Possibilities for Applying Blockchain Technology – a Survey

Mimoza Mijoska and Blagoj Ristevski
Faculty of Information and Communication Technologies – Bitola, University "St. Kliment Ohridski" – Bitola
Partizanska bb, 7000 Bitola, Republic of Macedonia
E-mail: mijoska.mimoza@uklo.edu.mk, blagoj.ristevski@uklo.edu.mk

The blockchain technology has the potential to be applied in a variety of areas of our daily life. From the original Bitcoin cryptocurrency to the current smart contracts, the blockchain has been applied to many domains. Its numerous applications result in much ongoing research in different practical and scientific areas. This new technology is being seen as a revolutionary solution in finance, decentralization, trust, identity, data ownership and data-driven decisions. This paper presents the novel solutions associated with some of the big data areas that can be empowered by the blockchain technology such as healthcare, decentralized personal data protection, digital property, Internet of Things, digital identity, financial services and infrastructure, e-commerce, educational records, educational system, knowledge sharing, insurance, food industry, accounting, auditing and e-voting. Blockchain technology could be used in electronic health records and the establishment and maintenance of birth registers, deaths, marriages, registration of business activities, but also in the organization of elections. The features of this technology can be the redefinition of Internet 3.0 defined as a new type of decentralized infrastructure or network of networks.

Povzetek: Pregledni članek prikazuje možnosti uporabe tehnologij veriženja.

1 Introduction

In 2008, powerful American financial institutions and insurance companies were on the edge of bankruptcy. These circumstances called for immediate intervention by the federal government to avoid domestic and possibly global financial collapse. These events illustrated the dangers of living in a digital, interconnected world that depends on transactional intermediaries and leaves people vulnerable to digital exploitation, greed, and crime.

Blockchain technology is a relatively new concept and a fast-growing part of the Internet and cloud computing. Similar data structures existed long before the famous bitcoin was conceived, but the main theories about blockchain architectures used today were originally defined in the original article on bitcoin written and published by a person (or a group of people) under the pseudonym Satoshi Nakamoto in 2008 [1]. The first blockchain innovational application was Bitcoin. Beyond their use in the economic domain, Bitcoin and blockchain technology as articulated by Nakamoto solve an important computer science problem that had been a barrier to having a functional digital monetary system for years: the double-spending problem. The double-spending problem refers to a case where money should only be spent once. The first Bitcoin transactions occurred in January 2009. With the first "release" of the Bitcoin network on January 3, 2009, the first Bitcoins (cryptocurrency units) were created. Nakamoto developed the software and he was the lead developer until the mid-2010s. Bitcoin was the first cryptocurrency created on blockchain technology basis in 2009. Later, it was noticed that blockchain as a technology could be used for other purposes than the realization of cryptocurrencies. Since 2015, many international financial organizations have planned to further develop the blockchain system. In 2014, a consortium called R3 was established to start research and development of blockchain technology. In March 2017, this group counted about 75 companies to reach 200 in March 2018, including Bank of America, Merrill Lynch, UniCredit Group and many other real estate companies with the goal of better education, law and technology development in blockchain technology [2].

This paper describes the interesting implementations of blockchain technology in various domains such as healthcare. That includes all healthcare stakeholders such as hospitals, healthcare facilities and physicians. Then, a proposed solution for protecting data privacy is described by finding a solution for the digital property register.

Next, a secure and distributed blockchain technology system is displayed that can serve as an IoT platform in which devices are connected reasonably and securely. The potential of this technology to replace all existing physical identities such as passports, driver's licenses and ID cards and to move them to a digital platform is presented. It is described how the application of this technology can improve financial services and payment opportunities, provide a clear and transparent supply chain management system in the retail industry. By using this technology, student records, as well as completed courses, test results, diplomas and more, can be stored in the form of a digital record. Also the attendance of online classes and the

realization of online teaching during the COVID-19 pandemic can be stored in digital form that cannot be changed.

Moreover, this paper depicts the decentralization of Wikipedia's knowledge base. This is followed by applications of blockchain technology in the insurance sector, the food industry, accounting, auditing and election management.

The remainder of the paper is organized as follows. Section 2 highlights the principles of blockchain technology. The application of blockchain technology is described in the subsequent section. Section 4 describes the key challenges in the implementation of blockchain technology. Finally, concluding remarks and directions for further works are given in the last section.

2   Blockchain technology

"Blockchain" is a coined word, composed of the words "block" and "chain". Blockchain is a distributed replicated database organized in the form of a single linked list - chain, where nodes are blocks of data for transactions. These blocks, after grouping, are protected by using cryptographic methods. Blockchain technology enables the accomplishment of digital transactions without intermediaries. Linking blocks use a cryptographic hash function, in a way that makes it impossible to change the content of a block without changing the contents of all subsequent blocks. This is a very important feature of the blockchain, as it ensures the unchangeability of the data which it contains. The SHA-256 hash function for the same input data always produces the same output with a fixed length. Regarding the blockchain technology, the benefit of using cryptographic hash functions is that they are cryptographically strong hash functions with requirements such as second pre-image resistance and can serve as a digital fingerprint.

Blockchain technology is based on P2P architecture, where the nodes involved in the implementation of the service have a copy of all records and they constantly communicate with each other and synchronize new records [41]. Blockchain technology covers techniques from several disciplines: cryptography, mathematics, algorithms and economic theory. They are combining P2P networks and use a distributed consensus algorithm to solve traditional distributed database synchronize problem. Blockchains are integrated multi-user databases that form a type of decentralized infrastructure. The blockchain technology is specified of the following six key features [7] [10]:

Decentralization. The basic feature of blockchain, which means that blockchain does not have to rely on a centralized node anymore, the data can be entered, stored and updated in a distributed manner.

Transparency. The data's record by blockchain system is transparent to each node. It is also transparent to update the data, enabling the blockchain to be a trustworthy technology.

Open Source. Most blockchain systems are open to everyone. The record can be check publicly and people can also use blockchain technologies to create any desired application.

Autonomy. Because of the principle of consensus, every node on the blockchain system can transfer or update data safely. The idea is to distrust individual network participants and to trust the integrity of the whole blockchain.

Immutable. Any records will be preserved forever, and cannot be changed unless someone can take control more than 51% of peer network nodes at the same time.

Anonymity. Blockchain technologies solve the trust problem between a node to node, so data transfer or even transaction can be anonymous. They only need to know the person's blockchain address.

The blockchain database is managed autonomously using a P2P network and a distributed timestamping server. It is empowered by mass collaboration driven by collective self-interest. The result is a robust workflow, where participants' uncertainty about data security is marginal. Blockchain removes the features of endless duplication of digital assets. This forms a consensus system which ensures that each unit of value is transferred only once, solving the longstanding problem of double spending and blockchain-based value exchange system can be faster, safer and cheaper than traditional systems.

2.1   Decentralization of the blockchain

Blockchain (distributed ledger technology) is a network software protocol that enables the secure transfer of money, assets, and information through the Internet, without a third-party organization as an intermediary [3]. It can safely store transactions such as digital cryptocurrencies or data/information about debt, copyrights, equity, and digital assets. The stored information cannot be easily forged and tampered because it requires individual approval of all distributed nodes. This significantly reduces the cost of trusting and accounting that commonly exist in non-digital economies and other social activities. Blockchain has four components [43]:

(1) hash, which uses one-way mathematical functions to assign unique indexes;

(2) a digital signature, which is implemented as a public cryptographic key;

(3) P2P network, which serves as a routing structure for nodes to use the distributed hash; and

(4) consensus mechanism, which is a set of digital procedures designed to ensure the accuracy and consistency of the stored information across the participating nodes.

The blockchain data structure is depicted in Fig.1 [4].

In the Blockchain Body, the bottom is a part of Merkle Hash Tree which can be either a binary tree or a multi-tree in the data structure. Specifically, data or information is recorded as the hash value stored in the Blockchain Body, and the generated Merkle root through Merkle tree's hash process will be recorded in Blockchain Head [42].

