Society and Economy
DOI: 10.1556/204.2019.007

BLOCKCHAIN AND DEMOCRACY[1]

PETER RACSKO

Department of Information Systems, Corvinus University Budapest, Hungary
Email: peter.racsko@uni-corvinus.hu

In the past few years in many countries people have experienced the erosion of trust in the main pillars of democracy, the voting and election systems. Many authors envisage the blockchain technology as a tool for restoration of trust (Tapscott 2016; Swislow 2016; Shin 2016). Our research is aimed at the potential use of blockchain technology in social systems for enhancing trust and increasing participation. We aim to explore whether the blockchain technology is suitable for voting or elections in large communities and the issues to be addressed for real world applications to leverage democratic rights. Our final conclusion is that there are both theoretical and practical obstacles in the way of such direct applications.

Keywords: blockchain, consensus protocol, voting

JEL codes: C88, D72, O33

1. INTRODUCTION

Blockchain is a collective digital memory of a group of people. It is a secure digital log of a set of transactions. There is no practical method of changing the blockchain with this interference remaining unnoticed for the controllers or the public. We do not provide a comprehensive description of the cryptographic and networking technology used for setting up and maintaining a public blockchain,

[1] This work was created in the framework of the National University of Public Service under the priority project KÖFOP-2.1.2-VEKOP-15-2016-00001 titled “Public Service Development Establishing Good Governance”.

see Satoshi Nakamoto (2008) for this. We do not discuss the economic impact of Bitcoin or other cryptocurrencies either, and only focus on the potential application of blockchain as a basic technology in providing a secure framework for elections and voting systems. Discussion of the technology will only be involved to the degree required for undestanding the content.

The security of the blockchain is provided by a specific information techology. After each addition of new transactions to a blockchain a digital footprint, called hash, is added to the chain. For the full explanation of the technology refer, e.g. to Antonopoulos (2017). After adding a new block to the existing blockchain, a new hash is generated from the previous chain, the past hashes and the new block, thus changing the old transactions afterwards is practically impossible, as the old hashes can be reproduced from intentionally changed data with a probability very close to zero. Computation of the hash values requires some work or other type of resources from the participants, who in turn must be compensated for their effort. Without motivation, perhaps nobody will take care of the maintenence of the blockchain. The method of compensation makes a substantial difference in various applications. For example, the compensation for computing a hash in the Bitcoin system is now 12.5 Bitcoins, and it will drop to 6.25 around 2020. The high compensation is reasonable as the verifiers have not only to generate an ordinary hash, but a very special one, with a prefixed number of leading zeros, and this operation requires a lot of computational power and a bit of luck. The Bitcoins used for compensation are newly minted coins, and they are added to the overall resources. As the number of the required leading zeros increases, the required computational time also increases. In average, the generation of a new block takes approximately ten minutes over the entire Bitcoin network, thus a new block is added to the existing blockchain once every ten minutes. The computation requires not only processing power, but also some luck when generating a random number (called nonce), which is added to the real block in order to produce the hash with the required attributes. The verifiers are in a permanent contest, and the first in the appropriate hash generation is the winner, and their solution is accepted by the others after being broadcasted on the public network. The winner takes the whole incentive. This operation is called Bitcoin mining. One can buy specially designed hardware for Bitcoin mining on the online market or use graphic processor cards. The only restriction for the verification and generation of new Bitcoins is the economic reasoning. The expected win must be bigger than the cost of energy and computer time used for the mining. As the complexity of the mining is continuously increasing, the economic incentive for the verification is decreasing. The consequences of the decreasing incentive for the Bitcoin system are not exactly known, but more than 80% of the possible bitcoin resources have already been found.

We used the Bitcoin example to demonstrate the importance of the verification of the transactions. The blockchain structure and the applications built on the blockchain framework will not operate without a sustainable verification method. In applications different from Bitcoin, several other verification and compensation frameworks might be applied, as for example volunteers, or payed employees, whose job is the computation of hashes (one with much less complexity than in Bitcoin). The hash value can be computed very quickly and easyly even for large blocks, if the specific conditions are not required as in the case of Bitcoin. The ultimate goal of the process is to include all transactions into the blockchain and "stamp" all blocks by a hash code, which is broadcasted on the network and accepted by the participants. This operation makes the fraudulent change of the past history very hard, as the participants "remember" exactly what happened in the past.

