BLOCKCHAIN FOR BUSINESS

BLOCKCHAIN COMPONENTS AND SECURITY METHODS

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

CONTENT

1. Introduction and Learning Goals;
2. Recap;
3. Quiz;
4. **Blockchain-specific technical features;**
5. **Important (security) terminology for information systems;**
6. **Essential security questions for business information systems**
7. **Blockchain-specific methods to tackle the essential security issues**
8. Bibliography;
9. Quiz;
10. Self-reflection questions;
11. Further readings.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

LEARNING GOALS

Explain the relationship between the key technological constructs of the blockchain and the security issues:

1. Recognize blockchain-specific technical features (the key blockchain components).
2. Introduce important terminology on information systems security.
3. Recognize the essential security issues in the deployment of information systems.
4. Explain what security methods are used to tackle the existing security issues in blockchain.

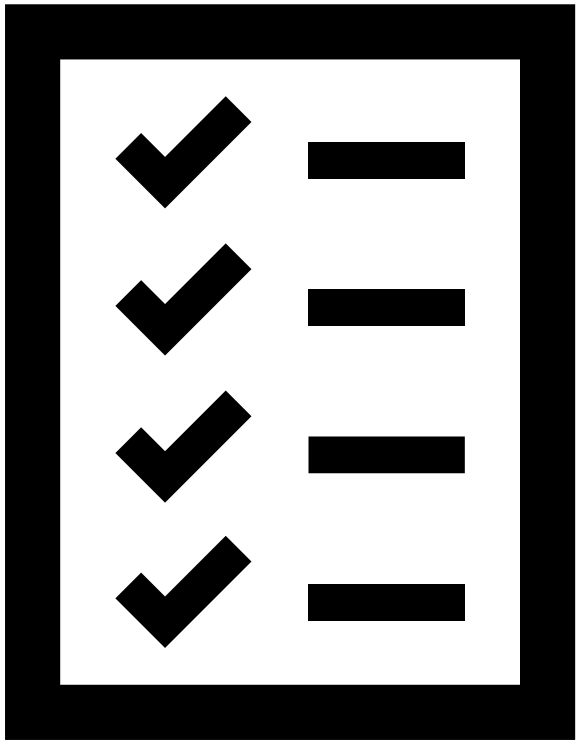
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

RECAP

1. What is innovation? Provide examples of different types of innovation.
2. How does blockchain impact business model innovation?
3. How can blockchain improve data management and validation?
4. What is blockchain role in enabling business development and innovation?

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

QUIZ:



- Follow the link to the quiz :
  - Moodle block “Blockchain components and security methods"

    Quiz #1 “The opening quiz”.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

THINK! IMPORTANT FACTS

- The choice of the right/appropriate technology to support business process is a key to business success or failure.
- Scholars and practitioners still lack systematic and reliable information on the blockchain technology, and the specificities of tasks related to the implementation projects involving blockchain.
- The lack of information and understanding about the technology is believed to be one of the reasons for the reported failure rate of 92,5 percent for blockchain projects (Forbes, 2019).
- Future blockchain professionals should have basic understanding how to connect the technical, business, legal and other aspects of this technology in a meaningful way.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

LEARNING GOALS

Explain the relationship between the key technological constructs of the blockchain and the security issues:

1. **Recognize blockchain-specific technical features (the key blockchain components).**
2. Introduce important terminology on information systems security.
3. Recognize the essential security issues in the deployment of information systems.
4. Explain what security methods are used to tackle the existing security issues in blockchain.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC TECHNICAL FEATURES

Those features make blockchain different from “traditional” business information systems:

1. Blockchain is based on **peer-to-peer (P2P) distributed network**, whereas most traditional business systems deploy client-server architecture.

2. Trust and integrity of data is dependent not on a trusted authority as it is in a traditional business, but on **the use of algorithms and cryptographic methods** in a distributed network.

3. Automation of transactions is established with the use of “**smart contracts**”. While there is nothing new or distinctive in the use of “smart contracts” per se, in combination with features 1. and 2. above some features of smart contracts in blockchain should be reviewed.

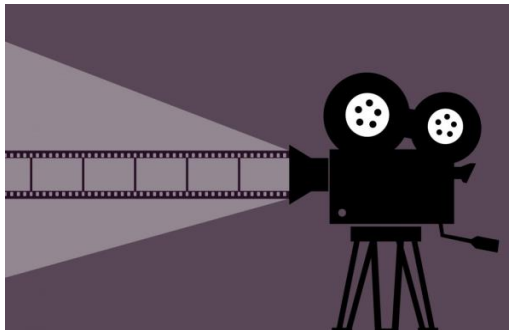
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

KEY BLOCKCHAIN COMPONENTS: SMART CONTRACTS

- Blockchain technology provides a platform for running smart contracts.
- ***Smart contracts*** are automated, autonomous programs that reside on the blockchain network and encapsulate the business logic and code needed to execute a required function when certain conditions are met.
  - For example, think about an insurance contract where a claim is paid to the traveller if the flight is cancelled.

Watch a video: 04:16 min

Smart contracts

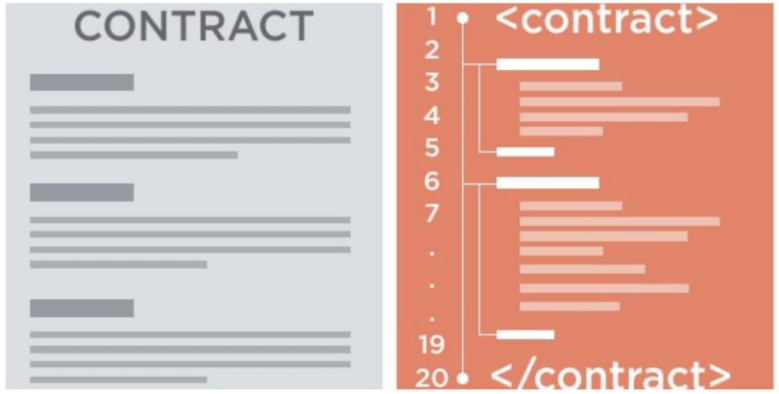


https://youtu.be/ZE2HxTmxfrI

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

SMART CONTRACTS: THE TECHNOLOGY PERSPECTIVE

… In other words, they are little programs that execute "**if this happens then do that"**, run and verified by many computers to ensure trustworthiness.



