Enhancing the Usefulness of Blockchain Technology in Finance Sector

Vedran Juričić
Faculty of Humanities and Social Sciences, University of Zagreb, Croatia
Matea Radošević
Faculty of Humanities and Social Sciences, University of Zagreb, Croatia
Ena Fuzul
Faculty of Humanities and Social Sciences, University of Zagreb, Croatia

Abstract

Blockchain technology has become widely popular with the appearance of cryptocurrencies that use the decentralized nature of blockchain in order to exchange funds between their users. In order to verify various needed details during an exchange, consensus mechanisms are used which solve simple but exhaustive calculations. Such operations fulfil their primary goal of verifying, but are a common target of public disapproval due to massive energy consumption and lack of usefulness. This work discusses different approaches and consensus mechanisms with a more useful secondary function, especially focusing on NP-complete problems as mediators in solving complex and resource-heavy problems. A new way of approaching these problems can benefit many areas, like science, healthcare, government and finance, optimizing the current infrastructure and business processes like markets, transactions, insurances, payments and supply chains, or creating more secure, reliable and efficient environment.

Keywords: blockchain, proof of work, optimization, problem solving
JEL classification: C61

Introduction

Blockchain technology has gained great public interest over the last few years. The new technology has emerged as a leading alternative to traditional billing and payment systems. In the field of finance, cryptocurrencies have enabled an almost revolutionary system and started a new age of digital payment. Technology has attracted and encouraged non-technical, wider audience, creating a new system that could potentially solve many problems. Blockchain technology has gained popularity with the range of advantages it offers in relation to the existing systems. The background logic inside blockchain offers a promising and just access, or a trusted system, which is why technology has gained a lot of attention, especially in the world of finance.

Blockchain works on the principle of equality and justice. All users participating within the network participate in decision making and its maintenance. User data is anonymous and protected against unauthorized use because there is no central system or central unit that privatizes, controls, charges or affects the system in any way. Because of this, blockchain, in its function and distribution, is called a decentralized system. By eliminating the central unit from the system, the network nodes involved in making decisions about further behaviour of blockchain make the

system completely dependent on its users, but also, they are making it secure, due to its different and fairer approach.

Security, transparency and efficiency are some of the reasons the blockchain technology has found its wide usage in finance sector. It has increased efficiency because only there exists only "single version of truth", that is, only one history of data. It has also increased customer experience due to faster processing and reduced loss and fraud because records and immutable and visible to all participants. Technology has changed or optimized business processes, decentralized point of sales systems, smart bonds, cross-border transactions, hedge funds, trading platforms, etc.

Above examples show that although cryptocurrency is currently the most popular and best-known implementation of blockchain technology, it is applicable to a much wider range of issues. Currently, the most popular systems are blockchain cryptocurrency technologies, especially Bitcoin and Ethereum (CoinMarketCap, 2019), which maintain the network under the same consensus. Specific consensus has proven to be the highest-quality and most secure form of network maintenance, with an incentive award for its users. This form of profit attracted a large number of users, creating the whole mining industry, but also causing massive energy consumption required to maintain the network. The consensus mechanism within the above-mentioned cryptocurrency refers to the users guessing solutions to the set up mathematical problem, which also maintains the network itself. The mathematical problem offered within this consensus does not bring the value out of the system, but so far, no adequate or satisfactory alternative has been found. If blockchain technology could adapt in a way that users solve math, science, finance or any other useful problems that require massive computing power, the contribution of new technology will become even bigger and would solve many issues.

The aim of this paper is to explore the current state of blockchain technology development and its application and adaptation to further help solving different problems in finance. Blockchain systems are based on extremely large computing power, which could be used to address nowadays almost unsolvable problems in different areas, but also to participate in financial analysis involving large amounts of data that need to be processed. The research focuses on the ability to change one of the fundamental functionalities of this technology in order to help solving problems from the NP-complete class, including route inspection problem, graph intersection number, bin packing problem, bottleneck traveling salesman etc.

