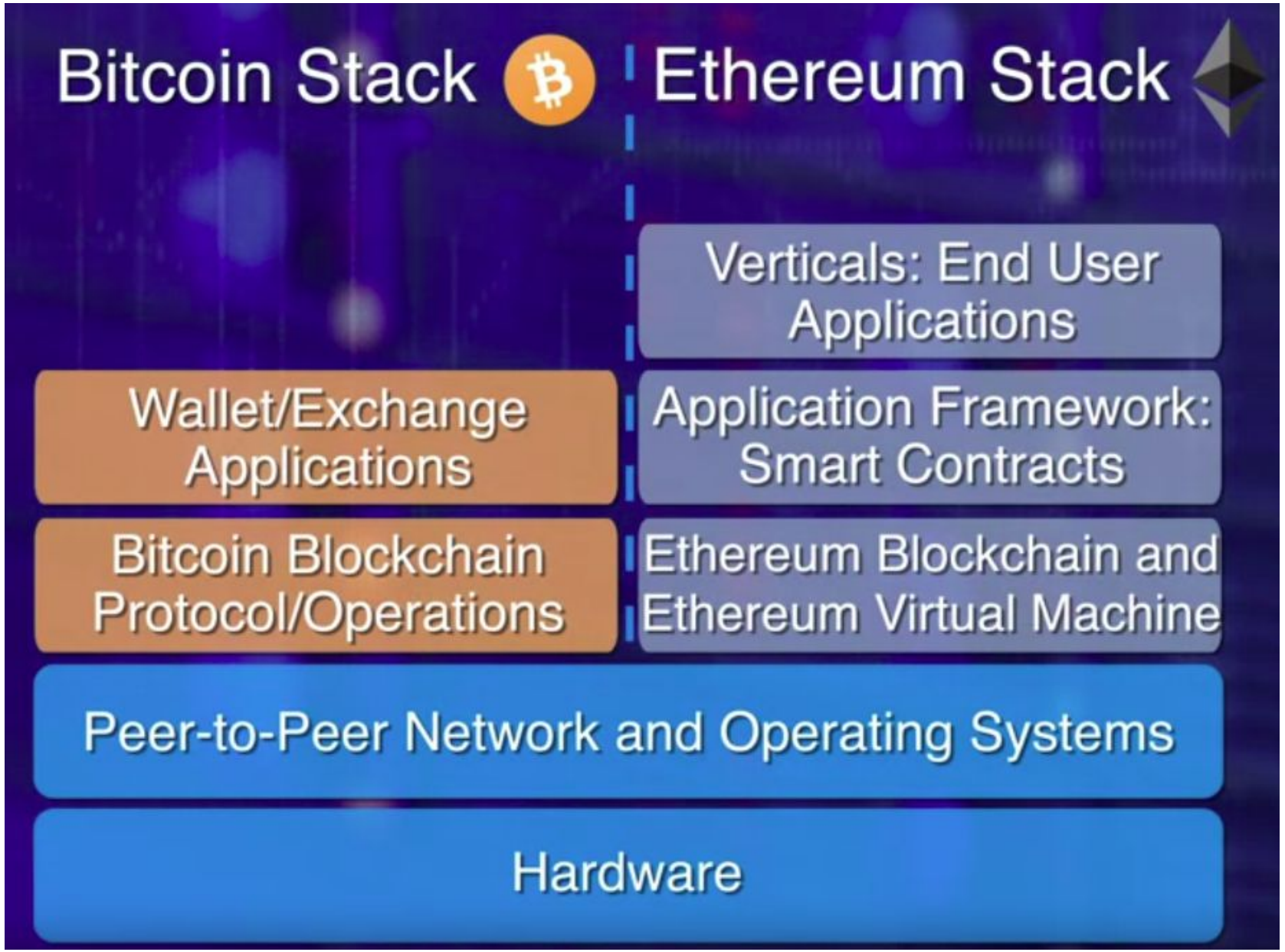
- Miners are not used for validation
- Suitable for IoT applications
- DAG, is resistance to quantum attacks

