



BRNO UNIVERSITY OF TECHNOLOGY

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

FACULTY OF MECHANICAL ENGINEERING

FAKULTA STROJNÍHO INŽENÝRSTVÍ

INSTITUTE OF SOLID MECHANICS, MECHATRONICS AND BIOMECHANICS

ÚSTAV MECHANIKY TĚLES, MECHATRONIKY A BIOMECHANIKY

UTILIZATION OF BLOCKCHAIN TECHNOLOGY IN THE AREA OF MECHANICAL ENGINEERING

VYUŽITÍ TECHNOLOGIE BLOCKCHAIN VE STROJÍRENSTVÍ

BACHELOR'S THESIS

BAKALÁŘSKÁ PRÁCE

AUTHOR

AUTOR PRÁCE

Oliver Džupa

SUPERVISOR

VEDOUCÍ PRÁCE

Ing. Marek Tamaškovič

BRNO 2022

Assignment Bachelor's Thesis

Institut: Institute of Solid Mechanics, Mechatronics and Biomechanics
Student: **Oliver Džupa**
Degree program: Applied Sciences in Engineering
Branch: Mechatronics
Supervisor: **Ing. Marek Tamašковиč**
Academic year: 2021/22

As provided for by the Act No. 111/98 Coll. on higher education institutions and the BUT Study and Examination Regulations, the director of the Institute hereby assigns the following topic of Bachelor's Thesis:

Utilization of Blockchain Technology in the Area of Mechanical Engineering

Brief Description:

This topic is about getting familiar with blockchain applications and finding their advantages and disadvantages. The student should identify problems within the industry of mechanical engineering, and he should find a solution by application of the blockchain into this field. The solution should be conceptual work and it should be evaluated with the existing centralized solutions.

Bachelor's Thesis goals:

1. Get familiar with the principles of the blockchains, their features, consensus protocols, and smart contracts.
2. Study existing applications of blockchains in various domains and explain the features of blockchains that are of particular benefit for studied applications.
3. Analyze existing areas of mechanical engineering and their problems related to features that blockchains offer.
4. Propose a few case studies of conceptual utilization of blockchains or smart contracts in the area of mechanical engineering.
5. Analyze the pros and cons of the proposed case studies and compare them with the centralized solutions.

Recommended bibliography:

HOMOLIAK, Ivan, et al. "The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses." IEEE Communications Surveys & Tutorials 23.1 (2020): 341-390.

CASINO, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current status, classification and open issues." *Telematics and informatics* 36 (2019): 55-81.

Deadline for submission Bachelor's Thesis is given by the Schedule of the Academic year 2021/22

In Brno,

L. S.

prof. Ing. Jindřich Petruška, CSc.
Director of the Institute

doc. Ing. Jaroslav Katolický, Ph.D.
FME dean

Abstract

This bachelor's thesis focuses on utilization of blockchain technology in the area of mechanical engineering. The first part is devoted to a full understanding of blockchain and smart contracts. The second part summarizes the use cases for both mechanical engineering and non-mechanical engineering fields and identifies features presented by blockchain. The third part is focused on case studies of conceptual utilization of blockchains in mechanical engineering and comparison with centralized solutions.

Abstrakt

Táto bakalárska práca sa zameriava na využitie blockchain technológie v oblasti strojárstva. Prvá časť práce je venovaná rešerši a zoznámeniu sa s blockchain technológiou a smart contractami. V druhej časti nájdeme zhrnutie využítí tejto technológie v strojárenských, ale aj mimo strojárenských oblastiach a identifikuje jej prednosti. Tretia časť je upriamená na koncepčné využitia blockchainu v strojárstve a ich porovnanie s centralizovanými riešeniami.

Key words:

blockchain, smart contract, use case, benefits, database

Klíčové slová:

blockchain, smart contract, využitie, prednosti, databáza

Reference:

DŽUPA, Oliver. *Využití technologie blockchain ve strojírenství*. Brno, 2022. Dostupné také z: <https://www.vutbr.cz/studenti/zav-prace/detail/139855>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta strojního inženýrství, Ústav mechaniky těles, mechatroniky a biomechaniky. Vedoucí práce Marek Tamaškovič.

Declaration:

I hereby declare that this Bachelor's thesis was prepared as an original work by the author under the supervision of Ing. Marek Tamaškovič. I have listed all the literary sources, publications, and other sources, which were used during the writing of this thesis.

.....
Oliver Džupa
May 16, 2022

Acknowledgements:

I would like to thank my supervisor Ing. Marek Tamaškovič for his guidance, time spent on consultations, and advice. A special thanks goes to my family and friends who always supported me through difficult times. And I also want to thank Sára for helping with proof reading and grammar.

Contents

1	Introduction	9
2	Theory and Background	10
2.1	Blockchain and Smart Contract history.....	10
2.2	Fundamentals.....	11
2.3	Cryptographic primitives used in blockchain.....	12
2.3.1	Asymmetric encryption.....	13
2.4	Blockchain features.....	14
2.5	Types of Blockchain.....	15
2.6	Consensus protocols.....	16
2.6.1	General examples.....	16
2.6.2	Examples for mechanical engineering purposes.....	16
3	Function and Application	17
3.1	Use cases in various fields.....	18
3.2	Analysis of qualities of blockchain versus traditional databases.....	22
3.3	Potential blockchain use cases for mechanical engineering.....	23
3.3.1	Internet of Things.....	23
3.3.2	Odometer.....	27
3.3.3	Supply Chain in Automotive Industry.....	28
3.3.4	Industry 4.0 and Cloud Manufacturing.....	30
3.3.5	Smart Grid.....	31
4	System Architectures for Blockchain-Based Systems	33
4.1	Infrastructure of distributed electric vehicle power stations.....	33
4.2	Inalterable odometer database.....	34
4.3	Automation of processes utilizing emerging technologies.....	36
5	Comparison of blockchain-based to centralized solutions	39
5.1	Advantages.....	39
5.2	Disadvantages.....	41
5.3	Challenges.....	42
6	Conclusion	43
	Bibliography	44
	List of Figures	52
	List of Tables	52

Chapter 1: Introduction

The pace of evolution in the mechanical engineering sector is growing exponentially, introducing new technologies to make processes faster, cheaper, more secure, and more efficient. To achieve such a level of advancement, systems must become automated and smarter. The profound digitalization and implementation of emerging technologies create a heavy burden on production, manipulation, and storage of data. The world became so data-driven that storing, securing, and transmitting information may be classified as the most crucial operation.

In this paper, an overview of how blockchain fits into this revolution is provided. To achieve a full understanding of this new technology and how it can be implemented into the engineering ecosystem, this study first explores the history and technical background behind blockchain. Explain some of the key concepts like asymmetric encryption and consensus protocol.

In the second stage, research of potential and already implemented use cases in various fields both in mechanical engineering and other fields to acknowledge the features of blockchain and most importantly, to understand why this technology fits certain applications.

In the last section of this thesis, there are presented three system architectures of different blockchain-based applications and their comparison to centralized systems.

Chapter 2: Theory and Background

2.1 Blockchain and Smart Contract History

When it comes to history of a blockchain technology, people have a widespread misconception that Bitcoin was the first blockchain created. The actual structure was first proposed in 1982, in David Chaum's dissertation (creator of e-cash). His specialization is in cryptography and computer science. His work offered a solution to protect digital data by using cryptography against manipulation and corruption. Chaum's work made it possible to secure sending and receiving messages without relying on a third party [1].

This was a huge steppingstone in solving a key mystery – data timestamping. In 1991 Stuart Haber with W. Scott Stornetta published a document called 'How to Time Stamp a Digital Document'. What they tried to achieve was to create a mechanism to store data verifiably and securely in a chronological manner [2].

With almost all steps necessarily made, in 2008 an anonymous figure(s) Satoshi Nakamoto released a white paper containing a model for Blockchain [4]. His/ers (Their) motivation for doing so, was a financial crisis in 2008. One year later, the first use case for blockchain called Bitcoin was launched.

After bitcoin was introduced to the public, there was a giant innovation boom in blockchain sector. Many new replications and variations of this new technology has appeared. Mostly in the financial ecosystem. Bitcoin took off and got many skilled developers interested to work and build on this project.

The concept of smart contracts was developed by Nicholas Szabo. An American computer scientist and cryptographer was the first with the goal of introducing law created purely through decentralized and digital manner [3].

"Smart contracts combine protocols with user interfaces to formalize and secure relationships over computer networks. Objectives and principles for the design of these systems are derived from legal principles, economic theory, and theories of reliable and secure protocols."

Szabo, N. (1997). Formalizing and Securing Relationships on Public Networks. *First Monday*, 2(9). <https://doi.org/10.5210/fm.v2i9.548>

2.2 Fundamentals

Blockchain is a decentralized, timestamped, append-only log with an auditable database. It is secured by cryptography:

- Hash functions for tamper resistance and integrity
- Digital signatures for permission
- Consensus mechanism to determine an agreement

Blockchain technology can be imagined as a data structure consisting of transactions, in as mentioned distributed append only and time-stamped ledger, ensuring non reliance on third parties. All the nodes (network validators) to reach an agreement, must run the system according to a consensus protocol [7].

Distributed ledger provides shared records among two or more entities, people, organizations, ... without an intermediary and therefore avoids dependance on any other participants of the ecosystem or paying any other service providing a master record. This record is then transparent and auditable by any authorized figure [7]. Transactions are performed in a peer-to-peer fashion. This mechanism is presented in Figure 2.1.

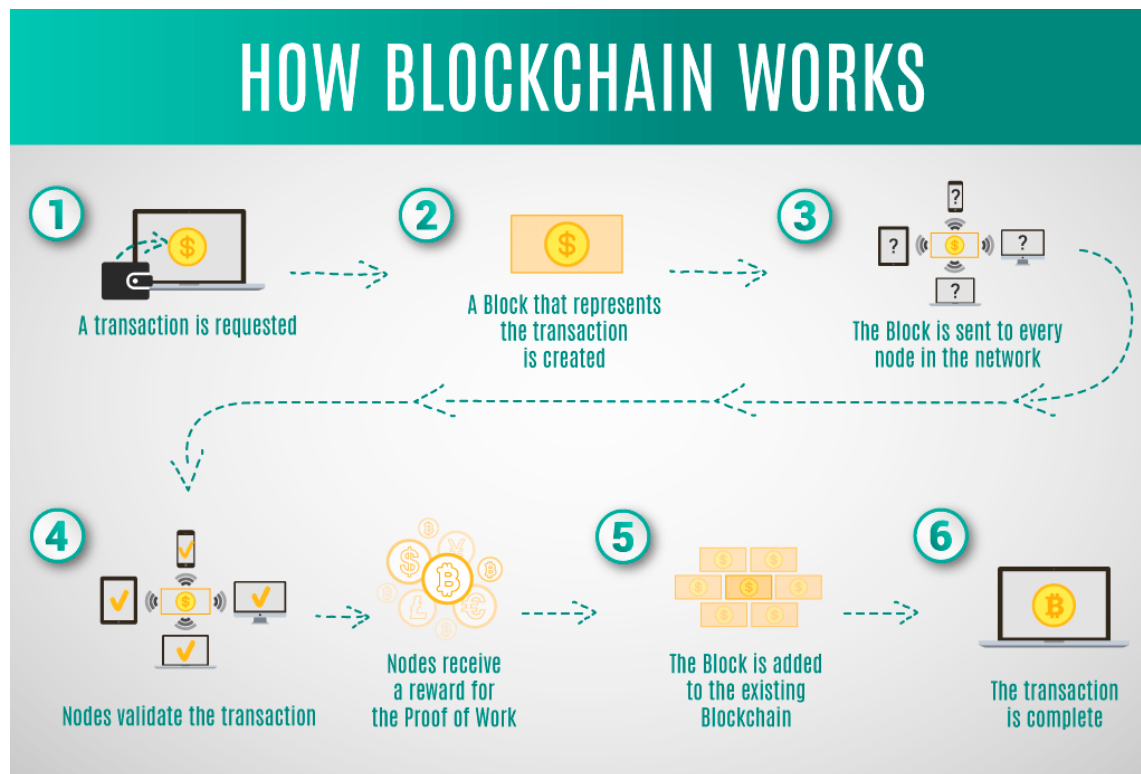


Figure 1: Transaction flow [14]

Data or transactions are bundled together to form a block-like structure, then linked to another block, to create linear chain-like structure. After a validated block gets added to the blockchain, it is broadcasted and updates every ledger in the network. The ability to link blocks together is provided by a hashing algorithm (more in section 2.3). Hash of a block is significant and unique [6].

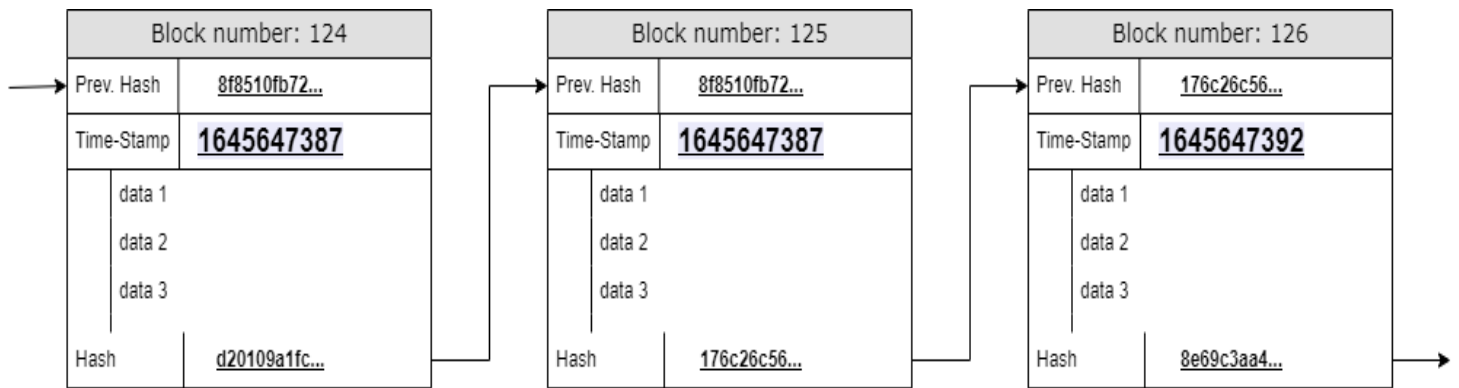


Figure 2: Blockchain structure

A smart contract is a computer program stored on the blockchain. It is a dynamic contract that can enforce its own provisions, take custody over assets on a ledger, track what has happened to date, and respond to incoming information or events e.g., parts have been successfully installed.