Blockchain technology

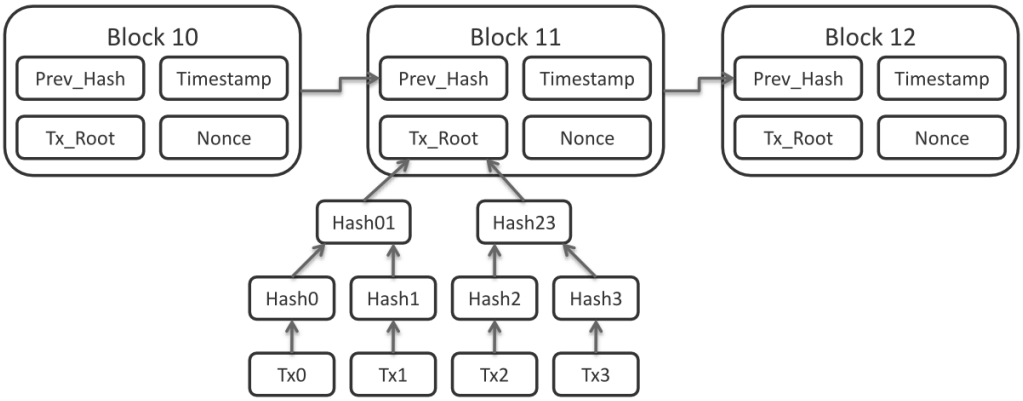
Blockchain technology is based on the principle of connected blocks that contain information about transactions within the network and special cryptographic functions by which they are interconnected to create a continuous array of chained blocks.

It is generally described as a distributed database maintained by all users in a network. A database contains all the transactions and is available to each individual user. When database changes, it is resent and updated throughout the network so that anyone can see the last state. It serves as a public, unprivatized source of all data within the system. Once stored in the database, data cannot be changed due to cryptographic methods involved in the process of creating new blocks. Because of this inability to modify stored data, blockchain technology is considered to be an extremely reliable source of data and a secure tool for transaction and asset sharing. Users are network nodes that are connected to a peer-to-peer network that connects them all at the same level without a hierarchy. Data is distributed by certain

cryptographic protocols to all nodes in the network and all nodes come to a mutual consensus that defines when and how the data will become part of the database.

Blockchain technology is based on blocks that contain information about transactions. Also, each block contains information that differentiate it from other blocks, and place it in an exact time and position within the chain of blocks. As shown in Figure 1, current block (11) contains information about the previous block (10), while future block (12) will contain information about block 11, which creates a chain that can be traced to the initial, generic block.

Figure 1
A Conceptual Diagram of the Bitcoin Blockchain



Source: Jones, 2017

Transactions are performed through asymmetric encryption using only public keys that serve as publicly available, personal user addresses. In this way, network users remain anonymous as the address itself does not reveal the user's identity, but the data integrity is preserved with respect to the nature of asymmetric encryption. After agreeing on both sides, the transaction is entered into the block. Special users, called miners, group the received transactions into a block. A binary hash tree algorithm is then performed, within which each transaction is encrypted with the hash function. Hash functions have an important role in cryptographic methods within blockchain because they ensure data authenticity and trustworthiness and protect against changes. Apart from the transactions themselves, the block also contains the so-called *nonce*, which presents the value of the solution for the mathematical task obtained, the information on the previous block, the difficulty target, the date and time mark etc. In order to continue the sequence, the next block records the hash value calculated over the data from the previous block. Through this method it is very easy for other users to check the order of blocks in a chain and to detect fake and false blocks. If the block's hash value does not show the same values that are entered in adjacent blocks, the block is false.

