sciendo

Optimizing the Resource Consumption of Blockchain Technology in Business Systems

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

Abstract

Background: Blockchain technology has gained a great public interest due to the appearance of cryptocurrencies, a digital asset used for exchanging funds. Although blockchain calculations offer the benefits of security and reduced costs, blockchain is still strongly criticised for its lack of usefulness and resource-heavy consumption. **Objectives:** The aim of this research is to provide different insights into blockchain technology and to propose NP-complete problems as a suitable alternative to the current consensus algorithm. **Methods/approach:** This research discusses the current state of proposed alternatives, projects such as distributed volunteering for scientific purposes and different consensus algorithms within cryptocurrencies but focusing on incorporating NP-complete problems as a secondary, more useful option. **Results:** Using the properties of NP-complete problems, it is possible to solve various problems in different areas, such as science, biology, medicine and finance, but also to improve business processes, optimize markets, payments and supply chains while decreasing environmental costs. **Conclusions:** This paper shows that the alternative mechanisms are being developed and used to substitute an existing Blockchain algorithm with a more efficient one. It also suggests further investigation in this area because the alternatives greatly improve blockchain's usability and efficiency.

Keywords: blockchain, proof of work, optimization, problem-solving, NP-complete problems
JEL classification: C61
Paper type: Research article

Received: Dec 15, 2019
Accepted: Apr 19, 2020

Citation: Juricic, V., Radosevic, M., Fuzul, E., (2020), "Optimizing the Resource Consumption of Blockchain Technology in Business Systems", Business Systems Research, Vol 11 No 3, pp. 78-92.
DOI: https://doi.org/10.2478/bsrj-2020-0028

Introduction

Blockchain technology became one of the most emerging and disruptive technologies in the last decade (Marrara et al., 2019; Hongdao et al., 2019; Leible et al., 2019). Its unique, robust and secure approach along with other advantages has attracted attention from a wider, non-technical audience, creating a system that could potentially solve many problems. With its far-reaching potential, it has extended its capabilities beyond the original intention and affected many different areas.

Initially developed as a system of digital payment in 2008, blockchain found its way to improve many traditional solutions.

Typically described as a distributed ledger of records (Lavanya, 2018) linked through a chain of blocks, blockchain is a decentralised system where a community maintains the whole network and where users are responsible for the system's sustainability. All users within the network are equal and mutually participate in decision making, therefore there is no central unit or any form of authority which can control or influence the system. This made Blockchain technology almost revolutionary in some fields, especially in the world of banking and finance. The lack of authority presented in blockchain has created plenty of possibilities and ideas for the improvement of existing systems, leading with cryptocurrencies as a potential replacement of the traditional payment and billing systems. Unlike the existing payment systems, the blockchain system is trustless (Wood & Steiner, 2016) so users can rely on underlying logic in making fair and secure access. This is due to its infrastructure and cryptographic algorithms involved in the process of creating new blocks. All data once recorded within the block is permanently stored, secured and immutable. Blockchain has also reduced the costs of transaction fees, offered anonymity to its users and provided better efficiency in exchanging funds.

The most popular cryptocurrency of today, with a market capitalization of 128 billion dollars and more than 40 million users in the world is Bitcoin (CoinMarketCap, 2019). Bitcoin facilitates transaction payments and it is the first attempt of cryptocurrency to do so. It uses a specific consensus algorithm which is built into the network and ensures that all payments are resolved, tamper-proofed and recorded within blocks. To achieve this, Bitcoin rewards its most efficient users for participating in validating transactions and maintaining the network. This form of profit creates a powerful incentive and attracts large numbers of users.

Consensus used in Bitcoin keeps the network secure and safe from most network attacks but it is also very resource consuming. Miners have to prove their work by doing an enormous amount of calculations, which require specialised hardware equipment, and vast amounts of electricity. These calculations are used only to maintain the network and validate transactions and do not add value to the system but so far, no adequate alternative has been found.

This paper aims to explore the current state of blockchain technology development, alternatives for future improvements and potential adaptation in helping to solve different problems in business systems. The research focuses on the ability to redirect blockchain computing power into a more useful manner and improving one of its fundamental functionalities to solve meaningful problems. This paper is organized as follows. The second section describes the blockchain technology and its operating principles, focusing on the consensus algorithm. It also gives an insight into computing power and resources used to maintain the blockchain network. The third section describes the potential of using blockchain technology in different fields. Fourth and fifth sections are introducing the NP-complete problems as a suitable alternative to current consensus algorithm. Finally, the last section presents our conclusions.