2.3 Cryptographic primitives used in blockchain

Cryptography is essentially a study of possibilities on how to securely communicate in private manner, in the presence of unauthorized entity. Process of converting a plain text into unintelligible message is called encryption [5].

Blockchain utilizes a particular one-way encryption process called hashing. The result of encrypting any size of data by hashing algorithm is a fixed size hexadecimal string of characters called hash. The most used hash function is SHA3-256, which generates unique 256-bit hash for any given data [5].

Hash functions must withstand various challenges:

- minimal collision resistance (different data can't return the same hash after encryption)
- irreversibility (impossible to decrypt hash into data)
- infeasible solvability
- meet the criteria of avalanche effect (one slight change of input completely changes the output)
- easily verifiable
- fast encryption

- predictability (same data always returns the same hash)

Table 1: Hashing examples

Input	Output
a	80084bf2fba02475726feb2cab2d8215eab14bc6bdd8bfb2c8151257032ecd8
A	1c9ebd6caf02840a5b2b7f0fc870ec1db154886ae9fe621b822b14fd0bf513d6
0001011100101	ef73b04e7ba9514e555f1a9464ac13c4f2862814a3a1247588fe5364c39d8d98
00010111001011	b3e071381d9e65211a7780a6819582567979c763b5ca5a11be7437fa6bab489

Any random binary input would produce a hash output, which means that anything digital can be hashed ex. pictures, digital signatures, music... This leads to authentication of ownership and storing information inalterably on blockchain.

2.3.1 Asymmetric encryption

Asymmetric encryption is used for publicly sending digital data, containing sensitive material. To ensure protection of such document and capability of decrypting it by receiver, asymmetric encryption is required [16].

First step is to generate a private and a public key, by using e.g., RSA algorithm [17]. Mentioned keys are mathematically linked to each other. Public key is used as a wallet address and private key signs the transactions.

Public key is visible by all network participants and is used to encrypt data. Private key allows receiver to decrypt such data and is hidden from any unauthorized figure [16]. Transmitter of digital documents encrypts data by using recipient's public key, allowing decryption only by the private key holder.

2.4 Blockchain features

Decentralization: system is being run by multiple nodes, which have a common agreement via consensus protocol. Each node should work simultaneously and independently. By following hard-set rules and a shared ledger, every participant (node) is partially responsible for the system's functionality. Therefore, central authority becomes dispensable. Upsides become resilient to a system failure and corruption.

Immutability: The shared ledger among participants is unalterable; any alteration would require great amount of computational power or consensus with at least 51% of nodes. The reason for this being the case is hashing. Every block contains data non-identical to the rest of the blocks, which is created by using hash algorithms a unique hash (explained in section 2.4 Cryptography and Hash Functions). This hash then links to the next block and becomes its previous hash. In conclusion, every alteration results in breaking up the chain.

Availability: Central servers are highly dependent on smooth running. Any server crashing could be devastating to the system because it is not functional, e.g., Facebook in Oct. 4, 2021 [30]. Replicated and shared ledgers may cause storage issues, but are highly desirable amongst applications, which cannot tolerate outages. Also, shutting down decentralized public platforms is out of any government's jurisdiction.

Auditability: Transparency of publicly known rules allow transaction validation. In classical databases, data is being held by one (trusted) figure and is for most instances kept private. Recorded immutable ledger can be checked by any participating node [7]. Such ledger represents transparent and fair treatment of all users.

2.5 Types of Blockchain

Appropriate categorization would be into three main classes: public, private, and permissioned blockchain.

Public: Permission of public access is granted. Everyone can participate and get to a shared ledger, therefore reach a full transparency and trust. Ownership of such type of blockchain cannot be obtained. Bitcoin serves as an example [8].

Private: Public access is denied. Shared ledger is private and contained by a single organization. Serves a small number of participants. Security, administration, validating comes within the organization [8].

Permissioned: Participants are also called trusted parties and must be granted a permission to access shared ledger. Exclusivity is necessary for acquiring a trust needed to run the system. Permissioned blockchain could work in a private or in a public manner. To access such type of a blockchain, certain credentials are obligatory, even if the system architecture is public [8].

Table 2: Summarized characteristics and features of each blockchain type

	Public Blockchain	Private Blockchain	Permissioned Blockchain
Access	-Anyone	-Single organization	-Multiple selected organizations
Participants	-Permissionless -Anonymous	-Permissioned -Known Entities	-Permissioned -Known Entities
Security	-Consensus Mechanism	-Approved Participants -Voting Consensus	-Approved Participants -Voting Consensus
Energy Consumption	-High	-Low	-Low
Ownership	-Public	-Centralized	-Semi-Centralized

2.6 Consensus protocols

To preserve decentralized structure and allow validation of P2P (peer-to-peer) transactions, nodes must reach a consensus or a general agreement. Consensus protocol is essentially a collective coordination system or set of rules followed by network participants. All nodes must carry a local copy of data history. Pursuit for reaching a consensus can be divided into a proof-based and consortium-based approaches [8]. Selecting a proper consensus protocol has a substantial impact on the application's performance, security, and throughput [9].

2.6.1 General examples

Proof-of-Work (PoW): Basic principle of PoW is to solve a complex mathematical problem, which requires big computational power [10]. Nodes (miners) are continuously encrypting data inside of a block and creating hashes. If one of the miners discovers a required hash with specific properties ex.7-leading zeros, then the individual gets a reward, and it can be broadcasted, verified by other miners, which results in mining a new block. When computational power becomes more extensive, then the computational problem is more robust.

Proof-of-Stake (PoS): Introduced as a more energy efficient path to reach consensus. Terminology for a miner in PoS protocols is a validator. Instead of having to spend enormous amount of energy to mine blocks, PoS uses an election like system, in which a validator is picked randomly to forge a new block. The probability for a validator being picked, is stated by a quantity of economic resources (stake) deposited into a network [10]. The relations between the chance of being picked and staked portion is linear. Reward for a forged block are network fees, and if fraudulent validator's behavior is detected, all the rewards with a part of stake gets burnt.

2.6.2 Examples for mechanical engineering purposes

HoneyBadger BFT (HBBFT): A consensus mechanism enabling a set of nodes to reach a consensus using unreliable links. The functionality resides in selecting a consensus group of validators via election process, who receive encrypted data or transactions as an input. Common agreement must be reached to form a new block and adding it into a blockchain [11].

HBBFT relies on a threshold encryption scheme, which grants validators a public key. Only if all the validators work together, all the transactions can be decrypted, achieving censorship resistance [12]. Mainly used for public blockchain based solutions.

Kafka: In Kafka consensus algorithm only, a leader is permissioned to perform ordering of transactions. Leaders are elected, but must be in-sync replicas, meaning having all access and all data available [13]. Kafka is crash-fault tolerant, so resilient to failing of certain components, however, lacks Byzantine Fault Tolerance [12].

Chapter 3: Function and application

The industry ecosystem is a complex structure consisting of many entities performing different tasks to ensure fast and faultless flow of goods and services. Necessary complexity inevitably generates errors and system delays. Reducing components in industries is highly desirable since it reduces mistakes, creates opportunities, and accelerates processes.

The storage and sharing of information in the system is critical to preventing system failures and management catastrophes. Current industries have relied on trusted third-party organizations to store and verify legal documents or used their own storages. Companies prefer to own as many industry sections as possible, so that all segments run correctly and are organized.

Blockchain technology (BCT) thrives in situations where proof of identity, ownership, transaction, or commitment is the main concern [24]. Reduction of ecosystem segments is inevitable, and processes may become faster, when non-trusting entities share common agreements on the same database.

Deciding whether a blockchain is suitable for a certain application depends mainly on key features mentioned in Section 2.4 Blockchain features.

Not all possible and existing applications are mentioned in this section. However, understanding the reasoning for using blockchain-based solutions in an application is crucial. Finding a suitable application may be a challenging task considering all the system priorities.

The number of use cases for BCT is growing rapidly and may seem limitless. With growing popularity, system engineers tend to overuse this technology and utilize it in non-fitting solutions. The fundamental problem category addressed by using blockchain-based solutions appears to be data management and process automation. If shared data storage is not needed, the use of blockchain as a base layer technology becomes irrelevant [10].

Since blockchain networks mainly consist of cryptocurrencies, the literature tends to categorize applications into financial and non-financial [10]. However, application-based categorization fits more purposefully into the goal of this thesis. The application-based categorization is shown in Table 2, where a multilevel analysis has been performed.

3.1 Use cases in various fields

Table 3: Blockchain use case by industry

Financial	Media	Asset Titles	Government
Trading Equities Fixed income Derivatives trading Collateral management Payments Transfer of value Know your client Anti-money laundering Crowd funding P2P lending Prediction markets	Digital rights management Game monetization Ticket purchasing Art authentication Fan tracking Resell of authentic assets Real time auction Purchase & usage monitoring	Diamonds Designer brands Car leasing and sales Home mortgages Land title ownership Digital asset records	Voting Vehicle registration Licensing and identification Copyrights
Insurance	Identity	Consumer	Payments
Claim filings Property payments Fraud prediction Telematics and ratings	Personal Digital assets Multifactor authentication Refugee tracking Credentials and badging Purchase and review tracking Employer and Employee review	Digital rewards Uber, Apple pay P2P selling Craigslist	Rethinking wallets and banks Tax filling and collection B2B international

Education: Storing educational records is crucial to receiving reputational rewards. Student achievements and credit scores can be securely stored, allowing credentials to be checked only by authorized entities [10]. Certificate management becomes protected, creating trusting digital infrastructures [18]. Digital accreditation distributes quality education around the world with unaffected legitimacy.

Services: The Internet of agreement could represent a next-generation innovation, connecting the internet to regulations, contracts, deals and allowing proof of ownership, integrity, and existence.

Pavilion.io provides shipment protection for companies such as eBay or Alibaba. Using a process in which the company receives payment after the shipment of certain goods to customers has been verified [21].

Government agencies are looking for the authentication of a digital solution for legal documents, which inevitably leads to the adoption of blockchains. Using a secure, distributed, and affordable database to reduce bureaucracy, cost, labor, and increase efficiency could potentially accelerate verification and more transparent taxation [10].

Decentralized Insurance: Standard insurance systems require complex studies and methodologies to create a consumer-provider contract. For many cases, this system is economically infeasible. Often, payments are delayed or claims for payments are denied by insurance companies after reviewing the contract.

The example related to a problematic insurance policy problem was thematically related to Indian crop farmers. Traditional insurance companies cannot afford to pay their employees and every involved institution to construct a legal contract affordable to individuals such as crop farmers [28].

A low-cost, efficient, and affordable decentralized insurance system built on a blockchain system was proposed and created on an Ethereum platform. System architecture Fig.3 shows the system flow, where a smart contract is built based on variable criteria, e.g., weather. All variables, including risks and possible outcomes, are built into the smart contract, which constantly checks an oracle at the same time. Oracle is a neutral and unbiased source of information. The consumer then allocates insurance payments to a money pool via a smart contract, exactly as a traditional insurance company would do. If a catastrophe or natural disaster occurs, smart contract facts check these events in the oracle and give money to the victim [29].

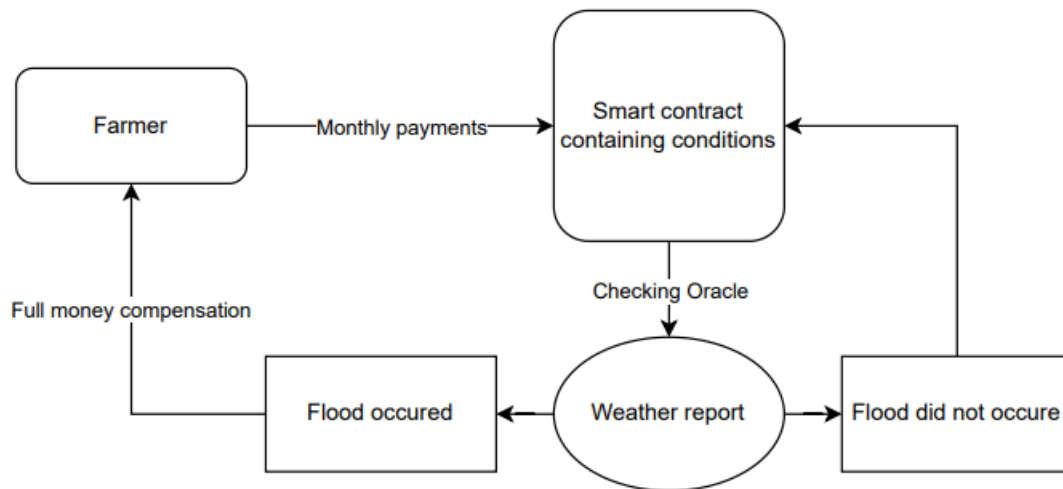


Figure 3: Flow scheme of a decentralized insurance system

Governance: The management of official records has always been governed by the government. No government in history has been incorruptible or a perfect candidate to hold public legal documents. The auditable, inalterable, and decentralized system appears to be a viable candidate for this role. The blockchain could potentially provide the same services while maintaining validity and easy data access. Services like taxes, marriage contracts, identification, legal documents, ownerships, and registrations could be handled by a blockchain based system. The World Citizen project functions as a decentralized passport service that recognizes the identity [20].