The blockchain technology platform is gradually shaping up into three directions: (1) underlying infrastructure which includes facilities for mining and
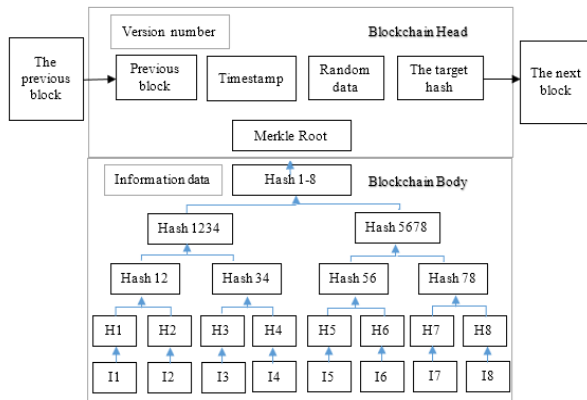
Figure 1: The blockchain data structure.

manufacturing of specialized computer hardware to perform blockchain-related tasks; (2) middle layer between the blockchain platform and client application services, including smart contracts, a blockchain platform, financial software, and other services; and (3) hotspot distributed applications in various industries, including finance (e.g., cross-border payments, liquidation, financial services, and asset digitization), cybersecurity (e.g., identity protection, data authenticity protection, and critical infrastructure protection), and supply chain management (e.g., logistics tracking and digital works tracking).

This distributed general ledger is replicated to thousands of computer nodes around the world and is publicly available. Despite its openness, it is also confidential and reliable. This is achieved through a mathematical puzzle and computer power embedded in its "consensus mechanism" - the process in which the nodes agree on how to update the blockchain with each transaction of moving the value from one person to another. Users use public and private keys to digitally sign and make transactions in the system in a secure way. Blockchain users can solve puzzles using cryptographic hash methods hoping to be rewarded with a fixed amount of cryptocurrency [5].

Blockchain systems seem very complex. However, they can be easily understood by examining each technology component individually. At a high level, blockchains utilize well-known computer science mechanisms (linked lists, distributed networking) as well as cryptographic primitives (hashing, digital signatures, public/private keys) mixed with financial concepts (such as ledgers) [6].

A ledger is a collection of transactions. Ledgers are often stored digitally in large databases owned and operated solely by centralized "trusted" third parties. However, we must trust the third party that the data are backed up, transactions are validated and complete, and the history is not altered. A ledger implemented using a blockchain can mitigate these issues through the use of a distributed consensus method. One of the aspects is that the blockchain ledger will be copied and distributed amongst every node within the system. When new transactions are submitted to a node, the rest of the network is alerted that a new transaction has arrived and

at this point, this is a pending transaction. Eventually, one of the nodes will include this new transaction within a block and complete the system's required consensus method. This new block will be distributed across the network and all ledgers will be updated to include the new transaction. When new users join the system, they receive a full copy of the blockchain, making loss or destruction of the ledger to be difficult. Each transaction submitted to the network passes through several steps to be included and published in a block of the blockchain:

A transaction is a record of a transfer of assets (digital currency, units of inventory, etc.) between involved parties. For each input transaction A, an output hash value #A is created using a cryptographic function.

Hashing is a method of calculating a relatively unique fixed-size output for an input of nearly any size (e.g., a file, some text, or an image). Even the smallest change of input will result in a completely different output digest. Hash functions are designed to be one-way: they are computationally infeasible to find any input that maps to any pre-specified output. If a particular output is desired, many inputs must be tried by passing them through the hash function until input is found that gives the desired result. Moreover, hash algorithms are designed to be collision-resistant, they are computationally infeasible to find two or more inputs that produce the same output. A commonly used hashing algorithm in many blockchain technologies is the Secure Hash Algorithm (SHA) with an output size of 256 bits (SHA-256).

Each block in a blockchain contains multiple transactions, which are grouped in sets. Hash values are further combined in a system called a Merkle tree [5].

Merkle tree is a data structure where the data is hashed and combined until there is a singular root hash that represents the entire structure. The root is an efficient mechanism used to sum up the transactions in a block and verify the presence of a transaction within a block. This structure ensures that the data sent in a distributed network are valid since any alteration to the underlying data would be detected and can be discarded. The result of all the hashing then goes into the block's header, and it is combined with the hash of the previous block's header and a timestamp. This combination becomes a part of the cryptographic puzzle. The solution for the puzzle is to find a nonce value. The nonce value is a number manipulated by the mining node to solve the hash puzzle and with this, it gives them the right to publish the block [5].

After creation, each block is hashed thereby creating a digest that represents the block. The change of even a single bit in the block would completely change the hash value. The block's hash digest is used to prevent the block from changes since all nodes will have a copy of the block's hash and can then check to make sure that the block has not been changed. An additional feature of blockchain systems is that they can run so-called smart contracts [6], which is an auto executable code that fires off once certain conditions occur. A smart contract is computer protocol or collection of code and data which runs automatically under defined criteria when deployed on the blockchain. The contract executes the appropriate method with the user-provided data to perform a service.

The code, being on the blockchain, is immutable and therefore can be used (among other purposes) as a trusted third party for financial transactions that are more complex than simply sending money between accounts. A smart contract can perform calculations, store information, and automatically send money to other accounts. It doesn't necessarily even have to perform a financial function.

Instead of relying on a central authority to securely deal with other users, blockchain uses innovative nodes consensus protocols, verifies transactions, and seamlessly records data. Because blockchain is a distributed ledger, similar to a database, the data stored must be authentic and accurate. Separate nodes in the network constantly confirm the authenticity of the entries in the chain and reject the proposed data blocks, if they do not pass verification. Taking control of a large number of nodes in the network (more than 50%) would be extremely complicated and expensive for attackers and is much more difficult than compromising any centralized service. Therefore, this approach to data storage is considered far more secure compared to centralized databases. Theoretically, it is possible to break a blockchain, if the attacker controls more than half the total network power, in which case it is called a 51% attack. But if someone succeeds to change the blockchain, it will destroy it and hence it will have no value.

2.2   Types of blockchain systems

Blockchain is a technology that is constantly evolving. Due to its basic technological features, new applications are constantly being developed using its framework. The most common types of blockchains are:
-    public blockchain;
-    private blockchain and
-    hybrid blockchain.

2.2.1   Public blockchain

A public blockchain is one that contains absolutely no restrictions. Public blockchains allow anyone to submit data to the general ledger with all participants holding an identical copy of the general ledger. As there is no single owner of the general ledger, this methodology is more suitable for anti-censorship applications (for instance, Bitcoin) 0. The public blockchain has the following features:
• Anyone can access it, i.e. see all the transactions that appear on the block. Several services allow you to view the public blockchain (known as block explorers), and the most famous is blockchain.info, which can track bitcoin blockchain.
• Anyone can make transactions. It is enough to download a mobile or desktop wallet (Wallet) or to use one of the online wallets and to carry out transactions freely.
• Anyone can participate in the creation of blocks and in the distribution of the reward that follows for adding blocks. Alternatively stated anyone can be a "miner".
• Everyone can have a say in deciding whether to amend the cryptocurrency protocol. In some cryptocurrencies,

miners make decisions, but there are cryptocurrencies in which other participants have a controlling stake.
• The protocol that controls the system is in the form of open source. Anyone can view this code, but anyone can suggest changes to that code. If the majority accepts the proposed changes, those changes become an integral part of the protocol. It is also very common to take the protocol from one cryptocurrency, modify it slightly and then launch it as a new cryptocurrency. The full openness of public blockchains reveals some of their advantages and disadvantages.

The main advantages of public blockchains are:
• Blockchain is resistant to potential attacks.
• Because anyone can be a node in a P2P network, the number of these nodes is very large and therefore it is more difficult to have more than 50% "unfair players", which is very expensive.

The main disadvantages of public blockchains are:
• The capacity of the blockchain is very limited, both in terms of the number of transactions that can be processed per unit time and the amount of data that can be stored in the blockchain. For more people to participate in network maintenance, the requirements must be relatively modest, both in the amount of hard disk space occupied by the blockchain and in the speed of the Internet connection. The Bitcoin network can currently process only a few transactions per second, and by comparison, Visa can process tens of thousands of transactions per second 0. Management mode is inefficient. To implement any, even the slightest changes of the system, it is necessary for the majority of the members of the network to agree to this change. In comparison, this would be roughly how a referendum would be organized for each decision in the country 0.