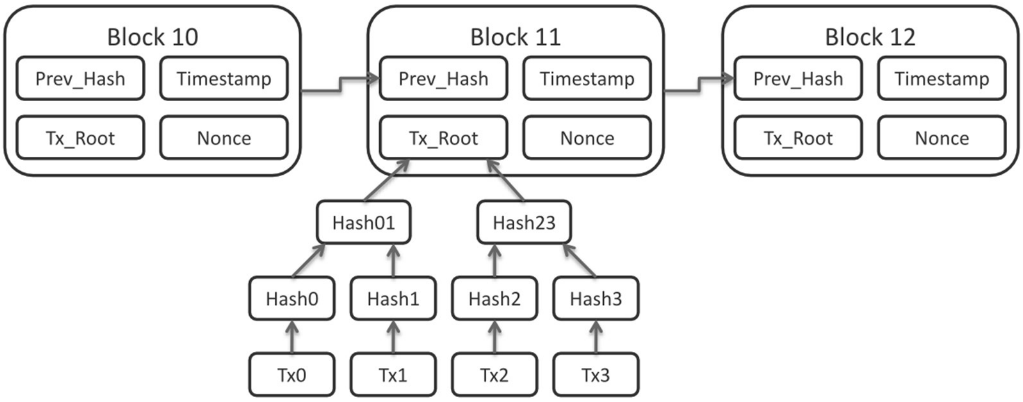
Blockchain technology

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 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, non-privatized 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. In addition, each block contains information that differentiates 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 concerning 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. 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

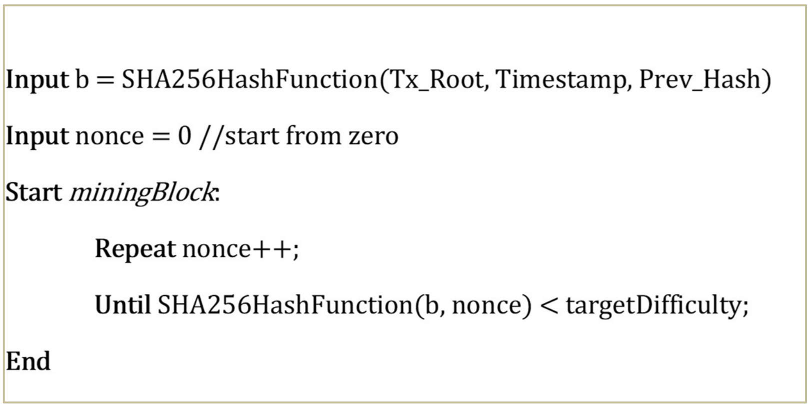
The block can be successfully added to the main blockchain only when it is processed by the network miners and then verified by other nodes in the network. Such a process is called a *proof of work* consensus. In the blockchain network, users are divided into multiple profiles. Most users have not downloaded 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 a number with a value within a 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 $H(b, n) < t$.

Figure 2 shows the simplified version of the operating principles of consensus.

Figure 2
A Simplified Pseudocode of the Proof of Work



```
Input b = SHA256HashFunction(Tx_Root, Timestamp, Prev_Hash)
Input nonce = 0 //start from zero
Start miningBlock:
    Repeat nonce++;
    Until SHA256HashFunction(b, nonce) < targetDifficulty;
End
```

Source: Author's illustration

H function is SHA-256 hash operation, a cryptographic mathematical function that was chosen from Satoshi Nakamoto in implementation of the first cryptocurrency Bitcoin. It ensures authenticity and validity of data and meets several criteria that ensure the quality of encryption and prevention from the collision and double spending problem (Nakamoto, 2008). Because of its unidirectional characteristic, the output of a hash function is 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.

