Grzegorz Borowik[1]
ORCID: 0000-0003-4148-4817
Zbigniew M. Wawrzyniak[2]
ORCID: 0000-0003-0052-4114
Paweł Cichosz[3]
ORCID: 0000-0003-0052-4114

Blockchain technology — innovation and security

[1] EngD Grzegorz Borowik — scientist, doctor of technical sciences. His current work focuses on machine learning algorithms, Big Data and image processing. Until 2016, he was an employee of the Cyber Security Department at the Institute of Telecommunications of the Warsaw University of Technology. In 2015, he won the 'Top 500 Innovators' internship and training programme of the Ministry of Science and Higher Education, implemented at the University of California in Berkeley, the United States, the aim of which was training in the area of business management in science and commercialisation of research. In 2016, he completed a postdoctoral internship at the Knowledge Engineering and Discovery Research Institute in Auckland, New Zealand, where he conducted research related to the practical application of artificial third generation neural networks. In 2016-2018, he was involved in modelling algorithms for secure P2P networks in the Golem project, which aims to create a decentralised supercomputer. In 2017-2019, he held the position of assistant professor at the Police Academy in Szczytno in the Cyber Security Department. Currently, he is a research and development manager at Nethone company, where he runs a project in cyber security. He is the author of an academic textbook and the author and co-author of over a hundred publications in scientific journals and conference materials. His research interests include computational intelligence, machine learning techniques, optimisation techniques, NLP, Internet of things, cryptography and blockchain. For many years, he has been involved in B+R projects, including the role of a manager and a main contractor.

Contact with the author via the editorial office.

[2] EngD Zbigniew M. Wawrzyniak — holder of a doctoral degree in electronics engineering awarded by the Faculty of Electronics and Information Technology of the Warsaw University of Technology in 1990; an assistant professor at the Institute of Electronic Systems of the Warsaw University of Technology. His scientific interests focus on the application of modelling techniques and methods of simulation and forecasting based on experimental observational and signal data, management and statistical exploration of signal and process data, including image data and ICT. He is the author and co-author of more than eighty publications in monographs, scientific journals and conference materials. He has extensive experience in the implementation of practical projects in the field of modelling and predictive analysis of data.

Contact with the author via the editorial office.

[3] EngD Paweł Cichosz — received a doctoral degree in computer science from the Faculty of Electronics and Information Technology of the Warsaw University of Technology in 1998; an assistant professor at the Institute of Computer Science of the Warsaw University of Technology. His scientific interests include the areas of machine learning, discovery of knowledge in data and artificial intelligence. He has extensive experience in the implementation of practical projects in the field of data analysis and predictive modelling.

Contact with the author via the editorial office.

Introduction

Blockchain is one of the most revolutionary technologies of the 21st century, which is still under development, and whose potential is not yet fully exploited. In essence, blockchain is simply a dispersed database of records. What makes it unique is that it is not a private database, but a public one, i.e. anyone who uses it has its full or partial copy, and a new record can only be added with the consent of other database owners. Moreover, thanks to the blockchain network, it is possible to implement cryptocurrencies and intelligent contracts.

Since blockchain is a distributed system which is not maintained by one specific institution, it can be treated as a kind of common infrastructure shared among all participants. This means that an inter-organisational workflow management system based on blockchain has one important advantage - there is no need for a central management body. Therefore, using a blockchain-based system as an infrastructure facilitates automation and simplifies the system. On the other hand, such a solution has to face challenges such as abuse, unclear responsibilities and differing user opinions.

There are two types of blockchain technology: public blockchain and private blockchain. Anyone can join a public blockchain. Bitcoin is an example of a public blockchain, where anyone who wants to buy the cryptocurrency can join the chain. The blockchain is open, which means that everyone can see all transactions. Private block chains are centrally administered and require permission to join; they are suitable for use within one organisation or between partner organisations. Both public and private solutions are secure because they cannot be altered (i.e. each record or block is unalterable and linked to all others), and adding new blocks requires consensus of the users. This means that they are natively safer than virtually any other network technology.

Although blockchain gained in importance in 2009, scientists and entrepreneurs are still unable to understand the mechanisms and fully appreciate its potential, especially from the perspective of technical challenges and technology limitations[4]. The article[5] mentions seven challenges and limitations to blockchain technology: throughput, latency, size, security, wasted resources, usability and versioning, hardforks and multichains.

Basics of technology

A blockchain consists of blocks which store valuable information. For example, bitcoin blocks store transactions, the essence of every cryptocurrency. In addition, a block contains some

[4] Beck R, Stenum Czepluch J, Lollike N, Malone S, Blockchain — The Gateway to Trust — free Cryptographic Transactions, 24th European Conference on Information Systems (ECIS), Istanbul, Turkey, 2016.

[5] Swan M, Blockchain. Blueprint for a New Economy, Sebastopol, 2015.

technical information, such as its version, the current timestamp and the hash of the previous block. In its simplified version, which contains only the relevant information, a block is illustrated in Figure 1.

Figure 1

Block

```
type Block struct {
      timestamp     int64
      data          []byte
      prevBlockHash []byte
      hash          []byte
}
```

Source: author's own material

Timestamp is a record which shows when a given block was created, *data* is the actual information contained in a block, *prevBlockHash* stores the value of the hash function for the previous block, and *hash* is a shorthand for a given block. In the bitcoin protocol description, the *timestamp, prevBlockHash* and *hash* fields are located in the block header, creating a separate data structure, while transactions (*data*) are a separate data structure.