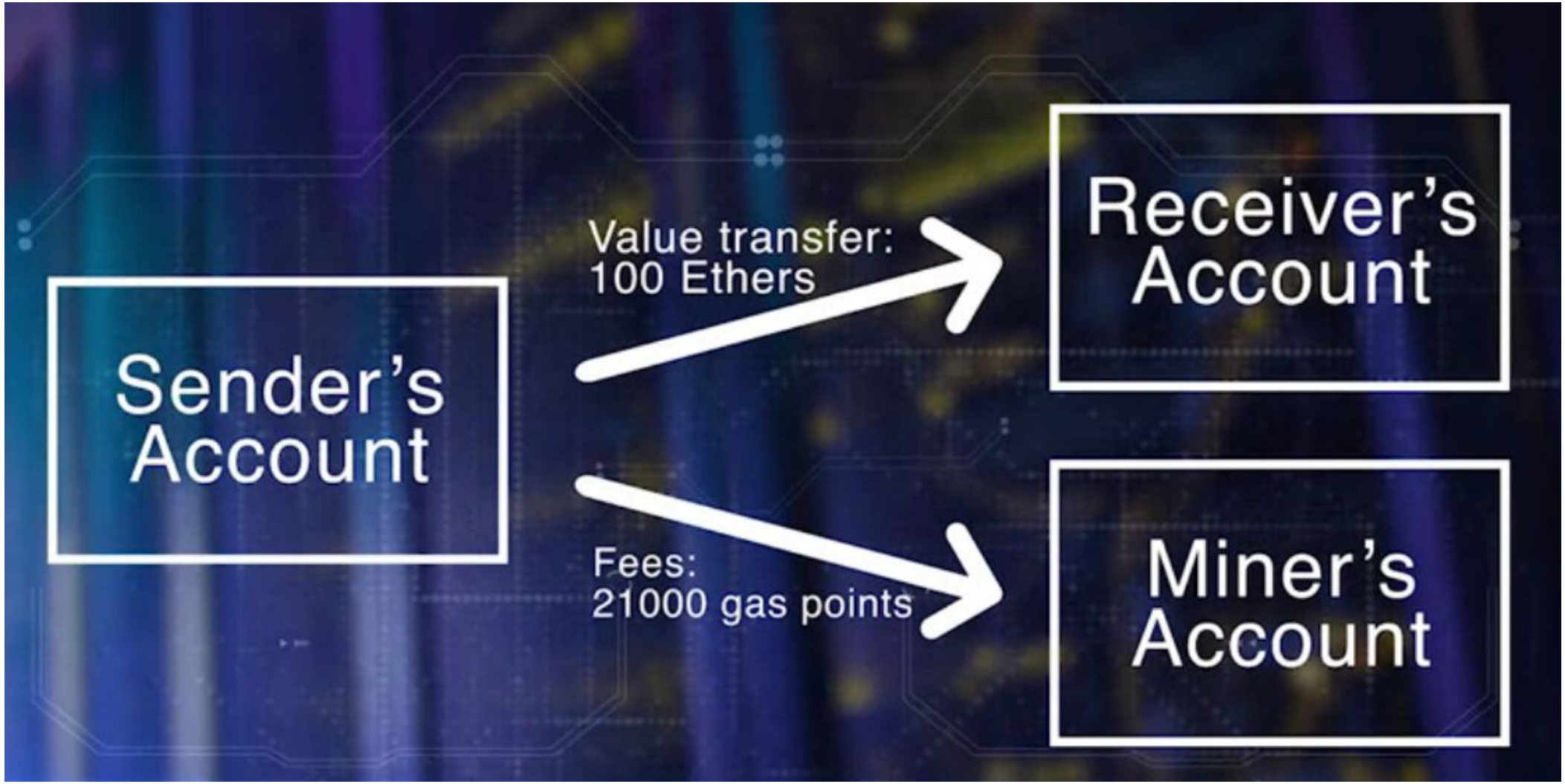
DLT – TYPES (1/2)

1. Federated - the toughest in terms of restrictions: limited access, much better scalability, transparency and confidentiality; e.g. Central Bank or R3 Consortium
2. Permission Required / Private - Access may be public or private, but permission to audit or audit is given only to a few persons; simplified approval and processing data;

DLT – TYPES (2/2)

3. Permission-free / public - public network with open source code; transparency ar anonymity because no third party is involved; minimum costs without the need f maintenance. Among the disadvantages: long processing time; e.g. Bitcoin.
4. Hybrid - a combination of a public / private network with partially limited participation; has flexible an approach to what is stored in the public domain and what is in the public. Improved scalability due to the fact that consent is not required from each node of the network; e.g. Hyperledger


Bitcoin Stack
Ethereum Stack
Verticals: End User Applications
Wallet/Exchange Applications
Application Framework: Smart Contracts
Bitcoin Blockchain Protocol/Operations
Ethereum Blockchain and Ethereum Virtual Machine
Peer-to-Peer Network and Operating Systems
Hardware


Sender's Account
Value transfer:
100 Ethers
Receiver's Account
Fees:
21000 gas points
Miner's Account

Etherium full node hosts the software needed for transaction initiation, validation, mining, block creation, and smart contract execution.