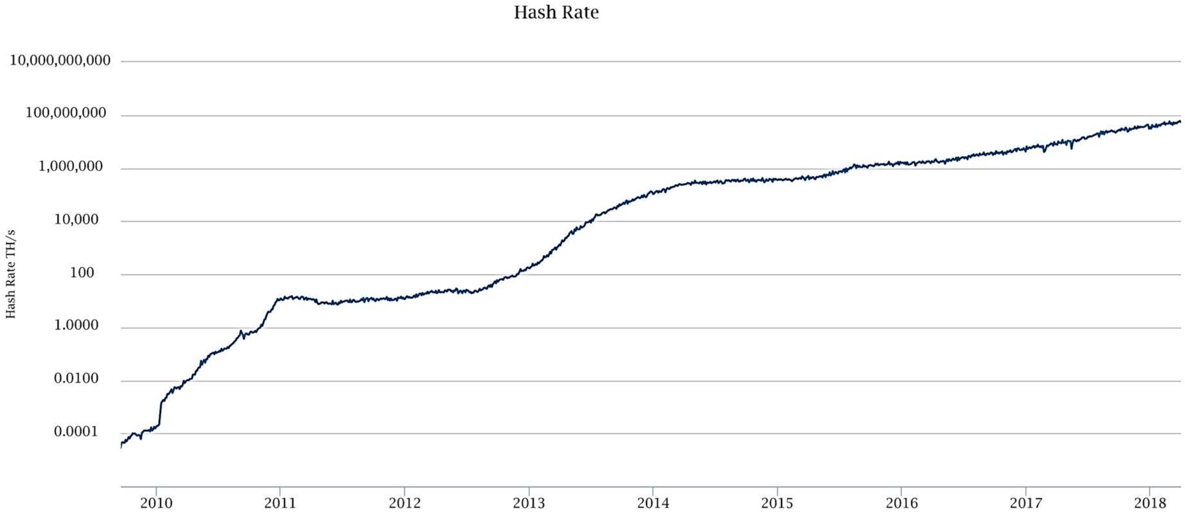
The miners begin to generate nonce from zero, incrementing it in each step until a new hash value satisfies the defined condition, i.e. until the value below the required number is found. Nonce is a 32-bit number, so several possible iterations is 2^{32}, meaning that a solution to the problem needs 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 computer equipment so that the user can compete with the rest of the network to be the first to solve a problem and to receive a reward.

Figure 3
Estimated Number of Terahashes per second in the Bitcoin Network (logarithmic scale)



Source: Smith et al. (2019b)

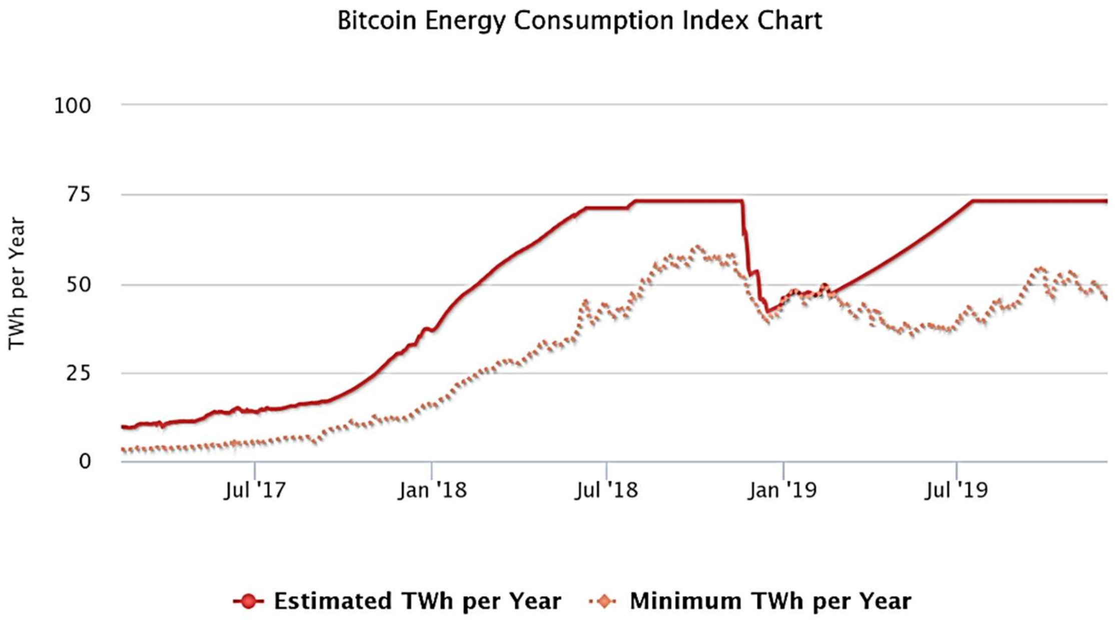
The number of miners has increased over the years and so the total computer power has increased. The graph in Figure 3 shows the growth of calculated hashes in one second. Although short downtrends exist, the overall power of the network is growing, and it is clear that a network like Bitcoin represents 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 (Strohmaier, et al., 2018), which shows that the most powerful supercomputers match 1-15% of the total Bitcoin power.