Calculating hash values for blocks is a very important, integral feature of a blockchain which affects its safety. The operation is computationally difficult and takes a certain amount of time, even on fast computers. It is a deliberate architectural element which makes it difficult to add new blocks and prevents them from being modified once added to a blockchain.

At its core, a blockchain is simply a structured database: it is an ordered one-way list pointing to the previous element - a block. This means that blocks are stored in the insertion order and that each block is linked to the previous one. This structure makes it possible to quickly read the latest block in the string and (efficiently) read a block by its hash. This structure can be implemented using a map or, in the simplest version for the purposes of this article, using a table (Figure 2). The table will then store ordered blocks and the map will store pairs (*hash, block*).

Figure 2

Blockchain

```
type Blockchain struct {
      blocks []*Block
}
```

Source: author's own material

In order to add a new block, an existing block is needed. Therefore, there must be at least one block in each blockchain. The first block in the chain is known as the *genesis block*.

However, in reality a blockchain is much more complex, and adding new blocks so that they can store data requires some work - calculations - such as in the bitcoin protocol. Next, the new block has to be approved by other network members - which is referred to as *consensus*. It should also be noted that blockchain is a distributed database which does not have a single decision-maker. All of these mechanisms make blockchain secure and consistent. A reward is paid for the work done and approval by other nodes - this is how people receive tokens/cryptocoins (depending on the technology) for *mining*. In blockchain, *miners* work to maintain the network, and add new blocks to it, and receive a reward for their work. As a result of their work, a block is incorporated into the chain in a secure way, which ensures the stability of the entire database. It is worth noting that the person who has finished their work has to prove it. The need to secure transactions is connected with the problem of *double spending*, because in a decentralised system, there is a natural possibility that the same number of tokens can be spent twice by one buyer.

In the most popular solution, before obtaining permission to add a block, calculations are performed - this mechanism is called proof-of-work (PoW). With the popularisation of the technology, new proposals have appeared to counteract double spending, because the biggest drawbacks of the proof-of-work method are: high energy consumption, demand for special computing units, such as ASIC or GPU, delayed transactions and lack of profitability in the long-term network maintenance. Other proposals for consensus building mechanisms include: proof-of-stake (PoS), proof-of-importance (PoI), proof-of-capacity (PoC) and proof-of-space (PoS).

The proof-of-work algorithms must meet the following requirement: the work is difficult to do, but the proof-of-work verification is easy. The work is difficult because it requires a lot of computing power. What is more, the difficulty of this work is being dynamically regulated. In bitcoin, blocks are added on average every 10 minutes. The aim of the work is to find a block hash that meets specific requirements, and it is this calculated hash that serves as proof. Therefore, finding a proof is a real job. Verification of the proof can be understood as substituting the result of previous calculations into the equation specified by the protocol and comparing the result, which does not take much time.

The process of obtaining a hash for specific data is called hashing. A hash is a unique representation of data. A hash function, sometimes called a mixing function, takes data of any size and creates a fixed size hash. Below, a few key features of a hash function are presented:

1. The original data cannot be restored from the hash. Therefore, mixing is not encryption.
2. A specific set of data may have only one hash - the hash is unique.
3. Alteration of even one byte in the input data generates a completely different hash. Well-designed hash functions should produce a hash which is at least 50% different for a small alteration.

Hash functions are widely used to check data integrity. Some software vendors publish checksums for software packages, which are a result of hash functions.

In blockchain, a hash calculation is used to guarantee integrity. The input data for the mixing algorithm contains the hash of the most recent block, making it impossible (or very difficult) to edit the block in the string - block modification causes its hash and the hashes of all other blocks added to the blockchain to be recalculated.

Bitcoin uses the hashcash algorithm. This is a proof-of-work algorithm that was originally developed to prevent spam from being generated in the form of unwanted e-mails. This algorithm can be described in the following steps:

1. Prepare publicly known data (in the case of an e-mail - the recipient's e-mail address, in the case of bitcoin - block headers).
2. Add the counter to the data - in the sense of concatenation of sets. The counter starts from 0.
3. Generate the hash for (*data*, *counter*).
4. Check that the hash meets the definitive requirements:
   a) if it does, calculations are completed,
   b) if it does not, increase the counter and repeat step 3 and 4.

As can be seen, it is a *brute-force* algorithm: increasing the counter, then calculating the hash, checking, incrementing the counter, calculating the hash, etc. The algorithm is computationally expensive.

The original *hashcash* algorithm requires that the first 20 bits of the generated output must be zero. In bitcoin, the requirement is adjusted as needed because it is assumed that a block must be generated every 10 minutes, despite the increasing computing power and the increasing number of servers/computers (*miners*) joining the network.

Blockchain is stored in a database. In the original article describing the bitcoin cryptocurrency[6], no specific database was defined. Bitcoin Core, which was initially published by Satoshi Nakamoto and is now the reference bitcoin implementation, uses LevelDB. In this database, the data is stored as key-value pairs. Then, the key-value pairs are stored in segments, which in turn are intended for grouping pairs similar to each other - analogically to tables in relational database management systems. Bitcoin Core uses two segments to store data: *blocks* - which store metadata describing all blocks in a string, *chainstate* - which stores the state of the string. In addition, blocks are stored as separate files on disk. This is done in order to increase efficiency - the reading of a single block does not require all of them to be loaded into memory.