The combination of blockchain data storage and biometric recognition, the certification of name, address, credit record, and pictures, becomes possible worldwide. Immigrants and refugees are, therefore, granted equality of opportunity even after a certain country denies sharing such information. Since the sixth world's population lacks proof of existence, a distributed international ledger would be a viable solution to this problem [22].

Voting: Electronic voting has been debated for almost 30 years now as a substitute for a regular paper solution to decrease unnecessary costs and fraudulent behavior. E-voting provides greater speed, reduced cost, and prevention of human failure; therefore, it builds stronger democracy. Making the argument that society would benefit by inventing an e-voting system is reasonable. However, existing digital solutions are based on the central organization system layer, which is designed by a single entity that harms trust [25].

Decentralized application is highly desirable as a solution for e-voting, with no leading entity and without the necessity to question the integrity of service provider. Blockchain makes e-voting possible, as it addresses problems of voters' access and voter' fraud.

Several e-voting solutions using BCT have already been tested. Nir Kshetri [26] suggested that one imagine each vote as one transaction and the receiver would be the candidate. The system was built upon encrypted keys and alteration proof IDs. The advantages are transparency, security, and a mathematically correct counting process that results in precise and trustworthy results. However, this solution was not done in a decentralized manner, and no consensus protocol was implemented.

Another study [27] attempted to implement blockchain in electronic voting using Go-Ethereum Proof-of-Authority for authorization. Utilizing smart contracts and centralized consensus, this attempt reached 5000 verified votes per minute.

The most profound architecture proposed, [25] used biometric systems that generate private keys to verify voters, enabling backtracking and changing votes before the deadline, and four layers of algorithms secure the database. The results of a simulations reached 6756 votes per minute and 9 generated blocks per minute. Vote counting is performed from sealed blocks, ensuring a mathematically reliable and fast election process. However, the amount of security demanded for this system may cause tremendous problems if the voter loses his credentials in the form of a private key.

Since no e-voting system other than blockchain-based is still nonexistent, comparison to a centralized database-based model is therefore impossible.

Financial applications: Classical centralized system is based on a central authority who is controlling the flow and amount of capital, e.g., governments, banks, etc. All custody services and regulatory rules are given to government officials. Expenses of classical centralized systems for a financial event represent a significant amount. Rules are regularly changed by ruling figures, often for their benefit [62].

Blockchain technology allowed for an alternative financial system to emerge called decentralized finance (DeFi). In such a system, every transaction is verified and written on a blockchain, creating a trusted decentralized payment structure. Rules are publicly available for any individual, and they are immutably decided via code, written in simple logic, and stored safely on the blockchain in a form of smart contracts [62].

DeFi can be divided into four pillars:

- **Stablecoins:** Digital substitute for a certain currency. Allows the owner to trade coins on different blockchains and forego transaction fees. International trading is instant and without fees attached to it.
- **Borrowing and Lending:** By using smart contracts, the lender can lend money to the borrower, keep custody of them, and earn interest. The borrower ensures to pay back the owed money by overcollateralizing his position [63].
- **Decentralized Exchanges:** Create a platform for trading different tokens in the system for low fees. Exchange rates are decided by code [63].
- **Margin Trading:** Usability of margin is when an individual is certain that the price of something is going to increase to multiply your financial input. In DeFi, margin trading is faster, open to any figure, more secure, and with almost no fees included.

Blockchain technology has spread tremendously throughout the financial sector. The cases in this category became so profound that the creation of a new economy ecosystem took place. Conservative banking systems are beginning to adopt blockchain-enabled applications to avoid consequences for doing otherwise.

This application segment is the most revolutionized mainly due to the longest timeline of BCT adoption. Use cases in this new ecosystem contain store of value, securities, currency, interest earning, derivative contracts, lending platforms, international digital transacting, decentralized organizations, initial coin offerings, prediction marketplace, multi-blockchain connectivity, digital property ownership and exchange, and much more.

The time horizon and scale of functioning financial blockchain-based ecosystem represent the best candidate in comparison to regular centralized ecosystem.

3.2 Analysis of the qualities of blockchain versus traditional databases

Advantages and disadvantages may vary in various fields, and some qualities are not shared amongst every studied class. Therefore, generalization simplifies the comparison, however, does not offer a detailed difference scheme of each class. A more detailed in comparison breakdown of each use case can be found in Section 3.3 Potential blockchain use cases for mechanical engineering and manufacturing.

Table 4: Summary of main differences between permissionless, permissioned blockchains, and regularly used databases [10].

		Permissionless	Permissioned	Database
Conditions	Auditability	Good	Good	Bad [10]
	Verifiability	Good	Good	Bad
	Transparency	Good	Good	Average
	Data notarization	Good	Good	Bad
	Security	Good	Good	Good
	Privacy	Good	Average	Bad
Performance	Transaction speed	Good [38]	Good	Good
	Dispensability	Good	Good	Average
	Scalability	Bad	Average	Good
System	System autonomy	Good	Good	Bad
Trust	Absence of third parties	Good	Good	Bad
	Accountability	Good	Good	Good
	Immutability	Good	Good	Average
	Multiple independent entities	Good	Good	Average

3.3 Potential blockchain use cases for mechanical engineering and manufacturing

3.3.1 Internet of Things

The Internet of Things (IoT) refers to connected devices that create a collective network. Any physical object that shares data over the Internet is called an IoT device.

IoT devices are generally built to do three things. First, capture of physical phenomena by using sensors, software, or other technologies. Second, digital data that can be processed, visualized, and organized. Third, the transmission of data.

The number of IoT devices connected to the Internet is growing rapidly due to its value in the industries. As shown in Figure 4, the number of connected devices will exceed the number of people by the factor of 10. Today, IoT devices can be seen anywhere, e.g., smart homes, cars, smart watches, etc.

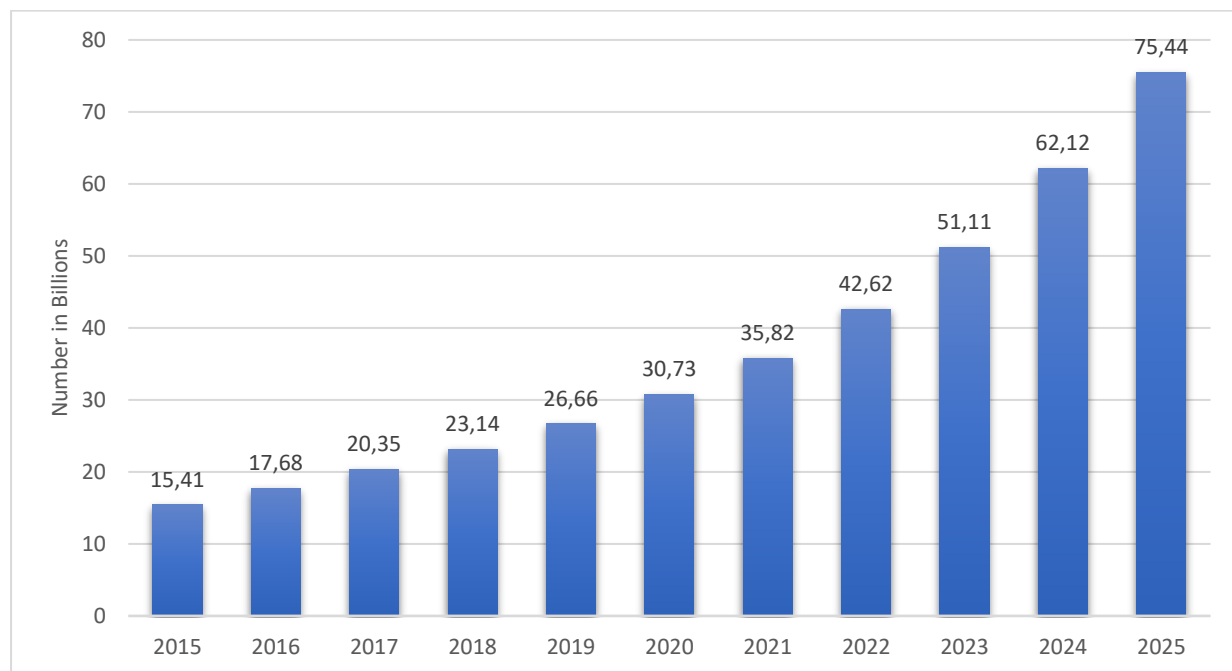


Figure 4: Statistical prediction of a number of connected devices [31]

The main weaknesses of the IoT present in today's ecosystems are the cloud infrastructure and the perception layer [32].

Cloud infrastructure would be a reasonable solution for the IoT infrastructure; however, as popularity grows and the number of connected devices reaches record highs each year, centralized solutions become exponentially costly and increasingly complex. Systems are often exposed to many threats and security issues, and even one vulnerable connected device to the cloud infrastructure could pose a risk to the entire structure [32].

The perception layer contains sensors, actuators that collect all physical phenomena. The perception layer establishes Wireless Sensor Network (WSN), in which many system breach possibilities are present and adapted to certain protocols, e.g., Radio Frequency Identification (RFID), Bluetooth, Near-field communication (NFC). The problems with IoT devices are identity theft and password theft performed using specific techniques and algorithms [33].

Blockchain can offer solutions to these problems, however, concerning drawbacks inevitably follow with the advantages. The distribution of control and verification provides high resilience to outages and excludes a single-point security breach. If only one device is compromised, the structure will not be affected. Using public-private key pairs for sending and signing data, as well as hash functions to systematically link time-stamped data, the blockchain-based system architecture utilizes high tamperproof properties [33]. The last two significant strengths, privacy and transparency, may sound contradictory but are key features in IoT space. The chain is public; therefore, any figure (in permissioned-based blockchain only those authorized) is capable to audit the linkage validity of each transaction with stated addresses and signatures proving identity of the device. From a privacy point of view, some strategies appeared that allowed the linkage of a blockchain address to an IP address [34]. As a result, ways to overcome these complications appeared, such as using VPN networks, or entirely new projects addressing these issues were created using, e.g., zero-knowledge proof, allowing the prover to show enough evidence to the verifier, to verify the transaction without seeing the content [35].

Inefficiency following all new revolutionary technologies relates to legalities and regulations. Regulation of a decentralized structure is difficult to navigate, mainly because it is infeasible to establish a general jurisdiction. Differences in titling and meanings in contracts, securities, and ownership create a hostile environment for a unanimous decentralized system [36].

Fees for using a decentralized platform could affect the economic incentive. Usability is highly dependent on profitability. Most of the time, tokens of these platforms are very volatile and based on supply and demand schemes.

High demands for data transfers are possible to satisfy; however, storing such information could be challenging. As stated above, a decentralized structure requires copies of the whole blockchain. Bitcoin requires 324 gigabytes of storage, and the number increases. Permissioned blockchains may be using external storage communicating with the blockchain, which would contain only principal information. There are some projects addressing this issue, e.g., Mina [37] established a blockchain, that has a permanent size of 22 kB.

High-frequency data-capturing sensors and real-time systems require high transaction speed. VISA can reach 24000 transactions per second, possibly capturing IoT requirements. Many resources indicate the lack of transaction speed; however, the most recent studies mention significant improvements, from the oldest Bitcoins 4,6 transactions per second to the most modern protocols reaching 1,000 transactions per second. In 2021, a new project

called Solana [38] emerged, performing 65000 transactions per second with negligible fees using a special consensus mechanism called Proof-of-History and a low-level programming language for building smart contracts.

The adoption cycle is still in the early stages, but many projects are being developed. It has only been a little more than a decade since the first use case for blockchain has appeared. However, this short time horizon proved to be enough for big adjustments and solutions never thought possible. Many functioning projects are beginning to represent a reliable platform for IoT ecosystems.

IOTA: This project is the most valued among the entire IoT blockchain field. The IOTA validation process is not based on a consensus, and there are no fees attached to transactions. To make it possible, IOTA uses an alteration of a classical blockchain database called “Tangle” Figure 5. The validation is done by every participant in the network, creating an equal environment in transactional processes. The Tangle is probabilistic, and the consensus is reached only once, almost the whole network repeatedly certifies the validity of transactions. Transactions are called a site, and connections of sites are called edges. If one wants to place a site, he needs to attach it to two randomly picked sites and check the validity of every site having edges with the two and continue until the end of the tangle. Since no validators are needed and no mining takes place all transactions are free [39].

