Blockchain

Instructor: Murat Tunc

Module 4

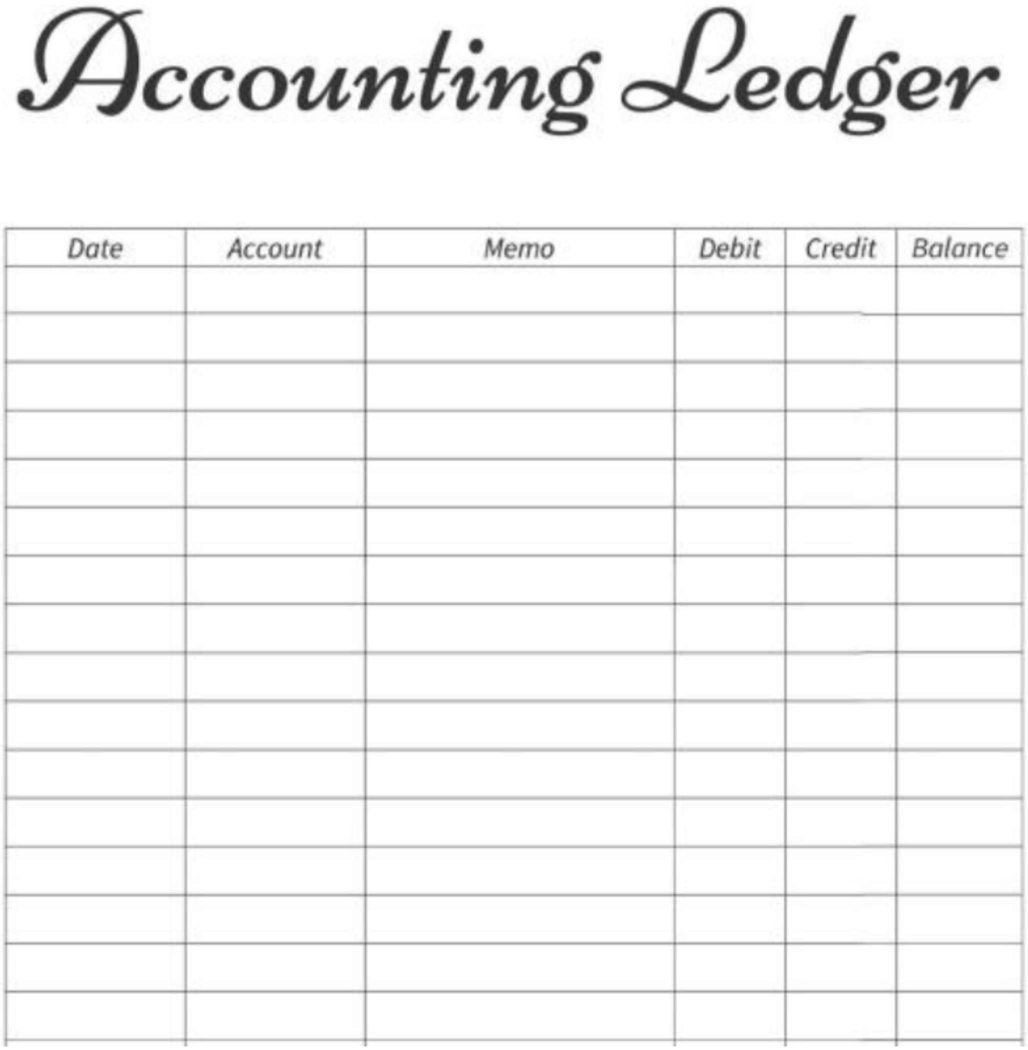
November 13th, 2023

What is a Blockchain?

- A unique type of computerized **ledger** relies on cryptographic techniques and new methods for **consensus** to capture and secure the data
  - Money transactions
  - Medical records
  - Buying and selling goods
  - Insurance policies

- What is so special about blockchain?
  - Distributed
  - Consensus mechanism
  - Encrypted
  - Immutable

What is a Ledger?



Accounting Ledger

Date	Account	Memo	Debit	Credit	Balance

What is so special about blockchain?

Distributed

Consensus mechanism

Encrypted

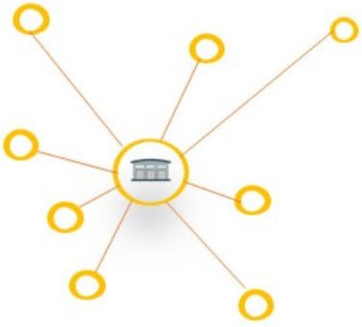
Immutable

Where is this ledger?

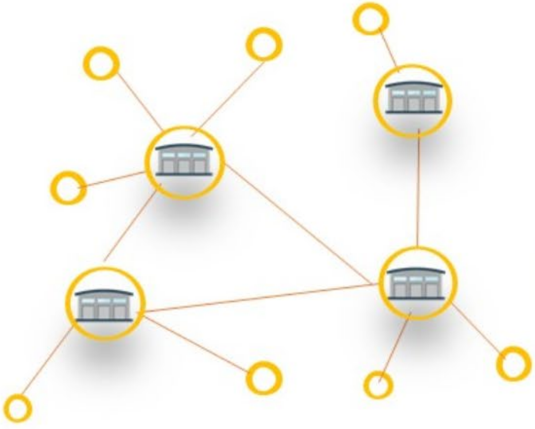
- In a **central** location?
  - Central banks, governments