However, **smart contracts do NOT have the same legal value as regular business contracts.**

In the context of blockchains and cryptocurrencies, smart contracts are:

1. **Pre-written logic** (computer code);
2. **Stored and replicated on a distributed storage platform** (e.g. a blockchain);
3. **Executed / run by a network of computers** (usually the same ones running the blockchain);
4. **Can result in ledger updates** (cryptocurrency payments, etc).

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

SMART CONTRACTS AROUND US

Smart contracts *are automated, autonomous programs that encapsulate the business logic and code needed to execute a required function when certain conditions are met.*

Given the definition of a smart contract, discuss whether or not the following examples are examples of the use of smart contracts:

1. Withdrawing money from ATM;
2. Buying soda from a soda dispenser;
3. Paying for a car wash service at automatic car wash facility;
4. Exchanging currency at the currency exchange teller machine at an airport.

What will your actions be if you do not receive the product or services you paid for in the examples above? That would establish the case of **repudiation** - refusal to fulfil or discharge an agreement.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

SMART CONTRACTS: THE BUSINESS PERSPECTIVE

- The immutability and lack of recourse options make smart contracts **inappropriate for use as legal contracts** as defined by traditional legislative standards.

- The immutability of a “smart contract” can cause significant issues **if the computer program representing the contract is faulty or malfunctions**, as occurred in the case of “The DAO”, where substantial financial loss was incurred.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

SMART CONTRACTS: THE BUSINESS PERSPECTIVE

- For smart contracts to become a viable commercial tool, they must be not only technically but also legally enforceable.
- The trustless and incorruptible character of the blockchain is of limited significance if the code of the smart contract executes outside of the blockchain and if self-enforcement is incapable of protecting the parties from the risk of computer errors or from the possibility of changed circumstances.
- The parties to a smart contract must retain the ability to rely on traditional legal protections. Such protections are, however, only reserved to those relationships that carry the indicia of a contract.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC TECHNICAL FEATURES

Those features make blockchain different from “traditional” business information systems:

1. Blockchain is based on **peer-to-peer (P2P) distributed network**, whereas most traditional business systems deploy client-server architecture.

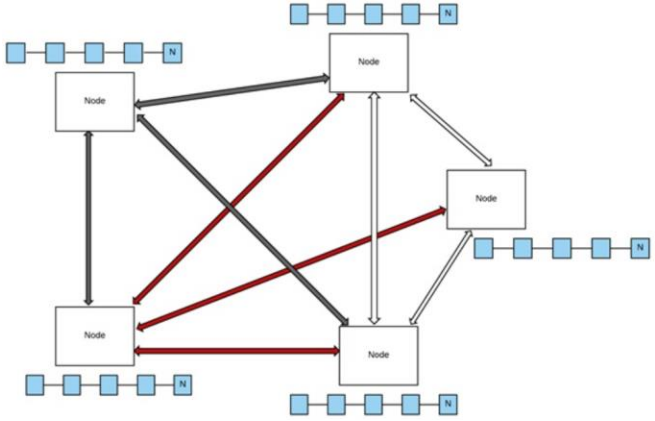
2. Trust and integrity of data is dependent not on a trusted authority as it is in a traditional business, but on **the use of algorithms and cryptographic methods** in a distributed network.

3. Automation of transactions is established with the use of “**smart contracts**”. While there is nothing new or distinctive in the use of “smart contracts” per se, in combination with features 1. and 2. above some features of smart contracts in blockchain should be reviewed.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC TECH FEATURES: DISTRIBUTED P2P NETWORK

- The backbone of blockchain methodology is formed by **peer-to-peer** (P2P) network architecture.
- This policy authorizes us to remove the dependency on a central decision-making source called a **server**.
- The user has to completely **trust** networks and hope they don't have a back door to quietly read or manipulate the reports.
- The nodes comprising computers, routers, etc., interact and share data directly with one another; thus, distributing all the data across all nodes in the grid rather than using a server.
- **All the nodes in the network will have a copy of the blockchain.**



KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

CENTRALIZED VS. DISTRIBUTED NETWORKS

The peer-to-peer network enables us to efficiently solve the obstacles faced in client-server architecture, i.e., single source of failure and scalability

Centralized	Distributed
Client-Server Architecture	P2P Architecture
The Server acts as the master and client as a slave	Peers are treated as nodes with equal capability
Adopted in small and large companies	Normally adopted small companies
Easy to set up and manage	Hard to set up and manage
Software installation is done on the server and it is accessed by the clients	Software installation is done on all the nodes and accessed by the nodes itself
Ex: Instagram	Ex: BitTorrent

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC TECHNICAL FEATURES

Those features make blockchain different from “traditional” business information systems:

1. Blockchain is based on **peer-to-peer (P2P) distributed network**, whereas most traditional business systems deploy client-server architecture.

2. Trust and integrity of data is dependent not on a trusted authority as it is in a traditional business, but on **the use of algorithms and cryptographic methods** in a distributed network.

3. Automation of transactions is established with the use of “**smart contracts**”. While there is nothing new or distinctive in the use of “smart contracts” per se, in combination with features 1. and 2. above some features of smart contracts in blockchain should be reviewed.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

LEARNING GOALS

Explain the relationship between the key technological constructs of the blockchain and the security issues:

1. Recognize blockchain-specific technical features (the key blockchain components).
2. **Recognize the essential security issues in the deployment of information systems.**
3. **Introduce important terminology on information systems security.**
4. Explain what security methods are used to tackle the existing security issues in blockchain.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

THREE ESSENTIAL SECURITY ISSUES FOR BUSINESS INFORMATION SYSTEMS

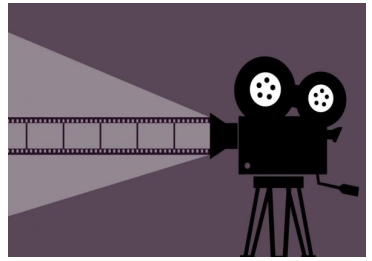
In developing and maintaining any (business) information system the same security questions have to be addressed:

1. How to ensure the identity of the sender and recipient of data/information is authentic/valid? This problem is referred to as **entity authentication.** **Prevent forgery at the origin**

2. How to ensure that the request of the sender (or the response of the recipient) has not been forged? This problem is referred to as **data origin authentication.** **Prevent forgery while in the transit**

3. How to ensure that data or business terms are kept in the system without allowing unauthorized modification? This problem is referred to as **integrity** and **non-repudiation.** **Prevent forgery at the destination**

Watch the video (05:30 min)
Security issues in P2P networks



https://youtu.be/2sPpuMclSQU

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES IN INFORMATION SYSTEMS

In developing and maintaining any (business) information system three essential security questions have to be addressed:

1: How to ensure the identity of the sender and recipient of data/information is authentic/valid? I.e., how to prevent forgery at the origin?