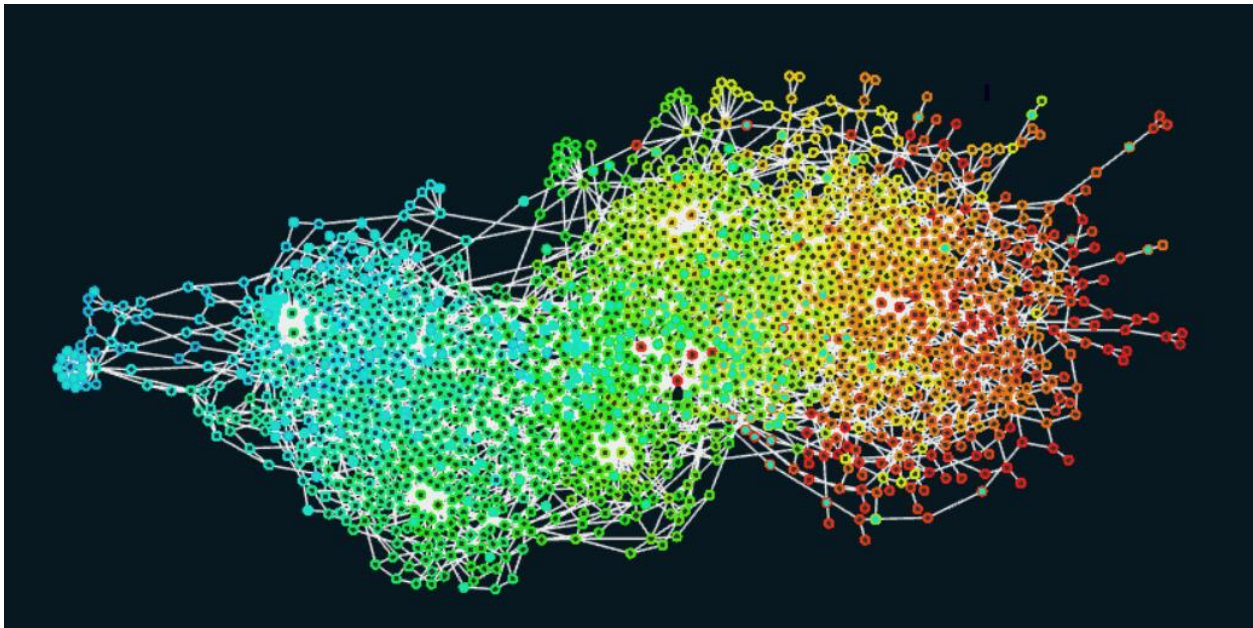


Figure 5: The Tangle [51]

The biggest advantage of IOTA is its scalability. The more users place sites, the faster and more secure the tangle becomes [39].

IoTeX: A public blockchain using a Delegated Proof-of-Stake consensus algorithm (DPoS), which functions similarly to PoS with a slight change. In DPoS stake holders are prompted to vote and choose 21-50 delegates, who mint new blocks. Delegates as well as voters for the delegate minting a new block are rewarded. By this mechanism, voters are incentivized to vote for a reliable delegate. Ensuring confidentiality of data sharing, IoTeX uses a modified signature technique RingCT2.0. This project also handles lightness in terms of hardware resource by using a periodic checkpoint, resulting in the need to carry the whole transaction history locally. Checkpoints can be verified by previous Checkpoints, so the auditor can check the entire blockchain without the need to download a large number of signatures and public keys to verify them [40].

IoTeX also came up with hardware parts, a Ucam camera, and a physical phenomenon measuring device called Pebble Tracker [41]. A Pebble Tracker consists of many sensors: environmental sensor, light sensor, GPS locator, 6-axis motion sensor, etc. This device is connected to the IoTeX blockchain, and only the owner of the private key is permitted to control his data. Reliable decentralized data sharing has many varieties of use cases, from supply chains to proof of presence. Data collected by many Pebble Trackers could potentially form a large pool of reliable data used by companies to create statistical analyses or perform machine learning.

The number of blockchain-based IoT projects is growing at a rapid speed and many are already in a functional stage. Companies such as Volkswagen, Microsoft, and even countries formed partnerships with some of the projects [33]. Proven domains of usage appear to be supply chains, smart cities, artificial intelligence, product tracking, healthcare. With that said, projects are still in an embryonic state.

The areas of concern remain storage, processing power, and CPU efficiency, regulation, and scalability [33].

The revolutionary potential for the decentralized IoT layer could be in machine-to-machine communication (M2M), with the use of smart contracts and immutable and auditable database, the possibility of automated M2M processes emerged.

3.3.2 Odometer

The odometer is a device that collects data on the mileage of the car. One of the simplest uses for BCT is prevention of odometer fraud. This problem affects the industry worldwide, with a total cost of 9 billion euros only in the European Union [42]. Since odometers and their data storages to this day consist of hardware parts, tampering of such data can be done using on-board-diagnosis dongles (OBDII).

Currently, tampering is only detectable by performing a mechanical vehicle examination and requires the expertise to indicate the true mileage of the vehicle, for example, by checking maintenance records, carpet wear, and dashboard manipulation [43]. However, physical factors can be easily manipulated and can only lead to a brief estimate.

Combining odometers and IoT technology creates the possibility of having more than one source of information on car mileage. In the case of centralized databases, the collected data could potentially be altered for the sake of the database owners and become vulnerable to system hacks, where the safety of all vehicle information could be compromised (Section 3.3.1 Internet of Things).

Many studies have stated that the public blockchain would present the best base layer option, on which the system is built. The advantages this system presents are transparency, auditability, time-stamped data, immutability, trustless verification, and decentralization [44].

The most promising system architecture presented combines odometers and IoT devices to create a reliable and accessible blockchain-based database. The implementation was done on an engine control unit (ECU) level not on OBDII, since the ECU can be modified only by the manufacturer. From a transactional standpoint, the cost and frequency of data transmission could affect system functionality and affordability; for that reason, the transaction interval must be fixed to a certain distance (1000 km) and every data set is assigned to a unique vehicle information number (VIN). By this distance, the vehicle loses significant value. The prototype has been built on an Ethereum platform (a functional blockchain that uses the Turing complete programming language to build smart contracts), so that all shared data is stored and accessible via VIN [44].

Currently, there is no viable solution to odometer fraud other than using blockchain technology, making any comparison impossible. The disadvantages may be fluctuating price per transaction when distribution of data occurs, using ECU; therefore taking some computational power, inconsistencies in transaction validating, and scalability. In conclusion, there is still room for improvement; however, blockchain seems to fulfill all the necessary requirements to prevent odometer fraud.

3.3.3 Supply Chain in Automotive Industry

As mentioned in the beginning of this chapter, industries are becoming more complex with globalization and their supply chains are becoming increasingly difficult to manage. Enormous amounts of money are spent to build a robust ecosystem that can withstand all demands and management requirements. Unfortunately, complexity often lies in division of supply chain segments. The lack of information flow, regulatory compliance, and traceability of products across companies creates an untrusted environment and increasingly requires automated systems. The solution to this problem was to own most of the supply chain; however, this solution is for most companies economically unreachable [45].

The automotive industry faces many difficulties in supply chain management, as listed in Table 4.

Table 5: Database driven supply chain issues [46,47,48]

Issue	Specification
Product and service traceability	High probability of information tampering and impossibility of relying on another party without good relationships
Numerous parties involved	Structuring of supply chains on many levels may cause delays, unorganized production states, and can be a problem for logistic providers.
Centralization	The holder of the central database may misuse information, fail at a certain level, or is predisposed to outages
Middlemen	An unauthorized figure tampering data and enforcing stagnation
Quality and compliance issues	Not knowing origins of certain parts an attempt of replacing faulty part can present a time costly process
Information access framework	The access of cross-party information requires a long process full of communication and regulatory interventions
Maintaining inventory quality ratio	Evaluation of current inventory against future demand

Blockchain technology has the potential to address some of these problems efficiently and without damaging other functioning areas. The blockchain-based system facilitates the provenance of the part, vehicle maintenance and part tracking, improves the inbound logistics (stream of raw material and parts from suppliers to manufacturing plant) [49].

Blockchain technology is still in its early stages and to fully implement it to current supply chains, a change in the entire structure must take place. The difference between a typical database-driven supply chain shown in Figure 5 and a blockchain-based supply chain shown in Figure 6 [49].

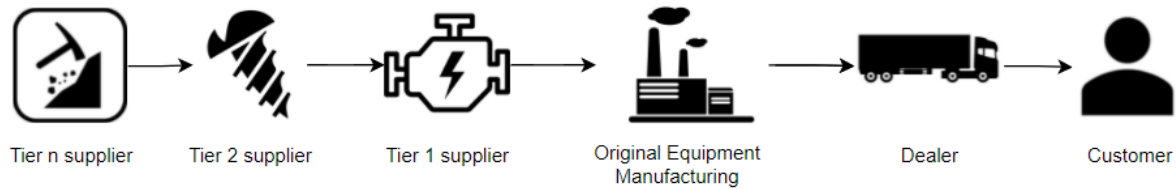


Figure 6: Representative automotive industry supply chain [49]

Today's automotive supply chains are highly dependent on good relationships, communication, and many difficult procedures must be finalized so certain actions can occur [48]. Traceability of goods and certainty becomes unreachable using multiple centralized databases unwilling to share data, or by potential modification of the data itself.

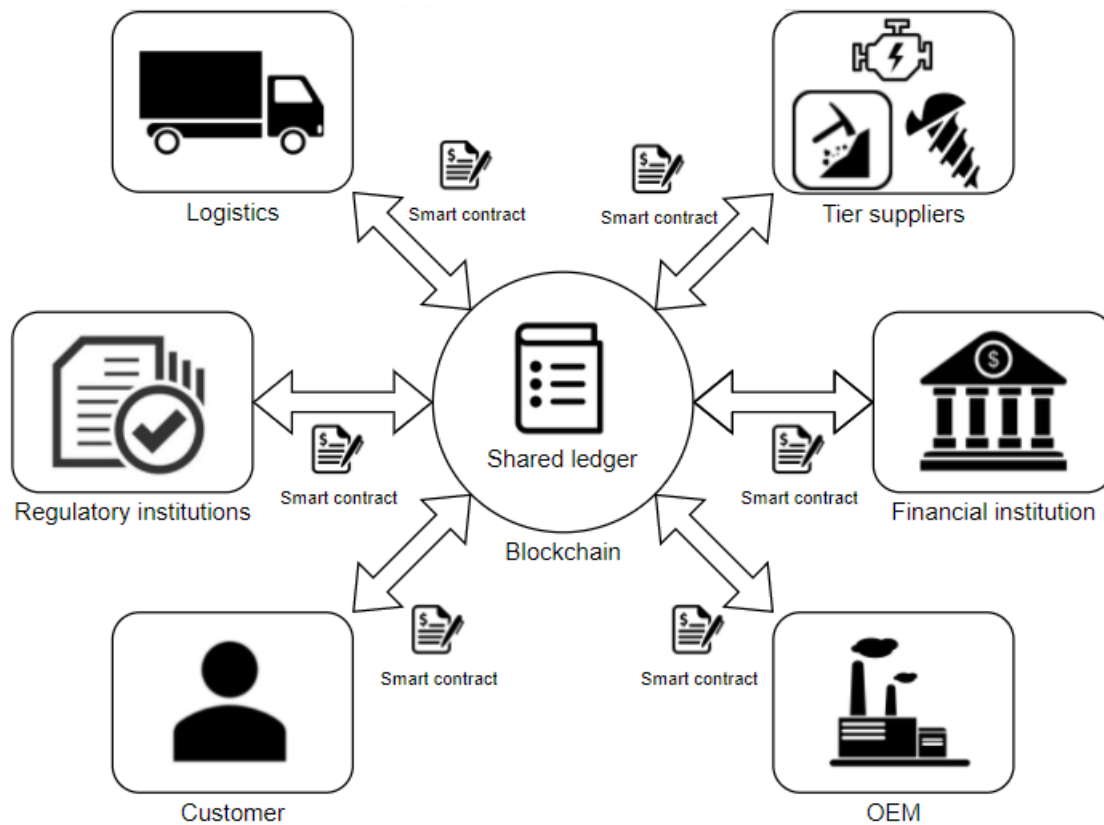


Figure 7: Blockchain-based architecture for automotive supply chain

By using a private blockchain combined with IoT systems and trustable authentication, where every member of this blockchain has access to the information only if authorized, reaching a trusted outcome outside of the untrusted environment is attainable. Also, automation of certain processes, introducing artificial intelligence, and biometric authentication connecting to such systems present new opportunities of evolution.

Blockchain seems to be built for today's supply chains; however, major steps are yet to be taken. Major challenges are waiting for blockchain adoption, and unfortunately to fully use this technology, every member of the system must have the same economic incentive to participate. Supply chains by nature require flexibility due to human connections, relationships, and the governance of system shifts, where any mathematical algorithm fails.

3.3.4 Industry 4.0 and Cloud Manufacturing

Industry 4.0 represents the fourth industrial revolution, which introduces decentralization, system automation, shared resources, distributed operations facilities, material efficiency, M2M communication, intelligence, and cloud manufacturing to every industry [51]. As demands and requirements are rising in every industrial environment, companies are forced to decentralize their production strategies and act as a cooperating organism rather than a single cell. Interconnectedness brings more cost-effective and better-quality services, integrating dynamic value-creation networks.

In industry 4.0, there is a connection between technological point solutions, creating new cyber-physical production systems, enterprise architecture, and information integration. The list of emerging new technologies required can be found in Figure 7. [52]. These point solutions on their own bring a massive change to certain domains. However, adoption of these technologies is happening at lightning speed, however, automating and connecting them in a safe and reliable way advances this massive change into a fourth industrial revolution [53].