- Why is it controversial to have the ledger in a central location?
  - Attack vulnerability
  - Single point of contact
  - Rely on middle-men
  - Operational inefficiency

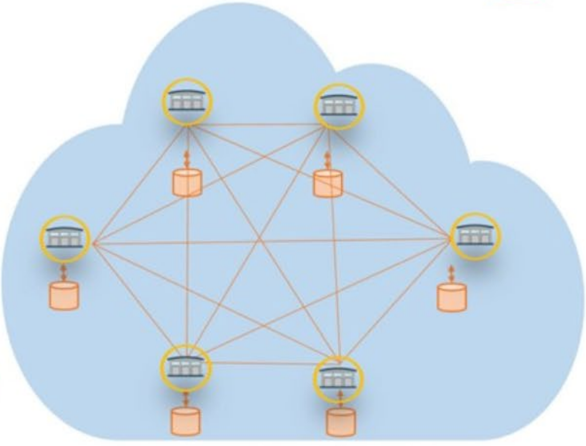
Types of ledgers



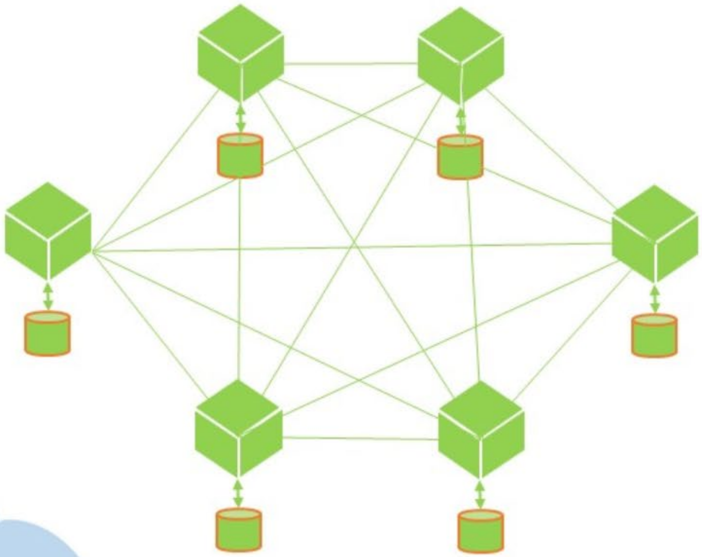
Centralized Ledger



Decentralized Ledger



Distributed yet Centralized



Distributed Ledger

Types of ledgers

- Control
    - Centralized: **One entity** controls the entire system
    - **Decentralized:** Multiple entities control the system
- Location
    - **Centralized:** Ledgers exist at the same location
    - Distributed: Ledgers exist at **different locations**
- Distributed yet centralized
    - Distributed servers but controlled by a single authority
        - Cloud service providers

Distributed Ledger Technology

- Distributed ledger technology
  - **Everyone** in the peer-to-peer network **have an identical copy** of the ledger
- **No** single entity is the **authority** of the system
- System is widely distributed among entities in the network
- Blockchain
  - One **type** of DLT
  - Based on a P2P network

What is so special about blockchain?

Distributed

Consensus mechanism

Encrypted

Immutable

Self-regulating system

- In a centralized system
  - Administrator has the **authority to update** and maintain the database
- In blockchain, everyone in the network can
  - **Read** the chain
  - Make legitimate **changes** in the chain
  - Write a **new block** into the chain
- Blockchain is a self-regulating system
  - Contributions by the participants
  - Authentication and verification of the transactions

Distributed consensus

- A well-known problem in computer science
- How multiple, independently run computers can **reliably agree** on a set of **common data** in the presence of faults?
  - Where there is a **risk** that one or more computers are programmed to introduce **false information**
- Satoshi Nakamoto (2008) proposed a solution to this problem
  - All computers in a blockchain network use a system of **distributed consensus** to agree upon continually updated history of transactions in a ledger
- There is only one version of the transaction ledger in bitcoin over a decade (The trust machine)

Consensus mechanisms

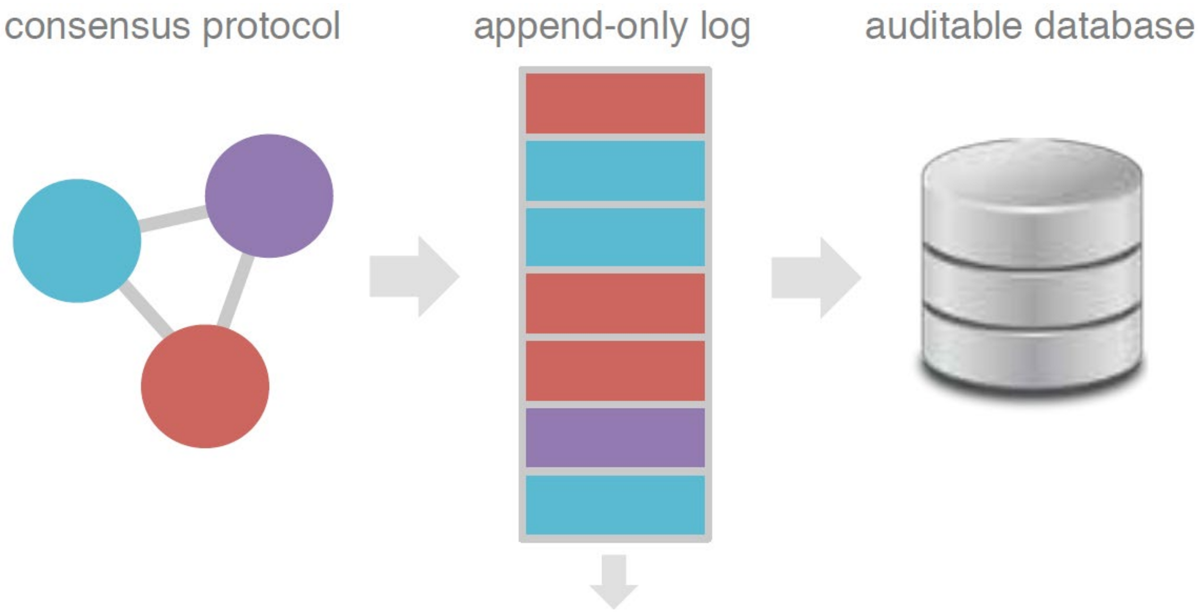
- Proof of work
  - Complex problem that needs **computational power** to solve (miners) based on an algorithmically adjusted difficulty
  - Bitcoin, Ethereum
- Proof of stake
  - A lottery-like system randomly rewarded to those **based on how much stake** (currency) they commit (have) (validators)
  - EOS, Cardano Ouroboros
- Proof of authority
  - Slightly adjusted proof of stake
  - Validators are selected **based on their reputation**
  - IBM Hyperledger