In the blocks segment, the key → value pairs are:

1. 'b' + 32-byte block hash → block index record,
2. 'f' + 4-byte file number → file information record,
3. 'l' → 4-byte file number: the last block file number used,
4. 'R' → 1-byte boolean: whether we're in the process of reindexing,

[6] Nakamoto S, Bitcoin: A Peer-to-peer Electronic Cash System, 2008 <https:// bitcoin.org/bitcoin.pdf>, *accessed* 17.09.2018.

5. 'F' + 1-byte flag name length + flag name string → 1 byte boolean: various flags that can be on or off,
6. 't' + 32-byte transaction hash → transaction index record.

In the chainstate segment, the *key* → *value* pairs are:

1. 'c' + 32-byte transaction hash → unspent transaction output record for that transaction,
2. 'B' → 32-byte block hash: the block hash up to which the database represents the unspent transaction outputs.

To create a blockchain, perform the following sequence:

1. Open DB file.
2. Check if a blockchain is stored in it.
3. If a blockchain exists:
   a) create a new blockchain instance,
   b) set the end of the blockchain instance to the hash value of the most recent block stored in DB.
3. If a blockchain does not exist:
   a) create a genesis block,
   b) b) save it in the DB,
   c) save the value of the genesis block hash as the hash of the last block.
   d) create a new blockchain instance and set the end of the blockchain instance to the hash value of the genesis block.

So, the blockchain structure looks like the one in Figure 3.

Figure 3

Blockchain structure

```
type Blockchain struct {

    tip []byte

    db *bolt.DB

    }
```

Source: author's own material

Transactions are the main application of blockchain. The goal is to store transactions in a secure and reliable way so that they cannot be modified after they have been created. In typical online payment applications, there are databases for accounts and transactions. The Accounts Database stores information about the user, including their personal data and balance, and the Transaction Database stores information about transfers. In the bitcoin protocol, payments are made in a completely different way. No accounts are kept, no information is collected about balances or addresses, and there are no coins, senders or recipients. The only thing which there is, is transactions. Since blockchain is a public and open database, it would not be desirable to keep confidential information about wallet owners. Coins are not collected in accounts. There

is no field or attribute in the structure that represents the balance of the account. Transactions do not send money in the manner in which banking systems do.

A bitcoin transaction is a combination of input and output data (Figure 4). The inputs of new transactions correspond to the outputs of the previous transaction. The following assumptions are fulfilled: there are outputs that are not linked to inputs; in a single transaction, input data can relate to the output of multiple transactions; the input must relate to the output. In other words, transactions block values using a script that can only be unblocked by the unit that has blocked them.

Figure 4

Structures for transactions

```
type Transaction struct {
          id   []byte
          vIn  []TXInput
          vOut []TXOutput
}

type TXOutput struct {
          value        int
          scriptPubKey string
}

type TXInput struct {
          txId      []byte
          vOut      int
          scriptSig string
}
```

Source: author's own material

Ethereum

Ethereum is a decentralised cryptographic system based on blockchain, as well as a platform for creating distributed applications. In Ethereum, it is possible to implement any complex rules required by the payment system as intelligent contracts in the high level programming language - Solidity. Moreover, Ethereum enables token fragmentation.

Ethereum stores the global state in a blockchain. This state is essentially a collection of accounts, each of which has its own unique address

and balance record in the ether currency. An account can store data and can contain a related contract code[7].

The global state changes according to the transaction. Each transaction has a sender's and recipient's address and a certain number of ethers between these addresses. If the recipient's account is linked to a contract code, the contract is made as the result of the transaction. The transaction may contain additional data available under the agreement. The agreement may trigger another agreement, which may trigger another agreement, but this execution chain must start with a transaction initiated by an external party/user. The contract cannot invoke any external service outside of Ethereum.

Contracts are concluded by the Ethereum Virtual Machine (EVM)[8]. Each EVM instruction consumes a certain amount of gas that reflects the calculation cost of processing the instruction through Ethereum nodes. The gas must be purchased in the ether currency by the user who wants to enter into a contract. The gas fee is equivalent to the transaction fee in bitcoins. The price of gas is market-based: each transaction determines the maximum price the sender is willing to pay for the gas unit and the 'miners' are willing to pay for it. Miners may give priority to transactions based on this information. In order to estimate the cost of a contract in USD currency, both the current average price of gas and the price of ether must be taken into account. Conversely, in order to compare different payment patterns through implemented Ethereum contracts, one can compare their cost in gas units.

The calculation model of Ethereum is deterministic: the result of each transaction is always the same when it is carried out in a given global state[9]. This limits the possibility of generating random values in Ethereum. A common solution is to rely on future blockchain data as a source of randomness. For example, a timestamp or a header abbreviation for a future block can be used to call a random number generator. Ethereum contracts have no mechanism for scheduling actions, for example, calling another contract or reading a time stamp to be carried out later. Therefore, any payment system using Ethereum will be based on users willing to perform the transactions required by the program protocol. In particular, users must be online during the execution of at least some phases of the protocol. They also need to have enough ether to pay for their transactions, which can be a problem for payment protocols that require nodes to take

[7] Atzei N, Bartoletti M, Cimoli T, A survey of attacks on Ethereum smart contracts SoK, *Principles of Security and Trust* 2017, Vol. 10024. pp. 164–186.