Proof of work

The block can be successfully added to the main blockchain only when it is processed by the network miners and then verified by other nodes in the network. Such a procedure is called a *proof of work* consensus. In the blockchain network, users are divided into multiple profiles. Most users have not downloaded all the data from the initial block, but only their headers that contain enough information to validate new

and past Transactions. Network miners are users that contribute to functionality, creating new blocks. The process of creating blocks is called mining. Block mining is a relatively long process that requires a lot of computing power and special hardware equipment, while validation of newly-created blocks takes little time for ease of calculating the mathematical operation. After creating the block and distributing it to the other nodes in the network, consensus needs to be achieved to allow the block to be included in the chain.

Block can become a part of a chain only when one of the miners solve a task, that is, when he finds a value that satisfies a predefined condition. A header of each block contains weight value *t*, which defines the difficulty of mining a block. The miner uses a trial and error method to discover a *nonce* value *n*, that in combination with a block value *b* satisfies a condition defined with *t*. This value is actually a number with a value within range from 0 to 2^{256} (Bowden et al., 2018) and the mining problem is to find a value smaller than the given weight value *t*, that is H(b, n) < t.

H function is SHA-256 hash operation, cryptographic mathematical function that was chosen from Satoshio Nakamoto in implementation of the first cryptocurrency Bitcoin. It ensures authenticity and validity of data, and meets a number of criteria that ensure the quality of encryption and prevention from collision and double spending problem (Nakamoto, 2008). Because of its unidirectional characteristic, the output of a hash function is really easy to calculate, but it is almost impossible to find an input value for a given output value. Each nonce has equal guess probability and the only method that can be used is brute force.

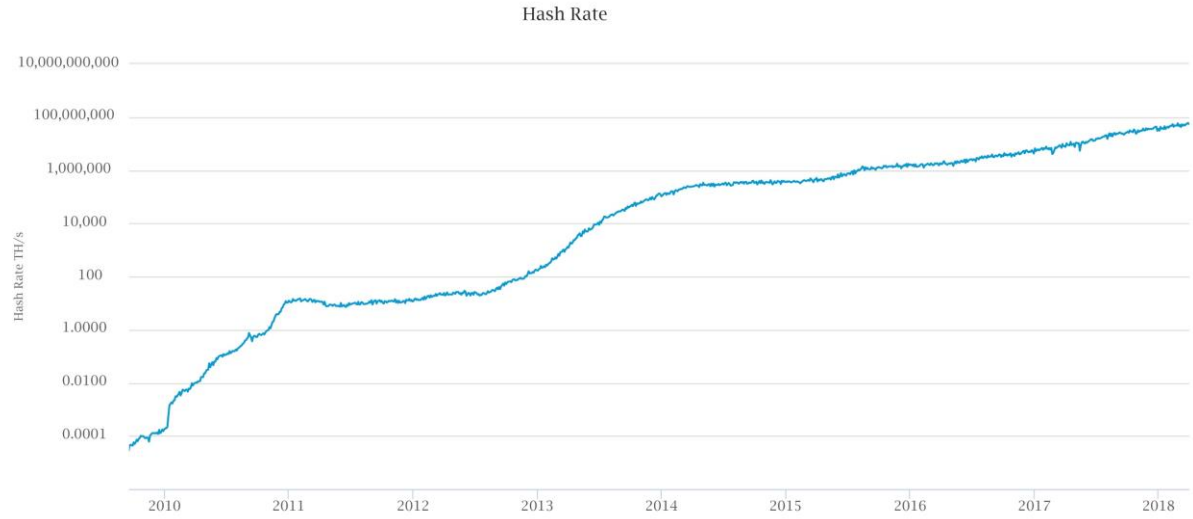
The miners begin to generate nonce from zero, incrementing it in each step until a new hash values satisfies the defined condition, i.e. until the value below the required number is found. Nonce is a 32-bit number, so a number of possible iterations is 2^{32}, meaning that a solution to the problem need up to 4.3 billion attempts. The weight value within a network is not always the same, but the network changes it, adjusting the weight of the solution, so that each block takes approximately 10 minutes of mining time.