Proof of work

- Bitcoin's **breakthrough** feature
- Participants (**miners**) competing to win rewards in bitcoin in the presence of a **computational cost**
  - Each miner collects a set of **pending transactions** (block: a list of ~2000 transactions)
  - While simultaneously **competing** to find a randomly chosen string (~10 minutes to find)
  - Once a miner finds the required string, they **broadcast** the string and the block (gets a reward of 6.25 BTC + fees)
- Fraud ?
  - Computationally **infeasible**
- Controversies
  - Energy intensive
  - Costly **barriers of entry** for miners

Consensus protocol

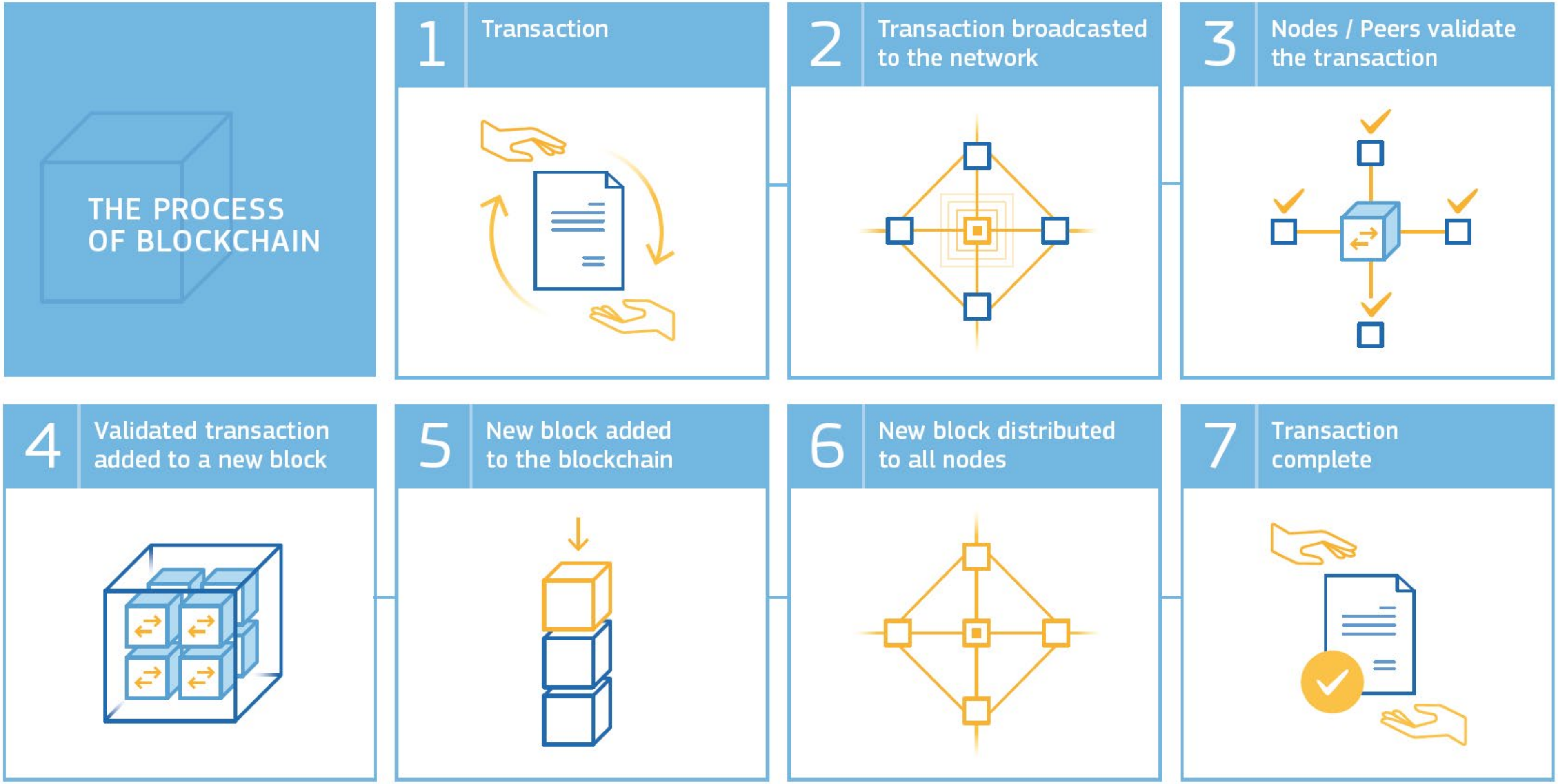
- Create append-only log
  - Transaction ledger
- To be used to form an auditable database
  - Who owns what



How to update the ledger?