Energy consumption

Bitcoin has become infamous for its energy consumption and has thusly raised many concerns amongst the public. Since the Bitcoin inception, the power necessary for mining Bitcoin has grown exponentially, using electric power as its primary resource. This has made cryptocurrencies subject of numerous regulation policies by the many governments.

Mining is an energy-intensive process, which also requires specialised computer equipment. To calculate hash values of the block, in other words, iterate through billions of guesses, a miner needs to run hardware-intensive operations. These operations typically rely on the computing power of the processing units. The common units used in the mining process are central processing units (CPUs) and graphics processing units (GPUs), with the latter showing much better performance in solving complex computer tasks (Böhm et al., 2009). Figure 4 shows Bitcoin energy consumption index through time.

Figure 4
Bitcoin Energy Consumption Index



Source: Vries et al., 2019.

However, recent research shows that the Bitcoin network currently consumes leastwise 2.55 GW of electricity and it could reach 7.67 GW shortly - an amount comparable to the energy consumption in Ireland (Vries, 2018). Moreover, the massive power consumption of the Bitcoin network could cause a significant carbon footprint because the regions where most of the mining facilities are located use coal power (Stoll, 2019) and thus face serious environmental consequences in the long term.

Alternative consensus algorithms

As the popularity of Bitcoin grew, the number of experimental alternative cryptocurrencies grew proportionally. The rapid increase of users on the Bitcoin network led to harder mining problems therefore causing the development of new cryptocurrencies, also called altcoins, as an alternative to the Bitcoin. There have been numerous attempts at substituting *proof of work* consensus with more efficient and less resource consuming algorithms. As a matter, building a currency without flaws related to energy consumption could potentially deliver success and triumph in the cryptocurrency world. Ethereum, which is the second-largest blockchain network in the world by market capitalization (CoinMarketCap, 2019) is trying to shift entirely from the *proof of work* to the *proof of stake* algorithm.

The *proof of stake* consensus largely differs in mining new blocks and rewarding users. It uses validators for block creation and validation of transactions with pseudo-random selection methods for selecting validators for any given block (King & Nadal, 2012). Resource consumption is low since the protocol does not use mining for block creation but instead, the user places their deposit as a stake. Once a validator is selected, he has the exclusive right to create a block. This reduces an enormous amount of calculations since there is no competition between users. The difference between *proof of work* and *proof of stake* also reflects in the rewarding system (Fanti et al., 2018). A potential flaw arises when selecting validators. Only the wealthiest users could be selected as validators because the higher stake has the most potential in the forging process but the problem was addressed by introducing pseudo-random methods in selection (King & Nadal, 2012). Although it is one of the most perspective alternatives in terms of achieving security while decreasing resource consumption and risks of network attacks (Sheikh et al., 2018), it remains largely unadopted. A modified version of this algorithm is the delegated proof of stake (Larimer, 2014).

Nevertheless, other alternatives have been presented to the wider audience and have gained public interest. Another alternative is a consensus algorithm called *proof of space* where users prove their utilization of space. It is similar to some extent to *proof of work* due to its usage of computer storage, but its energy consumption could decrease over time (Alsunaidi & Alhaidari, 2019). Other notable examples are *proof of luck* and *proof of elapsed time* (Nguyen & Kim, 2018; Alsunaidi & Alhaidari, 2019).