Computing power

The miners are competing in the speed of finding a satisfying nonce because the first miner that solves a problem gets a prize. The current reward for the new block is 12.5 Bitcoins or about 69 000 US dollars (BitInfoCharts, 2019). Blockchain technology in this way motivates its users to validate transactions and to maintain the network.

Since the growing popularity of cryptocurrencies, mining has become a certain type of industry. Earnings through mining, as one of the motivational factors for using cryptocurrency, resulted in a massive number of users and a massive computing power. At the very beginnings of Bitcoin, the use of the Hashcash (Back, 2002) algorithm could be run on standard equipment on home computers, but today it is necessary to invest large amounts of money in a computer equipment so that the user can compete with the rest of the network in order to be the first to solve a problem and to receive a reward.

Figure 2
Estimated Number of Terahashes Per Second in the Bitcoin Network (Logarithmic Scale)



Source: Blockchain, N/A

The number of miners has increased over the years and so the total computer power has also increased. The graph in Figure 2 shows the growth of calculated hashes in one second. Although short downtrends exist, the overall power of the network is growing, and it is clear that a network like Bitcoin represents an enormous source of power. Today's 500 most powerful supercomputers in the world together have a processor power of about six to eight times smaller than the mining processor's power (Santos, 2019). The estimated value of processor power goes above exaflops, which is about 10^{18} floating-point operations per second. The fastest computers in the world are currently working on petaflops. IBM Summit has 143 petaflops, Sunway ThaiuLight 93, and IBM Sequoia 17 (Top500, 2018), which shows that the most powerful supercomputers match 1-15% of the total Bitcoin power.

Application of blockchain technology

Cryptocurrencies like Bitcoin are the most famous applications of blockchain. There are services similar to currencies that can be based on blockchain, like securities transactions, loyalty point services, prepaid cards, gift card exchange and electronic coupons (NRI, 2015). But because of its architecture and implementation, blockchain has numerous benefits such as anonymity, persistency and decentralization and can be applied in different fields and problems (Zheng, 2018).

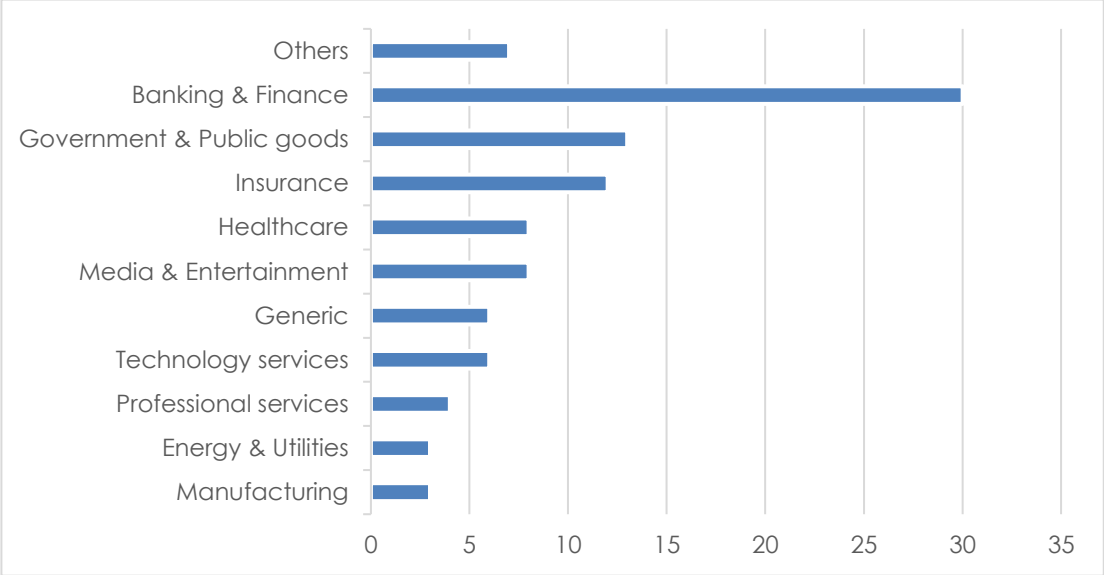
One of those fields is Internet of things (IoT), a global network that connects smart objects with an advanced Internet technology, in order to provide users with various services (Miorandi et al., 2012). An example of those services are systems like smart cities, smart environment, smart water, home automation, logistics etc. Blockchain could provide safe mean of communication between smart objects, keep an immutable history of smart objects or enable their autonomous work by removing the requirement of a centralized authority or human control (Panarello et al., 2018).