- John and Ashley are two peers in the **bitcoin** network
- John pays Ashley 0.05 BTC (~800 $) for the **rent**
  - John (-0.05) and Ashley (+0.05) add this transaction and update the ledger
- How does the others **see this update** on their identical copy of the ledger?

How to update the ledger?



THE PROCESS OF BLOCKCHAIN

1 Transaction

2 Transaction broadcasted to the network

3 Nodes / Peers validate the transaction

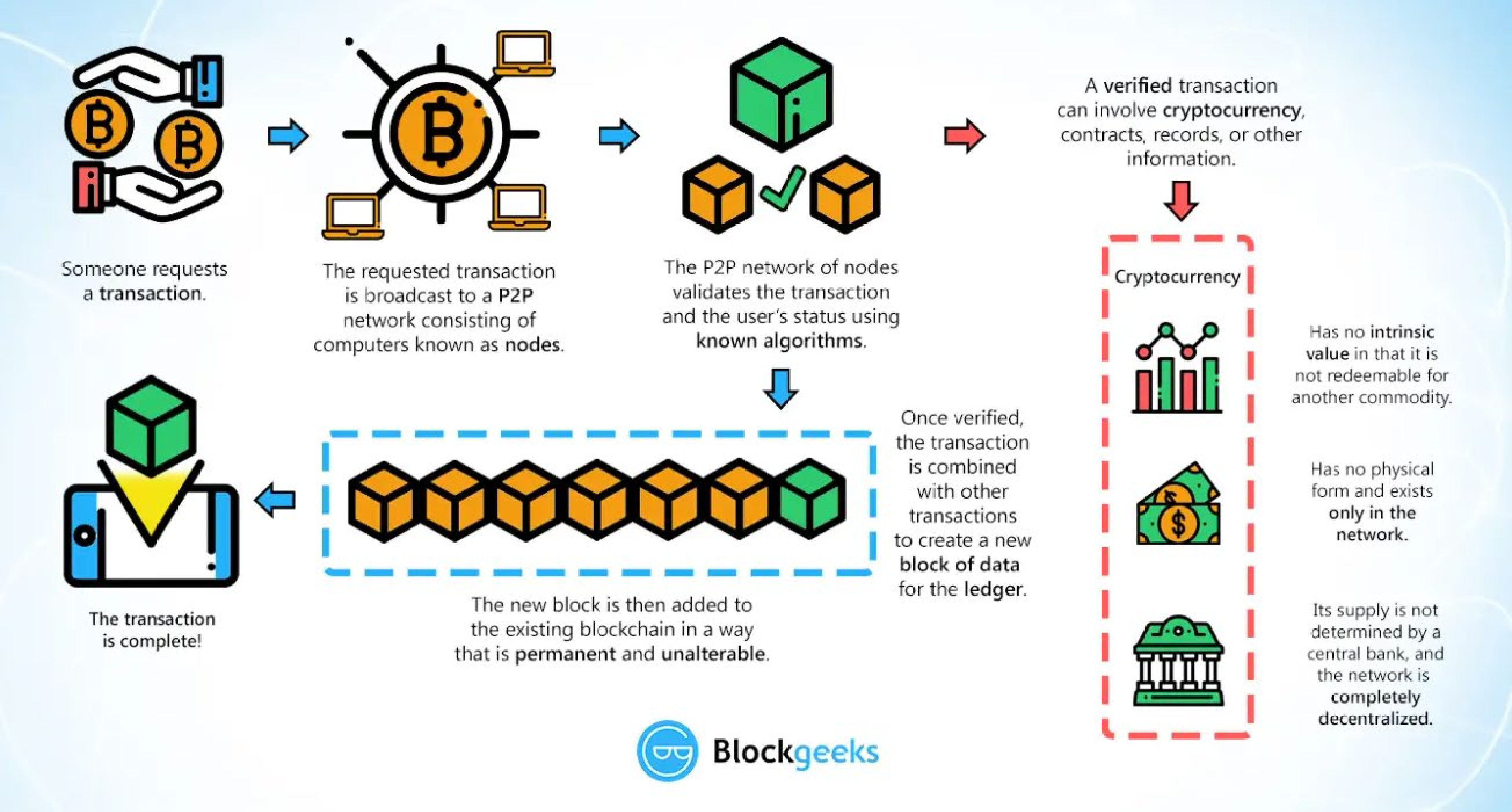
4 Validated transaction added to a new block

5 New block added to the blockchain

6 New block distributed to all nodes

7 Transaction complete

How to update the ledger?



Someone requests a **transaction**.

The requested transaction is broadcast to a **P2P** network consisting of computers known as **nodes**.

The P2P network of nodes validates the transaction and the user's status using **known algorithms**.

A **verified** transaction can involve **cryptocurrency**, contracts, records, or other information.

Cryptocurrency

Has no **intrinsic value** in that it is not redeemable for another commodity.

Has no physical form and exists **only in the network**.

Its supply is not determined by a central bank, and the network is **completely decentralized**.