The simplest example here is **authentication** we are used to in a form of “log-ins” - e.g., you have to enter your user name and password to to be allowed using an information system or a device: your Moodle account, your iPhone, e-banking, etc.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES: PREVENT FORGERY AT THE ORIGIN

1: How to ensure the identity of the sender and recipient of data/information is authentic/valid? I.e., how to prevent forgery at the origin?

In May 1803, as Britain was preparing to end the Treaty of Amiens and declare war on France, a letter was hand delivered to Sir Charles Price, the Lord Mayor of London at the Mansion-house. Allegedly written by Lord Hawkesbury, and sealed with his personal seal, the letter claimed that the dispute with France was amicably settled. The Mayor at once took the letter to the Stock Exchange to share the joyous news. Stocks immediately rose 5 per cent. By the time when it was determined that the letter was indeed a forgery, many stocks had changed hands at inflated rates and the Committee of the Stock Exchange called for reports from the Brokers, to determine who might have gained from the fraudulent letter. https://www.thesocialhistorian.com/fake-news/

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

IMPORTANT TERMINOLOGY: ENTITY AUTHENTICATION

- **Authentication** provides assurance about the identity of an entity or the validity of a message.
- **Entity authentication** is the assurance that an entity is currently involved and active in a communication session.
- Traditionally, users are issued a username and password that is used to gain access to the various platforms with which they are working. This practice is known as single-factor authentication, as there is only one factor involved, namely, something you know, that is, the password and username.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES IN INFORMATION SYSTEMS

In developing and maintaining any (business) information system three essential security questions have to be addressed:

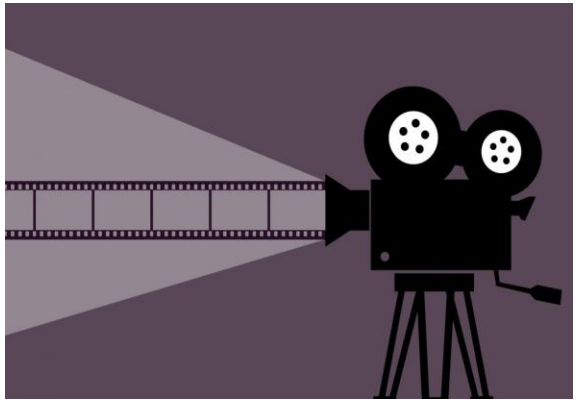
2: How to ensure that the request of the sender (or the response of the recipient) hasn't been forged? I.e., how to prevent forgery while in the transit?

Think of this as receiving news from a well known or unknown source. Which one will you trust more?

A (digital) **signature** is the most common method of ensuring the authenticity of the data origin.

Watch a video: 04:40 min

Symmetric and asymmetric encryption



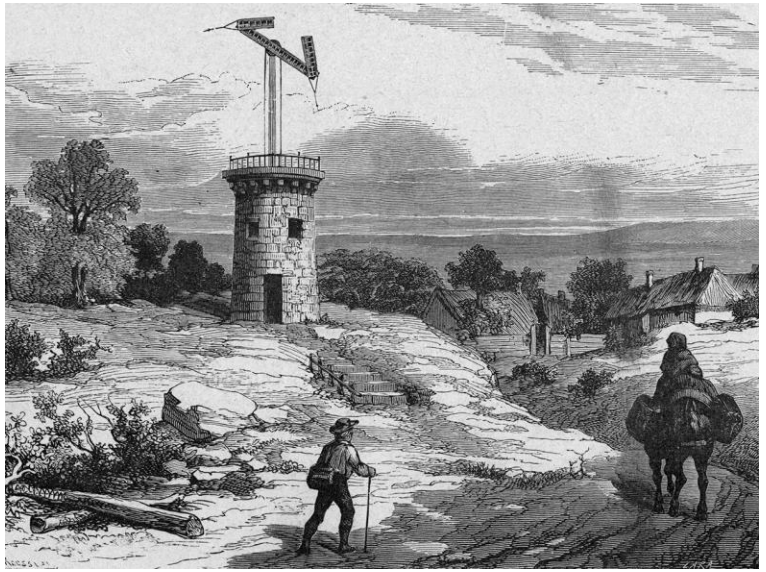
https://youtu.be/AQDCe585Lnc

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES: PREVENT FORGERY WHILE IN TRANSIT

2: How to ensure that the request of the sender (or the response of the recipient) hasn't been forged? I.e., how to prevent forgery while in the transit?

In the work of Alexadre Dumas "The count of Monte Cristo", Monte Cristo bribes the telegraph operator to send a message he has prepared to the ministry of the interior. As soon as the message arrives at the ministry, Debray rushes to Madame Danglars and tells her he's learned there is political trouble in Spain. He advises that her husband should sell all his Spanish government bonds. Danglars sells the bonds at a loss. But the next day, the report about Spain is determined to be false due to a misread telegraph signal. Spanish stocks double in value, and Danglars loses a million francs.
https://www.coursehero.com/lit/The-Count-of-Monte-Cristo/chapters-60-61-summary/



KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

IMPORTANT TERMINOLOGY: DATA ORIGIN AUTHENTICATION

- **Authentication** provides assurance about the identity of an entity or the validity of a message.
- **Data origin authentication,** also known as message authentication, is an assurance that the source of the information is indeed verified.
- **Asymmetric cryptography** refers to a type of cryptography where the key that is used to encrypt the data is different from the key that is used to decrypt the data. This is also known as **public key cryptography**. It uses both public and private keys to encrypt and decrypt data, respectively.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES IN INFORMATION SYSTEMS

In developing and maintaining any (business) information system three essential security questions have to be addressed:

3: How to ensure that data or business terms are kept in the system without allowing unauthorized modification or without allowing the authorized users deny their business commitments? I.e., how to prevent forgery at the destination?