Blockchain can also be used in public and social services, for example in land registration (NRI, 2015) in which the land information like status and rights can be registered and publicised on blockchains, but also enable more efficient services when transferring a land or establishing a mortgage. Another example is voting, where

the vote data is securely stored in a blockchain and is publicly verifiable and distributed in a way that no one can corrupt it (Ayed, 2017).

Blockchain technology has also found applications in the field of education. Students would have independence and anonymity of their personal data, independence of institution and immutability of records of official documents. It also offers a different approach in paying tuition, more customized and online studies, and a way to extend students' profiles, benefiting universities, students and employers (Grech et al., 2017; Juričić et al., 2019).

Figure 3
Blockchain Technology Usage Per Sector



Source: Hileman & Rauchs, 2017

Apart from that, blockchain has found its usage in medicine, sharing services, supply chain and digital asset management, data storage, authentication, communication, transportation, crowdfunding, visualization, legal services etc. Figure 3 shows its usage in different sectors, pointing out that banking and finance sector is the most represented one, with about 30%.

The main reasons for using blockchain technology in this sector are: efficiency, security and lower costs (Blockchain Technologies, 2019). The business is more efficient, because technology enables faster global trade across time zones, offering effective protocol to deal with cross border transactions (Fanning & Centers, 2016). The costs of smart contract-based transactions are minimal because there are no domestic or international wire fees or overdrafts. Smart contract is a transaction protocol that executes the terms of a contract (Tapscott et al., 2018). Blockchain in the finance sector can have benefits to: cross-border transactions, smart bonds, point of sales systems, lending and borrowing, trading platforms, clearing and settlements, bookkeeping and auditing, hedge funds, digital identity verification, credit reports etc. (Blockchain Technologies, 2019).

Improvements of blockchain technology

Applications listed in the previous chapter are the common ones and typically discussed in science papers, technical reports and literature. They are using an existing blockchain implementation using its common consensus protocols. Those protocols

are, with the blockchain's increasing computing power, the reason the blockchain technology is being criticized. Proof of work consensus is the most widely used protocol and is present in most of the leading cryptocurrencies, and currently the consensus that consumes the greatest amounts of power, energy and computer resources. The reason for the critique is found in the Hashcash algorithm whose goal is to find a random number that satisfies the given condition and has no greater function outside the network. For this reason, it is often characterized as an algorithm without a larger purpose or benefit, meaning there is no useful use of computed hashes that in any way improve or assist other than maintaining the network itself. The Hashcash algorithm was initially ideal, whose implementation provided a network without central authority, prevented double spending and achieved system integrity. Today, with the growing popularity and strength spent on blocking blocks, it is evident that such a system can bring much more useful solutions and can be utilized for more complex, necessary and more realistic problems.

A good example of such a problem is folding@home project (Beberg et al., 2009). Folding@home is a Stanford University project that uses a public distributed computer system in simulation of biomedical processes, such as stacking of proteins, that help science in researching various diseases. The volunteers that are included in this network share their computer resources in detailed statistical calculations.