[8] English M, Auer S, Domingue J, Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development, Computer Science Conference for University of Bonn Students, Bonn, Germany 2016.

[9] Konstantinidis I, Siaminos G, Timplalexis C, Zervas P, Peristeras V, Decker S, Blockchain for Business Applications: A Systematic Literature Review, International Conference on Business Information Systems, Springer Cham 2018, pp. 384—399.

action. This is particularly important in multi-participant protocols, where anyone can stop the protocol. Fortunately, smart contracts can implement reward mechanisms that provide an economic incentive to take action.

Application

Blockchain application research is focused more than 80% on bitcoin and less than 20% on other applications[10]. However, there are many applications available that go far beyond its first implementation[11].

For example, blockchain technology can be used as a marketplace for financial assets, a fraud-proof supply chain database[12], or as an environment for digital contracts and peer-to-peer data exchange[13]. Blockchain has been adapted to many industries and governmental agencies around the world. In Zug, Switzerland, it is used to identify citizens. Maersk and Walmart use it to track their supply chain. TUI Tourism Group wants to use blockchain for hotel and tourist reservations. In addition, governments in countries such as Brazil, Sweden and Georgia use blockchain for property and land registration. Malta uses blockchain to register its university diplomas and other educational and professional certificates. Companies such as Gem, Philips and YouBase are using it for healthcare, while MIT is developing a blockchain-based healthcare system called MedRec. Blockchain technology has the potential to revolutionise a broad spectrum of business processes[14]. Some authors claim that their approach can provide 'an automatic and constant history of transactions, a direct implementation of the mediation process control logic' (using smart contracts) and an 'audit trail for common business processes'[15]. Crosby and others[16] have distinguished between financial and non-financial applications that could potentially be addressed by blockchain. This groundbreaking innovation can not only change the nature of financial interactions, but also apply to many other areas of our daily lives.

---

[10] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K, Where Is Current Research on Blockchain Technology? A Systematic Review, *PloS one* 2016, No. 11, Vol. 10, <https://doi.org/10.1371/journal.pone.0163477>, *accessed* 21.10.2019.

[11] Beck R, Stenum Czepluch J, Lollike N, Malone S, Blockchain…, *op. cit.*

[12] Mattila J (2016) The Blockchain Phenomenon — The Disruptive Potential of Distributed Consensus Architectures, The Research Institute of the Finnish Economy, Mattila, Juri, 2016 <https://ideas.repec.org/p/rif/wpaper/38.html>, *accessed* 21.10.2019.

[13] Swan M, Blockchain. Blueprint for a New Economy, Sebastopol 2015.

[14] Weber I, Xu X, Riveret R, Governatori G, Ponomarev A, Mendling J, Untrusted Business Process Monitoring and Execution Using Blockchain, Springer, Cham 2016.

[15] *Ibid.*, p. 2.

[16] Crosby M, Nachiappan Pattanayak P, Verma S, Kalyanaraman V, Blockchain technology: Beyond bitcoin, *Applied Innovation Review*, No. 2, pp. 6–19.

Blockchain has a variety of applications, particularly in areas that have so far relied on the involvement of a trade intermediary to maintain a certain level of trust. Marcella Atzori suggests that policy and society as a whole can be restructured by blockchain[17]. Many existing methods and functions can lose their attractiveness if people start to organise and protect society through decentralised platforms. The article states that 'decentralisation of government services through blockchain is possible and desirable because it can significantly increase the functionality of public administration'[18]. Reorganisation of society is particularly important in underdeveloped and poor countries, where value can be better protected using blockchain, unless there are barriers to accessing digital networks and services. In Third World countries, landowners have a huge problem with documenting property if, for example, the local government is trying to expropriate the population. These existential threats can be controlled by integrating land titles with blockchain. Therefore, in some developing countries, blockchain is being implemented as a registration and property management system. However, as Florian Glaser indicated[19], the interface between the digital sphere and the physical world may prove to be a weak link that will adversely affect digital trust in the blockchain system.

A question of discussion among scientists and lawmakers is whether a cryptocurrency based on blockchain can work as real money[20]. Money can be defined as 'everything that is generally accepted in the payment of goods, services or debts'[21]. Wiliam J. Luther and Lawrence H. White claim that cryptocurrencies are rarely used as a medium of exchange today[22]. However, Florian Glaser, Kai Zimmermann, Martin Haferkorn, Mortiz Weber, and Michael Siering emphasise that bitcoin is primarily used as a speculative asset[23]. However, the popularisation of cryptocurrency may become possible thanks to an innovative approach of entrepreneurs who will accept cryptocurrency as a money substitute. Therefore, the financial

[17] Atzori M, Blockchain technology and decentralized governance: Is the state still necessary?, <https://ssrn.com/abstract=2709713>, *accessed* 21.10.2019.

[18] *Ibid.*, p. 31.

[19] Glaser F, Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis, Proceedings of the 50th Hawaii International Conference on System Sciences (HICSS 2017), Waikoloa Village, Hawaii 2017.