Once verified, the transaction is combined with other transactions to create a new **block of data** for the **ledger**.

The new block is then added to the existing blockchain in a way that is **permanent** and **unalterable**.

The transaction is complete!

Blockgeeks

What is so special about blockchain?

Distributed

Consensus mechanism

Encrypted

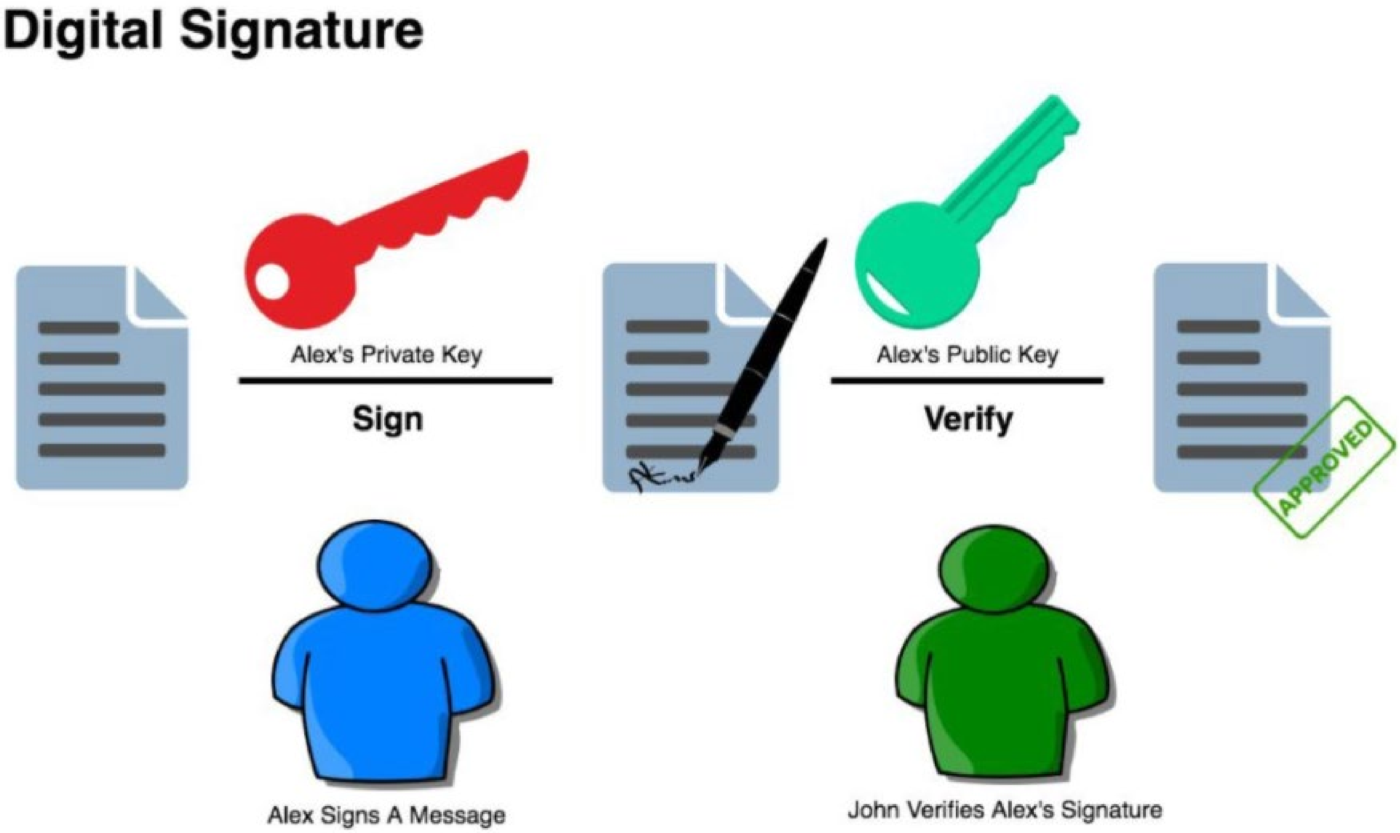
Immutable

How secure is blockchain?

- Users have control over their transactions (or cryptocurrencies) via a **digital signature** system by which they indicate consent to transfer goods (coins)
- These digital signatures are
  - public
  - cannot be forged
  - can be **verified** by anyone

Digital signatures

- Every user has a
  - private key (only the user can see it)
  - public key (everyone in the network can see it)



Digital signatures

- 256-bit **digital signature** is produced based on
  - the document (**message**)
    - John pays Ashley 100 $
  - **private key**
    - John’s private key
- How does Ashley (or anyone) can **verify** that it is indeed John that signed this document?
  - Verification function (True / False) based on
    - Digital signature (John’s Digital Signature)
    - The message (John pays Ashley 100 $)
    - Public key (John’s public key that anyone can see)
- When Ashley verify John’s signature
  - **Extremely** confident that it is indeed John

What is so special about blockchain?