A similar example is the SETI@home project, implemented by the SETI Institute in the United States (Anderson et al., 2002), which aims to research extra-terrestrial life. SETI@home is also a project built on a distributed network of volunteers sharing their computer resources in processing narrowband radio signals from the universe, collected by radio telescopes. SETI@home is just one of these projects in the field of astrophysics research (Newberg et al., 2013; Knispel et al., 2010). and folding@home, only one in the field of complex tasks whose processing needs more than average supercomputers and which can potentially be solved through distributed computing.

Through the theoretical insight into the background and the performance of blockchain technology, it is apparent that each problem does not correspond to a suitable substitution within the proof of work consensus. In order for the system to maintain self-sustainability and decentralization, it is necessary to propose a solution that will fulfil the same functions within the system as the Hashcash algorithm and will not in any way compromise network security. By analysing the current research and realized cryptocurrencies, the criteria of the problem were adopted. For blockchain systems based on a standard proof of work consensus, an appropriate replacement of the Hashchash method must meet the following conditions (Chatterjee et al., 2019; Ball et al., 2017):

- Checking solutions for problems should be significantly easier than the problem solving itself
- The solution or problem must have certain characteristics to determine that the miner has solved the problem
- The mining process must protect transaction and security of the whole network
- The difficulty of the set problems must be adjustable
- The problem should not have an input string.

As an appropriate alternative to Hashcash, NP problems from the computational complexity theory can be used (Oliver et al., 2017; Ball et al., 2017). NP problems are a set of problems for which a polynomial solution algorithm is not known but confirmation of their solution is reachable in polynomial time. P is another class of problem whose solution can be reached by a deterministic Turing machine in polynomial time and therefore not suitable as an appropriate replacement. NP problems meet the first requirement of checking the solution in relatively fast time,

enabling blockchain users to quickly and easily validate the solution. Due to unknown methods of solving problems in polynomial time, NP problems make the task of miners much more difficult.

A specially categorized problem category are NP-complete problems (Garey & Johnson, 2002), which are a subset of NP class problems. According to Cooker's theorem (Cook, 1971) there are two NP-complete criteria and we can say that the problem X is NP-complete if it satisfies the following two conditions: X is an element of NP and X is NP-hard. The first criterion indicates that problem X belongs to the NP class problems, that is, that every solution obtained can be verified in a polynomial time. The second criterion means that problem X must also be NP-hard, that is, that NP problem Y can be reduced in polynomial time to problem X.

Dunne (2008) created a list of more than 80 NP-complete problems that can be used as a substitute for the current consensus algorithm. There are numerous problems from mathematics like numeric, graph and hypergraph problems, from computing and programming, formal languages, string processing etc. Some of these problems are optimization problems and can be applied in various fields like biology, computing, astronomy and finance (Anastassiou, 2011), including traveling salesman problem, job scheduling problem, knapsack problem and longest path problem.

The traveling salesman problem assumes a list of cities and distances between them, and searches for the shortest possible route that visits each city and returns to the origin city. Some generalizations of this problem are travelling purchaser problem, that introduces a list of available goods, and vehicle routing problem, that introduces a list of customer orders. Job scheduling problem assumes a list of jobs with different processing times and a list of machines with different processing power. Problem is to find a schedule that represents a minimum processing time. Knapsack problem assumes a set of items with different weight and value, and the problem is to determine the number of each item so that the collection has the maximum value and the total weight is less or equal to the predefined limit. The longest path problem is the problem of finding a simple path of maximum length in a given graph.

Conclusion

Different implementations of blockchain technology today gains great popularity due to its non-traditional and decentralized model, which offers a range of features and different applications. The first example of the system on blockchain technology is the form of a digital currency called Bitcoin, now known as the leading cryptocurrency. Despite many advantages, one of the bigger objections remains the Hashcash algorithm whose random guessing to the correct hash value consumes enormous amounts of power, energy, and time. This paper shows an insight to other, non-standard usages of blockchain technology, where computing power is spent usefully, on solving problems in science and technology. By replacing the original Hashcash algorithm, system based on blockchain technology can help solving problems from the NP-complete class of problems, which can be then applied in different fields, like medicine, biology and finance.