The Bitcoin system, however, does not work, if the majority (at least 51%) of the participants decide to cooperate in a cheating action. If the network is big enough, even large consortiums have much less than 51% of the power. It is worth mentioning that if certain conditions are met, cooperation of 25% of the participants is enough for a so-called economic attack (Buterin 2016), which is, strictly speaking, not a technical hack. In a smaller, less public network with a lower number of participants, the necessary condition for operation is the trustworthiness of the majority of the stakeholders.

The role of collective memory is not new in society. The owner and the value of the "coins" on Yap Island in Micronesia for example was stored only in the memory of the local people (Friedmann 1991). The media of exchange were large solid stone wheels, ranging in diameter from a foot to twelve feet. The value of a particular wheel was agreed by the local society based on the work invested in the carving and transportation of the stone. The stone coins had their fixed location on the island, they were never moved even if the owner was changed. When the owner was changed in a sales–purchase transaction the seller and buyer simply informed their fellow villagers about the transaction. Thus the owner and the value of the coins existed only in the collective memory of the local society. The stone money on Yap Island is the "stone-age" predecessor of a contemporary blockchain based cryptocurrency.

The blockchain in fact is a database of all past transactions. The exact copies of the database are stored on several points of the network. Traditional transactional databases are usually set up, operated and fully controlled by a central organization. The fixed location of the database might serve as a well defined target for hackers, who may want to steel or manipulate the data. The database operator organization applies all countermeasures in its possession, but the motivation of the hackers is quite strong. The banks for example make significant effort to prevent malicious actions, but in spite of these efforts, thefts of data or money from banks electronically are not rare events. If those databases were public, anybody could make and store a copy, then anybody could check the integrity of the database by comparing it to the other copies. The distributed storage and lack of a central controlling organization in the blockchain prevents the hacker attacks against, or manipulation of a central database, as the copies of the database exist at several nodes of the network.

A natural question arises when adding transaction data to the blocks, and the change has to be broadcasted on the network. Which node with a copy of the blockchain will decide whether a change is valid or not and which the right order of the transaction is. Transactions may follow each other in a fraction of a second, and, in a payment infrastructure, the order of transactions is vital for obvious reasons. If there is no general consensus on the validity and order of the transactions, the set of blockchain copies are quickly desynchronized and nobody will know which copy is valid.

If the users of the system would agree on a fixed order of the computers verifying the transactions, the first verifier would have a privileged position and could influence the modification of the database on his own. This option clearly contradicts the original principles based on the equal opportunities of the participants. If this privileged computer fails, the whole process will fail. If the participants work out an ordering algorithm, the question is, who decides on the algorithm itself. As one can see, synchronization of all copies on the network is not an easy task if the participants require full agreement on the verification mechanism.

The solution in all cases is a set of rules, accepted by all participants. The name for this set of rules is the *consensus protocol*. An operational blockchain system always relies on its consensus protocol, which determines the nodes that are entitled to iniate or validate the changes on the nodes and the order of transactions. The consensus protocol ensures the synchronity of all nodes at any instant of time and prevents modification or data by any particular node. As a result of the proper application of the consensus protocol, all participants of the blockchain system will have the opportunity to check the integrity of the database.

Each block in a blockchain contains a reference to the preceeding block, and thus the order of the verified transactions is fixed for ever. Using this property, a new participant can reproduce the whole blockchain from the first – genesys – block and may check if the whole blockchain was ever manipulated.

2. VOTING WITH BLOCKCHAINS

Online voting systems with electronic voting hardware have been widely used in some countries, but due to several security and administrative issues have not earned unambigous trust. According to MSNBC (2011), researchers have developed a hack: for about $26 and an 8th grade science education, one can remotely manipulate the electronic voting machines used by millions of voters all across the U.S. Another US newspaper (CS Monitor 2012) asks the question if e-voting machines could be hacked. Security experts say a specific kind of electronic-voting machine is vulnerable to being hacked. Influencing a national election would be difficult, but the advance of malware makes it possible. The HBO documentary Hacking Democracy also challenges the reliability of the online voting.

