IPRPD
International Journal of Business & Management Studies
ISSN 2694-1430 (Print), 2694-1449 (Online)
Volume 02; Issue no 05: May, 2021

BLOCKCHAIN TECHNOLOGY: A SURVEY OF CROATIAN BUSINESS LEADERS

Dražen Zec [1], William G. Heninger [2]

[1] *Algebra University, Croatia*

[2] *Associate Professor, Brigham Young University, USA*

Abstract

Blockchain or distributed ledger technology emerged over ten years ago as the underlying technology of bitcoin. Blockchain is a special kind of database with individual records or blocks linked together in a sequential list called chain of blocks. These records are validated by multiple nodes in peer-to-peer networks and they are immutable. It is a decentralized system, with no need for intermediaries where all decisions are made using different consensus mechanisms. High expectations from blockchain technology, combined with a lack of deeper knowledge about the technology are expressed in the results from the survey conducted on a sample of Croatian C-level and middle managers from various industries. The results appear to indicate that Croatian business leaders perceive that we are still in the early phase of adoption with management expecting some disruption in the future but expecting it to occur mostly in the information technology and financial industry.

Keywords: Blockchain, Decentralization, Peer-to-peer network, Decentralized application.

1. Introduction

Blockchain technology presents a radical transformation in the way we do business. Since its first application in digital cryptocurrency, blockchain technology has evolved to become a collection of technologies that may enable value generation across many industries. This potential is enabled by trust, transparency and reduced friction across business systems. However, it is still not obvious in what way blockchain will provide greater value than current enterprise technologies as most industries are still in the proof-of-concept phase or just trying to figure out what this new technology means in their futures.

To gauge blockchain awareness and implementation in an Eastern European emerging market, we surveyed 71 Croatian C-level and middle managers and found that although these managers were aware of blockchain, most had only a cursory knowledge of the theory and technology behind blockchain. Although very few have seen the application of blockchain in their industry, a majority anticipate that it will affect their industry to at least some extent. Most interesting is that while few see blockchain providing much benefit to their individual work, most think that blockchain will have a major disrupting effect on their economy.

2. Background

In 2008 an author or group of authors under the pseudonym Satoshi Nakamoto published the groundbreaking paper entitled Bitcoin: A Peer-to-Peer Electronic Cash System (Nakamoto, 2008). The paper introduced the notion of bitcoin as a peer-to-peer electronic cash system with no intermediary bank for payment transfers between peers. In actuality he introduced the first fully decentralized digital currency. He introduced the term *block of chains* which evolved in the following years to become a single word – blockchain.

Blockchain is a digital record of transactions, characterized by a structure in which individual records (or blocks) are linked together in a single list, called a chain – therefore the name is straightforward and self-explanatory.

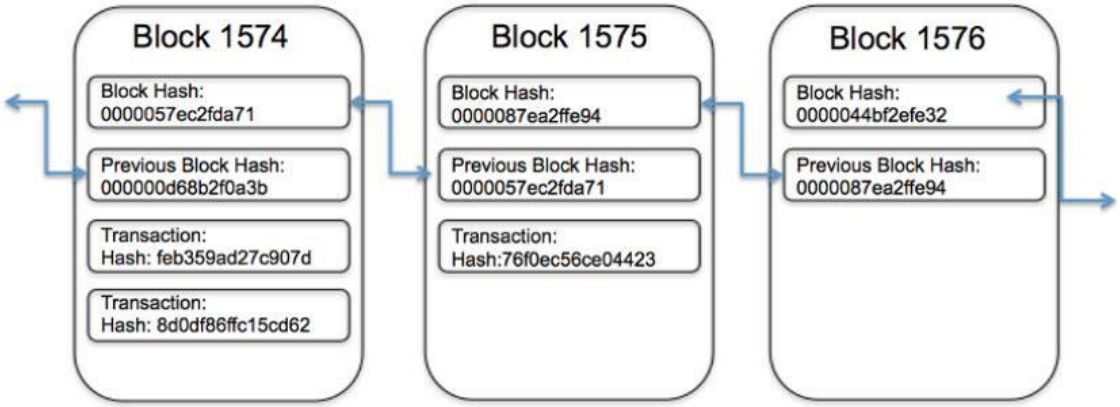

Figure 1. Transactions in the blockchain (Gupta, 2018)

A public ledger or database is where the transaction records are validated and shared by multiple computers or nodes in a peer-to-peer network. Blocks are linked to each other in such a way that, whenever a new block is added to the chain, it is done by using a cryptographic hash generated from the contents of the previous block, as shown in Figure 1, thus ensuring validity of the transaction. To put it simply, blockchain is a technology that records transactions in such a way that they cannot be altered or deleted later, and the chain of transactions can only be sequentially updated.

2.1 Theory behind blockchain

In order to understand blockchain technology, it is essential to realize that blockchain basically is a decentralized distributed system. A distributed system represents two or more nodes that work with each other in a coordinated manner to achieve a common objective, while end users see the whole system as a single logical platform.
Nodes are interacting with each other by sending and receiving messages. The main challenge in the system design is coordination between nodes and fault tolerance. If some nodes stop working, lose connection to the system or start sending faulty messages, a distributed system should still be able to operate flawlessly in order to achieve the correct outcome. This has been an area of active research for many years and numerous algorithms and mechanisms have been proposed to overcome these issues.

The problem with the design of a distributed system is that it cannot possess consistency, availability and partition tolerance are at the same time. Consistency is the ability of a distributed system to maintain the most recent copy of data on all nodes, while availability means that a system is accessible and delivering correct responses whenever it is required. Partition tolerance ensures that the distributed system continues to operate correctly even if some of the nodes in the system fail and an arbitrary number of messages have been dropped or delayed. To put it simply, the issue is in designing systems that consistently provide reliable data and is resistant to failure.

In order to achieve fault tolerance the most widely used method is replication. Consistency is ensured by using consensus algorithms to make sure that all nodes have the same data. It must be stated here that in blockchain, consistency is sacrificed in favor of availability and partition tolerance, which practically means that consistency on the blockchain is not achieved simultaneously with the other two, but it is achieved over time through validating multiple nodes. This results in slower processing of large numbers of transactions, which is one of the problems that researchers and developers are still trying to find an optimal solution.

2.2 Byzantine generals' problem

The concept of achieving consensus between multiple nodes in a distributed system is known as distributed consensus. In order to achieve it, certain consensus mechanisms need to be put in place. Development of these mechanisms started with Baran's (1962) idea of cryptographic signatures. Later, Lamport, Shostak, and Pease (1982) introduced a theoretical agreement problem known as the Byzantine Generals Problem and described it as a group of generals who, each commanding a portion of a Byzantine army, encircle a city. The army and the city have approximately similar forces and the generals can win the battle only if they are able to coordinate their attack simultaneously. The problem is that their communication is restricted to messengers going through the city, and that problem is additionally complicated by potential presence of treacherous generals (see Figure 2).