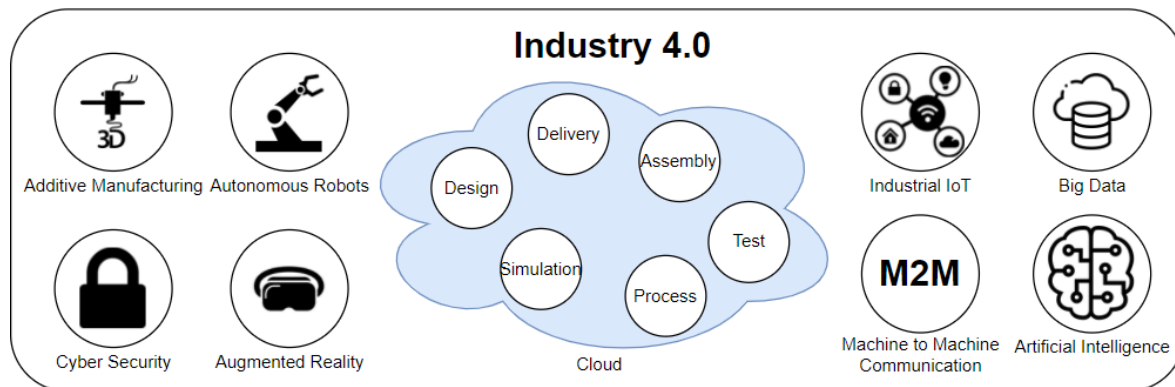


Figure 8: Connected components in Industry 4.0

Cloud manufacturing provides resource aggregation and on-demand services. The application aggregates all information produced by IoT and network participants into a cloud, creating a fully shared virtual resource space and manufacturing capabilities in the cloud. Offers access to data even if they lack resources or capabilities to obtain them or sets up a dynamic cooperating service chain [54].

By the distribution of information using the cloud, manufacturers can optimize allocation of the supply and demand resources or manage the lifecycle of the production in the cloud. Sharing and renting cloud design software to perfect, innovate, simulate, or finish online collaboration is now achievable.

The incentive to introduce blockchain into Industry 4.0 comes mainly from a cyber-security point of view. Private blockchain seems to be the most suitable application for such requirements due to its scalability, security, decentralization, and privacy. Authenticity can be achieved by cryptography (as described in Section 2.3.1) and biometric verification. Decentralized system securely connecting Internet of Things (discussed in Section 3.3.1), Cyber-physical systems, Artificial Intelligence, and human labor avoids distrust to third party providers. Automatization of systems is granted by using smart contracts, ensuring simple and logical processes paths, without relying on legal decree; all auditable and available stored on the blockchain system [55].

Inefficiencies share the same characteristics as in Section 3.3.3 and Section 3.3.1.

3.3.5 Smart Grid

As energy demands are growing and regulatory incentives to make green energy are getting more profound, the energy sector is on the verge of revolution. Smart grids are a decentralized model of an electricity distribution system and represent a potential solution to growing demand. Renewable energy sources such as solar or wind receive more economic attention, therefore the innovation and efficiency is increasing at a rapid rate [57].

Decentralized energy grids also provide the opportunity to create a sustainable electric vehicle charging station infrastructure. When the purchase power invested in such stations distributes not only to one large central entity but to everybody, the system can rapidly accelerate [56].

Table 6: Differences between approaches to the power grid system [60]

Entity	Traditional model	Smart grid
Generators	Centralized industry scale power plants	More decentralized: industry scale power plants, home/small size power generators
Power source	Mostly hydrocarbon	Local renewable energy
Transaction	Consumers bought power via energy companies	A direct transaction between generators and consumers (multi direction)
Pricing	Determined by government or power company	Every generator can set their price
Billing	Periodic billing (postpaid)/pay as you need (prepaid)	Prepaid

Researchers and industry leaders believe that blockchain technology could provide a smooth system transition into a smart grid. Energy sources and storage devices need a decentralized organization system. For such reasons, blockchain technology acquired a substantial interest in adoption of this technology in smart grids. Using this new system would ensure a proof of origin certification of the power entering the grid by assigning an identity to each microgrid. Shared immutable ledger also enables P2P energy trading, therefore efficiently eliminating intermediaries [58].

The main reasons for turning to the blockchain for an electrical power system are system trust, increased security, increased resilience, auditability, increased scalability, and less bureaucracy [58, 56].

Energy grids especially depend on perpetuity. Therefore, using smart grids combined with a blockchain technology, system architectures become resilient to outages from a software and physical point of view due to their decentralized nature. Local system failures will not destroy the whole structure [59].

The drawbacks that limit this system are visible mainly from the economic perspective. A whole new infrastructure with functional software would be required. Another major factor is the speed of the transaction. Requirements on micropayments would be causing data storage and validation demanding, reducing speed and security [58].

A decentralized power grid already existing and growing in Brooklyn. A relatively small neighborhood has obtained substantial number of solar panels and distribute their own made electricity to local resident consumers, local business consumers and bigger businesses. The exchange takes place in a P2P fashion using blockchain. Brooklyn represents one of many examples of already functional smart grids that demonstrate that the blockchain is the right fit for the software requirements [61].

Chapter 4: System Architectures for Blockchain-Based Systems

4.1 Infrastructure of distributed electric vehicle power stations

Building an economically efficient and technically achievable infrastructure for electric vehicle (EV) power stations is strenuous. Great efforts by governments and large companies have been made; however, the problem remains in most locations throughout the world. The need for electric vehicle power stations is growing rapidly because of the increasing attention this technology sector receives.

The power in EV charging lies in its decentralization that allows not only governments and enterprises to participate in the construction of infrastructure, but also human individuals. By building a shared database any individual entity can obtain a power station powered by a renewable source of energy, e.g., solar, wind, etc., releasing the pressure of great central energy demands.

The process of charging using blockchain is visualized in Figure 8. This process differs from the regular charging structure mainly in the payment system.

The initial blockchain should be built in a public manner, for global data access. Of course, customers must be protected from personal information leaks. To solve this issue, the data can be encrypted and proven by zero-knowledge proof to avoid dishonest entities in the system, as well as securing participants' privacy.

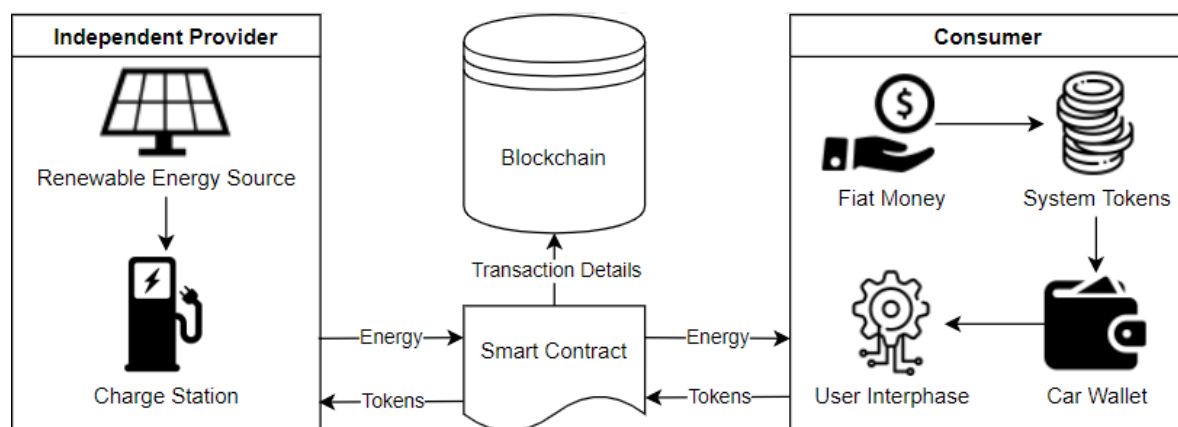


Figure 9: Schematic interpretation of a distributed electric vehicle charging system using blockchain

As shown in Figure 8., an independent provider can issue excessive energy collected by a renewable energy source to an EV user. By creating a digital wallet for his charging station and connecting it to a smart contract (which can take custody of the individual's capital), the provider can offer kWh of his energy in exchange for a token. The exchange takes place automatically if all actions taken are following the rules set in a smart contract. The transfer of electrical energy and monetary energy occurs in three steps. At first, the provider offers electricity through a smart contract; allocation of electricity into a smart contract ensures that the code is taking custody over the energy. Second, a customer allocates tokens into the same smart contract, which again takes custody over the funds. In the third step, the code checks if all conditions written in the contract are fulfilled and makes the exchange. This process is no different to classical ways of exchange through, e.g., a bank. The only difference is in the exclusion of a middleman.

The transaction then goes into a mempool (space where unconfirmed transactions are stored) and then sent to verifiers, who check the transaction validity and try to reach a consensus through the systems consensus protocol, which they follow. After the transaction is verified, it gets into a block with many other transactions and then is added to a blockchain.

The number of tokens for 1 kWh is decided by the donor. The token should be a stable coin (described in Section 3.1 Financial application) to avoid speculation and price fluctuation.

From the consumer point of view, an application layer can be built to locate available charging stations and their price status. By depositing fiat money into a decentralized app via bank transfer, the system will allocate the fiat into a smart contract and exchange it with the system token. When the tokens are allocated to an inbuilt car wallet (the car is a private key owner), the consumer is ready for a capital exchange, just by setting the amount of kWh needed on a User Interface in the car.

The process of charging a vehicle remains the same. Every transfer of tokens from the consumer wallet to the provider wallet is recorded on the blockchain. Any transaction can be accessible by legal authorities, so the transparency aspect is preserved. Taxation and accounting can be automated.

4.2 Inalterable odometer database

As discussed in Section 3.3.1 the blockchain presents a viable solution against odometer fraud. To visualize the system used for this problem, a schematic form is shown in Figure 9. For accuracy purposes and not to cause transactional overload, suggested transaction interval should be every 100 km. A public blockchain is highly desirable since odometer data is needed by more entities than just the manufacturer. In contrast to a study [44], faster validating public blockchains that are more prone to validation speed have appeared on the market in recent years, using more efficient consensus protocols, becoming a better fit for this architecture of the system.

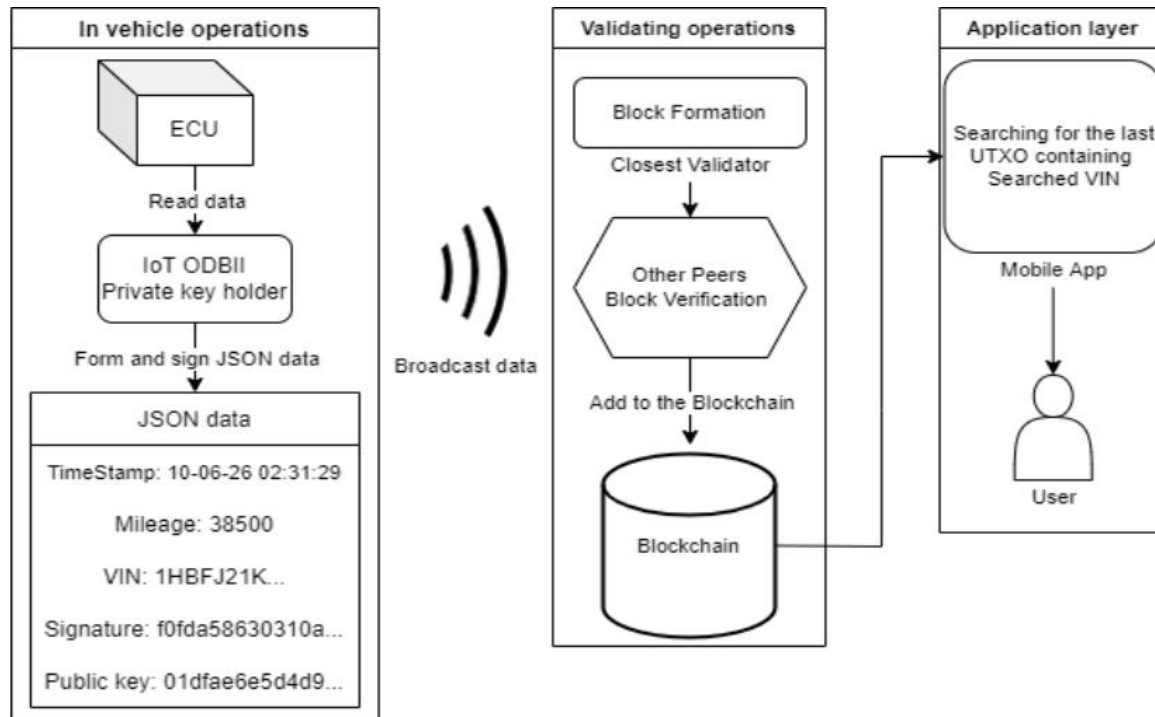


Figure 10: Blockchain-based odometer data sharing

From collecting odometer data by ECU, an IoT OBDII device (which can be manufactured with a private key, with the ability to sign data) can read the data, form a JSON, and broadcast it to the closest validator. The shared data contain the device signature and a public key, allowing validation of the JSON data. By signing the JSON data, the vehicle creates a proof that the information is coming from a certain vehicle. Adding a timestamp ensures the chronology of each transaction.

The validator forms a block, which saves the IoT device a large processing capacity, and sends it to other peers in the system. After a confirmation of the transaction validity by other validators (in PoS 66,7%), a block can be minted and added to a blockchain. The time of a block addition can be set by a calculated demand for transactions. The more vehicles send data, the faster addition of blocks is required to fulfill the transaction demand.

The blockchain is accessible by the public, meaning that after searching a blockchain database for the last UTXO (unspent transaction output) containing a certain VIN number, the car mileage can be easily checked. An application layer can be built for this exact purpose, so that the user can access the searched information.

A problem appears on the side of an economic incentive. The question arises how to reward validators for running this system. An answer to this question could be that the validators are all actors, who participate in the car trading market and regulating entities like government officials. However, this solution centralizes the infrastructure. Another answer could be a small fee attached to the data written on the blockchain, which would overcomplicate the entire process.