2.2.2   Private blockchain

In private blockchains, only invited participants are allowed to join the network. These networks are controlled by one or more designated network administrators. Private blockchains allow distributed duplicates of the registry, but only to a limited number of trusted users. Because the network may have an owner, this methodology is better for applications that require simplicity, speed, and greater transparency.

What companies do not like is the transparency and the fact that the system is accessible to everyone. That is why the idea of a private blockchain has emerged that will retain most of the benefits of the public blockchain, but will also eliminate the disadvantages that do not suit companies 0.

2.2.3   Hybrid blockchain

Hybrid blockchains, called consortium blockchains, are considered as semi-decentralized and use the characteristics of public and private blockchains. Hybrid blockchains contain licensing groups similar to private blockchains, but instead of one controlling organization, they are controlled by a group of contracted organizations to ensure the validation of transactions [42]. The consortium blockchain allows a group of individual

organizations to validate blocks, instead of having everyone participate in the process, or having only a single entity to decide the validation process. Hyperledger Fabric [38] and Hyperledger Burrow [39] are examples of consortium blockchain frameworks. For the consensus mechanism, the consortium blockchain uses consensus algorithms to validate transactions, such as Byzantine fault tolerance (BFT) and practical BFT (PBFT) consensus through the Tendermint algorithms, which are not expensive computationally.

2.3 Smart contracts

A smart contract is a code in a programming language that facilitates the exchange of money, real estate, shares, or any value [39]. Smart contracts are computer programs that automatically execute the terms parties have agreed on, to regulate their relations. This code can be written to a blockchain and executed on any computer in a distributed network. The smart contract is automatically executed when specific conditions are fulfilled. Because the code of the smart contract is written on the blockchain, the execution takes place without any possibility of censorship, interruptions, fraud or intrusion by third parties. We can say that the block on which smart deals are stored is a distributed operating system.

In the context of blockchain, smart contracts have existed before Ethereum. American developer Nick Shabo defined the concept back in 1996 in the book Smart Contracts: Building Blocks for Digital Markets. He wrote that the basic idea of smart contracts is that many types of contract clauses can be embedded in the hardware and software we communicate with, in such a way that breach of contract is costly for the offender [6].

3 Application of blockchain technology

Besides the first application of blockchain technology in the creation of cryptocurrencies such as bitcoin and many other altcoins, it is widely used in different domains of daily living where new innovative ways of working are introduced.

3.1 Healthcare system

One challenging implementation of blockchain technology is in the healthcare involving all stakeholders such as hospitals, healthcare authorities and clinicians by satisfying patient needs and protecting patients' privacy by using blockchain to pay fees with bitcoin [8].

Until now, doctors have faced many obstacles when it comes to digital storage and information sharing for patients. The authors in [10] identified three major barriers to effective digital record management:

- easy access to medical records;
- maintaining the patient's privacy and
- ensuring the sharing of records between different platforms without losing their meaning and proving their authenticity and credibility.

With blockchain technology, all three obstacles are reduced to an acceptable level or eliminated.

Firstly, decentralized blockchain databases can be accessed by authorized persons, whether they are healthcare providers, insurance companies or patients - anywhere, anytime, and in a format that can be used by all parties. An additional advantage of such a system would be the elimination of centralized data controllers. Secondly, blockchain technology provides security measures that are not available for other digital sharing methods, making it easier to address privacy concerns.

Finally, blockchain technology reduces the number of agents that manage each entry and maintains a consistent, timely record of each transaction, reducing the possibility of error while providing a high level of transparency and trust.

In the current system, where full records are kept on paper, if information seekers need to see a personal health record (PHR), they must complete a request form and send it to the registration office for approval. Upon approval, the information requester will pay for a copy at the cashier and receive a payment confirmation account. The information seeker then shows the account to the registration office to obtain a copy of the PHR. However, the PHR may be lost or duplicated for illegal purposes.

When the information seeker sends a PHR request to the publisher (hospital or healthcare institutions) and the publisher agrees with the information requestor, Bitcoin will be placed. Before sending a PHR to the information seeker, it requires the approval of a family doctor and the patient, so that only specific anonymized records are required for the patient to be sent [8].

Rapke in his approach to healthcare discussed that perhaps changes should come from a point where people own and can access data about their health [10]. With his working concept blockchain has a way of bringing this consumer-oriented approach to the healthcare sector. Data from the results and procedures can be stored on the blockchain, which will not rely on a single central storage facility. This will help the governments and other companies to be held accountable for that data. At the same time, the data will reside on the latest secure technology using cryptography. As data owners, patients will have the authority to decide with whom they share their data. Healthcare will be more patient-oriented, but it is still in balance with other important players in the healthcare system. In [12] authors explained how blockchain can enable the interoperable and secure exchange of electronic health records (EHR) in which health consumers are the ultimate owners. The proposed scenario is to store only health and medical metadata on the blockchain. Otherwise, blockchain's infrastructure storage capacity would have to be massively expanded to support full health records. So, metadata such as patient identity, visitor ID, provider ID, customer ID, etc. can be stored on blockchain but the actual records should be stored in a separate universal health cloud, as shown in Fig. 2. For instance, if a patient visits two hospitals today, they will store their data in two databases that the patient does not own. If hospitals need to communicate, they will use a standardized communication mediator such as web services, e-mail, or a shared file repository. In a scenario where blockchain is applied, the first hospital creates a
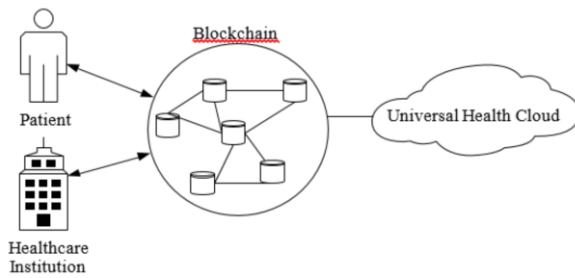
Figure 2: Overview of the Blockchain Healthcare System [13].

record of the universal health cloud. The hospital then creates a transaction in blockchain with metadata for visits and a URL (Uniform Resource Locator) for the cloud entry. The patient signs this transaction with his/her key. When a patient now visits a second hospital, he/she must provide his/her key reading blockchain transactions. Only those affected by the patient's key can decrypt the transactions. So this is an example of how people can own data and approve access. Even smart contracts can be encoded in blocks to carry insurance instructions, emergency contacts, wills etc. These smart contracts will be activated with events that a blockchain can read from another web service.

Transactions in blocks should contain a unique user identifier, a coded link to the health record, and a timestamp for the time when the transaction was made. The transaction may also contain the type of stored data. Depending on the implementation, this can help search and process the access data. This blockchain will contain a history of all medical data, including formal medical records, as well as data from mobile applications and various sensors being carried. Keeping data away from blockchain in a cloud pool can be a good basis for exploration, mining, analytics and machine learning. This type of analysis does not have to affect the privacy of each patient. These data have to be encrypted and digitally signed to ensure the privacy and authenticity of the information. The user will have the option to assign a set of access permissions and specify who can request and write data to their blockchain. Further development of the user interfaces for the patient to review their healthcare data and manage access privileges is entirely possible [14].

Another blockchain case study in healthcare uses Ethereum's smart contracts to create representations of existing medical records [15]. These contracts are stored directly in separate nodes on the network. The proposed solution called MedRec structures large amounts of data into three types of contracts. The first one is the Registrar Contract. It holds the identity of the participants with all the necessary details and of course the public keys. This type of identity registration can be restricted to authorized institutions only. The second contract is the relationship between the healthcare provider and the patient. The main use will be when there is a smart agreement between the care provider and the patient. A third type is a contract that helps the patient to locate his/her medical history. As a result of this agreement, all previous and current engagements with other nodes in the system are listed. MedRec also proposes a data mining model that incorporates the entire healthcare community into data mining. Medical researchers and healthcare stakeholders can work in the network.