Application of blockchain technology

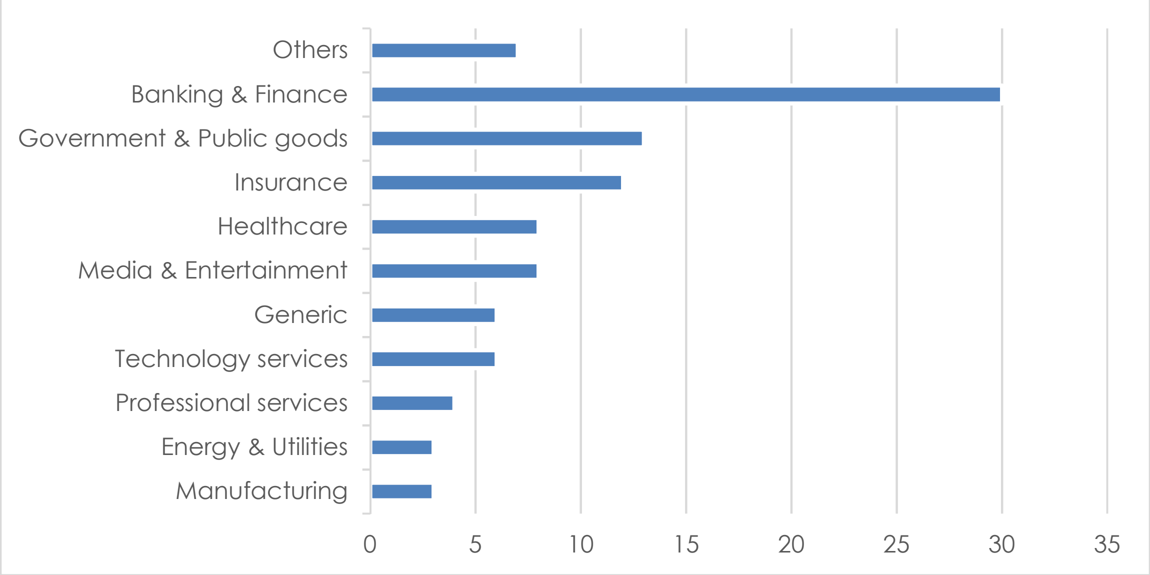
Cryptocurrencies like Bitcoin are the most famous applications of blockchain. There are services similar to currencies that can be based on blockchain, like securities transactions, loyalty point services, prepaid cards, gift card exchange and electronic coupons (NRI, 2015). However, because of its architecture 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 the Internet of things (IoT), a global network that connects smart objects with advanced Internet technology, to provide users with various services (Miorandi et al., 2012). Examples of such technology are systems like smart cities, smart environment, smart water, home automation, logistics etc. Blockchain could provide a 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 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 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 5
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 5 shows its usage in different sectors, pointing out that the 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. A smart contract is a transaction protocol that executes the terms of a contract (Tapscott, 2018). Blockchain in the finance sector can have the following benefits: 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, and others (Blockchain Technologies, 2019).

Improvements of blockchain technology

Applications listed in the previous chapter are the common ones and typically discussed in scientific papers, technical reports and literature. They are utilising 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 a 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 the folding@home project (Beberg et al., 2008). Folding@home is a Stanford University project that uses a public distributed computer system in the 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 (Knispel et al., 2010; Newberg et al., 2013). Folding@home and SETI@home are listed as two projects in the vast 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. 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 Hashcash method must meet the following conditions (Ball et al., 2017; Chatterjee et al., 2019):

- Checking solutions for problems should be significantly easier than the problem solving itself
- The problem must require a certain amount of work to guarantee to necessitate work
- The solution or problem must have certain characteristics to determine that the miner has solved the problem
- The mining process must protect the 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 (Ball et al., 2017; Oliver 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 a 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. The latter criterion explains that by solving one NP-complete problem it is possible to solve others.

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 travelling salesman problem, job scheduling problem, knapsack problem and longest path problem.

The travelling 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.

NP-complete problems within the blockchain

NP-complete problems satisfy all given conditions as an appropriate replacement of the Hashcash algorithm and are presented as a potential upgrade in the efficiency of the network. Furthermore, they also fulfil an additional requirement, improving the usefulness of the problem (Ball et al., 2017). The complexity of NP-complete problems makes them a distinct and universal category of computational problems whose solutions could be applied to many different areas. However, incorporating these problems to a blockchain is not simple nor effortless.