Distributed

Consensus mechanism

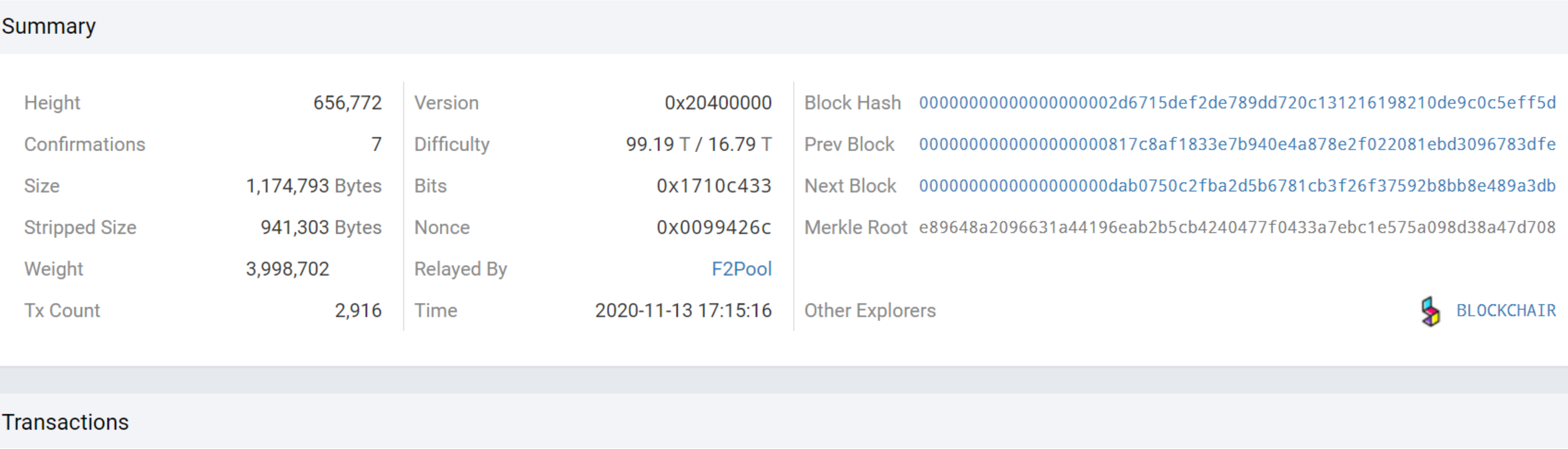
Encrypted

Immutable

What does a block store?

- Timestamp
  - the time when the block was mined
- Block number
  - the length of the blockchain in blocks
- Difficulty
  - the effort required to mine the block
- Hash
  - a unique identifier for that block
- A parent hash
  - the unique identifier for the block that came before (this is how blocks are linked in a chain)
- Transactions list
  - the transactions included in the block
- Nonce
  - a hash that, when combined with the mixHash, proves that the block has gone through proof of work

Block #656772



Summary

Height	656,772	Version	0x20400000	Block Hash	0000000000000000000002d6715def2de789dd720c131216198210de9c0c5eff5d
Confirmations	7	Difficulty	99.19 T / 16.79 T	Prev Block	0000000000000000000817c8af1833e7b940e4a878e2f022081ebd3096783dfe
Size	1,174,793 Bytes	Bits	0x1710c433	Next Block	0000000000000000000dab0750c2fba2d5b6781cb3f26f37592b8bb8e489a3db
Stripped Size	941,303 Bytes	Nonce	0x0099426c	Merkle Root	e89648a2096631a44196eab2b5cb4240477f0433a7ebc1e575a098d38a47d708
Weight	3,998,702	Relayed By	F2Pool		
Tx Count	2,916	Time	2020-11-13 17:15:16	Other Explorers	BLOCKCHAIR

Transactions

Changing Block #656772

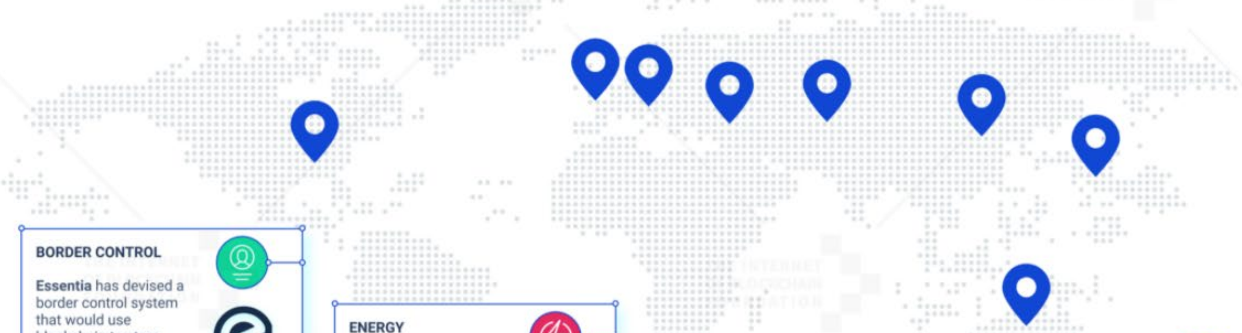
- Let's say that **someone** wants to change block #656772 and add the following
  - John pays Murat 1000 BTC (~16 million $)
- 2916 transactions + John pays Murat 1000 BTC
  - 2917 transactions
- Requires a new Hash #656772
  - **Difficulty:** It has to start with 19 zeros (2^19)
  - ~ 1 / 500,000 chance
- Also requires a new Hash for #656773
  - Since #656773's prev. hash (i.e. hash for #656772) has changed
  - ~ 1 / 500,000 chance
- Also requires a new Hash for #656774 …

Changing Block #656772

- One needs to compete with **all the other miners** in the network
  - To find new Hash for the **rest of the blocks**
- Unless someone has **more than 50%** of the computational power of **all the miners combined**
  - You **cannot** change a block in the blockchain
  - 51% attack
- Computationally **infeasible** to change a block
  - Immutability

Now and beyond

50+ BLOCKCHAIN
REAL WORLD USES CASES



GOVERNMENT

Essentia develops world's first blockchain solution to manage international logistics hub together with Traffic Labs and the Finnish Government

essentia.one

IDENTIFICATION

Voter registration is being facilitated via a blockchain project in Switzerland spearheaded by **Uport**.

uport

MOBILE PAYMENTS

The blockchain ledger that **Ripple** uses has been latched onto by a group of Japanese banks, who will be using it for quick mobile payments.

ripple

INSURANCE

A smart contract-based blockchain is being used by Insurer **American International Group Inc** as a means of saving costs and increasing transparency.