Two IS security concepts are relevant in addressing this question: **integrity** and **non-repudiation.**

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

ESSENTIAL SECURITY ISSUES: PREVENT FORGERY AT THE DESTINATION

3: How to ensure that data or business terms are kept in the system without allowing unauthorized modification or without allowing the authorized users deny their business commitments? I.e., how to prevent forgery at the destination?

Yves Chaudron is best known for his involvement in the infamous art theft of the Mona Lisa in 1911. The plan was concocted with Italian patriot Vincenzo Peruggia, who wanted to restore it to Italy. ***He made six copies of the painting whilst its location was still unknown and sold each of them to American buyers.*** *With each painting worth $330,000, he made off with a pretty penny.*
https://www.sleek-mag.com/article/art-forgers/

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

LEARNING GOALS

Explain the relationship between the key technological constructs of the blockchain and the security issues:

1. Recognize blockchain-specific technical features (the key blockchain components).
2. Recognize the essential security issues in the deployment of information systems.
3. Introduce important terminology on information systems security
4. **Explain what security methods are used to tackle the existing security issues in blockchain.**

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

INTEGRITY AND NON-REPUDIATION

How to ensure that data or business terms are kept in the system without allowing unauthorized modification or without allowing the authorized users deny their business commitments?

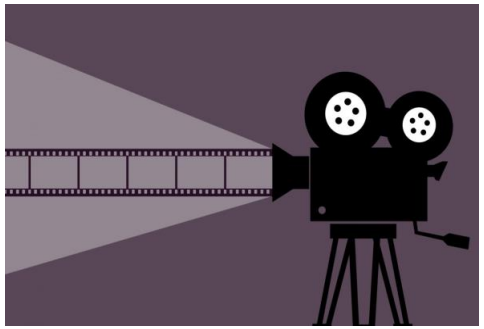
- In traditional bilateral or centralized IS the questions of **integrity and non-repudiation** are taken care of by one or more business or legal entities – e.g., a bank, or a stock-exchange, etc.
- For example, a bank will invest in the security of its systems, making sure all financial information is kept safe, without allowing unauthorized modifications to your bank account. The bank will also make sure you can not deny having withdrawn money from ATM – the **non-repudiation** in this case will be ensured by a combination of different methods: the fact that you used a PIN code which is known only to you (single factor entity authentication); the video recording from a camera in the ATM; and the business laws which protect the bank from malicious acts of customers.
- If two business partners cannot come to an agreement on whether or not a certain transaction does not fulfil the requirements / rules of the business terms previously agreed upon by those partners, they will ask an arbitrage (another business partner or a court) to rule out the case.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

IMPORTANT TERMINOLOGY: INTEGRITY AND NON-REPUDIATION

- **Non-repudiation** is the assurance that an entity cannot deny a previous commitment or action by providing incontrovertible evidence.
- It is a security service that offers **definitive proof that a particular activity has occurred**.
- This property is essential in debatable situations whereby an entity has denied the actions performed, for example, placement of an order on an e-commerce system.
- To ensure non-repudiation is: this service produces cryptographic evidence in electronic transactions so that in case of disputes, it can be used as a confirmation of an action.
- **Integrity** is the assurance that information is modifiable only by authorized entities.

Watch a video: watch first 02:31 min
Integrity & non-repudiation



https://youtu.be/4w2MTKx4d6A

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC SECURITY ISSUES

Blockchain is a distributed peer-to-peer (P2P) network, which has no centralized authority to maintain trust and security. Therefore, the trust and security mechanisms must be "built in" the network and its operation.

With no centralized server nor authority, how can we ensure data integrity and non-repudiation of transactions? I.e., how can we maintain the requirement that all the nodes in the network have the same copy of the blockchain?

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

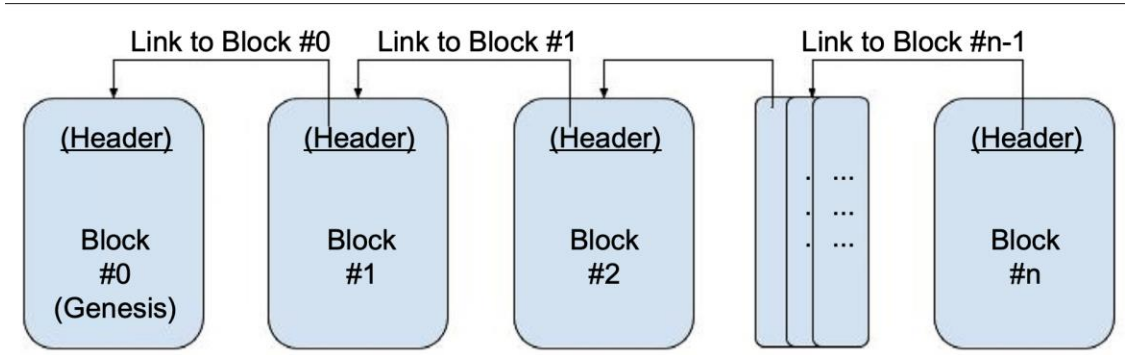
BLOCKCHAIN-SPECIFIC TECH FEATURES: WHAT MANAGERS MUST KNOW

- A choice of appropriate blockchain technology requires managers to understand how a blockchain validates transactions and creates and adds blocks to grow the blockchain.
- Blockchain nodes are either:
  1. Miners who create new blocks and mint cryptocurrency (coins);
  2. Block signers who validate and digitally sign the transactions.
- **Transaction verification**: Any transactions posted from the nodes on the blockchain are verified based on a predetermined set of rules. Only valid transactions are selected for inclusion in a block.
- A critical decision that every blockchain network has to make is to figure out that which node will append the next block to the blockchain.
- This decision is made using a **consensus mechanism.**

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

HOW TRANSACTIONS ARE CREATED AND VALIDATED IN BLOCKCHAIN

- If the signed transaction is properly formed, valid and complete**, it is included in a block**, which is then propagated onto the network. At this point, **the transaction is considered confirmed**.
- The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.



- Transactions are then reconfirmed every time a new block is created. For example, in the Bitcoin network six confirmations are required to consider the transaction final.

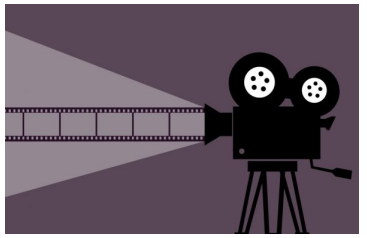
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN-SPECIFIC SECURITY ISSUES

With no centralized server nor authority, how can we ensure data integrity and non-repudiation of transactions? I.e., how can we maintain the requirement that all the nodes in the network have the same copy of the blockchain?