Big data in healthcare come from a variety of sources, such as clinical trials, EHRs, patient databases, medical measurements and imaging. All these data come in a wide range of formats and from different data streams. The data should be evaluated and interpreted temporally to benefit patients. But doctors need new tools to monitor, track, and provide quick feedback to individual patients. Appropriate data management will also help with prediction strategies, interventions, healthcare services and healthcare policies. Because medicine is always on the cutting edge of technology, moving forward with many innovations, healthcare data need a crucial transformation, as do big data.

3.2   Decentralized protection of personal data

From social networks, personal data, activities and behaviours of users are constantly being collected, without users to be conscious about the privacy issues. Users still do not have a clear idea of what precise data is being collected and for what purpose, they are losing whole control of what is happening with the data afterwards and cannot withdraw the permissions. Concerns about data privacy grow when faced with the consequences of what others have seen or learned about us. Zyskind in [16] has proposed a solution that is an access control management system that mainly focuses on mobile platforms and the inability of the user to recall authorized access to private data. By installing a mobile application, permissions are granted indeterminately and the users must uninstall the application and stop using the services if they want to revoke the access. The purpose of the new solution is for the user to be able to control and revise what data are stored and how they are used. The idea is to keep the personal data access policies on blockchain and then the nodes in the blockchain to control access to the DHT (distributed hash table).

The solution consists of three entities: the user, the company providing the service and blockchain. When a user wants to allow or block access to his/her data, blockchain comes into play as an intermediary. Here blockchain supports two types of transactions: access transaction and data transaction. These types of transactions allow access control management, data storage, and data extraction. When the user installs a new application, a shared identity is created and sent to blockchain along with the configured permissions at the user's request. All assigned permits are listed in the so-called policy. The shared keys, the public key of the user and the public key of the service, and the policy are sent through an access transaction in the blockchain. A new complex identity is being introduced into the proposed system. Complex identity is a shared identity between the user and the service. The user is the owner of the key, and the service is a guest. The complex key is composed of

pairs for signing on both sides, so that the data will be protected by all other parties in the system, except the owner and all his/her guests.

Sensitive user data are encrypted with the shared encryption key and sent with transaction data for storage. Blockchain sends data to a DHT and retains only the hash value as a pointer to the data. The value set in DHT is encrypted with the complex key. The value indicator is known to the user and the service. DHT only performs the already approved read and write functions. Both the user and the service can search the data using the data pointer. Each time the service accesses the data, its permissions are checked compared to the last access transaction. The user can revoke permissions at any time or modify them by initiating a new access transaction. To track this, it is possible to easily develop a web table showing the user's current permissions. Overview of the decentralized permitting system using blockchain is shown in Fig. 3.
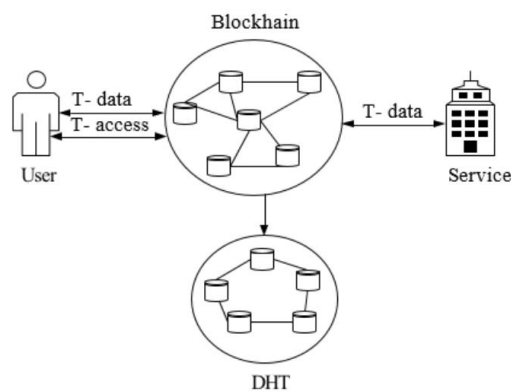

Figure 3: Overview of the decentralized permitting system [13].

Another study based on social media controlled by users on the blockchain is described in [17] by Ushare. Ushare's vision is that users should control their presence over the Internet by affecting the posts they share and controlling the ability to share again. Using P2P capabilities, Ushare created a decentralized content distribution network. The tool that blockchain manages, in this case, is the data that users publish. Ushare's proposed solution consists of a user-encrypted hash table, a system for controlling the maximum number of actions performed by user circles, a local Certificate Authority (PCA) that manages user circles and blockchain.

When a user shares a post with his/her circle, his/her PCA encrypts the data with the public key on the circle. Encrypted data are stored in a DHT. This table has three columns that allow users to share already published data they see. Each time a user shares a post, the first column stores hacked encrypted data about the post that is being viewed and shared. The second column records the hash of the encrypted data with the public key on its circle. The third column stores the encrypted data item.

The reason for using DHT in this second solution is the same - large data such as documents, images and videos should be stored in a decentralized manner. Blockchain only stores transactions for sharing user posts. The actual data cannot be stored because downloading the

entire chain to all nodes will create limitations in computer calculations and time constraints. When the user creates a post, he/she sends a new transaction to the blockchain with his/her identity, the hash key of the encrypted data and the token in which he/she states the allowed number of shares. Afterwards, the user sends a separate transaction to each member of his/her circle with the data encryption key. If another user who has received the post wants to share it, he/she sends a new transaction with his/her identity and the data key encrypted with the key to this new user's circle.

Again, more new transactions are sent to the subsequent users who can review the re-shared transaction. The number of tokens decreases with each action. All efforts to create these two blockchain solutions are because personal and sensitive data should not be entrusted to third parties. Because users create and publish data, they need to remain the main owners of the data. Regarding the monitoring done by following the procedures and interests of the users, the users should at least know that. A blockchain can be a filter for permissions to access private data or it can implement a fully decentralized social network, as shown in the second solution.

3.3 Digital property

The World Wide Web (www) started with simple links and laid the groundwork for making it visible what is original and what is being copied. After that, people thought of a way to preserve authorship by mentioning the author in references. But this system is far from perfect. People can always find a way to copy things, and the author will not know and will not be notified. Or, people may assign the copyright, but it's in one direction, so the author still won't know that someone has addressed his work. Or even worse, people may cite someone else who is not the original author. It is concluded that the main tool for digital content and digital sharing (www) ignores the need for digital ownership. But at the beginning of the development of the service www was different. The Xanadu Project was the first hypertext project, founded in 1960 by Ted Nelson [18]. Even then, the problem of digital ownership was approached by introducing a copyright scheme based on copyright, in a system that would provide storage and publishing services. The granting of copyright is built into this system. Two-way connections should be set up automatically each time someone uses another user's data. It was concluded that it was a complicated, unfeasible technology and the project was closed.

With blockchain technology, Ascribe [19] tries to achieve Xanadu's goals by finding a solution for the digital property registry and copy visibility. In terms of visibility, they try to find all the copies of the protected content that exist on the Internet. This can be done by searching the entire Internet and performing a match to match the content of the creator. This problem would be solved by machine learning techniques. When the copies are found, the system performs two-way automatic connections. The

author must then decide whether to apply for a license or perhaps a revocation request.

When it comes to selling intellectual property of digital art, it is not just selling a copy, it is selling property and the right to use, modify or resell the content. To make this type of sale of a property, it is necessary to conclude a legal agreement, hire a lawyer, etc. The idea of using blockchain to store and sell digital data ownership will be as simple as sending a signature e-mail that the user transfers ownership of its content. The terms of service provided by Ascribe are made in consultation with specialized lawyers. The complexity of legal licensing and ownership processes is achieved by accepting the terms of service. Blockchain is a publicly trusted book and will provide copyright to all users. Transaction time stamps can be used as evidence in court in the event of a property dispute.

Regarding blockchain implementation, Ascribe has created its protocol called SPOOL - Secure Public Online Ownership Ledger [20]. This protocol is made specifically for documenting digital ownership transactions. Ascribe allows the artist to set a fixed number of editions of the work that can then be transferred, ensuring that each edition is authentic to the artist. So, when a transaction with transfers is made, the user can transfer ownership for one or more editions. The editions are under a work preserved in BigchainDB [21] and used for use in the blockchain. So, when transferring ownership, the users create a transaction for one of their works, includes the value of the hash, the issue and the new owner. The user signs the transaction and sends it. Because Ascribe uses the Bitcoin blockchain, a public researcher who knows the hashtag of the work can track the ownership of the work and find all the addresses that each edition has.

Another blockchain implementation is Monegraph, which is proof that a new, modern and digital marketplace can be built that is easy for users. From the users' point of view, with Monegraph, it is easy to buy and sell fully licensed digital media directly with terms, rights and prices controlled by the authors. Monegraph facilitates the process of licensing and receiving revenue of art in many digital forms created by photographers, designers, illustrators and other media creators [24].