[20] European Central Bank, Virtual Currency Schemes, 2012 <https:// www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>, 30 November 2016; Federal Bureau of Investigation, Bitcoin virtual currency: intelligence unique features present distinct challenges for deterring illicit activity, 2012, <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf>, *accessed* 30.11.2016.

[21] Mishkin F.S, The economics of money and financial markets, Boston 2004.

[22] Luther W.J, White L.H, Can bitcoin become a major currency?, *Working Paper in Economics* 2014, No. 14–17.

[23] Glaser F, Zimmermann K, Haferkorn M, Weber M, Siering M, Bitcoin–asset or currency? Revealing users' hidden intentions, Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv 2014.

industry is afraid that a large part of their current activity may be replaced by blockchain. Indeed, if people pay today by credit card, the payment is made after a few days' delay. Using blockchain, however, payment can be made almost in real time.

Blockchain can contribute to how people will pay for goods in the real world. For example, homeowners incur significant transaction costs when buying and servicing property. According to Goldman Sachs, 'blockchain can reduce insurance premiums and generate $2-4 billion in savings in the US, reducing errors and direct handling'[24]. This breakthrough innovation can create new and change many existing business models and thus have a major impact on many industries.

The development of blockchain technology in recent years has led to the development of other concepts. The taxonomy of decentralised (consensus) compliance systems and an overview of the different types of systems are presented by F. Glaser and L. Bezzenberger in their paper entitled 'Beyond Cryptocurrencies - A Taxonomy of Decentralized Consensus Systems'[25]. Nick Shabo introduced the concept of 'smart contracts'[26], which link computer protocols to user interfaces for the purpose of implementing the conditions of the contract[27]. Thanks to the blockchain system, smart contracts are becoming more and more popular, as they can be more easily implemented in the blockchain structure compared to the technology available at the time they were developed. Such an innovative approach may, for example, replace the work of lawyers or banks participating in asset agreements under pre-determined conditions[28]. Smart contracts can also be used to control property ownership. These properties can be tangible (e.g. houses, cars) or intangible (e.g. stocks, access rights). The Ethereum network, which is a decentralised system proposed by Buterina[29], is an outstanding example of blockchain technology that implements intelligent contracts. The Ethereum technology allows contracts to be concluded using cryptography, replacing third parties (e.g. notaries), which were necessary to build trust in the past. Blockchain can

[24] Sachs G, Profiles in Innovation — Blockchain, <http:// www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf>, *accessed* 30.11.2016.

[25] Glaser F, Bezzenberger L, Beyond Cryptocurrencies — A Taxonomy of Decentralized Consensus Systems, materials from the 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany 2015.

[26] Szabo N, Smart contracts: formalizing and securing relationships on public networks. *First Monday* 1997, Vol. 2, No. 9.

[27] Kosba A, Miller A, Shi E, Wen Z, Papamanthou C, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, 2016 IEEE symposium on security and privacy (SP), Vol. 1.

[28] Fairfield J, Smart contracts, Bitcoin bots, and consumer protection, *Washington and Lee Law Review Online* 2014, Vol. 71.

[29] Buterin V, A next-generation smart contract and decentralized application platform, <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>, *accessed* 21.10.2019.

accomplish the entire transaction process by automatically executing contracts in a cost-effective, transparent and secure manner[30]. Architectural components of blockchain technology, their interactions, and a library for analysing impacts on digital ecosystems can be found in a publication by F. Glaser — 'Pervasive decentralisation of digital infrastructures: a framework for a blockchain enabled system and use case analysis'[31].

Another application of blockchain is so-called crowdfunding. A crowdfunding campaign allows a large number of parties to contribute funds to a certain social good. If the minimum goal of the grant is achieved before the deadline, then the donations are made to a designated party (entrepreneur), otherwise the donations are returned.

Another application is investment insurance using the financial instrument swap. A person with a risky investment portfolio (e.g. with a large number of bitcoins) can hedge against the risk by buying insurance (e.g. by effectively betting on the price of bitcoins with another person). The share price at a certain future date, determined by a trusted body specified in the public procurement contract, determines which of the two parties will receive the payout. A private contract ensures confidentiality in the context of the details of the contract, i.e. the price cap and the payout.

Blockchain technology can be used to establish voluntary regulatory systems. Hwyl Labs has proposed that blockchain could be used to support climate change measures. Under this model, an entity may enter into an intelligent agreement with another person, organisation, company or government to reduce the entity's GHG emissions. The contract would specify the payment for a specific set of measures that would reduce GHG (greenhouse gas), for example by using green energy. These commitments can be tracked using real-time sensors, e.g. sensors in vehicle engines, sensors in the industrial facility, and then the blockchain can be verified to see if the appropriate level has been reached. After a positive verification, the relevant funds are paid out. Individual contracts could be combined into greater collections to create large-scale reductions in greenhouse gas emissions. Units that are exposed to high GHG reduction costs could effectively buy credits (using smart contracts on their own account) to reduce GHG emissions. The result would be a fraud-proof GHG trading system.