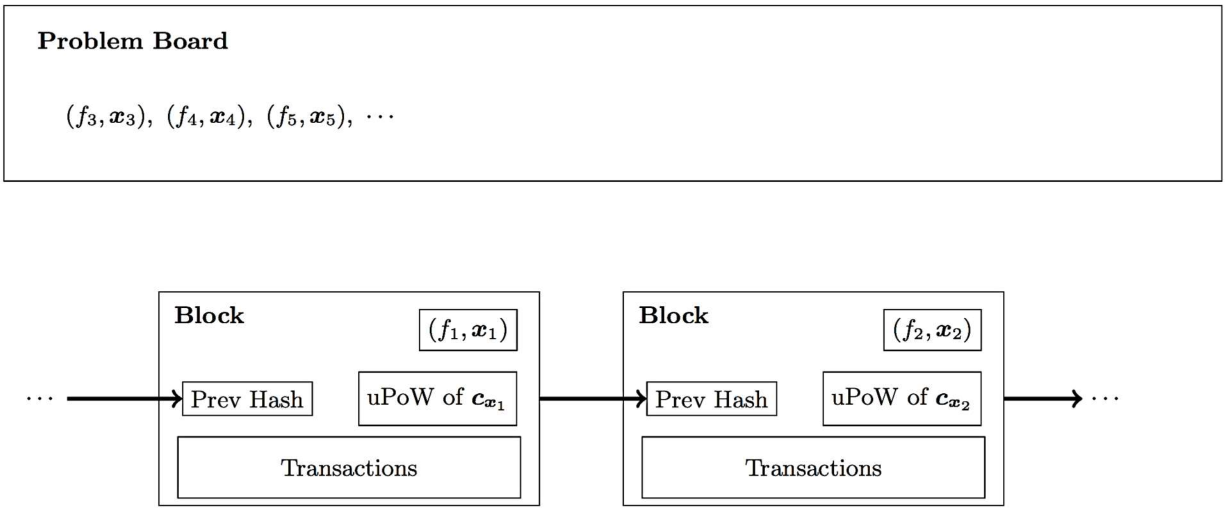
Changing the consensus algorithm implies creating an entirely new blockchain network, a new cryptocurrency. The third option is that the blockchain will have to diverge into two branches. Due to blockchain’s characteristic of immutability, it is not possible to retrospectively alter blocks or change the current mechanism of the system. Therefore, new cryptocurrencies were made in an attempt to solve problems, which are useful beyond the network itself. Such examples are Gridcoin and Curecoin cryptocurrencies, which reward its users for finding answers to medical, mathematical, and scientific problems (Halförd, 2019; Smith et al., 2019a). Both cryptocurrencies are facing an issue in terms of centralization because problems are delegated by a central authority. There have also been several attempts in constructing theoretical systems that could implement an NP-complete set of problems while maintaining all of the principal properties of a blockchain.

To switch, and entirely devote network power to solving useful, yet undelegated, new blockchain or a fork/branch should be made. One example of such cryptocurrency is Primecoin (King, 2013). Although Primecoin does not solve NP-complete problems, its mining algorithm discovers and verifies new prime numbers.

NP-complete problems can be incorporated into the blockchain in a few different ways. One way is creating a universal problem or set of problems whose solution can be further improved and optimised (Oliver et al., 2017). In this case, all miners in the network are solving the same problem and the miner who has a better solution than the solution in the previously attached block gets the chance to mine the block and submit his result along with it. An example of such a problem incorporated in the blockchain is the Orthogonal Vectors problem (Ball et al., 2017). Blockchain can be modified in a way that its genesis block stores the initial problem state and each new block contains a solution (Oliver et al., 2017). A possible flaw of the system could appear when the solution to the problem cannot be further optimised or when it needs a great deal of effort to find a better result. To address this issue, new solutions are proposed.

The most common approach among researches and explorations is combining two consensus algorithms within the same network. This approach is called hybrid mining. It allows users to choose their preferable mining process between *the proof of work* consensus using Hashcash algorithm or solving an NP-complete problem. Using these method miners can provide solutions for concrete problems while reducing the usage of spent energy without endangering the safety of existing systems.

Figure 6
Public Board with Problem Units


Problem Board
$(f_3, \boldsymbol{x}_3),\ (f_4, \boldsymbol{x}_4),\ (f_5, \boldsymbol{x}_5),\ \cdots$
Block
$(f_1, \boldsymbol{x}_1)$
Prev Hash
uPoW of $\boldsymbol{c}_{\boldsymbol{x}_1}$
Transactions
Block
$(f_2, \boldsymbol{x}_2)$
Prev Hash
uPoW of $\boldsymbol{c}_{\boldsymbol{x}_2}$
Transactions
$\cdots$
$\cdots$

Source: Ball et al. (2017)

To avoid the problem with a limited number of solutions, new problem units can be delegated by users (Ball et al., 2017; Chatterjee et al., 2019). Figure 6 shows the conceptual diagram of the public board that users post problems. Miners are producing proof of useful work (uPow of C_{x_n}) which is attached to the block.

All users in the network are free to delegate their problem to the blockchain in the specified form. Using this method, new problems will be continuously appended thus providing miners with an unlimited source of new challenges. By allowing users to employ the enormous computing power of the network, it opens a vast field of possibilities in solving various problems. From healthcare and government problems, infrastructural and processing issues, finance and business intelligence, such power could offer solutions in a faster, more convenient and less time and energy consuming manner.