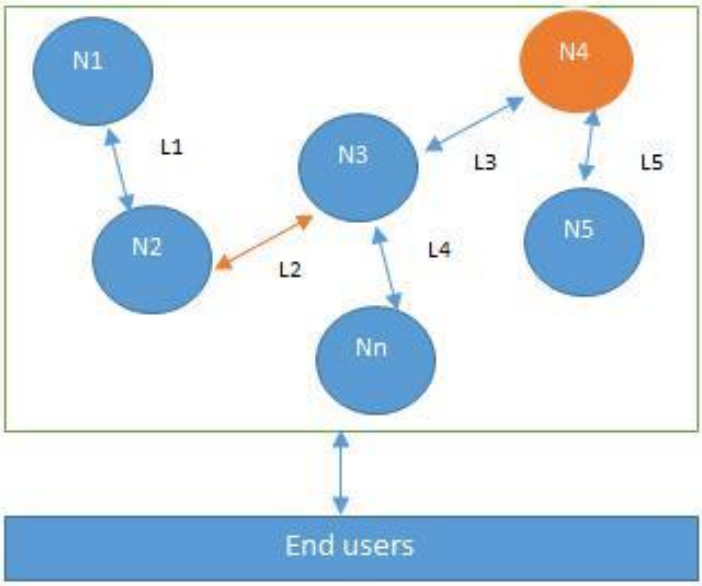

Figure 2. Design of a distributed system (Bashir, 2017)

This problem was solved in 1999 with the introduction of Practical Byzantine Fault Tolerance (PBFT) algorithm by Miguel Castro and Barbara Liskov (1999). They applied hash functions and cryptography. The first practical implementation was made ten years later with the invention of bitcoin. The Proof of Work (PoW) algorithm was developed as a mechanism to reach consensus. It was actually a solution to the double-spending problem in the electronic cash system using a peer-to-peer network. The double-spending problem is the risk of digital currency being spent twice, as digital information can be easily reproduced, thus allowing the potential manipulator to make a copy of the original record (digital token) and use it for payment, all the while retaining the original payment.

2.3 Decentralization using blockchain

The main advantage provided by blockchain is decentralization which eliminates the need for intermediaries in the process and enables different parties to compete to become the decision-making factor via consensus mechanisms. Blockchain uses consensus algorithms to detect a leader who will decide the contents of the next block. As already mentioned, the most commonly used method for consensus is the Proof of Work (PoW). In PoW, a solution to a particular mathematical problem needs to be found (Narayan, Bonneau, Felten, Miller, and Goldfeder, 2016). In a peer-to-peer network, nodes are competing with each other to find the solution to a certain mathematical problem and a random node is selected to build a new block. Proof of Work is actually a proof that enough computational resources have been spent in order to build a valid block. In simple words, proof of work is a piece of data which is hard to produce but can easily be verified by others. To produce it, a lot of trial and error computation is required until the right solution is found (Konstantopoulos, 2017).

The problem with the Proof of Work is that, over time, it requires more and more computational power which leads to more and more energy consumption. Another potential issue is the centralization of computational power, which again is not in line with the general idea of decentralization. However, PoW drawbacks have led to the invention or application of other consensus algorithms. One of these is the Proof of Stake (PoS), which is based on the concept that every individual can mine or validate new blocks based not only on the processing power, but on the combination of other criteria like random selection and "coin-age" (value derived from the number of coins/tokens in possession and the period of time these coins are being held). To put it simply, the more coins they have, the higher is their mining capability, but only to a certain extent as otherwise decentralization could be endangered. In PoS, miners are basically replaced by validators which lock up some of their coins at stake in order to become able to validate the blocks. The main advantage of PoS is that there is not as much need for computational power as with PoW.

Proof of Weight or Directed Acyclic Graph (DAG) is another example. DAG is actually a form of data structure where data is stored topologically in a seamless graph, so this algorithm is moving beyond chains and blocks and introduces so-called sidechains, allowing different transactions to perform independently on multiple chains. The advantages of DAG are much lower costs and better scalability. Obviously, there is no single consensus algorithm that is perfect; however, as blockchain technology has developed, these algorithms improved and eventually will lead to a faster and more scalable technology which in turn will be easier to implement and adopt. As with any other new technology, it is a subject of extensive research and will result in a final solution(s) which will likely become a widely adopted standard.

2.4 Different types of blockchains

There are many different blockchain models with various consensus algorithms, levels of privacy for their users, levels of energy and scalability. The models often get classified as public vs. private blockchains. Within the private type there is also a subgroup of federated or consortium blockchains. Another classification differentiates between permissionless and permissioned type based on the access to the platform which can be restricted or not. Permissioned blockchain is the one where access is restricted, while the permissionless one is open to anyone who has a computer.

On the other hand, classification on public, consortium and private blockchains has to do with platform management and the level of anonymity of users, which is all directly connected to the level of decentralization, as shown in Figure 3.

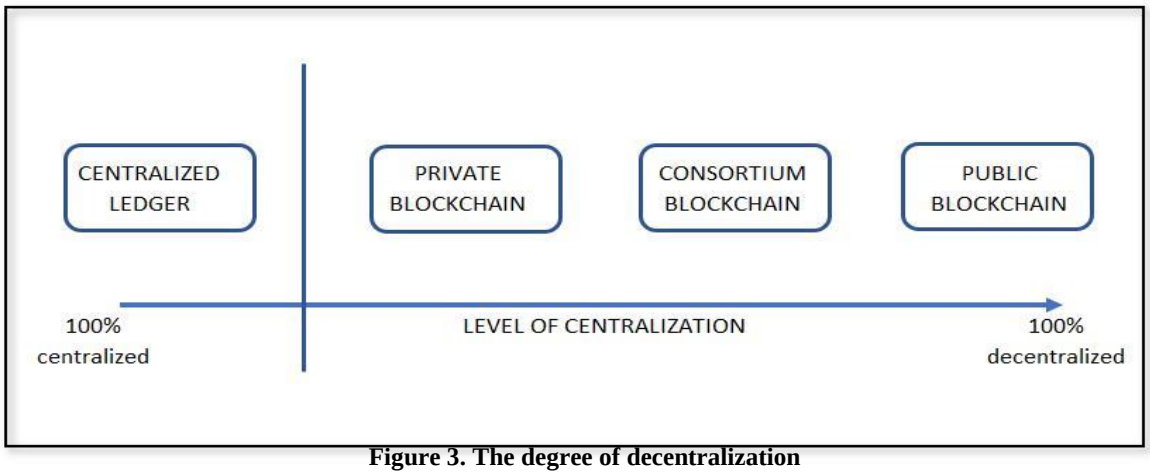

Figure 3. The degree of decentralization

Public blockchain is characterized by the lack of an entity managing the platform, all transactions are visible to anyone and users are anonymous. The platform does not rely on a trusted party to validate transactions and nodes need to come to a consensus for the transaction to be stored in the ledger. Most public blockchains are permissionless, however it is possible to have a permissioned public blockchain when transaction validation is based on some precondition which needs to be fulfilled.