References

1. Anastassiou, G. A. (2011), Handbook of computational and numerical methods in finance, Springer Science & Business Media.
2. Anderson, D. P., Cobb, J., Korpela, E. J., Lebofsky, M., Werthimer, D. (2002), "SETI@home: An Experiment in Public-Resource Computing", Communications of the ACM, Vol. 45, No. 11, pp. 56-61.

3. Ayed, A. B. (2017), "A conceptual secure blockchain-based electronic voting system", International Journal of Network Security & Its Applications, Vol. 9, No. 3, pp. 1-9.
4. Back, A. (2002), "Hashcash-a denial of service counter-measure", Tech Report paper, Hashcash.
5. Ball, M., Rosen, A., Sabin, M., Nalini Vasudevan, P. (2017), "Proofs of Useful Work", IACR Cryptology ePrint Archive.
6. Beberg, L. A., Ensign, D., Jayachandran, G., Khaliq, S., Pande, S. V. (2009), "Folding@home: Lessons from eight years of volunteer distributed computing", in the Proceedings of the 23rd IEEE International Symposium on Parallel and Distributed Processing, Rome, Italy, IEEE, pp. 1-8.
7. BitInfoCharts (2019), "Bitcoin (BTC) price stats and information", available at: https://bitinfocharts.com/bitcoin/ (2 July 2019).
8. Blockchain (N/A), "Hash Rate", available at: https://www.blockchain.com/charts/hash-rate?timespan=all&scale=1 (30 June 2019).
9. Blockchain Technologies (2019), "Blockchain Financial Services Applications Explained", available at: https://www.blockchaintechnologies.com/applications/financial-services/ (5 July 2019).
10. Bowden, R., Keeler, H., Krzesinski, A., Taylor, P. (2018), "Block arrivals in the Bitcoin blockchain", CoRR.
11. Chatterjee, K., Goharshady, A., Pourdamghani, A. (2019), "Hybrid Mining: Exploiting Blockchain's Computational Power for Distributed Problem Solving", in the Proceedings of the 34th ACM Symposium on Applied Computing (SAC), Limassol, Cyprus, ACM, pp. 374-381.
12. CoinMarketCap (2019), "Cryptocurrency Market Capitalizations", available at: https://coinmarketcap.com (1 July 2019).
13. Cook, S. (1971), "The complexity of theorem proving procedures", in the Proceedings of the Third Annual ACM Symposium on Theory of Computing, Shaker Heights, Ohio, USA, ACM, pp. 151-158.
14. Dunne, P. E. (2008), "An annotated list of selected NP-complete problems", COMP202, Department of Computer Science, University of Liverpool.
15. Fanning, K., Centers, D. P. (2016), "Blockchain and its coming impact on financial services", Journal of Corporate Accounting & Finance, Vol. 27, No. 5, pp. 53-57.
16. Garey, M. R., Johnson, D. S. (2002), "Computers and intractability", Vol. 29, wh freeman, New York.
17. Grech, A., Camilleri, A. F. (2017), "Blockchain in education", Publications Office of the European Union, Luxembourg, No. 132.
18. Hileman, G., Rauchs, M. (2017), Global blockchain benchmarking study, Cambridge Centre for Alternative Finance, University of Cambridge.
19. Jones, S. (2017), "Trusted Timestamping of Mementos", available at: https://ws-dl.blogspot.com/2017/04/2017-04-20-trusted-timestamping-of.html (1 July 2019).
20. Juričić, V., Radošević, M., Fuzul, E. (2019), "Creating student's profile using blockchain technology", in the Proceedings of the MIPRO 2019 42nd international convention on information and communication technology, electronics and microelectronics, Opatija, Croatia, IEEE.
21. Knispel, B., Allen, B., Cordes, J. M., Deneva, J. S., Anderson, D., Aulbert, C., Bhat, N. D. R., Bock, O., Bogdanov, S., Brazier, A., Camilo, F. (2010), "Pulsar Discovery by Global Volunteer Computing", Science., Vol. 329, No. 5997, p. 1305.
22. Miorandi, D., Sicari, S., De Pellegrini, F., Chlamtac, I. (2012), "Internet of things: Vision, applications and research challenges", Ad hoc networks, Vol. 10, No. 7, pp. 1497-1516.
23. Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system".
24. Newberg, H.J., Newby, M., Desell, T., Magdon-Ismail, M., Szymanski, B., Varela, C. (2013), "MilkyWay@home: Harnessing volunteer computers to constrain dark matter in the Milky Way", in the Proceedings of the International Astronomical Union, Vol. 9, No. s298, pp. 98-104.