AIG

ENDANGERED SPECIES PROTECTION

The protection of endangered species is being facilitated via a blockchain project that records the activities of these rare animals.

CARBON OFFSETS

IBM is using the Hyperledger Fabric blockchain in China to monitor carbon offset trading.

IBM HYPERLEDGER

ENTERPRISE

Ethereum's blockchain can be accessed as a cloud-based service courtesy of **Microsoft Azure.**

Microsoft Azure

BORDER CONTROL

Essentia has devised a border control system that would use blockchain to store passenger data in the Netherlands.

essentia.one

SUPPLY CHAINS

IBM and **Walmart** have partnered in China to create a blockchain project that will monitor food safety.

IBM Walmart

HEALTHCARE

A number of healthcare systems that store data on the blockchain have been pioneered including **MedRec.**

MEDREC

SHIPPING

Shipping is a natural fit for blockchain, and **Maersk** have been trialling a blockchainbased project within the maritime logistics industry.

MÆRSK

REAL ESTATE

Blockchain is now being used to complete real estate deals, the first of which was conducted in Kiev by **Propy**.

PROPY

ENERGY

Essentia is developing a test project that will help energy suppliers track the distribution of their resources in real time, whilst maintaining data confidentiality.

essentia.one

LAND REGISTRY

Land registry titles are now being stored on the blockchain in Georgia in a project developed by the **National Agency of Public Registry**.

NATIONAL AGENCY of PUBLIC REGISTRY

COMPUTATION

Digital Currency Group are helping Amazon Web Services examine ways in which the distributed ledger technology can help improve database security.

DIGITAL CURRENCY GROUP

ADVERTISING

New York Interactive Advertising Exchange has been experimen- ting with blockchain as a means of providing an ads marketplace for publishers.

NYIAX

BORDER CONTROL

Essentia is developing a blockchain project for border control that will allow customs agents to record passenger data from an array of inputs and safely store it.

essentia.one

JOURNALISM

Decentralized journalism, as enabled by blockchain technology, has the potential to prevent censorship and increase transparency, as **Civil** has shown.

CIVIL

WASTE MANAGEMENT

Waltonchain is using **RFID** technology to store waste management data on the blockchain in China.

ENERGY

Food importation is another industry where blockchain is proving its worth, with **Louis Dreyfus Co** trialling a soybean importation operation using this technology.

LDC.

DIAMONDS

The **De Beers Group** is using blockchain to track the importation and sale of diamonds.

De Beers

FINE ART

By storing **certificates** of authenticity on the blockchain, it's possible to dramatically reduce art forgeries, as one blockchain project is proving.

NATIONAL SECURITY

For the past two years, the **US Department of Homeland Security** has been using blockchain to record and safely store data captured from its security cameras.

TOURISM

In a bid to boost its tourism economy, **Hawaii** is examining ways in which blockchain-based cryptocurrencies can be adopted throughout the US state.

TAXATION

In China, a tax-based initiative is using blockchain to store tax records and electronic invoices led by **Miaocai Network**.

ENERGY

Chile's National Energy Commission has started using blockchain technology as a way of certifying data pertaining to the country's energy usage as it seeks to update its electrical infrastructure.

CNE COMISIÓN NACIONAL DE ENERGÍA

RAILWAYS

Russian rail operator **Novotrans** is storing inventory data on a blockchain pertaining to repair requests and rolling stock

НОВОТРАНС

ENTERPRISE

Google is building its own blockchain which will be integrated into its cloud-based services, enabling businesses to store data on it, and to request their own white label version developed by **Alphabet Inc**