Conclusion

A widespread platform of distributed computing called Bitcoin offers many advantages when compared to traditional solutions. It facilitates payment transactions in a more efficient, secure and reliable manner but it is also taking its toll regarding significant resource consumption. More and more questions are made concerning the usefulness of the network and its mining process. Mining cryptocurrencies has become rather its massive industry with mining facilities all over the world but it became apparent to the public that the network would lack sustainability soon. Despite the many benefits that the Bitcoin network provides, one of the biggest subject to criticism is its Hashcash algorithm commonly used in the *proof of work* consensus. Hashcash algorithm validates the user's transactions and secures the network by preventing double-spending, but it also consumes vast amounts of electric power, time and computer equipment. Alternative mechanisms are being developed to substitute Hashcash with a more efficient algorithm. One of these solutions could be in adopting a special category of NP-complete problems within a blockchain. By implementing NP-complete problems, the network could redirect its power into more useful calculations, solving problems in a variety of different areas, such as technology, medicine, finance and business systems.

References

1. Alsunaidi, S. J., Alhaidari, F. A. (2019), "A survey of consensus algorithms for blockchain technology", in 2019 International Conference on Computer and Information Sciences, 3-4 April, IEEE, Sakaka.
2. Anastassiou, G. A. (2011), Handbook of Computational and Numerical Methods in Finance. Edited by Rachev, S. T. Springer Science & Business Media, New York.
3. 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.
4. 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.
5. Back, A. (2002), "Hashcash - A denial of service counter-measure", available at: https://cryptorating.eu/whitepapers/Bitcoin/References/hashcash.pdf (5 January 2019)
6. Ball, M., Rosen, A., Sabin, M., Nalini Vasudevan, P. (2017), "Proofs of useful work", IACR Cryptology ePrint Archive, available at: https://eprint.iacr.org/2017/203.pdf (9 January 2019)
7. Beberg, L. A., Ensign, D., Jayachandran, G., Khaliq, S., Pande, S. V. (2009), "Folding@ home: Lessons from eight years of volunteer distributed computing", in 23rd IEEE International Symposium on Parallel and Distributed Processing, 23-29 May, IEEE, Rome.
8. BitInfoCharts. (2019), "Bitcoin (BTC) price stats and information", available at: https://bitinfocharts.com/bitcoin/ (2 July 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", available at: https://arxiv.org/abs/1801.07447 (1 July 2019)
11. Böhm, C., Noll, R., Plant, C., Wackersreuther, B., Zherdin, A. (2009), "Data mining using graphics processing units", In Transactions on Large-Scale Data-and Knowledge-Centered Systems, Springer, Berlin, Heidelberg, pp. 63-90.

12. Chatterjee K., Goharshady A., Pourdamghani A. (2019), "Hybrid mining: Exploiting blockchain's computational power for distributed problem solving", 34th ACM Symposium on Applied Computing, 8-12 April, ACM Symposium on Applied Computing (SAC), Limassol, pp. 374-381.
13. CoinMarketCap. (2019), "Cryptocurrency market capitalizations", available at: https://coinmarketcap.com (1 Jul 2019).
14. Cook, S. (1971), "The complexity of theorem proving procedures", 3rd Annual ACM Symposium on Theory of Computing, 3-5 May, Association for Computing Machinery, Shaker Heights, pp. 151-158.
15. Dunne, P. E. (2008), "An annotated list of selected NP-complete problems", available at: https://cgi.csc.liv.ac.uk/~ped/teachadmin/COMP202/annotated_np.html (1 July 2019)
16. 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.
17. Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., Wang, G. (2018), "Compounding of wealth in proof-of-stake cryptocurrencies", In Meiklejohn, S., Kazue, S. (Eds.), *22nd International Conference on Financial Cryptography and Data Security*, 26 February-2 March, Springer, Cham, Nieuwpoort, pp. 42-61.
18. Garey, M. R., Johnson, D. S. (1979). Computers and intractability (Vol. 174). Freeman, San Francisco.
19. Grech, A., Camilleri, A. F. (2017), "Blockchain in education", Publications Office of the European Union, Luxembourg.
20. Halförd, R. (2019), "Gridcoin whitepaper: The computation power of a blockchain driving science & data analysis", available at: https://gridcoin.us/assets/img/whitepaper.pdf (1 December 2019)
21. Hileman, G., Rauchs, M. (2017), "Global blockchain benchmarking study", Cambridge Centre for Alternative Finance, University of Cambridge, Cambridge.
22. Hongdao, Q., Bibi, S., Khan, A., Ardito, L., Khaskheli, M.B. (2019), "Legal technologies in action: The future of the legal market in light of disruptive innovations", Sustainability, Vol. 11 No. 4, Article 1015.
23. 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)
24. Juričić, V., Radošević, M., Fuzul, E. (2019), "Creating student's profile using blockchain technology", 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 20-24 May, IEEE, Opatija, pp. 521-525.
25. King, S. (2013), "Primecoin: Cryptocurrency with prime number proof-of-work", avialable at: https://c3.coinlore.com/pdf/primecoin-white-paper.pdf (11 July 2019)
26. King, S., Nadal, S. (2012), "PPCoin: Peer-to-Peer crypto-currency with proof-of-stake", avialable at: https://decred.org/research/king2012.pdf (9 July 2019)
27. 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", Science, Vol. 329 No. 5997, pp.1305-1305.
28. Larimer, D. (2014), "BitShares history: Delegated Proof-of-Stake (DPOS)", available at: https://steemit.com/bitshares/@testz/bitshares-history-delegated-proof-of-stake-dpos (21 June 2019)
29. Lavanya, B. (2018), "Blockchain technology beyond bitcoin: An overview", International Journal of Computer Science and Mobile Applications, Vol. 6 No. 1, pp. 76-80.
30. Leible, S., Schlager, S., Schubotz, M., Gipp, B. (2019), "A review on blockchain technology and blockchain projects fostering open science", Frontiers in Blockchain, Vol. 2, Article 16.
31. Marrara, S., Pejić Bach, M., Seljan, S., Topalovic, A. (2019), "FinTech and SMEs: The Italian case", in FinTech as a Disruptive Technology for Financial Institutions, IGI Global, Hershey, pp. 14-41.