Private blockchain, on the other hand, relies on an entity managing the platform, which means that this entity is controlling who can validate and write data on the blockchain. Validation of transactions is usually allowed to a restricted number of nodes which reduces decentralization but increases the speed and reduce energy consumption. Permission to read the data can be restricted which ensures the participant's privacy.

Finally, consortium blockchain is a private blockchain managed by a group of entities, usually a consortium of companies, which indicates a partially decentralized platform. Both private and consortium blockchains are usually permissioned platforms, as they regularly contain private business information which should not be disclosed in public.

2.5 Bitcoin

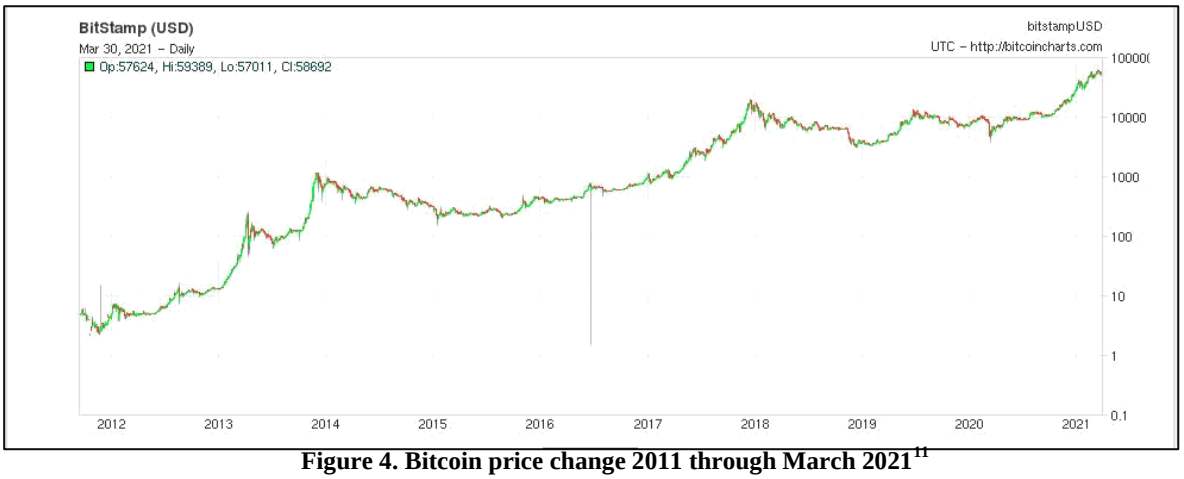

Figure 4. Bitcoin price change 2011 through March 2021[1]

[1]https://bitcoincharts.com/charts/bitstampUSD#rg2920zczsg2010-10-02zeg2019-02 13ztgSzm1g10zm2g25zl

The history of blockchain started with the introduction of bitcoin in 2008. Bitcoin was the first fully decentralized digital currency and is the most successful and popular digital currency with the current market capitalization of 600 billion USD (as of March 2021). The value of bitcoin was not recognized at the beginning, however it has increased dramatically since 2011, as shown in Figure 4. This growth is fueled by economies of scale (or simply a network effect). Recent volatilities in price reflect, among other things, the effects of regulatory actions from different countries (including the largest world economies like the USA and China).

Bitcoin is a form of digital cash, a decentralized digital currency based on the results of extensive research in public key cryptography, hash functions and digital signatures. This digital or electronic cash is defined as a chain of digital signatures and it is registered to bitcoin addresses.

A bitcoin address is essentially a string of characters created by combining public and private cryptographic keys (generated by elliptic curve cryptography) and hashing them with different algorithms. Finally the encoding scheme is applied and the resulting address looks like this example: 1BvFMSEYzgWetqTFn5Au4n2GFg7qJaNVN2. This string of characters simply represents a possible destination for a bitcoin payment. There are currently three bitcoin address formats in use: P2PKH, P2SH and Bech32. Bitcoin addresses can be generated by any user of bitcoin.

Transfer of ownership of electronic coin, which is a basic transaction in the blockchain, is executed by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the chain, as presented in Figure 5.

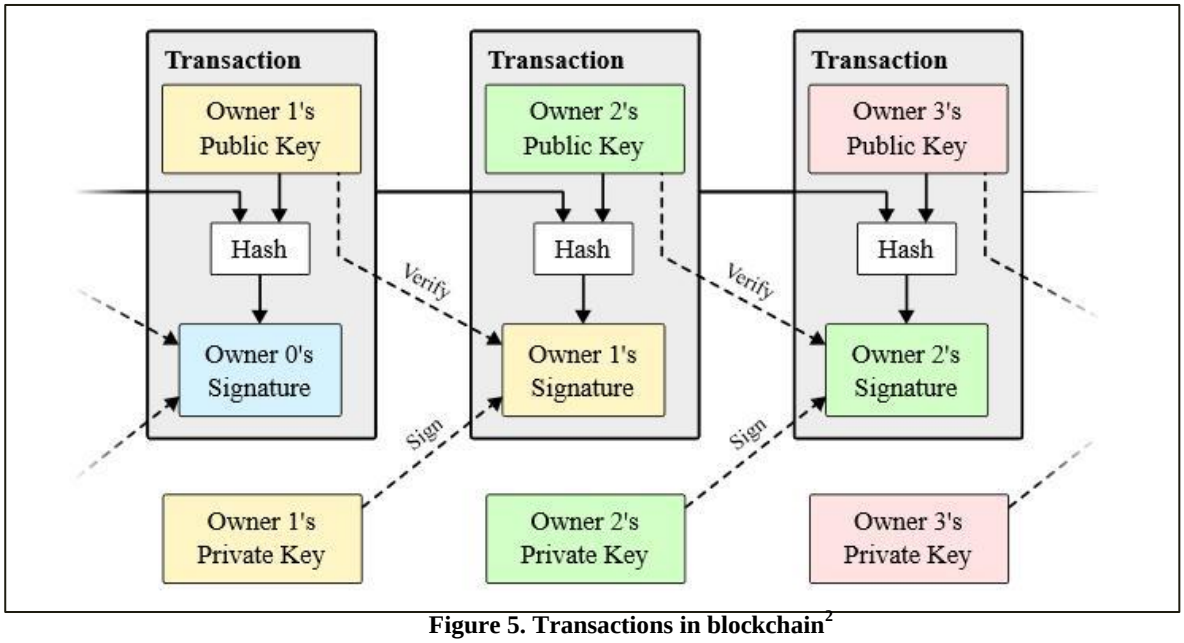

Figure 5. Transactions in blockchain[2]