Google Alphabet

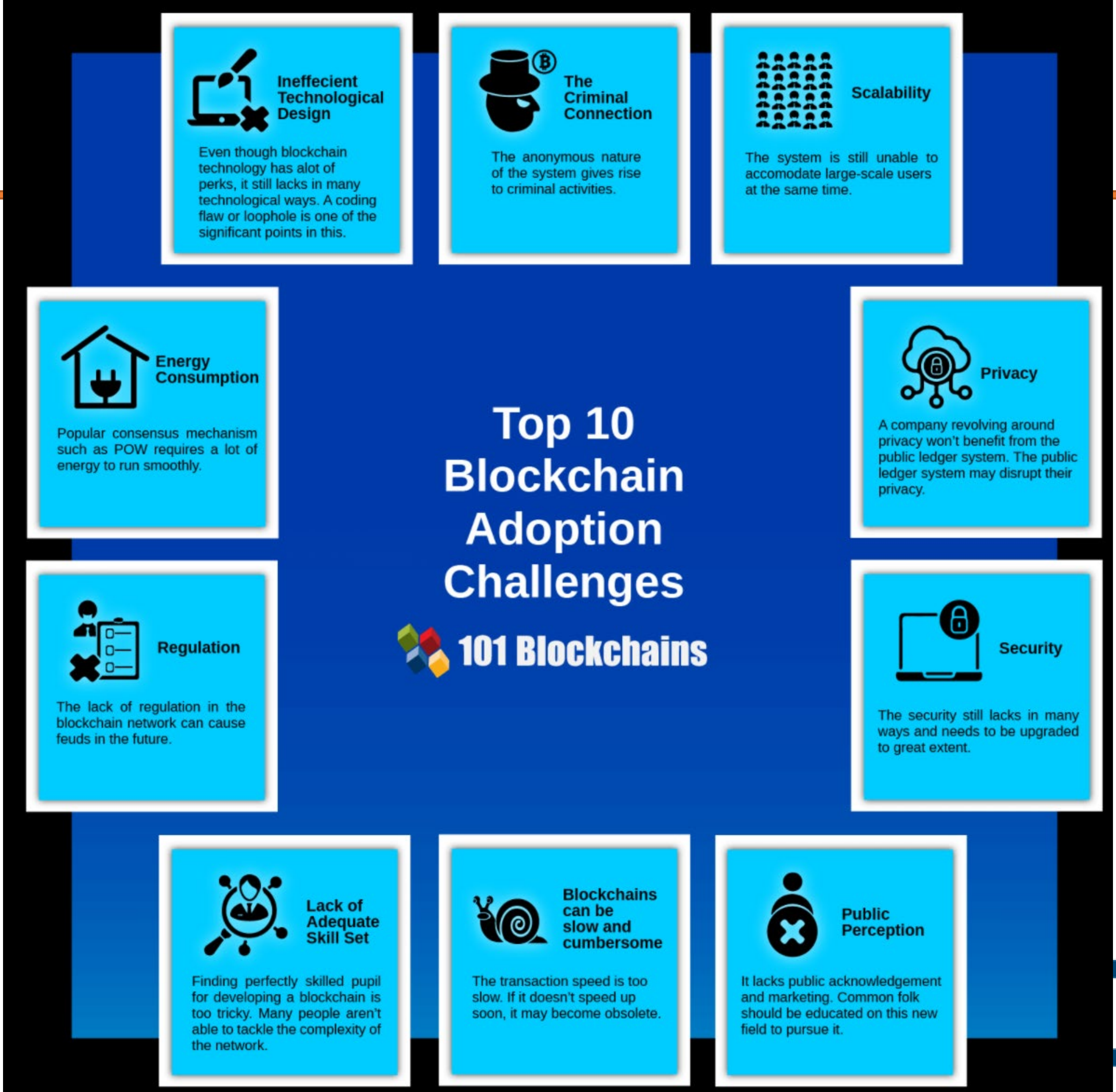
MUSIC

Arbit is a blockchain-based project led by former Guns N Roses drummer Matt Sorum seeking a fairer way to reward musicians for their creative efforts.

arbit

FISHING

Blockchain technology has been used to provide a transparent record of where fish was caught, as a means of ensuring it was legally landed.



Top 10 Blockchain Adoption Challenges

101 Blockchains

Ineffecient Technological Design

Even though blockchain technology has alot of perks, it still lacks in many technological ways. A coding flaw or loophole is one of the significant points in this.

The Criminal Connection

The anonymous nature of the system gives rise to criminal activities.

Scalability

The system is still unable to accomodate large-scale users at the same time.

Energy Consumption

Popular consensus mechanism such as POW requires a lot of energy to run smoothly.

Privacy

A company revolving around privacy won't benefit from the public ledger system. The public ledger system may disrupt their privacy.

Regulation

The lack of regulation in the blockchain network can cause feuds in the future.

Security

The security still lacks in many ways and needs to be upgraded to great extent.

Lack of Adequate Skill Set

Finding perfectly skilled pupil for developing a blockchain is too tricky. Many people aren't able to tackle the complexity of the network.

Blockchains can be slow and cumbersome

The transaction speed is too slow. If it doesn't speed up soon, it may become obsolete.

Public Perception

It lacks public acknowledgement and marketing. Common folk should be educated on this new field to pursue it.

Readings

- Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. Bitcoin.–URL: https://bitcoin.org/bitcoin.pdf.
- Ellervee, A., Matulevicius, R., & Mayer, N. (2017). A Comprehensive Reference Model for Blockchain-based Distributed Ledger Technology. In ER Forum/Demos (pp. 306-319).

References

- Casey, M., Crane, J., Gensler, G., Johnson, S., & Narula, N. (2018). The impact of blockchain technology on finance: A catalyst for change.
- Pease, M., Shostak, R., & Lamport, L. (1980). Reaching agreement in the presence of faults. Journal of the ACM (JACM), 27(2), 228-234.
- Anderberg, A., Andonova, E., Bellia, M., Calès, L., Inamorato Dos Santos, A., Kounelis, I., Nai Fovino, I., Petracco Giudici, M., Papanagiotou, E., Sobolewski, M., Rossetti, F. and Spirito, L. (2019). Blockchain Now And Tomorrow. Editors: Figueiredo Do Nascimento, S. and Roque Mendes Polvora, A.
- Anwar, H. (2018). Top 10 Blockchain Adoption Challenges. https://101blockchains.com/blockchain-adoption-challenges/
- Essentia (2018). 50+ Examples of How Blockchains are Taking Over the World. https://medium.com/@essentia1/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b
- Rosic, A. (2018) What is Blockchain Technology? A Step-by-Step Guide For Beginners. https://blockgeeks.com/guides/what-is-blockchain-technology/