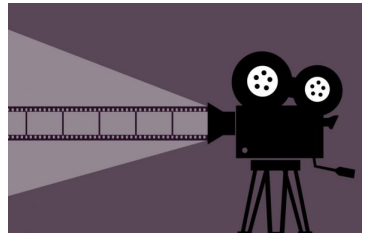
- Blockchain **consensus protocol** creates an **indisputable system of understanding** between various nodes across a distributed network.
- This permits us to keep all the nodes on the grid **synchronized with one another**.

Watch a video: 03:54 min
Understanding consensus mechanisms



https://youtu.be/dylgwcPH4EA

Watch a video: 04:00 min
Blockchain consensus mechanisms: PoW, PoS, PoA



https://youtu.be/ojxfbN78WFQ

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BLOCKCHAIN CONSENSUS MECHANISMS

There are two main categories of consensus mechanisms in blockchains:

1. Proof-based, leader-election lottery based, or the Nakamoto consensus whereby a leader is elected at random (using an algorithm) and proposes a final value.
    - This category is also referred to as the ***fully decentralized*** **or** ***permissionless*** type of consensus mechanism. This type is well used in the Bitcoin and Ethereum blockchain in the form of a Proof of Work (PoW) mechanism.
2. Byzantine Fault Tolerance (BFT)-based is a more traditional approach based on rounds of votes. This class of consensus is also known as the ***consortium*** **or** ***permissioned*** type of consensus mechanism.

BFT-based consensus mechanisms perform well when there are a limited number of nodes, but they do not scale well. On the other hand, leader-election lottery based (PoW) type consensus mechanisms scale very well but perform very slowly.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

CONSENSUS MECHANISMS

- Public blockchains underlie the vast majority of cryptocurrency-based platforms, such as Bitcoin, Ethereum, and Litecoin. These types of blockchains are ***permissionless***, ***decentralized*** computing architectures ***open to the public*** and ***maintained by arbitrary users*** who possess Internet access.

- Anyone with Internet access can participate in the exchange of digital assets in these (public blockchain) platforms.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

CONSENSUS MECHANISMS

- Public blockchains must guarantee that the shared ledger of transactions always provides the same snapshot to whoever accesses the chain at a given time to avoid incurring large volumes of digital asset exchanges.
- As a result, public blockchains typically implement the most robust mechanisms to reach consensus in highly decentralized global networks.
- These mechanisms may be more time consuming than others used in permissioned blockchains, but they more resilient to attacks from (minority) rogue players.
- Transactions in public ledgers are therefore immutable and transparent.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

MINI-CASE: *FIRST INFORMATION REPORT (FIR)*

The first information report (FIR) is the written document maintained by the police department that has the information collected about any criminal offense. It is generally a complaint lodged with the police by the victim of a cognizable offense or by someone on his or her behalf, but anyone can make such a report either orally or in writing to the police, after which an investigation is started by the police. The person giving information has the right to see what is being mentioned and has to affix his signature to it, stating it's correct. The existing system is handwritten, time-consuming and less secure; and there is no way to track if events are being recorded properly. The FIR acts as sensitive data and provides clues for the investigation. Thus, the data stored must be secured and should not be tampered with or influenced by external pressure once the report is written. The FIR details are stored in a ledger where they can be manipulated. So, to mitigate this we can use blockchain technology once the data is stored in a block since it has its hash value and it is linked. Whenever anybody tries to change even a small character or even a space the hash value immediately changes due to the avalanche effect and hence indicates that data has been tampered with. This provides high security of data and eliminates the manipulation of information. The person who provided the information can keep track of it by using the hash value that is generated when the data block is added. The advantages of the FIR is that it reduces cost and time, eliminates manual errors, and online information can be seen by anybody. The FIR consists of information like place, time, date, and detailed descriptions, all of which are stored in a block of the blockchain and the hash value is given to the user to check whether the details are provided correctly and to make sure no information is misinterpreted. Thus, by using blockchain technology a major problem is solved and data integrity is ensured.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

WHAT A MANAGER MUST KNOW ABOUT CONSENSUS MECHANISMS

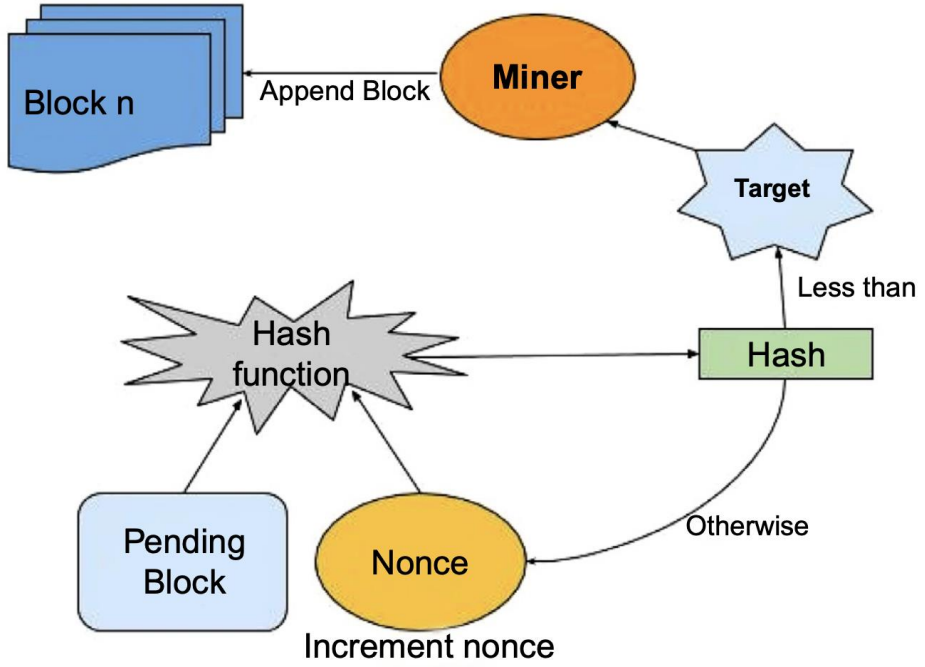
- The choice of the right/appropriate technology to support business process is a key to business success or failure.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

PROOF OF WORK (POW)

- With PoW, as new, unverified transactions become available or broadcast to the entire blockchain network, each node that maintains a copy of the ledger (also known as a “miner”) verifies a set of those transactions by balancing the incoming and outgoing digital assets with previously validated transactions to prevent so called “double spending”.