The idea is based on the peer-to-peer version of electronic cash, allowing payments to be sent directly from one party to another, without a bank or any other financial institution as an intermediary. One part of the solution is the digital signature, however the other problem, double-spending (using the same funds more than once), is solved by using a peer-to-peer network. The network timestamps the transactions by hashing them into a chain of hash-based proof-of-work, thus creating a growing record which cannot be changed. The only way to change the record is by redoing all previous proof-of-work, an action which would require enormous CPU power or, in other words, control over the majority of nodes in the network. Since we are addressing a network of random nodes, it is hard to imagine and it is practically impossible that the majority of nodes would be controlled by one party.

The process of adding transaction records to blockchain is called mining. Bitcoin mining is performed by high-powered computers solving complex computational math problems. The mining process is intentionally designed to be resource-intensive and difficult so that the number of blocks remains more or less steady on a daily basis. Bitcoin mining allows bitcoin nodes to reach a secure consensus and it is also the way new bitcoins are introduced into the system. Miners are rewarded by the number of newly created coins. Miners are also rewarded with transaction fees for transactions included in the blocks.

New blocks are added to the network approximately every 10 minutes and, in order to maintain that level of block creation, the difficulty of mathematical problems is adjusted dynamically every 2016 blocks. The calculation for bitcoin network difficulty is as follows:

[2] https://bitcoin.stackexchange.com/questions/69082/how-do-transactions-in-the-blockchain-work

*Target = Previous target * Time/2016 * 10 minutes*

The amount of new bitcoin released with each new block is called the "block reward". This reward is being cut in half approximately every four years.

Transactions in bitcoin networks are composed of inputs and outputs, where inputs can be imagined as spending coins, whereas creation of new coins represents an output. If a transaction is sending coins from one user to another, the sender has to sign it with his private key and a reference to a previous transaction is required so as to confirm the origin of the coins. Transactions can be seen in the blockchain as they are not encrypted. The most common transaction type is P2PKH (Pay To Public Key Hash) and it is used to send transactions to bitcoin addresses.

In a Bitcoin network a simple language called script is used to describe the transactions. Operations in scripts are defined by functions or Opcodes. Scripts are evaluated from left to right based on Last-In-First-Out (LIFO) stack. A combination of ScriptSig and ScriptPubKey is used for evaluation of the transaction, ScriptSig being the unlocking script and ScriptPubKey the locking script. A user who wants to unlock the transaction provides the ScriptSig, and ScriptPubKey specifies conditions which need to be fulfilled for output to be spent as displayed in Figure 6.

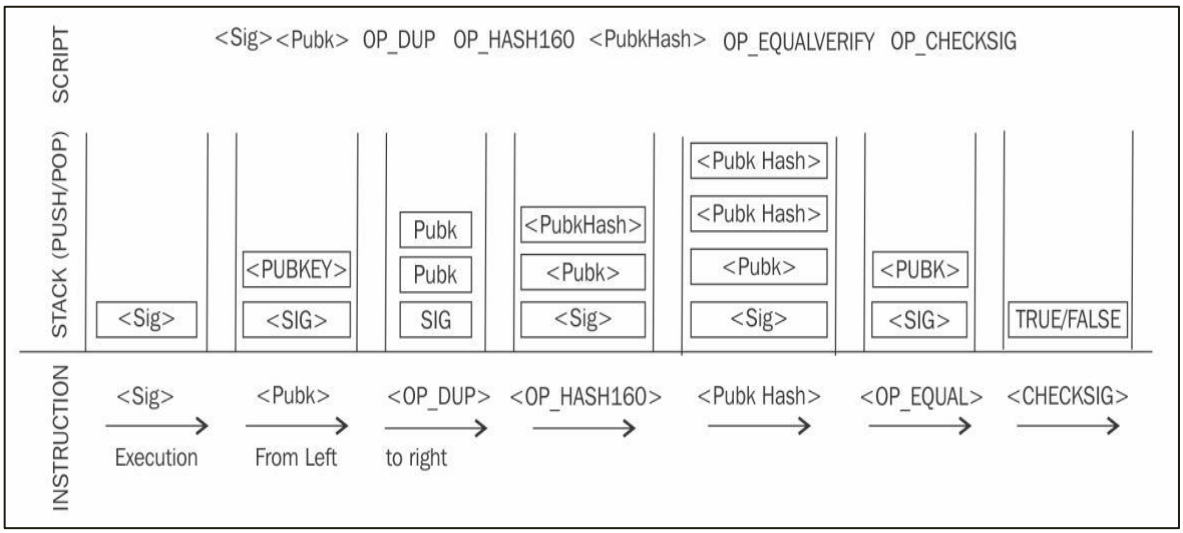

Figure 6. P2PKH script execution[33]

Bitcoin is the most widely used digital currency in the world, however it needs to be mentioned that there are many other cryptocurrencies in circulation (usually referred to as Altcoins or alternatives to bitcoins), and some of the most popular are Bitcoin Cash, Litecoin, Ethereum, NEO, Ripple XRP, Stellar, Cardano, EOS, Tron. This changes almost daily.

3. Methodology, Results and Discussion

In order to provide an overview of the current level of knowledge about technology in the Croatian market and to assess the likelihood of applying blockchain in business in a foreseeable future, we surveyed 71professionals. The participants were mostly members of upper or middle management from various industries. Table 1 provides demographic data on the participants in our study. Over half (51%) of the participant were from upper management in their organization, 21 % were from middle and junior management and the remaining 28% of the participants held administrative, support, professional, consultant, researcher, self-employed or other positions. The participants came from organizations that ranged from less than 50 people (41%), to organizations of 51 to 250 people (24%), to organizations of 251 to 1,000 people (14%), to large organizations of over 1,000 people (21%). The top 7 represented industries are Information Technology (21%), Finance and Insurance (18%), Education (13%), Hotel and Food Services (8%), Telecommunications (7%), and Wholesale (4%). The remaining 29% ranged from Construction to Publishing. 74% of our participants are men and 26% are women.