32. 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.
33. Nakamoto, S. (2008), "Bitcoin: A peer-to-peer electronic cash system", available at: https://git.dhimmel.com/bitcoin-whitepaper/ (9 July 2019)
34. Newberg, H. J., Newby, M., Desell, T., Magdon-Ismail, M., Szymanski, B., Varela, C. (2013), "Harnessing volunteer computers to constrain dark matter in the Milky Way", Proceedings of the International Astronomical Union, Vol. 9 No. S298, pp. 98-104.
35. Nguyen, G. T., Kim, K. (2018), "A survey about consensus algorithms used in blockchain", Journal of Information Processing Systems, Vol. 14 No. 1, pp. 101-128.
36. Nomura Research Institute. (2015), "Survey on blockchain technologies and related services", available at: https://www.meti.go.jp/english/press/2016/pdf/0531_01f.pdf (6 December 2019)
37. Oliver, C. G., Ricottone, A., Philippopoulos, P. (2017), "Proposal for a fully decentralized blockchain and proof-of-work algorithm for solving NP-complete problems", available at: https://arxiv.org/abs/1708.09419 (10 December 2019)
38. Panarello, A., Tapas, N., Merlino, G., Longo, F., Puliafito, A. (2018), "Blockchain and IoT integration: A systematic survey", Sensors, Vol. 18 No. 8, Article 2575.
39. 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)
40. Sheikh, H., Azmathullah, R. M., Rizwan, F. (2018), "Proof-of-Work Vs Proof-of-Stake: A comparative analysis and an approach to blockchain consensus mechanism", International Journal for Research in Applied Science & Engineering Technology, Vol. 6 No. 12, pp. 786-791.
41. Smith, J., Sanchez M. (2019a), "White paper: 2019 Curecoin model", available at: https://curecoin.net/white-paper/ (5 December 2019)
42. Smith, P. Cary, N., Baynham-Herd, X., McGarraugh, C. Khil, M., Tuzzolo, M., Wilson, P. (2019b), "Hash rate", available at: https://www.blockchain.com/charts/hash-rate?timespan=all&scale=1 (30 June 2019)
43. Stoll, C. (2019), "The carbon footprint of bitcoin", Joule, Vol. 3 No. 7, pp. 1647-1661.
44. Meuer, H., Strohmaier, E., Dongarra, J., Simon, H., Meuer, M. (2018), "Top 500 list", available at: https://www.top500.org/lists/2018/11/ (1 June 2019)
45. Tapscott, D., Tapscott, A. (2018), Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World, Portolio, New York.
46. Vries, A. (2018), "Bitcoin's growing energy problem", Joule, Vol. 5, pp. 801-805.
47. Vries, A. (2019), "Bitcoin energy consumption index", available at: https://digiconomist.net/bitcoin-energy-consumption (25 October 2020)
48. Wood G., Steiner J. (2016), "Trustless computing—The what not the how", In Banking Beyond Banks and Money, New Economic Windows, Springer, Cham, pp. 133-144.
49. 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 a master's degree in Computer Science that he received at Faculty of Electrical Engineering and Computing, University of Zagreb. He received a 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 a master's degree in Mathematics and Computer Science Education that she received at the 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 the 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**.