Monegraph allows authors to create and customize a license agreement that sets out the usage parameters for their media. There are four types of licenses:
- license for works of art - for non-commercial usage,
- photo news license - for editing,
- product image license - commercial license and
- picture of the situation is a license that gives all the rights.

The authors have a public catalogue as a portfolio of their work that is publicly available and sold. Blockchain takes into account the history of ownership. But storing only information for owners may not be enough in the market. There is a lot of data on the sales' contracts and product metadata that is just as important as the product. Due to the size of that data, these data cannot be included in the blockchain. That's why Monegraph sees the need for a blockchain system that can be implemented in other digital markets. What is needed for the solution is

integration with other services. So, ownership data are stored in the blockchain to remain confidential, traceable and irreversible. But other documents related to the product can be stored in the database, such as MongoDB or CouchDB. Documents can be public, encrypted or not. Digital art itself can be stored in a document repository that can be accessed with HTTP or P2P. For example, the file can be stored in the Amazon Simple Storage Service (S3). The ecosystem, shown in Fig. 3, needs to find a way to connect blockchain, the document repository, and the digital art repository.

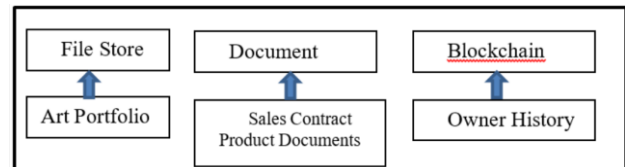The Bitmark real estate transfer system allows the

Figure 4: Blockchain ecosystem [13].

transfer of both digital and physical objects [22]. When storing information about physical objects as an abstract property, a problem arises. Digital fingerprint can be easily traced using the hashtag algorithm, but when it comes to physical objects, there is a new solution called ObjectMinutiae [24].

It can be concluded that so far the Internet has left a lot of material with lost authorship. But looking to the future, blockchain can provide reliable proof of ownership by preserving the hash value of digital art in a time frame for a transaction. The concept is the same for all examples: the owner will have the private key and the original copy of the hashed art. No one can prove otherwise and no institution can change the data. The author can sell digital work, and the new owner will now have the private key to the digital work.

3.4   Internet of Things (IoT)

Current IoT systems rely on a centralized client-server architecture. All devices are identified, authenticated and connected via cloud servers. The connection between the devices goes through the Internet. Even if this solution works well, for now, it may not be able to meet the needs of larger IoT systems in the future [25]. Blockchain technology can become an ideal component and a basic element for tracking billions of connected devices, processing transactions, and coordinating devices. Because blockchain is a decentralized mechanism, it allows the distribution of digital information between different nodes without copying. This can create a new kind of Internet that is safe and resistant to unauthorized modification.

A secure and distributed blockchain system can serve as a platform for the IoT to connect devices seamlessly and securely. Blockchain will allow P2P messaging, file distribution, and autonomous coordination between devices without the need for a centralized cloud. Each device will have its role and will manage its behaviour in the new Internet in a decentralized and autonomous way [26]. The user controls IoT devices from a central point.

The central point may be the user's mobile device. All activities, commands and rules are set by the user. Although this is good for personal control, it is not automated in many ways. The secure model of blockchain technology allows easy human interaction with devices without the need for a central cloud-based central system, which is usually more expensive.

Additionally, because there will be no central control, such as a cloud, the possibility of damaging or stopping the entire IoT system is negligible. This ensures continuity, ease of operation, robustness, scalability and IoT security at a very low cost. A real revolution can happen if all devices are controlled by blockchain instead of direct user control. This is possible by using smart contracts. A smart contract is a code which enforces conditions and business rules that must be met before a transaction can be included in the blockchain. A transaction written in blockchain can be more complex than just transferring ownership. Smart contracts have an integrated mechanism for implementing different types of agreements between nodes. The smart deal is also autonomous and technically it is a computer code that can be self-sustaining and self-executing. Once in force, no human factor is needed to control it [27].

Execution of smart contracts is made possible by Ethereum, which is a platform for creating blockchain systems. Ethereum has its network of nodes and miners, just like Bitcoin. Slock.it is the first implementation of IoT and blockchain using the Ethereum platform [28]. The so-called Slocks are real physical objects that can be controlled by blockchain. They use a computer, Ethereum, which is a piece of electronics that brings blockchain technology into the whole home, allowing to rent access to any compatible smart object and accept payments without intermediaries. Slock.it allows anyone to rent, sell or share anything - without intermediaries. It works as follows: the owner of a smart object (Slock) creates a smart agreement for its use by setting the price and the deposit. Users can find Slock and then pay using Ethereum blockchain, which will allow them to open or close that Slock, which means using it as agreed. The smart contract is implemented automatically, and the deposit is returned to the user minus the rental price. In practice, this means that by installing a smart door lock for the apartment, users can rent an apartment on the blockchain. The smart contract will unlock it and make it available, as stipulated in the contract. In addition to smart doors, this system allows you to rent, sell or share any smart item that has built-in Slock.it technology. Bicycles, cars and any item that can be provided with a physical lock is a case of potential use. Due to the shortcomings of existing IoT architectures, a new secure, private and easy-to-use IoT architecture for a smart home based on the blockchain technology is being proposed [29]. Here, block mining is considered the first problem because IoT devices are devices with limited resources and cannot perform such an operation. IoT devices must also operate at the same time for a detected or assigned command. The time required for mining in blocks, in most cases, may not be acceptable. The proposed solution [29] contains three levels: local network, folding network and cloud storage.

The local network contains all the smart home objects and a local computer that acts as a local blockchain that is constantly on the Internet. This local blockchain is centrally managed by its owner. When there is a new smart device in the home, the user adds it to the blockchain. All transactions related to a particular device are linked to a chain. The folding network is a P2P network that connects multiple smart homes and users. This network manages public keys, allowing users access to smart home data and public keys to smart homes that provide accessible data. Cloud storage is included as a solution for devices that may want to store data in the cloud so that a third party can access the data and provide certain smart services. Using blockchain, the IoT can switch to a network of devices that can communicate with each other and the environment without human intervention. The devices will also make smart decisions, so that many workflows will be automated in new ways, achieving significant time and cost savings.

3.5   Digital identity

Due to a security mechanism that protects against disruption, blockchain can play a key role in securing digital identities 0. Blockchain can protect identity by encrypting. Also, blockchain can be used to build a very strong, secure and impenetrable identity system, which can prevent unauthorized activity. Blockchain technology has the potential to replace all existing physical identities and move them to a digital platform. Identity ranges, such as passports, driver's licenses, ID cards, and even votes election, can be digitally generated using blockchain technology [30]. It is also possible for all identities to be kept together and secured with a blockchain. The use of blockchain, unauthorized modification of various certificates, such as educational, marital, death certificates or registry books, cannot be performed, thus preventing unauthorized and malicious modification.

3.6   Financial services and infrastructure

Blockchain technology can provide a platform for better financial services and payment opportunities. The use of cryptocurrencies such as bitcoin can restore existing payment systems and other financial services [31].

For example, if one person sends money to others in another country, possible transfer funds are banks, payment applications (such as PayPal) or other intermediary organizations. But their service costs are high, even for small transactions.

All of these intermediaries can be eliminated and the money can be transferred directly from the sender to the recipient using cryptocurrencies such as bitcoin, without the involvement of an intermediary. Tracking transactions and property rights can also be implemented in the financial sectors using blockchain. The use of blockchain technology in the financial sector will not only provide a free payment system but will also provide a secure way to conduct online transactions.

3.7   E-commerce

If implemented properly, blockchain technology can massively support e-commerce and retail in terms of growth, sales and marketing. Retail has already begun to witness the growth and profit from the sale of consumer goods and services using blockchain technology.

The Internet acts as a great platform for promoting local businesses and other content, but there is always a risk that the content will be used without proper permission. Overall plagiarism can be limited with timestamping techniques of blockchain and thus preserve the originality of any content. Implementing blockchain technology in the retail industry will also provide a clear and transparent supply chain management system that will allow users to gain insight into the origins of their food and other products.