In the United States, one of the important social problems is the control of firearms. Defenders of the right to possess weapons do not accept the registration or tracking of weapons for constitutional reasons, fearing that any registration will be a step towards infringing their freedom. Supporters of arms control highlight the problem of the use of weapons in crime and the fact that legally purchased weapons can be used by someone with bad intentions. Until now, the problem has not been solved. In the blockchain model, it would be possible to use Internet of Things (IoT) to create a non-governmental but controlled database, which would register purchases and the use of weapons as a transaction on the blockchain,

[30] Fairfield J, Smart…, *op. cit.*

[31] Glaser F, Pervasive…, *op. cit.*

assuming that the weapons are registered on the blockchain during production. Throughout the life of a weapon, and at every point in its history, every transfer of property will be registered on the blockchain. A transaction may be private, but with intelligent contracts, there may be a mechanism to control the blockchain, for example, by means of a search warrant. As part of the transaction, each party would be protected by a strong encryption standard that is offered by the blockchain and the dispersed nature of the system would prevent fraud. Moreover, since the blockchain exists in the public space, weapons owners could be sure that their property rights would be minimally violated. If the weapons were equipped with biometric locks, they could be used to prove transfer of ownership.

In a joint police foundation report prepared together with the CGI from the UK[32], we read that digitisation and new technologies, particularly blockchain, can improve processes and connect services. The range of technologies and potential applications for the CJS (criminal justice system) is broad. At the same time, a greater use of automation can improve the speed and quality of tasks such as conducting audits. In the future, it can even help solve problems such as subjective prejudice in decision-making processes. Blockchain technology can provide a unique opportunity to increase the accuracy and transparency of processes through secure and possible-to-verify dispersed records. The same report explains that the UK justice system is largely based on paper solutions, archaic practices and old IT systems, the use of which results in inefficient services. An example of this is that, throughout the judicial system in Great Britain, only half of the meetings take place on the day they were supposed to take place, and manual trials result in unnecessary duplication of documents and in an increase in error-making.

Weaknesses in the technology

Although blockchain is a promising technology for business process reorganisation and many industrial applications, it still has numerous weaknesses despite different implementations in many existing forms.

Experts and analysts also warn that this technology is not suitable for every trading process. Implementation is slower and more expensive than traditional transaction technologies such as a centralised relational database. The autonomy of the blockchain has a big impact on the lack of efficiency. Since new blocks require cryptographic verification before being added to the blockchain, it can be inefficient for business applications that require rapid transaction accounting. By their nature, blocks need to be serialised, which means that the update rate is slower than

[32] Crowhurst L, Reforming justice for the digital age The Police Foundation, in partnership with CGI, July 2017, <http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/pf_cgi_digital_justice.pdf>, *accessed* 17.09.2018.

that of a traditional database, which in turn, can update data in parallel. The biggest advantage of the blockchain is one-time recording and dispersion into nodes. It can be easily scattered across different network nodes, but each record still contains its own shortcut, which makes it invariable. A blockchain-based distributed database can provide a richer, more comprehensive transaction history. This does not mean, however, that transaction data must be part of the chain. For example, if blockchain users included multimedia data as part of their transactions, the database volume would increase rapidly - as would network load. For reasons of distribution, all data must be replicated to all nodes in the chain. Therefore, for some transactional tasks, it is better to use a relational database.

When creating a private blockchain, its architecture is a key issue. In order to reach a consensus, it is necessary to announce and add a transaction to the blockchain. Such communication must take place between nodes, each of which stores a copy of the blockchain and informs other nodes about new events, i.e. the last transaction submitted or recently confirmed. Blockchain users can request information about who has the rights to work in a given node and how the nodes are connected. A node with more links will get information faster. Similarly, nodes may be able to maintain the number of links that are active. A node that restricts the transmission of information or provides inaccurate information must be treated and handled with special care in order to safeguard the integrity of the system. A private blockchain trading e.g. in raw materials may require a more central position in the network in order to develop the network of trading partners. It may also require new nodes to maintain a connection to one of these central nodes as a security measure to ensure that their behaviour is as expected.

Another security problem in the development of network structures is the way in which non-communicative or irregularly active nodes are treated. Nodes may also be excluded for harmless reasons, but the network must be prepared for normal operation - getting consensus in the previously verified transactions and correct verification of new transactions without offline nodes. The network must also be able to restore nodes to working order very quickly if they become active.

Intelligent contracts are one of the most attractive features of the blockchain as they limit or even completely reduce the administrative costs related to the lack of trust in the transaction. Once certain contractual conditions are met, money, property or goods are automatically released, as is the case of commercial arbitration involving a third party, such as a bank, a quality control body or a public trustee.

For example, an insurance company can use intelligent contracts to pay claims for incidents such as hurricanes, droughts or aircraft delays. However, this is questionable, because these contracts are neither intelligent nor are they contracts in the legal sense. They are in fact a form of automation and acceleration of business processes. In order to automate business processes, it is necessary to agree on what the process is to be and what rules are to be enforced in this transaction process, and then precisely write it down in the form of an executable code.

However, the lack of maturity of the scripting language to write the contract representation in the programming language can lead to errors or vulnerabilities in the security features that will not be noticed or handled. Blockchain users must also agree among themselves - as contract terms - what will happen in the case of a dispute while carrying out the contract. If something that is not written in the contract code happens - regardless of if the reason is deliberate or unintentional - a method to fix or to stop the code must then exist.

Creating a new business process as a conscious action also requires the establishment of an agreement on various conditions, including the legal ones. There are cases of blocking blockchain projects because the parties have not reached agreement on all of the conditions under which this activity should be carried out (the transaction contract). In fact, translating transaction terms in various aspects into a formal record in the script language is crucial for the security of such an operation, where the use of blockchain may help, but does not replace the proper analysis and preparation of the project.