- The miner next groups validated transactions into a tentative block. Each miner then competes in solving a computationally expensive algorithmic “puzzle” to ensure that their block is valid and that it follows in sequence from the last block in the current chain. Only the winner with a correct answer is privileged to append their block of transactions to the shared ledger and gains a mining reward in cryptocurrency (e.g., Bitcoins).



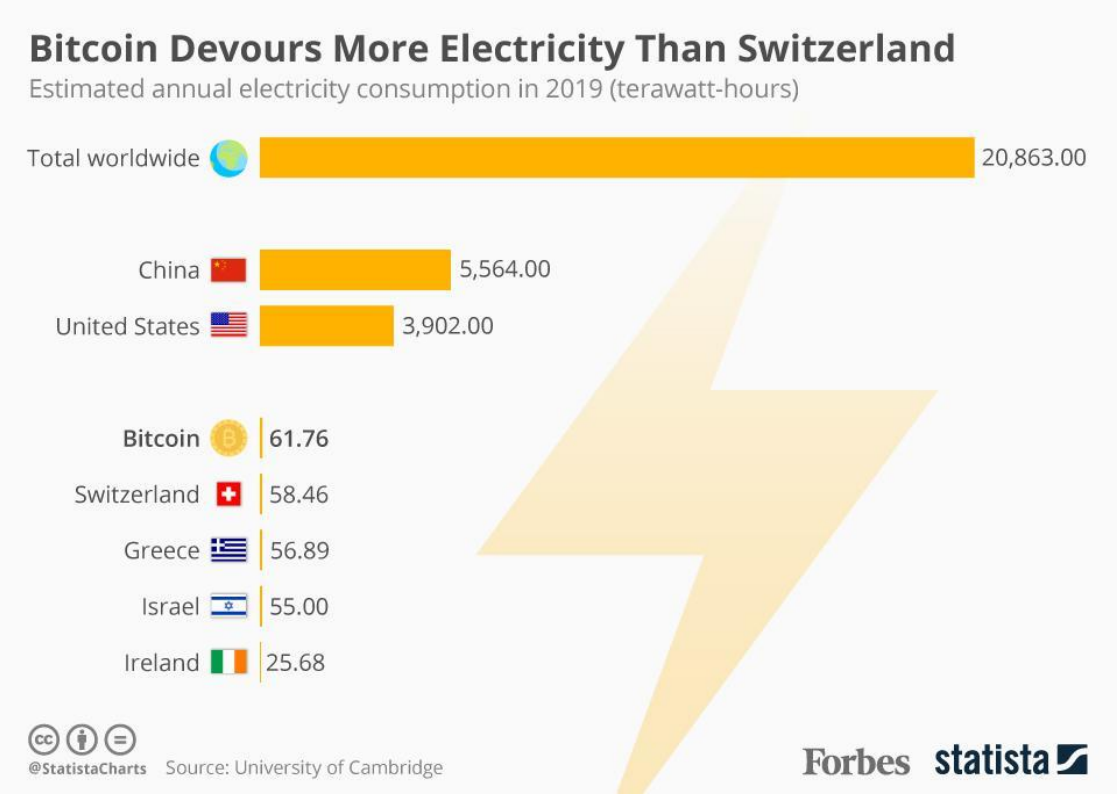
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

PROOF OF WORK (POW): DRAWBACKS

- Two major drawbacks of PoW mechanism are **high energy consumption and long time required to solve computational puzzle**, thus resulting in long time needed to confirm a transaction.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

POW: HIGH ENERGY CONSUMPTION



- Bitcoin uses an estimated 61.76 terawatt-hours (TWh) of electricity per year - more than many countries and approximately 0.28% of total global electricity consumption.
- If Bitcoin was a country, it would be the 41st most-energy-demanding nation on the planet.
- See how much electricity is consumed by bitcoin network using online real-time Cambridge Bitcoin Electricity Consumption Index: https://www.cbeci.org

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

POW: SLOW TO APPROVE TRANSACTIONS

- The transaction throughput is the number of transactions per second *Tx/s* a network can process, which is vital to the performance of the network especially when there are many pending transactions.
- *Tx/s* can be calculated by:

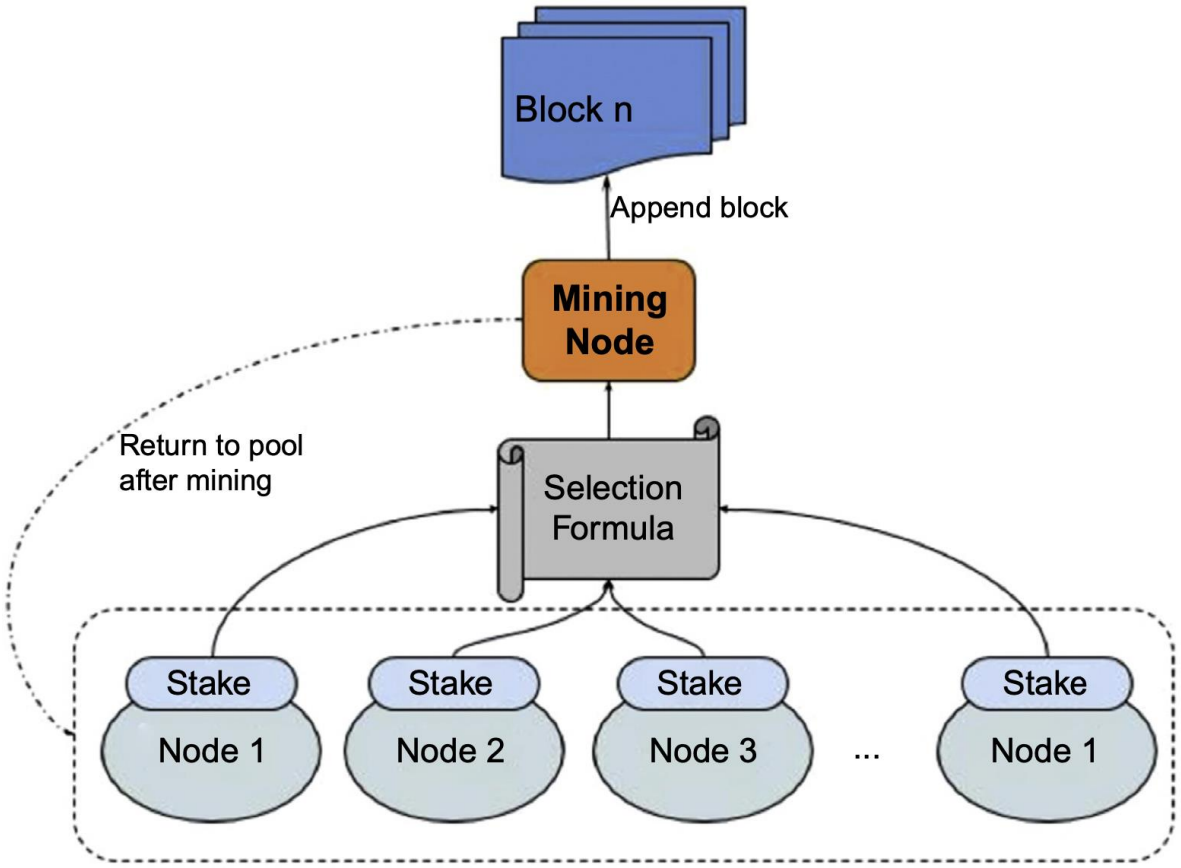
$$Tx/s = \frac{Block_{size}}{Tx_{size} \times Block_{time}}.$$