E-commerce websites and other companies such as OpenBazaar, Provenance, Everledger, Ascribe, and BlockVerify are some of the business activities supported by blockchain involved in the retail industry [30]. This eliminates brokers and commissions and can set up a direct transaction channel between the buyers and sellers. In this way, online sales will promote retail business transactions and the economy.

3.8   Educational records

Sony Corporation, in partnership with Sony Global Education, recently applied for a blockchain-based repository patent that would include student records, including completed courses, test scores, diplomas, and more, in the form of a digital record 0. Such a system can allow teachers and students to access relevant data while maintaining privacy. It can also provide potential educational institutions and potential employers with a transparent, secure place to acquire applicants' credentials.

3.9   Education system

In this time of pandemic when teaching in schools takes place online, many problems arise. Classes are shortened and the teacher has to spend valuable time constantly checking which students are present in the class. Also, the principal of each school wants to know if the staff teachers hold their classes regularly and on time. These problems could be overcome if the data from each class was recorded on a blockchain. In that way, no one will be able to manipulate that data. You can check at any time which professor and when he/she taught and which student attended the class. If students knew that everything was recorded and the data could not be changed, they would surely attend classes more regularly. And that is the most important condition for them to improve their success. Improved student achievement is the best satisfaction for teachers. Parents would also be more satisfied with such behaviour of their children. The whole society would benefit the most from a good education because knowledge is strength and power.

3.10   Sharing knowledge

Everipedia, the world's first blockchain encyclopedia, has announced plans to build a new open-source wiki network that decentralizes the Wikipedia knowledge base, allowing any editor to become a webmaster. According to Larry Sanger, one of the founders of Wikipedia and now acting director of information at Everipedia, it will rely on a blockchain program that allows users to contribute more responsibly. Editors will start earning "tokens" based on their "IQ" (earned points for useful contributions) that will represent the virtual shares of the platform [35].

Theodor Forselius, co-founder and CEO of Everipedia, noted that the ability of the individual to be a stakeholder in the encyclopedia, he/she edits and in turn to gain real monetary value is an exciting idea. Customers will have to pay a deposit before making contributions. If their changes are considered incorrect, they will lose the token and those whose changes are correct will receive an original deposit and additional tokens as a reward.

Forselius also listed two additional benefits of moving Everipedia to the blockchain. The first benefit is that the data will no longer be stored on a centralized server, which means that they will survive even if the central organization, Everipedia, ceases to exist. The second benefit is that it will be impossible to censor the data, which means that governments that currently censor Wikipedia will not be able to prevent users from contributing to the platform.

3.11   Insurance

Blockchain technology has many applications in the insurance sector because the sector is based on agreements and trust between two parties. The use of blockchain in this regard would mean that both the insurance contract and the consumer's personal information can be stored in the distributed book, while the consumer controls who has access. The data remains on the user's device and this can eliminate the need for brokers and other intermediaries between insurance companies and consumers.

The presence of smart contracts is already being felt in the insurance sector. The insurance company AXA worked with a website called Fizzy, which ensured consumers against flights delayed by two or more hours 0. Fizzy noted the procurement of airline tickets on Ethereum blockchain and linked the resulting smart contracts to global air traffic databases. If sufficient delay is observed, the fee was paid automatically. Another example of using smart contracts in the insurance sector is to compensate farmers in the event of a drought or other disaster that harms their property. The other application of blockchain in the insurance industry is its role in potentially reducing fraud 0. In this case, the blockchain records all policies and all claims in a single distributed book.

3.12   Food industry

This technology is potentially beneficial for everyone in the food industry. When foodborne illness occurs, restaurants serving food or grocery stores often have

difficulty discovering the source of the contamination. Monitoring with blockchain will help to immediately track affected objects and their origins, quickly locate the problem so that contaminated products can be removed from menus, shelves and supply chains 0.

The standards and reputation of blockchain-based vendors will ensure the integrity of marketing claims. Certificates and reports on the existing audit of existing facilities will be registered on the site to prove the above claims. If all suppliers in the supply chain follow these rules and write down the data on the origin of food in decentralized monitoring systems, those who make false claims or misrepresent the origin of their products will be destroyed. Blockchain technology allows farmers and producers real-time access to commodity prices and market data. In this way, farmers have better information about the market and they can be more competitive and more productive. More and more people want to know what the products they consume contain. They want to be able to make reliable food choices for themselves, their families, and their communities. Blockchain technology will help build that trust.

3.13   Accounting and audit

Because changing transactions or whole blocks are almost impossible in blockchain, the use of blockchain technology makes it easy to prove the integrity of electronic files. One approach is to generate hash arrays for existing evidence, such as invoices. This set of hash strings is a digital print. Furthermore, this imprint is immutable and is recorded on the blockchain through a transaction. At any later time, it is possible to prove the integrity of that file by re-creating a digital fingerprint and comparing it to the digital fingerprint stored in the block. In case the digital prints are identical, it is proved that the document remained unchanged since the first block placement in the blockchain [34]. Companies will benefit from this type of blockchain implementation. Standardization will allow financial auditors to automatically verify much of the most important financial reporting data. The costs and time required to carry out the audit will be significantly reduced and the time-released can be spent on checking very complex transactions or internal control mechanisms.

3.14   Cross-border payment

Cross-border payments generally refer to the transnational and transregional transfer of funds between two or more countries or territories through international trade, international investment, and other international claims and debts using certain settlement instruments and payment systems. The traditional cross-border payment is based on the banking system which has such characteristics as time-consuming, high cost, more funds occupied, and low security. However, all these bottlenecks can be effectively overcome by applying blockchain to reconstruct the credit system and expand the payment boundary. Researchers pointed out that applying blockchain technology to the cross-border payment has a high potential effect. Holotiuk et al. in [44] stated that the

blockchain technology will improve the payment system by providing a solid structure for cross-border transactions and removing expensive intermediary costs and gradually weaken or alter the business model of the existing payment industries. Yao and Zhu have proposed that the blockchain technology can be adopted for the cross-border payment based on the application of VISA and SWIFT blockchain. R3 has been working with 22 of its member banks to build a real-time, cross-border payments solution on Corda that is the consortium's "blockchain-inspired" distributed ledger [51].

3.15   SARS-CoV-2 virus vs. the Red Cross: better solutions via blockchain and artificial intelligence

Beijing has ordered all public donations for the Wuhan crisis to be funnelled to five government-backed charity organizations. This is a throwback to pre-2016 China before the Charity Law of China was introduced to enable the establishment of private charities. The Charity Law was intended to develop the charity field and protect the interests of relevant stakeholders. Although all charities in China are required to have in place sound internal governance structures, the funnelling order implicitly assumes that the five government-backed charities are fit for purpose and better able to manage the current crisis. That assumption may be at odds with historical and more recent evidence suggesting organizations responsible for responding to crises appear to struggle to manage their core responsibilities. And if Beijing's implicit assumption is wrong then the centralizing effect produced by funnelling merely serves to compound the problem [46].

In this instance, and not for the first time, the Red Cross in China is in the crosshairs of public anger. 'One of the lessons learned was that emergency response must be better developed at the local level'. This is what the Red Cross said in 2017 on the 10th anniversary of the deadly Wenchuan earthquake in Sichuan province in western China. Billions of dollars had been donated following the Sichuan earthquake but had been 'mishandled'. What has been learned? The public in China has again been angered by the mishandling of donations, and this impacts on the willingness to donate, which retards the objective of addressing a problem.

Blockchain and AI are now in frequent use by global technology companies and represent tools that can be used to better manage crises. A private blockchain network would enable the recording and tracking of anything that is donated, from donation to N95 masks. It also creates clear points at which it is possible to hold a person or organization to account, from the loading of donations for delivery through to its final end-use. Importantly, the blockchain can also be given public visibility, providing transparency to all stakeholders - donors and donees, as well as public oversight bodies. Anyone could track the progress and use of their donation.

3.16 E-voting

The use of blockchain technology would prevent any participant from fraud, from the voters themselves to the vote counters in conducting the election. Blockchain technology would make sure that the individual could not vote several times because there is an unchanging record of their voice and identity. Also, no one could delete votes because, as has been said, blockchain is immutable. Those responsible for counting votes will have a final record of the number of votes that regulators or auditors can control at any one time. The results can be encrypted, which would enhance transparency while maintaining a key sense of privacy. The results entered and saved in the blockchain are not only immutable and transparent but also available. This means that voting with blockchain is more efficient than traditional voting 0. Blockchain technology can also be used to improve voting processes in public and private companies and organizations.