Threats

It is assumed that the spread of blockchain technology began with the creation of an online service where drugs could bought. The online auction platform Silk Road, which operated on the TOR network, was closed down in 2013 by US law enforcement authorities. Most of the goods offered by the sellers were illegal. The platform was used for drug trafficking, which took place with the consent and knowledge of its creator. However, it was forbidden to provide items or services that would undoubtedly harm other people, such as child pornography, weapons of mass destruction or stolen credit cards. The Silk Road was a platform where, for the first time, most people had heard about bitcoins and cryptocurrency. After transactions worth over a billion dollars in just over two years, the Silk Road was closed after an FBI investigation. Despite this fact, the technology behind that drug exchange platform (blockchain technology) is now being advertised as the most revolutionary advance since the creation of the Internet.

Special software is necessary to perform analyses of a public blockchain database. It allows you to review the information and then interpret which transactions appear to be suspicious. This is becoming increasingly difficult as users move to anonymous cryptocurrency systems. A recent report by Europol, the European Union police agency, reveals that 'cryptocurrencies such as Monero, Ethereum, and Zcash are gaining popularity in the digital underground'[33]. While offering advanced privacy features, Monero and Zcash hide the sender, the recipient and the value of the transaction, which makes it almost impossible to conduct an investigation. The team

[33] Internet Organised Crime Threat Assessment (IOCTA) 2017, 27 September 2017, p. 11, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>, *accessed* 17.09.2018.

behind Zcash claims that increased privacy does not mean that there is evidence of the system being used for criminal purposes. However, despite the additional security features for privacy, a factor facilitating analysis is the point in time that the criminals try to withdraw or exchange money for dollars or euros, which can be traced in regulated exchanges.

Phishing is a major trend in the activity of criminals in blockchain networks, where criminals usually use a fake e-mail link. Research has shown more than 115 million dollars of stolen value from nearly 17,000 victims in the Ethereum blockchain alone. Cryptophishing targets potential investors, which results in their money being sent to the wrong address as they try to pre-buy alleged tokens in an initial public offering (Initial Coin Offering, ICO), and Twitter often spreads disinformation. Allegations of misinformation are quite common during the life of an ICO offer.

So far, no blockchain-based system has been completely broken. However, the software that is built on this infrastructure has many shortcomings. An example is a venture capital fund, called DAO, which raised more than $150 million in one month in 2016 (then the biggest crowdfunding event in history), and a month later thieves used a flaw in the DAO code to steal more than $74 million from 11,000 investors. Also in 2016, BitFinex lost 120,000 bitcoins worth $68 million due to theft. Reports indicated that Bitfinex was using BitGo's portfolio from a supplier that might have had vulnerabilities in the software.

It is estimated that in total, about 10 per cent of the money invested in the Ethereum-based ICO ended up in the hands of criminals. Despite the theoretically safe blockchain network, this technology is not necessarily fully secure. Taking the value being put into several major blockchains, that is, Bitcoin and Ethereum, into account, the code of this software must be perfect. In spite of the fact that open source software makes it easier to find loopholes, if there is an error in the system software, we could be looking at billions of dollars being stolen, fraudulently taken by hackers, even before people know about it.

Conclusions

Blockchain technology enables individuals to create an exchange network without a physical third party transaction by applying supervision or virtual contractor risk management as a working algorithm created on the basis of trading arrangements. As a result, blockchain networks are generally not trustworthy because they do not require mutual knowledge or trust between the parties in the network. The creation of the blockchain network enables individuals to perform activities that were previously based on institutional control, that is, governmental or similar types of institutions of public trust. The blockchain can replace the supervision of government or of its agencies in areas where entities carrying out transactions of various types recognise the need to regulate joint actions, but they do not trust governments or other institutions. In a low-trust environment, the

blockchain operates a mechanism by which units can cooperate without interference or intervention of supervising or controlling third parties. However, such cases are not limited to developing countries. Many problems in developed countries can be solved by using blockchain to establish voluntary, self-preserving regulatory systems, which is similar for different types of contracts between parties, which are elements of the authority system (central and local), enterprise, or the whole sphere of specialised services.

Blockchain technology essentially replaces the internal trust between people or corporate entities with mathematical rules. Unfortunately, strong security measures require high computing power and become expensive. This costly and slow process is justified for a global network in which all participants can be potentially malicious. In a closed corporate environment, there is no point in devoting energy and time for essentially no additional benefits. When operating in a commercial environment, total transparency is usually not a good solution. For example, if blockchain technology is used as part of a trading platform and as a mechanism for immediate settlement, each blockchain user can view what the other user is doing, which would allow for dishonest behaviour towards each other. In another example, if a manufacturer uses blockchain for its suppliers, it would allow one contractor to immediately observe all other subcontractors in the blockchain, which is not necessarily desirable for reasons of competitiveness and preservation of advantage in various aspects.

References

Publications

Atzei N, Bartoletti M, Cimoli T, A survey of attacks on Ethereum smart contracts SoK, *Principles of Security and Trust* 2017, Vol. 10204.

Beck R *et al.*, Blockchain — The Gateway to Trust — free Cryptographic Transactions, 24th European Conference on Information Systems (ECIS), Istanbul, Turkey, 2016.