[3] Bashir I., Mastering Blockchain, Packt Publishing Ltd., 2017, page 124

Variable	Mean or Percent
Role Within your Organization	
Upper Management	51%
Middle Management	15%
Junior Management	6%
Adminstrative Staff	7%
Support Staff	3%
Trained Professional	6%
Consultant	7%
Researcher	1%
Self-Employed / Partner	3%
Other	1%
Organization Size by Number of Employees	
Less than 50	41%
51 – 250	24%
251 – 1,000	14%
1,001 and above	21%
Industry	
Information Technology	21%
Finance and Insurance	18%
Education	13%
Hotel and Food Services	8%
Telecommunications	7%
Wholesale	4%
Construction	3%
Government and Public Administration	3%
Health Care	3%
Mining	3%
Retail	3%
Transportation and Warehousing	2%
Broadcasting	1%
Military	1%
Publishing	1%
Other	9%
Gender	
Men	74%
Women	26%

Table 1: Demographic Information

Our first objective was to gauge the level of awareness and the potential for future implementation of the technology. We posited that a higher level of awareness would allow for more realistic expectations in terms of the impact that blockchain technology could have on respective industries. Our goal was to determine the degree to which managers from various market segments are familiar with blockchain technology and to detect their expectations this technology in the future. Our results presented in Figure 7 indicate that over half (54%) of the participants had read about blockchain, 20% answered that they were only aware of bitcoin and associated the technology only with cryptocurrencies, 14% had researched the technology, 4% claimed to be experts, and 8% indicated that they had no knowledge of blockchain.

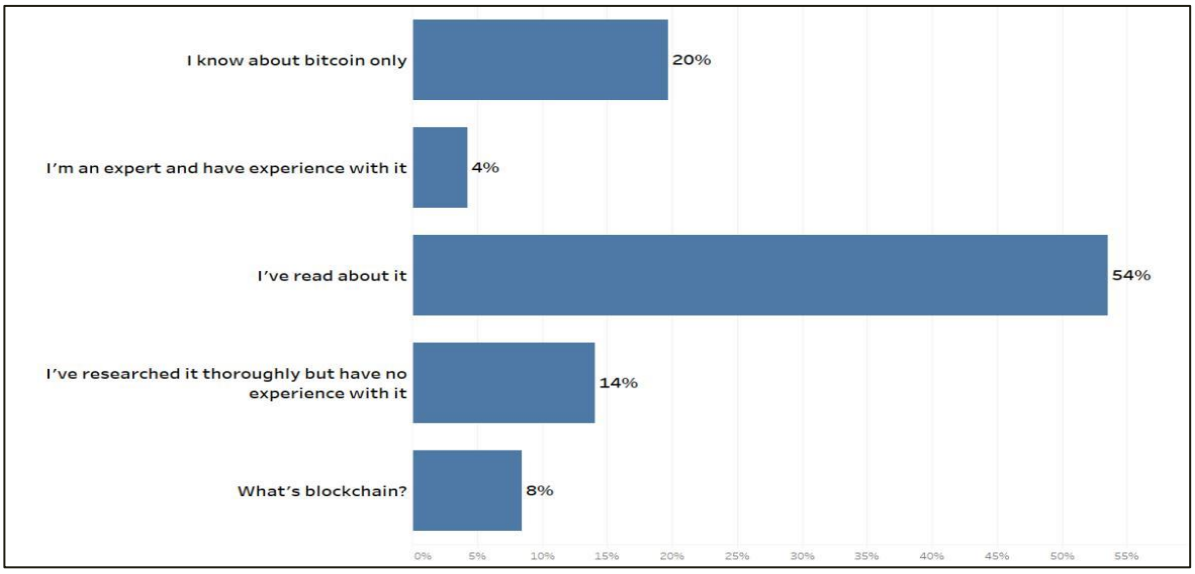

Figure 7: How would you describe your knowledge of blockchain technology?

In order to assess how closely our participants followed blockchain we asked how familiar they were with blockchain technology applications. As shown in Figure 8, our results show that only 8% of participants follow the blockchain news regularly, but almost 60% have at least read a few article about it. While 24% had no familiarity with blockchain appliations and 8% only followed bitcoin.

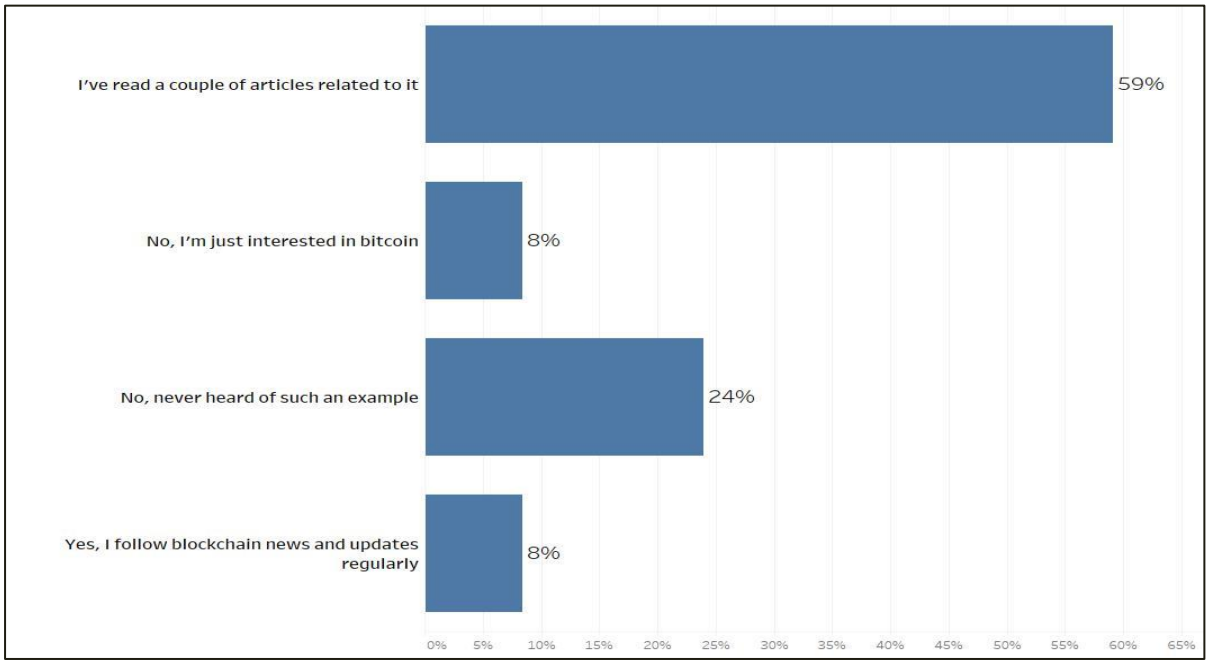

Figure 8: Are you familiar with any examples of blockchain technology applications?