4   Key challenges in the implementation of blockchain technology

Implementation of blockchain in all industrial sectors will potentially lead to several issues as well as new dependencies [44]:

Awareness and understanding. The principal challenge associated with blockchain is a lack of awareness of the technology, especially in sectors other than banking, and a widespread lack of understanding of how it works. This is hampering investment and the exploration of ideas.

Organization. The blockchain creates the most value for organizations when they work together on areas of shared pain or shared opportunity – especially problems particular to each industry sector. The problem with many current approaches, though, is that they remain stove-piped: organizations are developing their blockchains and applications to run on top of them. In any one industry sector, many different chains are therefore being developed by many different organizations to many different standards. This defeats the purpose of distributed ledgers, fails to harness network effects and can be less efficient than current approaches.

Culture. A blockchain represents a total shift away from the traditional ways of doing things – even for industries that have already seen a significant transformation from digital technologies. It places trust and authority in a decentralised network rather than in a powerful central institution. And for most, this loss of control can be deeply unsettling.

Cost and efficiency. The speed and effectiveness with which blockchain networks can execute P2P transactions come at a high aggregate cost, which is greater for some types of blockchain than others. This inefficiency arises because each node performs the same tasks as every other node on its copy of the data in an attempt to be the first to find a solution.

Regulation and governance. Regulations have always struggled to keep up with advances in technology.

Indeed, some technologies like the Bitcoin blockchain bypass regulation completely to tackle inefficiencies in conventional intermediated payment networks. One of the other challenges of the blockchain approach, which was also one of its original motivations, is that it reduces oversight.

Security and privacy. While cryptocurrencies like Bitcoin offer pseudonymity (Bitcoin transactions are tied to 'wallets' rather than to individuals), many potential applications of the blockchain require smart transactions and contracts to be indisputably linked to known identities and thus raise important questions about privacy and the security of the data stored and accessible on the shared ledger.

5   Conclusion and further work

Blockchain is as much a political and economic hypothesis as a technological one. Blockchain technology provides a new way to think about how we agree on things. For the first time, multiple untrusted parties can create and agree on a single source of truth, without the use of a middleman. The advance of blockchain technology claims and has the potential to revolutionize many areas of human activity, especially the financial and business worlds. Other applications of blockchain technology discussed previously are equally important. Some of the displayed applications are already implemented, and some can be very easily implemented soon. A major area of future work will focus on implementing blockchain technology for use in EHRs. It will consider how an external stakeholder can use or request a patient's health records from the hospital or health authority without violating patient privacy.

The technology can also be used to maintain birth registers for births, deaths, marriages, business registrations, but also to enable the right to vote in elections without the physical presence of the polling station and to prevent fraud during the voting process. With the application of decentralization enabled by Blockchain technology, stock market fraud would no longer be possible, preventing the emergence of issuing more shares than the presented number, and companies will not be able to hide the profit.

Large companies have a monopoly on electricity sales. But with the help of blockchain, everyone can be involved in the production of electricity through the possibility of micro-transactions. The surplus electricity produced by solar panels in an individual house can be sold to someone who needs it, and the transaction can be done through a crypto-wallet. The application of blockchain in smart contracts allows executing certain simple contracts when all the conditions are met. This innovation can have enormous implications for any kind of agreement that has the potential to digitize output. Without control and supervision, smart contracts can revolutionize the work done by lawyers. Crowdfunding is a very interesting concept that shows that people want to invest in new products and ideas and contribute to their development. Using smart contracts would make it impossible to sell the same things over and over again,

which would give a new dimension to this type of financing.

Another application of blockchain technology is the platform for predicting market movements. When asking a particular question, many people answer it. It is known that 100 thousand average intelligent people will give a better answer to the question than one very intelligent person on the same topic. Such systems provide accuracy and reward if you have given an answer that turned out to be accurate. Such applications already exist - the Augur platform, on which in just a few dollars, a question can be asked, and there is no cost for agency intermediaries, and the answer is always correct and unchanging 0.

With the numerous blockchain technology applications, it should be noted that it requires a lot of resources and is currently not the most cost-effective option for achieving most of these technological advances. It is about spending huge amounts of computing power to implement and verify the information. Blockchain technology is trying to enter revolutionizing many of today's systems, enabling the development of many previously unimaginable technologies. An interesting offspring of this technology can be the redefinition of Internet 3.0 defined as a new type of decentralized infrastructure or network of networks.

References

[1]   Satoshi Nakamoto (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System",
      https://doi.org/10.2139/ssrn.3440802

[2]   Dragana Tadić Živković (2018). "Blockchain technology: opportunity or a threat to the future development of banking", Proceedings of *Ekonbiz*, http://www.ekonbiz.ues.rs.ba/ojs/article/view/139.html (last accessed 06/10/2021)

[3]   Swan M. (2015). "Blockchain: Blueprint for a new economy",
      https://www.goodreads.com/work/best_book/44338116-blockchain-blueprint-for-a-new-economy (last accessed 06/10/2021).

[4]   Li Zhang, Yongping Xie, Yang Zheng, Wei Xue, Xianrong Zheng, Xiaobo Xu (2020). "The challenges and countermeasures of blockchain in finance and economics", John Wiley & Sons, Ltd. https://doi.org/10.1088/1755-1315/825/1/012017 https://doi.org/10.6028/NIST.IR.8202

[5]   Julija Basheska, Vladimir Trajkovik (2018). "Blockchain based Transformation in government: review of case studies", ETAI 2018, http://www.etai.org.mk. (last accessed 06.10.2021)

[6]   Nick Szabo (1997). "The idea of smart contracts". Nick Szabo's Papers and Concise Tutorials. https://fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html (last accessed 06.10.2021)

[7]   J. Garay, A. Kiayias, and N. Leonardos (2015). "The Bitcoin Backbone Protocol: Analysis and Applications", pp. 281-310, Springer Berlin Heidelberg.

[8]   A. Gervais, G. O. Karame, V. Capkun, and S. Capkun (2014). "Is bitcoin a decentralized currency?", IEEE, Security Privacy, vol. 12, pp. 54-60.
      https://doi.org/10.1109/MSP.2014.49.

[9]   Pinyaphat Tasatanattakool, Chian Techapanupreeda (2018). "Blockchain: Challenges and Applications", 978-1-5386-2290-2/18/$31.00 ©IEEE.
      https://doi.org/10.1109/ICOIN.2018.8343163.

[10] Roderick Neame (2013). "Effective Sharing of Records and Maintaining Privacy", Online Journal of Public Health Informatics,
      https://doi.org/10.5210/ojphi.v5i2.4344.

[11] Tal Rapke, MD (2016). "Blockchain Technology & the Potential for Its Use in Healthcare. https://oncprojecttracking.healthit.gov/wiki/download/attachments/14582699/24-Blockchain%20Technology_Tal%20Rapke%20MD.pdf?version=1&modificationDate=1474475152000&api=v2 (last accessed 06/10/2021).

[12] Nitesh Gupta, Anand Jha, and Purna Roy (2016). "Adopting Blockchain Technology for Electronic Health Record Interoperability".
      https://doi.org/10.1109/ColComCon.2018.8466733.

[13] Elena Karafiloski (2017). "Blockchain Solutions for Big Data Challenges", IEEE *EUROCON*.
      https://doi.org/10.1109/EUROCON.2017.8011213.

[14] Laure A. Linn, Martha B. Koo, M.D. (2016). "Blockchain For Health Data and Its Potential Use in Health IT and Health Care Related Research". https://www.healthit.gov/sites/default/files/11-74-ablockchainforhealthcare.pdf.
      (last accessed 06/10/2021).