Crosby M *et al.*, Blockchain technology: Beyond bitcoin, *Applied Innovation Review* 2016, No. 2.

English M, Auer S, Domingue J, Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development, Computer Science Conference for University of Bonn Students, Bonn, Germany 2016.

Fairfield J, Smart contracts, Bitcoin bots, and consumer protection, *Washington and Lee Law Review Online* 2014, Vol. 71.

Glaser F, Bezzenberger L, Beyond Cryptocurrencies — A Taxonomy of Decentralized Consensus Systems, Proceedings of the 23rd European Conference on Information Systems (ECIS 2015), Muenster, Germany 2015.

Glaser F, Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis, Proceedings of the 50th Hawaii International Conference on System Sciences

(HICSS 2017), Waikoloa Village, Hawaii 2017.
Glaser F *et al.*, Bitcoin–asset or currency? Revealing users' hidden intentions, Proceedings of the 22nd European Conference on Information Systems (ECIS 2014), Tel Aviv 2014.
Konstantinidis I *et al.*, Blockchain for Business Applications: A Systematic Literature Review, International Conference on Business Information Systems, Springer Cham 2018.
Kosba A *et al.*, Hawk: The blockchain model of cryptography and privacy-preserving smart contracts, 2016 IEEE symposium on security and privacy (SP), Vol. 1.
Luther WJ, White LH, Can bitcoin become a major currency?, *Working Paper in Economics* 2014, No. 14–17.
Mishkin FS, The economics of money and financial markets, Boston 2004.
Swan M, *Blockchain. Blueprint for a New Economy*, Sebastopol 2015.
Szabo N, *Smart contracts: formalizing and securing relationships on public networks*, "First Monday" 1997, Vol. 2, No. 9.
Weber I *et al.*, *Untrusted Business Process Monitoring and Execution Using Blockchain*, Springer, Cham 2016.

Other sources

Atzori M, Blockchain technology and decentralized governance: Is the state still necessary?, <https://ssrn.com/abstract=2709713>, 21 October 2019 r.
Buterin V, A next-generation smart contract and decentralized application platform, <http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf>, 21 October 2019 r.
Crowhurst L, Reforming justice for the digital age The Police Foundation, in partnership with CGI, July 2017, <http://www.police-foundation.org.uk/2017/wp-content/uploads/2017/08/pf_cgi_digital_justice.pdf>, 17 September 2018 r.
European Central Bank, Virtual Currency Schemes, 2012, <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyscheme s201210en.pdf>, 30 November 2016 r.
Federal Bureau of Investigation, Bitcoin virtual currency: intelligence unique features present distinct challenges for deterring illicit activity, 2012, <https://www.wired.com/images_blogs/threatlevel/2012/05/Bitcoin-FBI.pdf>, 30 November 2016 r.
Internet Organised Crime Threat Assessment (IOCTA) 2017, 27 September 2017, <https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017>, 17 September 2018 r.
Mattila J, The Blockchain Phenomenon — The Disruptive Potential of Distributed Consensus Architectures, The Research Institute of the Finnish Economy, 2016, <https://ideas.repec.org/p/rif/wpaper/38.html>, 21 October 2019 r.

Nakamoto S, Bitcoin: A Peer-to-peer Electronic Cash System, 2008, <https:// bitcoin.org/bitcoin.pdf>, 17 September 2018 r.
Sachs G, Profiles in Innovation — Blockchain, <http:// www.the-blockchain.com/docs/Goldman-Sachs-report-Blockchain-Putting-Theory-into-Practice.pdf>, 30 November 2016 r.
Yli-Huumo J *et al.*, Where Is Current Research on Blockchain Technology? A Systematic Review, *PloS one* 2016, No. 11, Vol. 10, <https://doi.org/10.1371/journal.pone.0163477>, 21 October 2019 r.

DOI: 10.5604/01.3001.0014.1135
http://dx.doi.org/10.5604/01.3001.0014.1135

Keywords: blockchain, smart contract, security, innovation, cryptocurrency, Bitcoin, Ethereum, proof-of-work

Summary: Blockchain is one of the most revolutionary technologies of the 21st century, which is still under development, and whose potential is not yet fully exploited. Although blockchain gained importance in 2009, scientists and entrepreneurs are still at an early stage of understanding its mechanisms and fully appreciating its potential, especially from the perspective of the technical challenges and limitations of the technology. Blockchain finds a variety of applications, especially in areas that have so far been based on third-party transactions in order to maintain a certain level of trust. Although blockchain is a promising technology for the reorganisation of business processes and many industrial applications, it still has many weaknesses despite various implementations in many forms. An innovative element, and one of the most attractive functions, of blockchain is intelligent contracts, as they reduce or even completely eliminate the administrative costs associated with the lack of trust in the transaction. However, the existing software that is built on this infrastructure has many shortcomings and unfortunately, combined with the lack of maturity of the scripting language to write the contract representation in the computer language, leads to errors or gaps in security that are not noticed or addressed by the author of the script. So far, no blockchain-based system has been completely broken. Nevertheless, phishing is the main trend in the operation of criminals in blockchain networks. Research has shown that over $115 million has been stolen from nearly 17,000 victims in the Ethereum blockchain alone. It is estimated that in total about 10% of the money invested in Ethereum's ICO has ended up in the hands of criminals.