4.3 Automation of processes utilizing emerging technologies

With the growing demand for automated processes, companies are adopting new systems to reduce production costs and inconsistencies in production time. Utilizing emerging technologies like AI, 3D printing, cloud manufacturing, and augmented reality will come as a necessity for companies considering future growth. Most processes in industries can be automated by allowing M2M communication. When trying to reach such a management state, many concerning obstacles appear.

The use of BCT can connect these point solutions mentioned above and become a base layer, so they can safely cooperate with each other. Since it can provide verifiable and auditable M2M communication that is always accessible on the ledger, and automate tasks with the use of smart contracts, futuristic system architectures, which were never possible before can be built.

The visualized system architecture prototype is shown in Figure 10, where technologies like AI, 3D printing, IoT, cloud manufacturing are implemented. All this was done on top of a blockchain-based structure.

The blockchain should be private, as there is no need to be transparent with the ongoing transactions. No other figures than participants should have access to the transactions and data on the chain. Therefore, validators become members of cooperating companies.

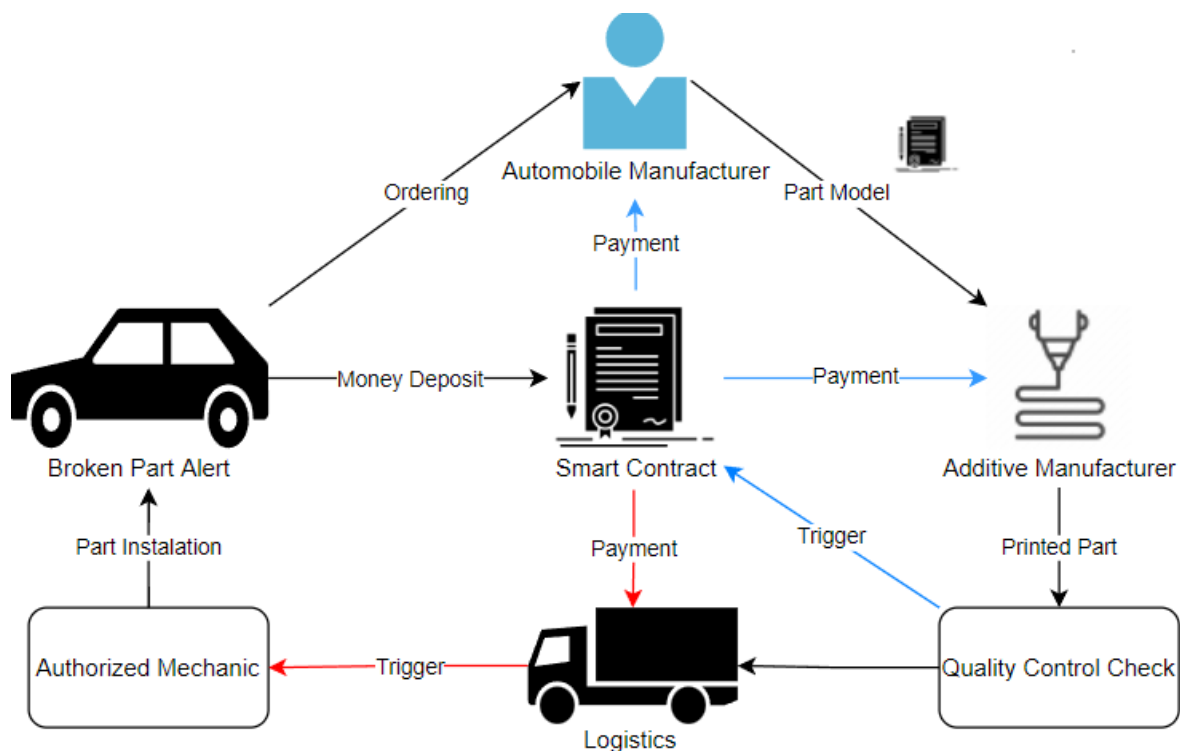


Figure 11: Automated repair of damaged car parts

When a failure of a certain auto part is detected, the owner of a vehicle is immediately alerted and asked by the AI if the owner wants to order a replacement of this part for a following price provided by the automobile manufacturer. After transaction confirmation, the AI launches an order specifying all the details needed. By using a BCT, the actions and identity are verified utilizing asymmetric encryption. This step would not be possible in a classical financial system since non-human entities cannot perform transactional efforts.

The automobile manufacturer confirms and creates a smart contract, which can be seen by everyone present in the transaction and connected to the blockchain. This contract specifies all the events that have to take place and prepare administration documents necessary.

The additive manufacturer enables cheap distribution of car parts, because of its location independence. By utilizing cloud information exchange, automobile manufacturer can enable access to a 3D printer at the location of additive manufacturer, until the printed part is completed. This information can be seen only to a 3D printer using asymmetric encryption and keeping intellectual property safe from other entities. The access to the digital model of the part, is done through the smart contract for a limited time.

After finalization, the part is subjected to a quality examination performed by a classified individual, whose credentials are verified and stored on the blockchain. Successful examination is then signed by the quality control check with his unique private key, which can be represented by, e.g., fingerprint. When a quality check is performed, an event is triggered in the smart contract, which can result in a payment to the automobile manufacturer, the additive manufacturer, and informing the logistics provider about the product for shipment.

The logistics provider, who is responsible for shipping undamaged parts and connected to the blockchain, can undergo a process shown in Figure 11.

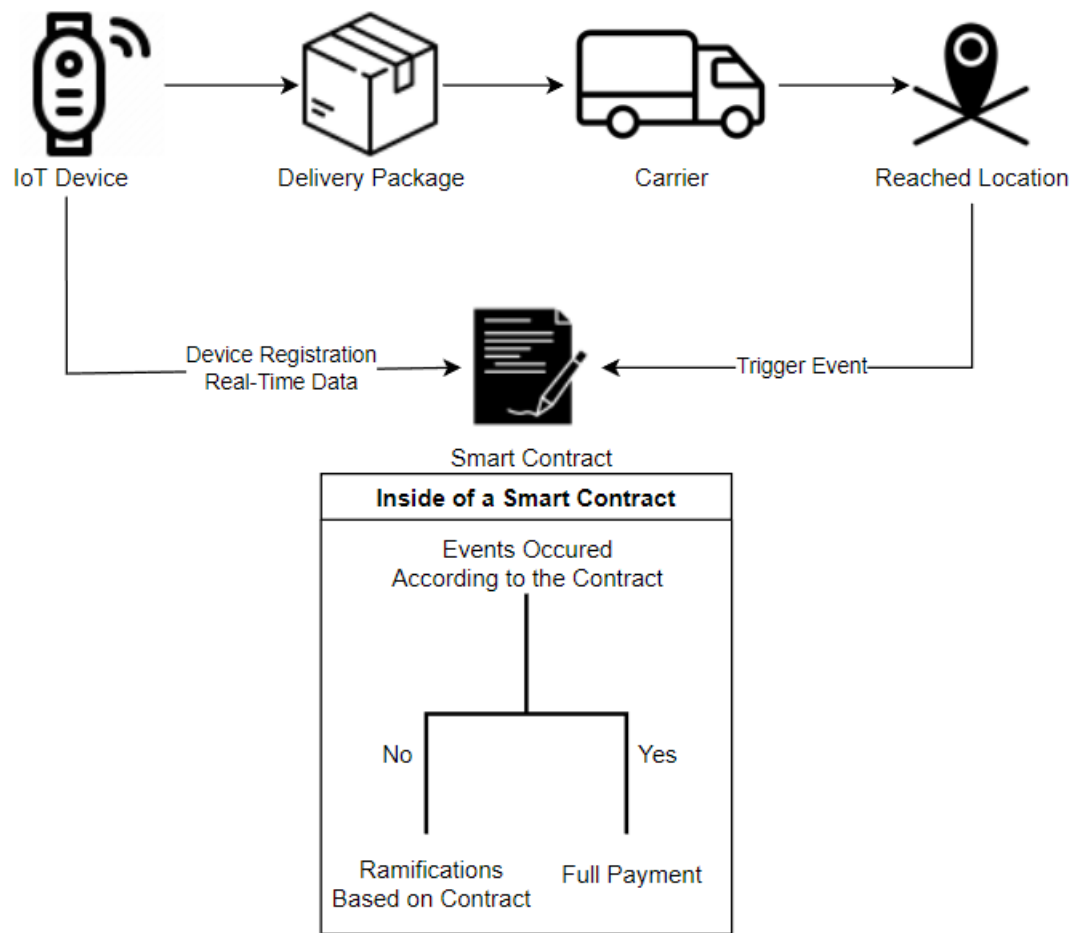


Figure 12: Automated shipment of new parts using blockchain and IoT

In a packaging process, an IoT device registered on the blockchain, e.g., Pebble Tracker [41] with its unique public key, is added to the package with the parts. The device broadcasts all the necessary information, i.e., location, temperature, humidity, pressure applied on the package, so verifiers can check the legitimacy of the information and add it to the blockchain. When reaching the desired destination, a trigger event is performed, where the logistics provider is paid in full, and customer is notified.

The mechanic is authorized, hired by the AI from free market and connected to the transaction. His credentials can be verified but not shown by using a zero-knowledge proof. By using augmented reality, parts installation instructions, and updated documentation, the mechanic can safely substitute damaged part with a new one. Access to the documentation can be also granted to the mechanic through a smart contract for a time necessary to install the part.

In all stages of the transaction, every participant has certain access to the part state information.

Chapter 5: Comparison of blockchain-based to centralized solutions

5.1 Advantages

Inalterable Odometer Database

So far automobile industry has always been dependent on a hardware odometer data storage. After a long period of technological evolution, hardware storages were developed in such a way as to make any data alteration rigorously demanding. However, there are still methods to execute an odometer fraud [68].

By utilizing BCT, a hardware manipulation does not affect the data stored on the ledger in the past; however, the odometer mileage counting correctness can be compromised, which is an unavoidable threat.

The blockchain seems to be the best fit to store odometer data in a secure and transparent way. By creating an additional user interface for finding recent mileage data, one can comfortably and reliably find needed information about the state of a vehicle [69].

Centralized database-based system would be irrelevant because of its dubiety. The potential risk of data alteration by an entity who holds the data in custody is substantial. The economic incentive to manipulate the data is too high.

Infrastructure of distributed electric vehicle power stations

In Section 4.1, a system architecture of EV charging infrastructure has been discussed. Allowing people to contribute to a power grid creates a tremendous release of pressure put on power demands, since the energy creation would come from renewable energy sources built by providers themselves. In case of a centralized infrastructure, governments, or big companies a great amount of capital is required to create an efficient power grid for all EVs. Connecting all charging stations to the existing power grid could destabilize the system [73].

By using blockchain, energy price manipulation will be eliminated, because of a free market structure, where every provider sets the price for a kWh independently. A basic supply and demand-driven ecosystem emerges, leading to energy sector democratization.

The composition of blockchain allows regulators to access transactions, making it easier for them to identify criminal behavior. From an accounting perspective, taxation and other necessary bureaucratic processes can be automated by using smart contracts [74].

No currency exchange fees. Cross country payments often require a currency exchange for a transaction with big fees attached to them. Also, the transaction can sometimes take several days to be approved by a financial organization e.g., a bank, making transacting inconvenient [75].

Security of both private information and transacting presented by blockchain-technology out scales centralized database systems [76].

Automation of processes utilizing emerging technologies

The system presented and running among the transaction participants is still futuristic, however it is almost impossible in a traditional centralized system. To trustfully perform all the steps presented in Figure 10, the provider company would need to have all sections of the system in their possession.

Steps included in the system could be potentially replaced by a centralized solution, e.g., the cloud-like data exchange from an automobile manufacturer with the additive manufacturer, can be managed with an Amazon web service (AWS) [67]. Some parts however, i.e., trusted IoT tracking device and its process automation is not feasible.

Outages resistance is a crucial factor for a smooth operation process. Since BCT is not reliant on one server to run properly, even if one node is attacked or stops functioning, the system is still running.

5.2 Disadvantages

Infrastructure of distributed electric vehicle power stations

In a classical centralized system, all responsibilities caused by emerged issues fall on the owner of the business. The owner in a decentralized system is the provider. All repairs, system failures, renewable energy source damage, are strictly dealt with by the provider. The consumer then, if any problem emerges has no customer service, no additional security normally provided by companies.

Locations of charging stations picked randomly without proper planning may waste resources at the beginning stages of implementation. Charging station infrastructure planning is a process that requires great amount of attention not to over-equip certain locations with too many chargers and leave some locations without enough charging options [72].

Inalterable odometer database

Use of a truly decentralized consensus protocol e.g., PoW, for keeping a public database safe and functional, requires a great amount of energy [70]. More energy efficient consensus protocols e.g., PoS could sacrifice the distributed validating power, if a big amount of stake comes from a few entities.

A great pressure applied on transaction throughput. Considering all the transactions consistently uploaded by all the cars simultaneously, a fast consensus protocol is required. Using an existing platform Solana with a transactional throughput of 65000 transactions per second, would present a viable solution [38]. By this decision we would sacrifice some safety measures. Solana is still a young project without proper robustness testing.

The presented system is not built for a single company. If for example, Kia wanted to track odometer data in their cars, a centralized database would be a better solution for them. Blockchain is not efficient in single-company solutions because no lack of trust among peers is present. The only strong argument for a blockchain solution of this sort is the extra layer of security and resilience to outages.

The distributed ledger can be demanding in terms of storage. Running a central database means that there are no copies needed. Every validator would need to store the whole history of transactions. Also, the blockchain database is immutable. This feature could however be a disadvantage considering the amount of useless data created by cars that are no longer functional, or present on the market. Deletion of a single transaction would result in breaking the chain.