- For example, the Bitcoin network has *Blocksize* = 1 *MB*, *Txsize* = 250 *bytes*, and *Blocktime* = 600*s*, so it can process around 7 transactions per second. The *Tx/s* determines how quickly a transaction is added to the chain, whereas the block confirmation time dictates how fast the transaction is confirmed after it is added. The block confirmation time depends on *Blocktime*, i.e., the average time it takes for a new block to be added to the chain, and the finality of the consensus mechanisms. In the Bitcoin network, a transaction usually has to wait for $k = 6$ blocks before it can be confirmed, so the average confirmation time is $k \rightarrow Blocktime = 3600s = 1hr$

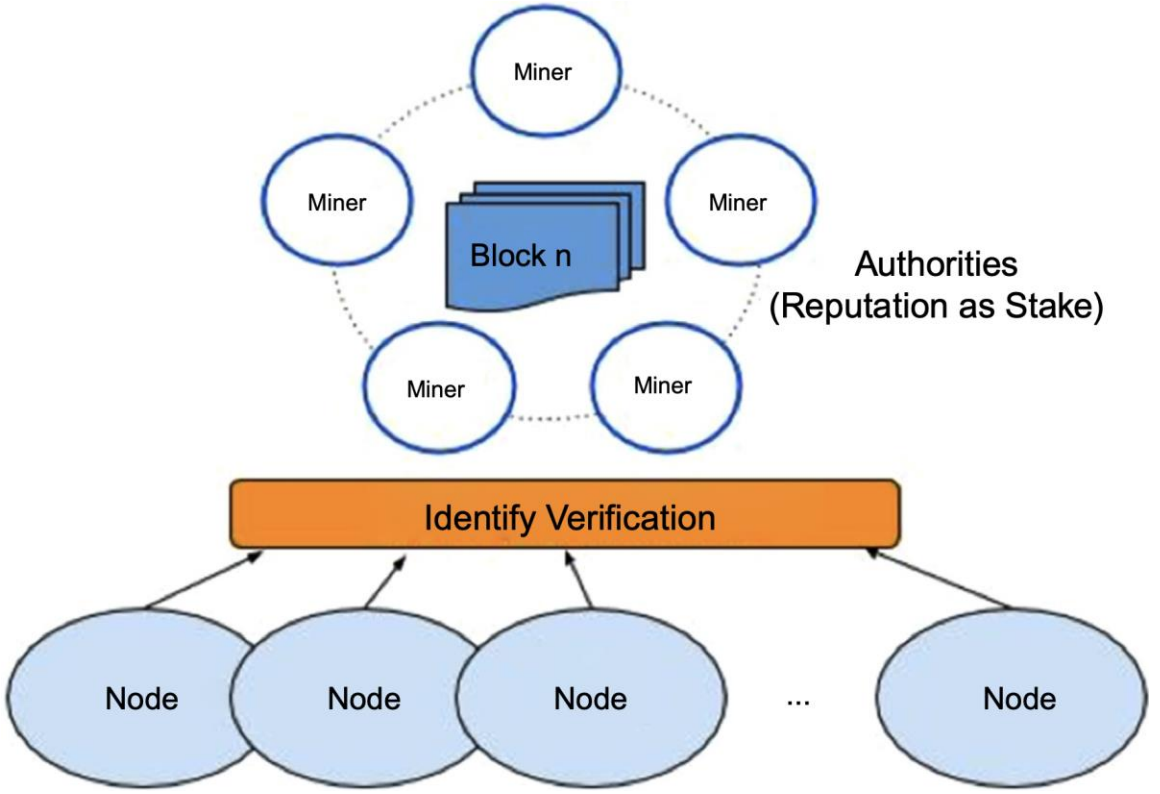
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

OTHER CONSENSUS MECHANISMS

Proof of stake (PoS)



Proof of authority (PoA)



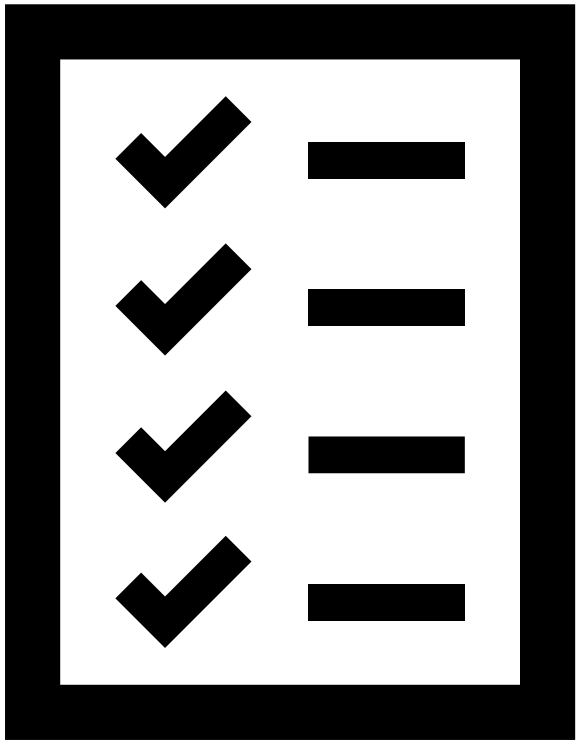
KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

CONSENSUS MECHANISMS: SUMMARY

- Each consensus mechanism can optimize at most two of the three attributes in a DLT network:
  1. **Degree of decentralization** (number of network miners/maintainers/members);
  2. **Scalability** (transaction throughput; number of transactions per second);
  3. **Randomness in block generation and miner selection** (dependencies in mining hardware, stakeholding, impact and importance to the network).