25. NRI (2015), "Survey on Blockchain Technologies and Related Services", Technical Report.
26. Oliver, C. G., Ricottone, A., Philippopoulos, P. (2017), "Proposal for a fully decentralized blockchain and proof-of-work algorithm for solving NP-complete problems", CoRR.
27. Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A. (2018), "Blockchain and IoT integration: A systematic survey", Sensors, Vol. 18, No. 8.
28. Santos, M. (2019), "Not even the top 500 supercomputers combined are more powerful than the Bitcoin network", available at: https://99bitcoins.com/not-even-the-top-500-supercomputers-combined-are-more-powerful-than-the-bitcoin-network/ (30 June 2019).
29. Tapscott, D., Tapscott, A. (2018), Blockchain revolution: how the technology behind bitcoin and other cryptocurrencies is changing the world, Portfolio.
30. Top500 (2018), "Top 500 list", available at: https://www.top500.org/lists/2018/11/ (1 June 2019).
31. Zheng, Z., Xie, S., Dai, H. N., Chen, X., Wang, H. (2018), "Blockchain challenges and opportunities: A survey", International Journal of Web and Grid Services, Vol. 14, No. 4, pp. 352-375.

About the authors

Vedran Juričić, PhD, is an Assistant Professor at the Department of Information and Communication science, Faculty of Humanities and Social Sciences, University of Zagreb. He has master's degree in Computer Science that he received at Faculty of Electrical Engineering and Computing, University of Zagreb. He received PhD in Information systems and Informatology at the Faculty of Humanities and Social Sciences Zagreb with the dissertation thesis "Plagiarism detection in the multilanguage environment". His fields of interests are security, plagiarism detection, text similarity and web, Windows and mobile development. He published several scientific papers in international and national journals and participated in many scientific international conferences in the field of information and communication sciences. The author can be contacted at **vedran.juricic@ffzg.hr**.

Matea Radošević is an assistant at the Department of Information and Communication science, Faculty of Humanities and Social Sciences, University of Zagreb. She has master's degree in Mathematics and Computer Science Education that she received at Faculty of Science, University of Zagreb. She is currently enrolled in the Postgraduate doctoral study of Information and Communication Sciences and working on her doctoral thesis. Her fields of interest include application of information technology in education and blockchain technologies. The author can be contacted at **matea.radosevic@ffzg.hr**.

Ena Fuzul is a student enrolled in the master's degree programme at the Faculty of Humanities and Social Sciences, Department of Information and Communications Sciences, and in the bachelor's degree programme at the Zagreb Polytechnic. Her primary field of interest is blockchain technology in education. Her other interests include cryptography, e-learning, networks and big data. She attended numerous workshops and summer programmes, some of them being Big Data at the National University of Science and Technology in Moscow, and Advanced Optimisation Algorithms at the Gdansk University of Technology in Poland. The author can be contacted at **efuzul@ffzg.hr**.