[15] Ariel Ekblaw, Asaph Azaria, John D. Halamka, MD, Andrew Lippman (2016). "A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data". https://doi.org/10.1109/ICOIN.2018.834316310.1109/ICOIN.2018.8343163

[16] Guy Zyskind, Oz Nathan and Alex 'Sandy' Pentland (2015). "Decentralizing Privacy: Using Blockchain to Protect Personal Data", Security and Privacy Workshops (SPW), IEEE.
      https://doi.org/10.1109/SPW.2015.27

[17] Antorweep Chakravorty and Chunming Rong (2017). "Ushare: user controlled social media based on blockchain", International Conference on Ubiquitous Information Management and Communication.
      https://doi.org/10.1145/3022227.3022325

[18] Roy Rosenzweig (2001). "The Road to Xanadu: Public and Private Pathways on the History Web", The Journal of American History, 88.2. https://chnm.gmu.edu/digitalhistory/links/cached/introduction/link0.27a.pathwaysonhistweb.html (last accessed 06.10.2021)

[19] Trent McConaghy and David Holtzman (2015). "Towards an Ownership Layer for the Internet", ascribe GmbH.

http://trent.st/content/2015-06-24%20ascribe%20whitepaper.pdf (last accessed 06.10.2021)

[20] Dimitri de Jonghe (2016). "SPOOL Protocol", https://github.com/ascribe/spool. (last accessed 06.10.2021)

[21] Trent McConaghy, Rodolphe Marques, Andreas Muller, Dimitri De Jonghe, T. Troy McConaghy, Greg McMullen, Ryan Henderson, Sylvain Bellemare, and Alberto Granzotto (2016). "BigchainDB: A Scalable Blockchain Database", ascribe GmbH, Berlin, Germany. http://blockchain.jetzt/wp-content/uploads/2016/02/bigchaindb-whitepaper.pdf (last accessed 06.10.2021).

[22] The Guardian (2015). "PRS for Music takes legal action against SoundCloud streaming service" https://www.theguardian.com/technology/2015/aug/27/prs-for-music-takes-legal-action-against-soundcloud. (last accessed 06.10.2021).

[23] Christopher Hall, Casey Alt, Lê Quý Quốc Cường, and Sean Moss-Pultz (2016). "Bitmark: The property system for the digital environment". https://docs.bitmark.com/assets/pdf/bitmark-technical-white-paper.pdf (last accessed 06.10.2021)

[24] Tzu-Yun Lin, Yu-Chiang Frank Wang, Sean Moss-Pultz (2015). "ObjectMinutiae: Fingerprinting for Object Authentication". https://doi.org/10.1145/2733373.2807989.

[25] FTC Staff Report (2015). "Internet of Things: Privacy & Security in a Connected World", https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf. (last accessed 06.10.2021)

[26] Executive Report (2015). "Device democracy - Saving the future of the Internet of Things", IBM Institute for Business Value. https://www.ibm.com/downloads/cas/Y5ONA8EV (last accessed 06.10.2021)

[27] Vitalik Buterin (2016). "A next generation smart contract & decentralized application platform", Ethereum White Paper. https://www.weusecoins.com/assets/pdf/library/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf (last accessed 06.10.2021)

[28] Christoph Jentzsch (2015). "Decentralized Autonomous Organization to Automate Governance". http://cryptochainuni.com/wp-content/uploads/Decentralized-Autonomous-Organization-To-Automate-Governance.pdf. (last accessed 06.10.2021)

[29] Ali Dorri, Salil S. Kanhere, and Raja Jurdak (2016). "Blockchain in Internet of Things: Challenges and Solutions". https://arxiv.org/abs/1608.05187, (last accessed 06.10.2021)

https://en.wikipedia.org/wiki/Digital_identity, (last accessed 06.10.2021).

[30] TechGenix (2018). "Blockchain technology: Why it will change the world", [Internet], URL: https://techgenix.com/blockchain-technology, (last accessed 06.10.2021).

[31] Quora (2017). "How will blockchain impact accounting, auditing & finance?", https://www.quora.com/How-will-blockchain-impact-accounting-auditing-finance, (last accessed 06.10.2021).

[32] Object Computing (2017). "8 ways blockchain is changing the world", https://objectcomputing.com/news/2017/12/20/8-ways-blockchain-changing-world, (last accessed 06.10.2021).

[33] Blockchain Expo (2018). "How will blockchain impact the insurance sector?", https://www.blockchain-expo.com/2018/02/blockchain/blockchain-insurance, (last accessed 06.10.2021).

[34] Forbes (2018). "3 Innovative Ways Blockchain Will Build Trust In The Food Industry", https://www.forbes.com/sites/samantharadocchia/2018/04/26/3-innovative-ways-blockchain-will-build-trust-in-the-food-industry/#285bfa832afc, (last accessed 06.10.2021).

[35] Hacker Noon (2018). "How Blockchain Will Make Electronic Voting More Secure", https://www.bitcoininsider.org/article/27800/how-blockchain-will-make-electronic-voting-more-secure, (last accessed 06.10.2021). https://www.augur.markets (last accessed 06.10.2021). https://www.axa.com/en/magazine/axa-goes-blockchain-with-fizzy, (last accessed 06.10.2021).

[36] Aleksandar Matanović, "Osnove kriptovaluta i blokčein tehnologije", http://fzp.singidunum.ac.rs/demo/wp-content/uploads/Osnove-kriptovaluta-i-blok%C4%8Dein-tehnologije.pdf, (last accessed 06.10.2021).

[37] Gu, J.; Sun, B.; Du, X.; Wang, J.; Zhuang, Y.; Wang, Z. (2018). "Consortium blockchain-based malware detection inmobile devices", IEEE. https://doi.org/10.1088/1742-6596/1693/1/012025

[38] Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; De Caro, A.; Enyeart, D.; Ferris, C.;Laventman, G.; Manevich, Y.; et al. (2018). "Hyperledger fabric: A distributed operating system for permissioned blockchains". In Proceedings of the Thirteenth EuroSys Conference ACM, Porto, Portugal, 23–26 April;pp. 1–15. https://doi.org/10.1145/3190508.3190538

[39] Hyperledger Burrow - Hyperledger. Available online: https://www.hyperledger.org/projects/hyperledger-burrow (last accessed 06.10.2021).

[40] Domina Hozjan (2017). "Blockchain", Sveučilište u Zagrebu Prirodoslovno–Matematički Fakultet matematički Odsjek, Zagreb.

https://repozitorij.pmf.unizg.hr/islandora/object/pmf
:779 (last accessed 06.10.2021).

[41] Miroslav Minović (2017). "Blockchain technology: usage beside cripto currencies". Available online: https://www.researchgate.net/publication/31872273 8

[42] Dejan Vujicic, Dijana Jagodic, Siniša Ranđić (2018). "Blockchain technology, bitcoin, and Ethereum: A brief overview", Available online: https://doi.org/10.1109/INFOTEH.2018.8345547

[43] Mijoska M. and Ristevski B. (2020). "Blockchain Technology and its Application in the Finance and Economics", 10th International Conference on Applied Information and Internet Technologies – AIIT 2020, October, Zrenjanin, Serbia. http://www.tfzr.uns.ac.rs/aiit/files/AIIT2020%20ePr oceedings.pdf. P.197-202
(last accessed 06.10.2021).

[44] https://www2.deloitte.com/content/dam/Deloitte/uk/ Documents/Innovation/deloitte-uk-blockchain-key-challenges.pdf, (last accessed 06.10.2021).

[45] Holotiuk, F., Pisani, F., & Moormann, J. (2017). The impact of blockchain technology on business models in the payments industry. Wirtschaftsinformatik 2017 Proceedings. Retrieved https://wi2017.ch/images/wi2017-0263.pdf   (last accessed 06.10.2021).

[46] Crosman, P. (2017). "R3 to take on Ripple with cross-border payments blockchain". American Banker; New York, N.Y. Retrieved from https://www.bitcoinisle.com/2017/10/31/r3-to-take-on-ripple-with-cross-border-payments-blockchain/
(last accessed 06.10.2021).

[47] Syren Johnstone (2020). A Viral Warning for Change. COVID-19 Versus the Red Cross: Better Solutions Via Blockchain and Artificial Intelligence, University of Hong Kong Faculty of Law Research Paper No. 2020/005
http://researchblog.law.hku.hk/2020/02/syren-johnstone-on-wuhan-coronavirus.html,
(last accessed 06.10.2021).