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

QUIZ:



- Follow the link to the quiz :
  - Moodle block “Blockchain components and security methods"

    → Quiz #2 “The closing quiz”.

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

SELF-REFLECTION QUESTIONS:

1. Can you tell what technical features make blockchain-based information systems to be different from what can be referred to as “traditional” or “centralized” information systems used by business and private entities?

2. Do you understand the importance of the three essential security questions (how to prevent a forgery at the source, in the transit, and at the destination) in supporting business operations with information systems and technologies? Have you had to deal with any of these in your own private or business activities?

3. Which security measures would you trust more, those based on algorithms or those based on organizational policies and efforts? For example, would you trust your money is safer in a bank or on the blockchain-based crypto-currency platform?

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

BIBLIOGRAPHY:

1. Bashir, I. (2018). „Mastering Blockchain: Distributed ledger technology, decentralization, and smart contracts explained“ (Second Edition). Packt Publishing Ltd.
2. Copigneaux, B., Probst, L., Lefebvre, V., Brown, J. (2018). „Digital Transformation Monitor. Blockchain.“ European Commission, Directorate-General Internal Market, Industry, Entrepreneurship and SMEs. Access: https://ec.europa.eu/growth/tools-databases/dem/
3. Forbes.com. (2019, May 20). Why Enterprise Blockchain Projects Fail. https://www.forbes.com/sites/dantedisparte/2019/05/20/why-enterprise-blockchain-projects-fail/#72a94c4f4b96
4. Forbes.com (2019). „Bitcoin Devours More Electricity Than Switzerland“. Access: https://www.forbes.com/sites/niallmccarthy/2019/07/08/bitcoin-devours-more-electricity-than-switzerland-infographic/
5. Mik, E. (2017). „Smart contracts: Terminology, technical limitations and real world complexity“. Law, Innovation and Technology, 9(2), pp.269–300. Access: https://doi.org/10.1080/17579961.2017.1378468
6. Morabito, V. (2017). “Business Innovation Through Blockchain: The B³ Perspective”. Springer.
7. Mulligan, C., Zhu Scott, J., Warren, S., Rangaswami, J. (2018). „Blockchain Beyond the Hype A Practical Framework for Business Leaders“. Access: http://www3.weforum.org/docs/48423_Whether_Blockchain_WP.pdf
8. Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T. Dutkiewicz, E. (2019). „Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities“. IEEE Access, Vol.7, pp.85727–85745. Access: https://doi.org/10.1109/ACCESS.2019.2925010
9. Shrivastava, G., Le, D.-N., Sharma, K. (Eds.) (2020). „Cryptocurrencies and Blockchain Technology Applications“. Wiley.
10. The DAO Attack. We take a look at the most significant event in cryptoeconomics since the birth of Bitcoin and it's impact on the Ethereum Blockchain. https://www2.deloitte.com/ie/en/pages/technology/articles/DAO-Attack-Analysis.html
11. Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., Mendling, J. (2016). „Untrusted business process monitoring and execution using blockchain“. In International Conference on Business Process Management, pp. 329–347. Springer. Access: https://link.springer.com/chapter/10.1007/978-3-319-45348-4_19
12. Zhang, P., Schmidt, D. C., White, J., Dubey, A. (2019). „Consensus mechanisms and information security technologies“. In Advances in Computers (Vol. 115, pp. 181–209). Elsevier. Access: https://doi.org/10.1016/bs.adcom.2019.05.001

This project has been funded with support from the European Commission. This publication reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein. Project Number: 2018-1-LT01-KA203-047044

FURTHER READINGS:

1. Podcast: Unchained – Shin, L., Cuomo, J. (2017). “IBM’s Jerry Cuomo On Everything From Blockchain Security To Hyperledger To The Internet Of Things”. Access: https://unchainedpodcast.com/ibms-jerry-cuomo-on-everything-from-blockchain-security-to-hyperledger-to-the-internet-of-things/

2. Lumineau, F., Wang, W., Schilke, O. (2020). „Blockchain governance—A new way of organizing collaborations“. Organization Science. Access: https://ssrn.com/abstract=3562941

3. Forbes.com. (2019). „Why Enterprise Blockchain Projects Fail“. Access: https://www.forbes.com/sites/dantedisparte/2019/05/20/why-enterprise-blockchain-projects-fail/#72a94c4f4b96

4. Zhang, P., Schmidt, D. C., White, J., Dubey, A. (2019). „Consensus mechanisms and information security technologies“. Advances in Computers, Vol.115, pp.181–209. Elsevier. Access: https://doi.org/10.1016/bs.adcom.2019.05.001

5. Nguyen, C.T., Hoang, D.T., Nguyen, D.N., Niyato, D., Nguyen, H.T. Dutkiewicz, E. (2019). „Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities“. IEEE Access, Vol.7, pp.85727–85745. Access: https://doi.org/10.1109/ACCESS.2019.2925010

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044

VIDEO MATERIALS:

1. Symmetric and asymmetric encryption (04:40 min): https://youtu.be/AQDCe585Lnc
2. Integrity & non-repudiation (watch the first 02:31 min): https://youtu.be/4w2MTKx4d6A
3. Main security issues in P2P networks (05:31 min): https://youtu.be/2sPpuMclSQU
4. Understanding consensus mechanisms (03:54 min): https://youtu.be/dylgwcPH4EA
5. Blockchain consensus mechanisms PoW, PoS, PoA (04:00 min): https://youtu.be/ojxfbN78WFQ
6. Smart contracts (04:16 min): https://youtu.be/ZE2HxTmxfrI

KA2 - Cooperation for Innovation and the Exchange of Good Practice Strategic Partnerships for higher Education 2018, no. 2018-1-LT01-KA203-047044