We then asked about the possible effect that blockchain technology could have on the participant's industy, more than half of the participants expected either high (24%) or some impact (37%) as presented in Figure 9. Thirty four percent (34%) of the participants were indecisive, which can be connected to the previous question where almost a similar percentage stated that they never saw any examples of implementation or they were not interested in more than bitcoin. Only 4% thought that blockchain would have no effect on their industry.

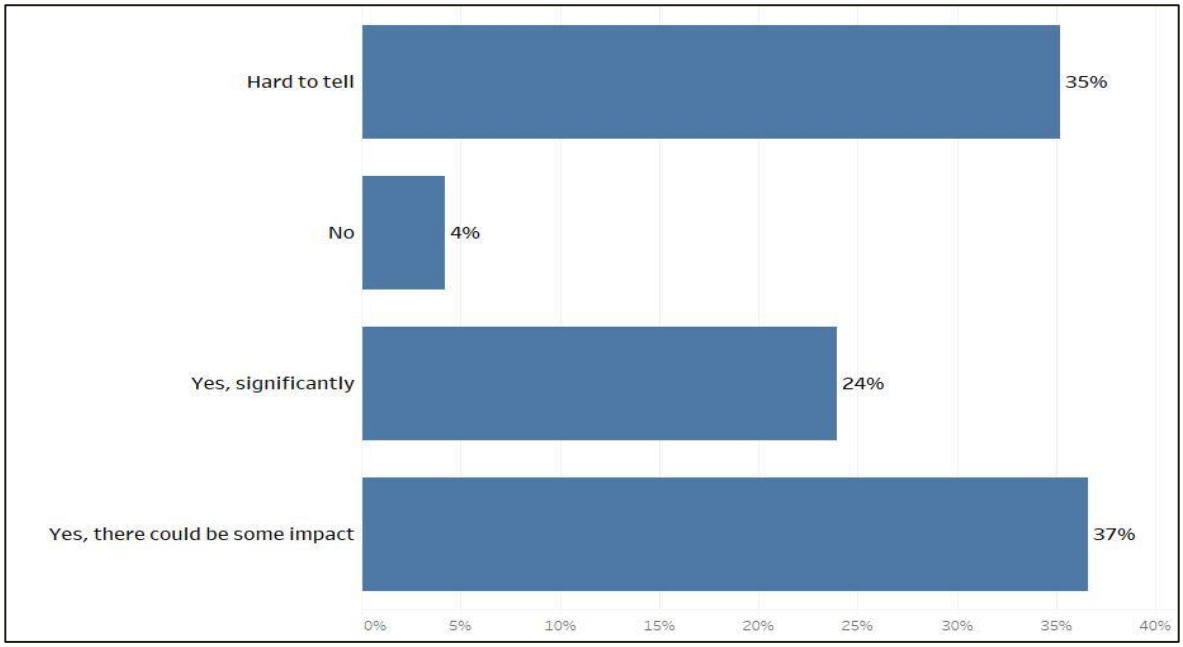

Figure 9: Do you think blockchain will affect your industry?

In order to ascertain blockchain adoption we asked participants if their company had adopted or planned to adopt blockchain technology. As shown in Figure 10, of all the participants, 14% confirmed that there are plans or actual implementation in place. Sixty one (61%) percent of the participant's indicated that there was no adoption or plans for adoption and 25% were unaware of any adoption or plans for adoption.

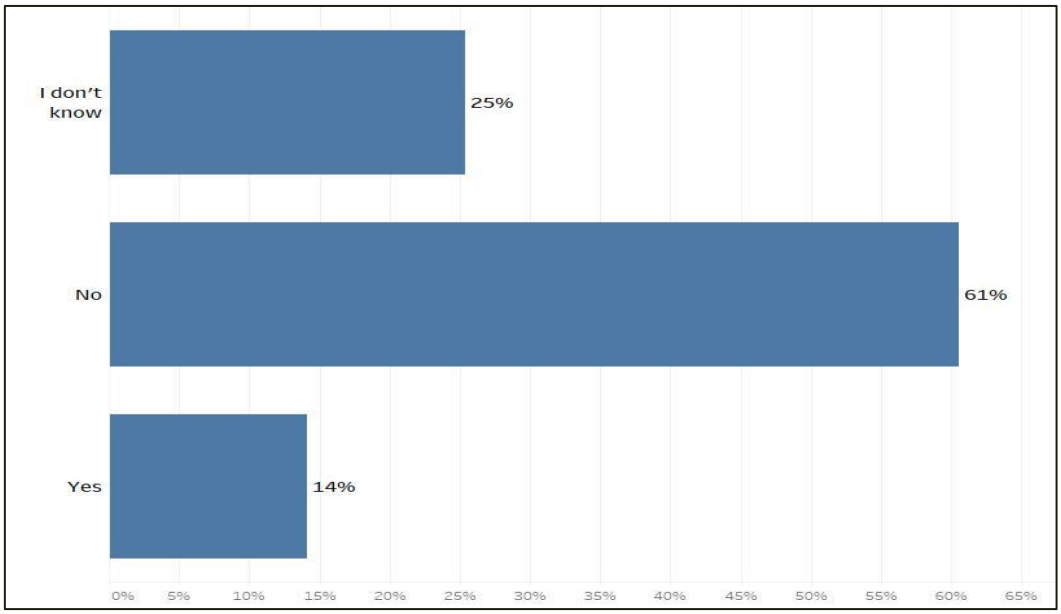

Figure 10: Have your company already applied, or is planning to apply, blockchain technology in some way?

To learn how much participants think blockchain technology will impact their work personally, we asked if blockchain technology could be useful to their work. As displayed in Figure 11, over 60% thought that blockchain technology would be useful to some extent. Specifically, One fifth (20%) thought that blockchain technology would definitely be useful to their work, 24% thought that it probably would be useful and 23% thought it would be useful to some extent. Thirty one (31%) percent were not sure and 3% did not think blockchain technology would be useful for their work.