Automation of processes utilizing emerging technologies

As with the Inalterable Odometer database, storing all the data on the blockchain can be demanding from the storage point of view. Every validator needs to download and update the entire blockchain. Can be partially resolved by an on-chain and off-chain way of storing data, where only the most crucial information is stored on the blockchain and other, more excessive information can be stored in a classical database, which is linked to the blockchain [71].

5.3 Challenges

Distributed electric vehicle power station infrastructure

Legal policies for blockchain based solutions are still missing. The system would require a high amount of flexibility to comply with multiple jurisdictions. Also, the financial sector is not yet capable of clearly dealing with digital tokens as a form of payment [77].

Charging in full capacity of EV chargers, depending on a type, can be around 22 kW [65]. This is the amount of power that needs to be generated by a renewable energy source, to serve this system. If a capacity is not reached, either lowering the quality of service must take place, or a battery storing excessive energy must be added for the station to fully function. By adding a battery, a big load of demand for batteries would emerge. The shortage of raw materials to make batteries is already a problem without building a new decentralized power grid. Consistent renewable energy sources, e.g., whirlpool turbines [66] could potentially present a solution for this matter.

Automation of processes utilizing emerging technologies

The emerging technologies are still not 100% proven and cannot be implemented with complete trust.

Today's processes require a high level of flexibility. Evolution in businesses is necessary on everyday bases, therefore many system alterations must take place. The problem with multiparty system owners appears to be in the final decision making. Many questions emerge like: Who has the right to shift the system to other directions? Who decides what solution to apply when a problem appears? etc. The more decision-making entities are present, the harder it is to reach a unanimous decision [78].

Chapter 6: Conclusion

The purpose of this thesis is to identify the utility of BCT in mechanical engineering and manufacturing. A thorough survey of use cases in various fields has been conducted, and their comparison to database driven systems. The main focus was applied to five sectors, in which BCT would present a substantial improvement. The mentioned sectors are Industry 4.0 and Cloud Manufacturing, Supply Chains, Odometer fraud, IoT, and Smart Grid. After careful examination of initial issues in each class and how the use of BCT could solve them, in addition to discovery of its flaws. To conclude the research, BCT appears to be suitable for industry applications that outweigh the negative characteristics. Finally, three conceptual uses of blockchain and smart contracts were designed and compared with centralized systems. Despite the inefficiencies, BCT unquestionably must be taken into consideration when designing complex systems containing data transmissions amongst untrusting entities and identification of individuals in today's industries.

Bibliography:

- [1] CHAUM, David Lee. *Computer Systems Established, Maintained, and Trusted by Mutually Suspicious Groups* [online]. University of California, San Diego, April 1982 [cit. 2021-11-14]. Dostupné z: https://www.chaum.com/publications/research_chaum_2.pdf. Disertace. University of California.
- [2] Haber, S. and Stornetta, W. S. *How to Time-Stamp a Digital Document*. 1991. DOI: 10.1007/BF00196791.
- [3] SZABO, Nick. *Formalizing and Securing Relationships on Public Networks* [online]. 1997 [cit. 2022-02-16]. Dostupné z: <https://nakamotoinstitute.org/formalizing-securing-relationships/>
- [4] Nakamoto, S. *Bitcoin: A peer-to-peer electronic cash system* [online]. bitcoin.org, Mar 2009 [cit. 2021-11-13]. Dostupné z: <http://www.bitcoin.org/bitcoin.pdf>.
- [5] WEIMIN, Sun a Wu XUN. *Blockchain Quick Start Guide*. Packt Publishing, 2018. ISBN 1789807972.
- [6] SINGHAL, Bikramaditya, Gautam DHAMEJA a Priyansu Sekhar PANDA. *Beginning Blockchain: A Beginner's Guide to Building Blockchain Solutions*. Berkeley: CA: Apress L. P, 2018. ISBN 9781484234433.
- [7] Homoliak, I., Venugopalan, S., Reijsbergen, D., Hum, Q., Schumi, R. et al. *The Security Reference Architecture for Blockchains: Toward a Standardized Model for Studying Vulnerabilities, Threats, and Defenses*. IEEE Communications Surveys & Tutorials [online]. Institute of Electrical and Electronics Engineers (IEEE). 2021, vol. 23, no. 1, p. 341–390, [cit. 2021-03-05]. DOI: 10.1109/comst.2020.3033665. ISSN 2373-745X. Available at: <http://dx.doi.org/10.1109/COMST.2020.3033665>.
- [8] PARISI, Alessandro. *Securing Blockchain networks like Ethereum and Hyperledger fabric : learn advanced security configurations and design principles to safeguard Blockchain networks*. Birmingham, England: Mumbai : Packt, 2020. ISBN 1-83864-645-0.
- [9] STEFANOS, Leonardos, Reijsbergen DANIEL a Piliouras GEORGIOS. *PREStO: A Systematic Framework for Blockchain Consensus Protocols*. IEEE: transactions on engineering management [online]. Scopus, 2020, 2020-11, (67), 1028-1044 [cit. 2022-02-10]. ISSN 0018-9391. Dostupné z: doi:10.1109/TEM.2020.2981286
- [10] CASINO, Fran, Thomas K. Dasaklis, and Constantinos Patsakis. "A systematic literature review of blockchain-based applications: Current

- status, classification and open issues." *Telematics and informatics* 36 (2019): 55-81.
- [11] Helium. *The Helium Consensus Protocol* [online]. [cit. 2022-02-13]. Dostupné z: <https://docs.helium.com/blockchain/consensus-protocol/>
 - [12] DRISCOLL, K, B HALL, M PAULITSCH, P ZUMSTEG a H SIVENCHRONA. *The real Byzantine Generals*. The 23rd Digital Avionics Systems Conference (IEEE Cat. No.04CH37576): Piscataway NJ: IEEE, 2004. ISBN 9780780385399.
 - [13] *Consensus in Hyperledger Fabric* [online]. Kumar Gaurav, March 12, 2019 [cit. 2022-02-13]. Dostupné z: <https://jktech.com/blogs/consensus-in-hyperledger-fabric/#:~:text=Hyperledger%20Fabric%20follows%20a%20modular,new%20block%20to%20the%20blockchain.>
 - [14] LASTOVETSKA, Anastasiia. *How Blockchain Works. Blockchain Architecture Basics: Components, Structure, Benefits & Creation* [online]. 2021, November 12, 2021 [cit. 2022-02-15]. Dostupné z: <https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture>
 - [15] SMITH, Will H. *What is blockchain technology?* [online]. London, 2020, 15 July 2020 [cit. 2022-02-15]. Dostupné z: <https://www.ig.com/en/trading-strategies/what-is-blockchain-technology--200710>
 - [16] DAS, Abhijit. *Public-key cryptography: theory and practice*. Place of publication not identified: Pearson Education, 2009. ISBN 9786612652271.
 - [17] KALAICHELVI, V, P MEENAKSHI, P VIMALA DEVI, H MANIKANDAN, P VENKATESWARI a S SWAMINATHAN. *A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique*. *Journal of ambient intelligence and humanized computing* [online]. Berlin, 2020, 2020-08-20, (12), 7235-7243 [cit. 2022-02-16]. ISSN 1868-5137. Dostupné z: doi:10.1007/s12652-020-02398-w
 - [18] YUQIN, Xu, Zhao SHANGLI, Kong LANJU, Zheng YONGQING, Zhang SHIDONG a Li QINGZHONG. *ECBC: A High Performance Educational Certificate Blockchain with Efficient Query*. In: *Theoretical Aspects of Computing*. 14. Hanoi: ICTAC, 2017, s. 288-304. ISBN 978-3-319-67728-6.
 - [19] CHEN, Yi, Shuai DING, Zheng XU, Handong ZHENG a Shanlin YANG. *Blockchain-Based Medical Records Secure Storage and Medical Service Framework*. *Journal of medical systems* [online]. 2018, 2018-11-22, 2018(43), 1-9 [cit. 2022-02-17]. Dostupné z: doi:10.1007/s10916-018-1121-4
 - [20] *World Citizenship Passports with Bitcoin-like Blockchain* [online]. Carlo C, 2014 [cit. 2022-02-18]. Dostupné z: <https://cointelegraph.com/news/world-citizenship-passports-with-bitcoin-like-blockchain>
 - [21] *Featured Startup Pitch: Pavilion.io is using Bitcoin's underlying tech to build a new level of consumer trust in ecommerce* [online]. Duhamel

- Brendan, 2014 [cit. 2022-02-18]. Dostupné z: <https://startupbeat.com/featured-startup-pitch-pavilion-io-id4024/14538/>
- [22] Microsoft and Accenture Unveil Global ID System for Refugees [online]. Roberts Jeff John, 2017 [cit. 2022-02-18]. Dostupné z: <https://fortune.com/2017/06/19/id2020-blockchain-microsoft/>
- [23] KARIAPPA, Bheemaiah. *The Blockchain Alternative: Rethinking Macroeconomic Policy and Economic Theory*. Berkeley: Apress, 2017. ISBN 1-4842-2674-7.
- [24] MOUGARAY, William. *The business blockchain: promise, practice, and application of the next Internet technology*. Hoboken, New Jersey: John Wiley, 2016. ISBN 1-119-30033-9.
- [25] ARUNA, S, M MAHESVARI a A SARANYA. *Highly Secured Blockchain Based Electronic Voting System Using SHA3 and Merkle Root*. IOP conference series [online]. 2020, (993), 9 [cit. 2022-02-28]. ISSN 1757-8981. Dostupné z: doi:10.1088/1757-899X/993/1/012103
- [26] KSHETRI, Nir. *Blockchain-Enabled E-Voting*. IEEE Software [online]. 2018, 2018(35), 95-99 [cit. 2022-03-02]. ISSN 1937-4194. Dostupné z: doi:10.1109/MS.2018.2801546
- [27] HJÁLMARSSON, Friorik, Gunnlaugur HREIÐARSSON a Mohammad HAMDAQA. *Blockchain-Based E-Voting System*. IEEE [online]. 2018, 2018(11), 983-986 [cit. 2022-03-02]. Dostupné z: doi:10.1109/CLOUD.2018.00151
- [28] NISHANT, Jha, Prashar DEEPAK, Khalaf OSAMAK, Yuseef ALOTAIBI, Abdulmayeedy ALSUFYIANI a Saleh ALGHAMDI. *Blockchain Based Crop Insurance: A Decentralized Insurance System for Modernization of Indian Farmers*. Sustainability [online]. 2021, (13) [cit. 2022-03-03]. Dostupné z: doi:10.3390/su13168921
- [29] CHAN, C, X NI a Felix WU. *Fundamentals of operating reserve procurement using decentralized approach with insurance theory application*. Electric power systems research [online]. 2002(63), 229-238 [cit. 2022-03-03]. Dostupné z: doi:10.1016/S0378-7796(02)00115-3
- [30] ISAAC, Mike a Sheera FRENKEL. *Gone in Minutes, Out for Hours: Outage Shakes Facebook*. The New York Times [online]. The New York Times, 2021 [cit. 2022-03-07]. Dostupné z: <https://www.nytimes.com/2021/10/04/technology/facebook-down.html>
- [31] ALYASIRI, Hasanen, John CLARK, Ali MALIK a Ruairí DE FRÉIN. *Grammatical Evolution for Detecting Cyberattacks in Internet of Things Environments* [online]. 19.07.2021 [cit. 2022-03-10]. Dostupné z: doi:10.1109/ICCCN52240.2021.9522283
- [32] SUMITRA, B, C PETHURU a M MISBAHUDDIN. *A Survey of Cloud Authentication Attacks and Solution Approaches*. International Journal of Innovative Research in Computer and Communication Engineering [online]. 2014, 2014(2), 6245-6253 [cit. 2022-03-11]. ISSN 2320-9801. Dostupné z: <https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.1045.870&rep=rep1&type=pdf>