Etherium full node hosts the software needed for transaction initiation, validation, mining, block creation, and smart contract execution.

Sample fees in gas points

Operation name	Gas Cost
Step	1
Load from memory	20
Store into memory	100
Transaction base fee	21000
Contract creation	53000
...	...

DLT Smart contractions. Application (1/2)

● Clearing - reduction of errors, costs. According to research by Santander InnoVentures
By 2022, implementation could reduce annual infrastructure costs by 12–20 billions of $
● Supply chain - a solution for servicing the supply chain from raw materials to finished ones
of products
● Health - combining into one registry will help to conduct research and anonymous polls, and if scientists decide to reward those who share information,
smart contracts - the best way to ensure payment upon transfer
of information

DLT Smart contractions. Application (2/2)

- Internet of things - the ownership of gadgets can be fixed in the blockchain, and it means that the user will be able to sell or donate the device without leaving the blockchain networks and without involving third parties

- Media industry - a problem is relevant for copyright holders and content creators Royalty - fees for the use of intellectual property. Smart here contracts can be used for transparent distribution of funds.

Conclusion: Blockchain is a subset of DLT (1/2)

Distributed Ledger Technology and Blockchain in particular are needed for a decentralized / distributed business model whose members are geographically distant from each other, or have a large-scale community.

This business model must be scalable and use Network effects.

Conclusion: Blockchain is a subset of DLT (1/2)

If necessary, you can manage access rights to the blockchain; rights management models are added:

- Read: public vs limited
- Write: unlimited vs restricted by rights

The level of decentralization affects whether the nodes will belong to a closed group of people or will be to anyone

Laboratory

Block Explorer

Search for things like address, transaction, block

All Blockchains

Search

Bitcoin
$8,744.97

- Blocks
- Transactions
- Average Fee
- Average Value
- Difficulty
- Hashrate
- Mempool

Latest blocks

View more blocks

Height	Hash	Mined	Miner	Size
612988	0..10a0548731c3fadb1fcfb368b6c484054263acb...	2 minutes	BTC.TOP	1,275,437 bytes
612987	0..ba2b80d1d7fe01fe411f716d3e05a8c60dda3d3...	14 minutes	F2Pool	1,283,298 bytes
612986	0..db8d2f075607d4aea57ef21a70e7790a76f17f62...	17 minutes	F2Pool	1,245,576 bytes
612985	0..bfde19f5f6d554178493e362db1b68bec2df904...	22 minutes	F2Pool	1,176,531 bytes
612984	0..109a55b34532cd988b0a658af6d6584fce9b15...	26 minutes	Unknown	1,204,369 bytes
612983	0..2fe5d3f0a211773aa534e36147bc136230dc311...	31 minutes	F2Pool	1,345,705 bytes

Practice exercise:

1 Go to https://www.blockchain.com/explorer

2 Find block 43515

3 Locate *Hash of previous block and send it to me via chat*

Optional SIS1 (SIS + all participation points)

Task: Launching python Django based Etherium calculator/web scraper

As a User, I want to enter amount of my Etherium (Eths), so that I can see how much USD I can exchange.

1. System must have: GUI (web front end) and back end on Django python.

2. User must enter the following attributes:
- Amount of Eths
- Is it Etherium of Erherium classic (just a checkbox)

3. System must respond with the following:
- Amount of Eths * USD exchange rate = number -> how much in USD

!! This task is optional. IT should be submitted with source codes before 12 September 0:00 (Night between Friday and Saturday). Submission – via telegram @AskarAi or aaituov@gmail.com.
Criterions – if 1-3 points will be included = then equivalent of all SIS + participation points will be awarded

Useful links:
https://www.youtube.com/watch?v=xocy7YU9Qik Django beginning
https://www.youtube.com/watch?v=Qmuc6kNxSLs Calculator on Django