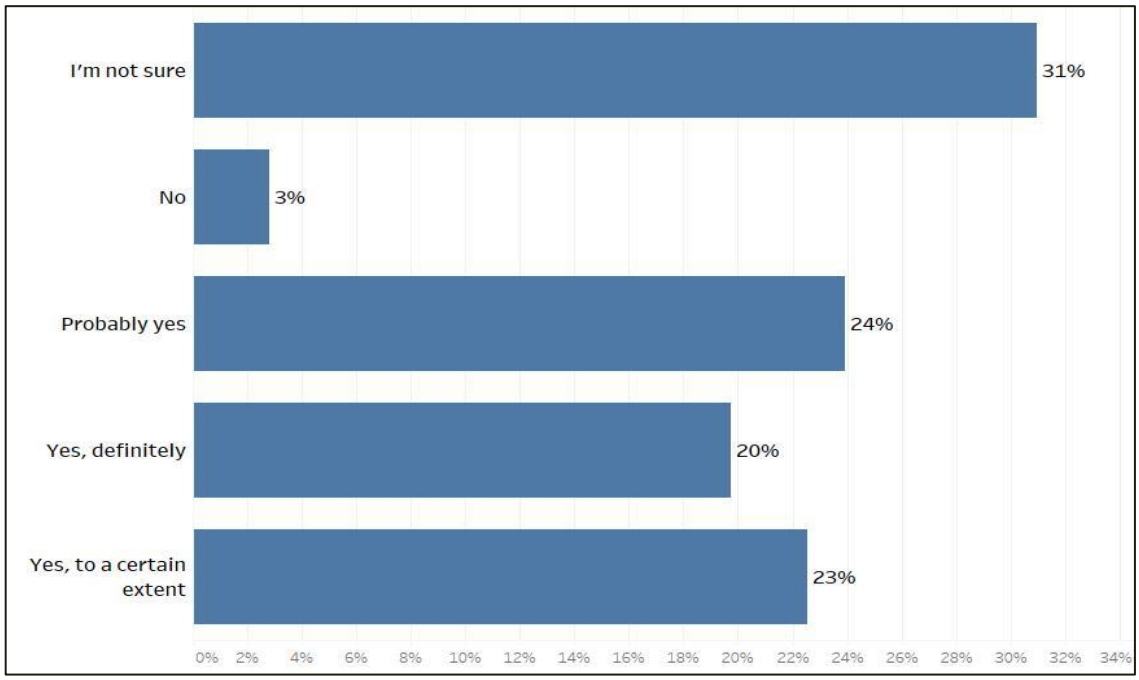

Figure 11: Do you think blockchain technology could be useful for your work?

Participants were then asked to identify which industries would benefit from blockchain technology. Participants were given a list of 20 broad industry categories and were asked to select all industry categories they felt would benefit from blockchain technology. The top 10 most selected industry categories were as follows (as presented in Figure 12): Finance and Insurance (52) and IT industry (47), Telecommunications (26), Wholesale (24), Legal Services (23), Health Care (20), Hotel and Food Services (19), Utilities (18), Retail (18), and Other Information Focused Industries (16).

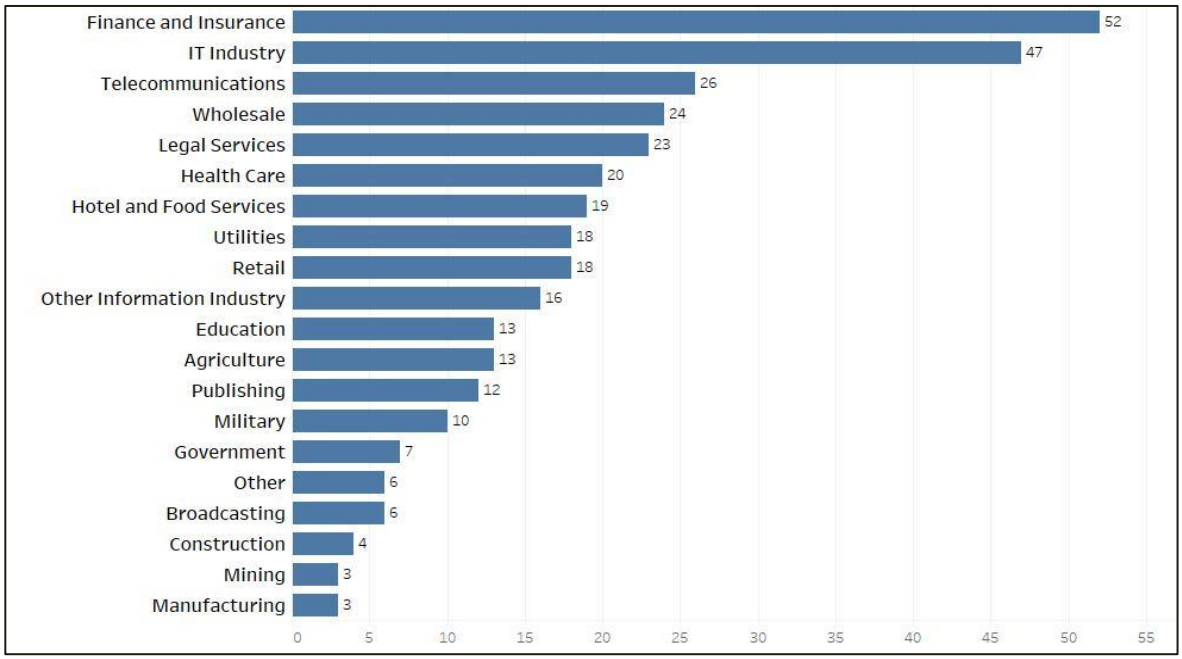

Figure 12: Which industries do you think blockchain technology can create the most value? Please check all that apply

Finally, participants were asked their opinion on the disrupting effect of blockchain technology on the economy in general. Almost three quarters of them answered affirmatively that blockchain technology would have some disrupting effect on the economy (as presented in Figure 13: Definitely – 15%, Probably – 35%, To a Certain Extent - 23%). A minority of 25% were indecisive and 1% did not see any impact.