- [33] PIERONI, Alessandra, Noemi SCARPATO a Lorenzo FELLI. *Blockchain and IoT Convergence--A Systematic Survey on Technologies, Protocols and Security*. *Applied sciences* [online]. 2020, 2020(10) [cit. 2022-03-11]. Dostupné z: doi:10.3390/app10196749
- [34] SASSON, Ben. *ZeroCash: Decentralized Anonymous Payments from Bitcoin* [online]. 2014 [cit. 2022-03-11]. Dostupné z: doi:10.1109/SP.2014.36
- [35] SOEWITO, Benfano a Yonathan MARCELLINUS. *IoT security system with modified Zero Knowledge Proof algorithm for authentication*. *Egyptian Informatics Journal* [online]. 2021, 2021(22), 269-276 [cit. 2022-03-11]. Dostupné z: doi:<https://doi.org/10.1016/j.eij.2020.10.001>
- [36] *Bitcoin Legality by Country Summary* [online]. coin.dance [cit. 2022-03-11]. Dostupné z: <https://coin.dance/poli/legality>
- [37] Mina. *Mina is building the privacy and security layer for web3* [online]. [cit. 2022-03-11]. Dostupné z: <https://minaprotocol.com/>
- [38] *A Solana Cluster*. Solana [online]. 2021 [cit. 2022-03-11]. Dostupné z: <https://docs.solana.com/cluster/overview>
- [39] *The tangle* [online]. Serguei Popov, 2018/4/30 [cit. 2022-03-13]. Dostupné z: <http://www.descriptions.com/Iota.pdf>
- [40] *IoTeX: A Decentralized Network for Internet of Things Powered by a Privacy-Centric Blockchain* [online]. The IoTeX Team, May 18, 2018 [cit. 2022-03-13]. Dostupné z: <https://whitepaper.io/document/131/iotex-whitepaper>
- [41] *Pebble Tracker* [online]. IoTeX, 2018 [cit. 2022-03-13]. Dostupné z: <https://docs.iotex.io/verifiable-data/pebble-tracker/quick-start>
- [42] *Research for TRAN Committee - Odometer tampering: measures to prevent it*. In: . European Union: Policy Department for Structural and Cohesion Policies, European Parliament, 2017. Dostupné také z: [https://www.europarl.europa.eu/RegData/etudes/STUD/2017/602012/IPOL_STU\(2017\)602012_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2017/602012/IPOL_STU(2017)602012_EN.pdf)
- [43] ABBADE, Lucas, Filipe RIBEIRO, Matheus SILVA, Allison MORAIS, Everton MORAIS, Estevan LOPEZ, Antonio ALBERTI a Joel RODRIGUES. *Blockchain Applied to Vehicular Odometers*. *IEEE network* [online]. 2020, 2020(34), 62-68 [cit. 2022-03-17]. Dostupné z: doi:10.1109/MNET.001.1900162
- [44] PREIKSCHAT, Katarina, Moritz BÖHMECKE-SCHWAFERT, Jan-Paul BUCHWALD a Carolin STICKEL. *Trusted systems of records based on Blockchain technology - a prototype for mileage storing in the automotive industry*. *Concurrency and computation* [online]. 2021, (33) [cit. 2022-03-17]. Dostupné z: doi:10.1002/cpe.5630
- [45] ABID, Haleem, Abid HALEEM, Shahbaz KHAN, Mustufa Haider ABIDI a Abdulrahman AL-AHMARI. *Implementing Traceability Systems in Specific Supply Chain Management (SCM) through Critical Success Factors (CSFs)*. *Sustainability* [online]. 2018, (10) [cit. 2022-03-24]. Dostupné z: doi:<https://doi.org/10.3390/su10010204>

- [46] QUIEROZ, Marciel M. a Samuel Fosso WAMBA. *Blockchain adoption challenges in supply chain: An empirical investigation of the main drivers in India and the USA*. International Journal of Information Management [online]. 2019, 2019, (46), 70-82 [cit. 2022-03-25]. Dostupné z: doi:<https://doi.org/10.1016/j.ijinfomgt.2018.11.021>
- [47] MUZAMMAL, Muhammad, Qiang QU a Bulat NASRULIN. *Renovating blockchain with distributed databases: An open source system*. Future Generation Computer Systems [online]. 2019, (90), 105-117 [cit. 2022-03-25]. Dostupné z: doi:<https://doi.org/10.1016/j.future.2018.07.042>
- [48] KHANFAR, Ahmad A. A., Muhammad IRANMANESH, Morteya GHOBAKHLOO, Madugoda Gunaratne SENALI a Masood FATHI. *Applications of Blockchain Technology in Sustainable Manufacturing and Supply Chain Management: A Systematic Review*. Sustainability [online]. 2021, 14 July 2021, (13) [cit. 2022-03-25]. Dostupné z: <https://doi.org/10.3390/su13147870>
- [49] NESNIR, Ada, Ethirajan MANAVALAN, Kumar ANIL, K VIMAL, Simon Peter NADEEM, Yigit KAZANCOGLU a Jayakrishna KANDASAMY. *Blockchain Technology for Enhancing Traceability and Efficiency in Automobile Supply Chain—A Case Study*. Sustainability [online]. 2021, (13) [cit. 2022-03-24]. Dostupné z: doi:[10.3390/su132413667](https://doi.org/10.3390/su132413667)
- [50] Big data for cyber physical systems in industry 4.0: a survey. *Enterprise Information Systems* [online]. 2019, 01 Mar 2018, (13), 148-169 [cit. 2022-03-30]. Dostupné z: doi:<https://doi.org/10.1080/17517575.2018.1442934>
- [51] The Tangle main net. *The IOTA tangle* [online]. [cit. 2022-03-30]. Dostupné z: <http://tangle.glumb.de/>
- [52] OJANPERÄ, Matti Yli, Seppo SIERLA, Nikolaos PAPAKONSTANTINOU a Valeriy VYATKIN. *Adapting an agile manufacturing concept to the reference architecture model industry 4.0: A survey and case study*. Journal of Industrial Information Integration [online]. 2019, (15), 147-160 [cit. 2022-03-31]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S2452414X18301377>
- [53] RIEDL, Matthias, Holger ZIPPER, Marco MEIER a Christian DIEDRICH. *Automation meets CPS. IFAC Proceedings Volumes* [online]. 2013, (46), 216-221 [cit. 2022-03-31]. Dostupné z: doi:<https://doi.org/10.3182/20130522-3-BR-4036.00071>
- [54] LI, Zhi, Ali Vatankhah BARENJI a George Q. HUANG. *Toward a blockchain cloud manufacturing system as a peer to peer distributed network platform*. Robotics and Computer-Integrated Manufacturing [online]. 2018, (54), 133-144 [cit. 2022-03-31]. Dostupné z: doi:<https://doi.org/10.1016/j.rcim.2018.05.011>
- [55] BINNI, Wang, Wang PONG a Tu YILIU. *Customer satisfaction service match and service quality-based blockchain cloud manufacturing*. International Journal of Production Economics [online]. 2021, (240) [cit. 2022-03-31]. Dostupné z: <https://www.sciencedirect.com/science/article/pii/S0925527321001961>

- [56] MENGELKAMP, Esther, Benedikt NOTHEISEN, Carolin BEER, David DAUER a Christof WEINHARDT. A blockchain-based smart grid: towards sustainable local energy markets. *Computer science* [online]. 2017, (33), 207-214 [cit. 2022-04-01]. Dostupné z: doi:10.1007/s00450-017-0360-9
- [57] YOLDAŞ, Yeliz, Ahmet ÖNEN, S. M. MUYEEN, Athanasios V. VASILAKOS a İrfan ALAN. Enhancing smart grid with microgrids: Challenges and opportunities. *Renewable and Sustainable Energy Reviews* [online]. 2017, (72), 205-214 [cit. 2022-04-01]. Dostupné z: <https://doi.org/10.1016/j.rser.2017.01.064>
- [58] Blockchain Applications in Smart Grid-Review and Frameworks. *IEEE* [online]. 2019, (7), 86746-86757 [cit. 2022-04-01]. Dostupné z: doi:10.1109/ACCESS.2019.2920682
- [59] SEONG-KYU, Kim a Huh JUN-HO. A Study on the Improvement of Smart Grid Security Performance and Blockchain Smart Grid Perspective. *Energies* [online]. 2018, (11), 1973 [cit. 2022-04-01]. Dostupné z: 10.3390/en11081973
- [60] ANAK AGUNG GDE, Agung a Handayani RINI. Blockchain for smart grid. *Journal of King Saud University - Computer and Information Sciences* [online]. 2022, (34), 666-675 [cit. 2022-04-01]. Dostupné z: <https://doi.org/10.1016/j.jksuci.2020.01.002>
- [61] *Brooklyn Microgrid (BMG) is an energy marketplace for locally-generated, solar energy.* Brooklyn Micro Grid [online]. Brooklyn, 2019 [cit. 2022-04-01]. Dostupné z: <https://www.brooklyn.energy/>
- [62] HARVEY, Campbell R, Ashwin RAMACHANDRAN, Joey SANTORO, Fred EHRSAM a Vitalik BUTERIN. *DeFi and the Future of Finance*. New Jersey: John Wiley & Sons, Incorporated, 2021. ISBN 9781119836018.
- [63] *AAVE LIQUIDITY PROTOCOL* [online]. Josh Stevens [cit. 2022-04-03]. Dostupné z: <https://aave.com/>
- [64] *UNISWAP PROTOCOL* [online]. Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, Dan Robinson, 2021 [cit. 2022-04-03]. Dostupné z: <https://uniswap.org/whitepaper-v3.pdf>
- [65] *What power do I need to charge my electric vehicle?* [online]. Andersen [cit. 2022-04-17]. Dostupné z: <https://andersen-ev.com/charging-academy/what-power-do-i-need-to-charge-my-electric-vehicle/>
- [66] *WHIRLPOOL TURBINE CREATES FISH-FRIENDLY HYDROPOWER: New Belgian energy company uses a simple turbine construction to create round-the-clock water-powered electricity for remote communities without harming the environment.* [online]. Germany: Spring Wise, 2018 [cit. 2022-04-17]. Dostupné z: <https://www.springwise.com/whirlpool-turbine-creates-fish-friendly-hydropower/>
- [67] *About AWS* [online]. Amazon, 2006 [cit. 2022-05-01]. Dostupné z: <https://aws.amazon.com/about-aws/>
- [68] SEIL, Kim, Aram CHO a Dong Hoon LEE. Analysis of Threats and Countermeasures for Odometer Protection. *International Journal of*

- Automotive Technology* [online]. 2020, Oct 2020, 5(21), 1271-1281 [cit. 2022-05-07]. Dostupné z: doi:10.1007/s12239-020-0120-x
- [69] FERDOUS, MD Sadek, Mohammad Javed Morshed CHOWDHURY, Kamanashis BISWAS, Niaz CHOWDHURY a Vallipuram MUTHUKKUMARASAMY. Immutable autobiography of smart cars leveraging blockchain technology. *The Knowledge Engineering Review* [online]. 2020, (35) [cit. 2022-05-07]. Dostupné z: doi:10.1017/S0269888920000028
- [70] DE VRIES, Christian, Alex GALLERSDÖRFER, Ulrich KLAASSEN a Lena STOLL. Revisiting Bitcoin's carbon footprint. *Joule* [online]. 2022 [cit. 2022-05-07]. Dostupné z: doi:10.1016/j.joule.2022.02.005
- [71] MIYACHI, Ken a Tim K MACKEY. HOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Information processing & management*. 2021, (58), 102535. Dostupné z: doi:10.1016/j.ipm.2021.102535
- [72] METAIS, M.O, O JOUINI, Y PEREZ, J BERRADA a E SOUMALAINEN. Too much or not enough? Planning electric vehicle charging infrastructure: A review of modeling options. *Renewable & sustainable energy reviews* [online]. 2022, (153), 111719 [cit. 2022-05-07]. Dostupné z: doi:10.1016/j.rser.2021.111719
- [73] HUANG, Xingjun, Yun LIN, Ming K LIM, Fuli ZHOU, Rui DING a Zusheng ZHANG. Evolutionary dynamics of promoting electric vehicle-charging infrastructure based on public-private partnership cooperation. *Energy* [online]. 2022, (239), 122281 [cit. 2022-05-07]. Dostupné z: doi:10.1016/j.energy.2021.122281
- [74] DERYA, Yayman. Blockchain in Taxation. *Journal of Accounting and Finance* [online]. 2021, 4(21), 140-155 [cit. 2022-05-07]. Dostupné z: <https://www.proquest.com/docview/2573030444/89F2C7D16B4D45D9PQ/4?accountid=17115>
- [75] *Stablecoins 101: What are crypto stablecoins, and how do they work?* [online]. COINTELEGRAPH [cit. 2022-05-07]. Dostupné z: <https://cointelegraph.com/altcoins-for-beginners/stablecoins-101-what-are-crypto-stablecoins-and-how-do-they-work#:~:text=Stablecoins%20were%20primarily%20used%20to,commodities%20like%20gold%20or%20silver.>
- [76] ALFANDI, Omar, Salam KHANJI, Liza AHMAD a Asad KHATTAK. A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. *Cluster computing* [online]. 2020, 1(24), 37-55 [cit. 2022-05-11]. Dostupné z: doi:10.1007/s10586-020-03137-8
- [77] *Stablecoins: Implications for monetary policy, financial stability, market infrastructure and payments, and banking supervision in the euro area* [online]. European Union: European Central Bank, 2020 [cit. 2022-05-11]. Dostupné z: <https://www.ecb.europa.eu/pub/pdf/scpops/ecb.op247~fe3df92991.en.pdf>

- [78] FRAGAPANE, Giuseppe, Dmitry IVANOV, Mirco PERON, Fabio SGARBOSSA a Jan Ola STRANDHAGEN. Increasing flexibility and productivity in Industry 4.0 production networks with autonomous mobile robots and smart intralogistics. *Annals of operations research* [online]. 2020, **1-2**(308), 125-143 [cit. 2022-05-11]. Dostupné z: doi:10.1007/s10479-020-03526-7

List of Figures

Figure 1: Transaction flow [14].....	11
Figure 2: Blockchain structure.....	12
Figure 3: Flow scheme of a decentralized insurance system.....	19
Figure 4: Statistical prediction of a number of connected devices [31].....	23
Figure 5: The Tangle [51].....	25
Figure 6: Representative automotive industry supply chain [49].....	29
Figure 7: Blockchain-based architecture for automotive supply chain.....	29
Figure 8: Connected components in Industry 4.0.....	30
Figure 9: Schematic interpretation of a distributed electric vehicle charging system using blockchain.....	33
Figure 10: Blockchain-based odometer data sharing.....	35
Figure 11: Automated repair of damaged car parts.....	36
Figure 12: Automated shipment of new parts using blockchain and IoT.....	38

List of Tables

Table 1: Hashing examples.....	13
Table 2: Summarized characteristics and features of each blockchain type.....	15
Table 3: Blockchain use case by industry.....	18
Table 4: Summary of main differences between permissionless, permissioned blockchains, and regularly used databases [10].....	22
Table 5: Database driven supply chain issues [46,47,48].....	28
Table 6: Differences between approaches to the power grid system [60].....	31