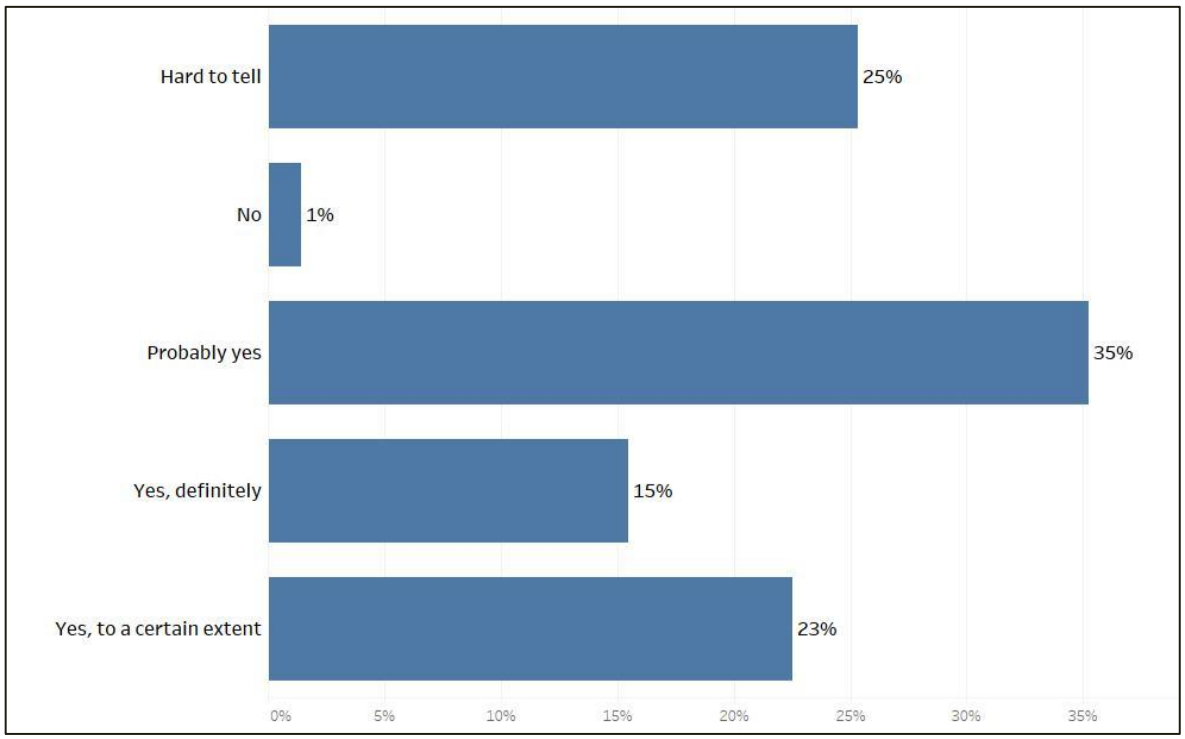

Figure 13: Do you think blockchain will have a major disrupting effect on the economy in the future?

Based on the results of this survey we see that almost 30% of the respondents are not familiar with the blockchain technology or are mistakenly associating it with cryptocurrencies (mainly bitcoin). This result is accompanied by the fact that more than 30% of participants in the survey answered they either never came across an example of blockchain technology application or they are simply not interested in anything more than a bitcoin. In addition to that, only 14% of respondents claimed that their organization applied or planned to apply blockchain technology in some way, while more than 60% confirmed there is no such plan. It is possible that companies in the Croatian market, especially small and medium sized businesses may not see the potential impact of blockchain technology on their organizations. This is appears to be much less so with the Croatian technology companies; however, it is clear that the overall market needs more time (and resources) to understand the potential impact and benefits. However, considering that close to 70% of participants responded they thought blockchain technology could be, at least to a certain extent, useful for their work, and even a higher percentage of respondents expressed their opinion that this technology will have a major disrupting effect on the economy in the future. As more and more global organizations see in which way blockchain may improve their business processes, realize cost savings and competitive advantages, implementation may become more wide-spread. For Croatian companies, it could be a part of an upgrade to digital transformation processes and should enable all of them, including the small ones, to better participate in the global economy.

3. Conclusion

Our aim was to gain some insight into the exposure and impact of blockchain technology among Croatian business leaders. The level of knowledge and awareness about the possibilities of blockchain technology is somewhat questionable – it is still widely recognized and associated to bitcoin and cryptocurrencies in general, resulting in the hype and irrational expectations reflected in the rise and fall of market capitalization of many digital currencies in 2021. Nevertheless, blockchain technology has the potential to empower companies around the world to make business transactions more quickly and efficiently, in a secure, transparent and immutable manner, and the business community has started to realize that. The business value-add of blockchain will exceed $3,1 trillion by 2030, as stated in Gartner's forecast, and the following 5-10 years is the period of large investments in this technology.

The initial common understanding that implementation of blockchain is linked mainly to the IT industry and financial sector has changed significantly in recent years – today it is evident that blockchain technology may have sa ignificant impact on various industries, from public and health services to manufacturing and telecommunications. One of the segments that will presumably have the highest expectations from this technology is supply chain: blockchain adoption could significantly improve the performance of the supply chain system by making it more transparent, secure and reliable. As supply chain consists of many different elements from production plant to the end customer, including all types of industries and services on the way, clearly the importance of potential improvements becomes even more relevant.

Works Citation

Baran, P. 1962. On Distributed Communications Networks, Santa Monica, California:*RAND Corporation*, P-2626, Available at:https://www.rand.org/pubs/papers/P2626.html

Bashir I. 2017. *Mastering Blockchain: Distributed ledgers, decentralization and smartcontracts explained.* Birmingham, UK: Packt Publishing Ltd.

Castro M., and B. Liskov. 1999. Practical Byzantine Fault Tolerance. Proceedings of the third symposium on Operating systems design and implementation, 173-186.

Deloitte. 2018. Breaking blockchain open: Deloitte's 2018 global blockchain survey Availalbe at: https://www2.deloitte.com/content/dam/Deloitte/cz/Documents/financial-services/cz-2018-deloitte-global-blockchain-survey.pdf

Gupta, M. 2018. *Blockchain for dummies*, 2nd IBM Limited Edition, Hoboken, NJ, John Wiley & Sons.

Konstantopoulos, G. 2017. Understanding blockchain fundamentals, part 2: Proof of work proof of stake. Loom. Available at: https://medium.com/loom-network/understanding-blockchain-fundamentals-part-2-proof-of-work-proof-of-stake-b6ae907c7edb

Lamport, L., R. Shostak, R. And M. Pease. 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems* 4 (3): 382-401.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. Available at: https://nakamotoinstitute.org/bitcoin/

Narayanan, B., J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. 2016. *Bitcoin and Cryptocurrency Technologies*, Princeton, NJ: Princeton University Press.

Szabo, N. 1997. *Formalizing and Securing Relationships on Public Networks.* First Monday, 2(9), Available at: https://firstmonday.org/ojs/index.php/fm/article/view/548

Swan, M. 2015. *Blockchain: Blueprint for a new economy*. Newton, MA. O'Reilly Media, Inc.

Vilner, V. 2018. No more hype: Time to separate crypto from blockchain. Jersey City, NJ. Available at: https://www.forbes.com/sites/yoavvilner/2018/11/14/no-more-hype-time-to-separate-crypto-from-blockchain-technology/?sh=435b67b8171c