The application of blockchain in online voting is supposed to increase the embattled trust in electronic voting. Recent research shows the increasing interest in the implementation of blockchain technology in online voting. Many schemes have been proposed, although, unfortunately comprehensive technical documentation is not available. In a paper published by Hardwick et al. (2018), the authors propose a potentially new e-voting protocol that utilises the blockchain as a transparent ballot box. It offers a limited decentralisation and allows for the voter to change/update their vote (within the permissible voting period). The paper also highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage. Ayed (2017) argues for leveraging the open source blockchain technology and proposes a design for a new electronic voting system that could be used in elections. The paper also draws a roadmap for blockchain technology to be able to support complex applications. McCorry et al. (2017) describe a board-room blockchain voting system, the “Open Vote Network”, which is suitable for boardroom elections and is written as a smart contract for Ethereum. Moura et al. (2017), in a conference presentation, argued that the current methods, specially those based on electronic platforms, “provide unsatisfactory levels of transparency to voters, thus harming the trust voters have in their vote being counted by election officials, a problem known as voter confidence.” Instead, they suggest the modernization of state structures by the use of emerging technologies. In a Bitcongress Whitepaper (BitCongress 2016) a bitcoin based voting system was proposed, with further description and criticism in Caiazzo (2016). On their website, the Followmyvote.com (2017) company gives an overview of their ambition “to build a secure online voting platform that will allow for greater election transparency.”

In 2018 blockchain based electronic voting systems were tested in a few countries, the analysis of the results, however, has not been published yet. For example, South Korea developed a blockchain voting system for the private sector that went on trial in December 2018 (Zdnet 2018). Polls in West Virginia's primary election on May 8, 2018 used the first government-run, blockchain-supported vote in US history. The blockchain-based mobile voting platform was only available to a select group of voters (Cointelegraph 2018).

3. CONSENSUS PROTOCOLS

Applied blockchain technology heavily depends on the method of verifying the validity of the blocks. There are several different processes – consensus protocols – for creating a consensus of the stakeholders on the validity of the inspected data. They are different in several aspects, e.g. type and amount of required resources, number of "censors", etc. A consensus protocol is an integral part of the given blockchain application, and thus the application itself in every aspect depends on the protocol. We will analyze the most frequently used consensus protocols of blockchain applications. We will show that none of them is perfect for a blockchain based electronic voting system.

First let us give the high level definitions of the most important protocols. The definitions are descriptive rather than formal as all protocols have variants due to different implementations.

Proof of Stake (PoS): a protocol by which a blockchain network aims to achieve distributed consensus. In PoS-based blockchains, the validator of the transactions is chosen via wealth or another interest in the blockchain ("the stake").

Proof of Work (PoW): the algorithm of proof-of-work-based blockchains solves computationally intensive mathematical tasks (i.e. mining) to validate transactions and create new blocks. The success of the miner depends on their computer resources and luck.

Proof of Elapsed Time (PoET): this algorithm is often used on blockchain networks where the participants compete for the mining rights. Based on random draws, where every node has an equal chance to get the mining rights, the node in the network is required to wait for a randomly chosen time period, and the first one to complete the designated waiting time wins the new block (Investopedia 2018a).

Proof of Capacity (PoC): an algorithm that allows the mining devices in the network to use their available hard drive space to decide the mining rights. The higher the available disk space, the higher the chances of a node getting the mining rights (Hackernoon 2018).

Proof of Burn (PoB): this algorithm works on the principle of allowing the nodes which participate in the verification of the transactios to "burn" or "destroy" the virtual currency tokens, which grants them the right to write blocks in proportion to the coins burnt. Burning a coin means sending the coin to a publicly known address where the coins cannot be retrieved from (Bitcoin.it 2018).

Proof of Activity (PoA): a hybrid of PoW and PoS. In PoA, the mining process starts as a standard PoW process with various miners trying to outpace each other with higher computing power to find a new block. When a new block is found (mined), the system switches to POS, with the newly found block containing only a header and the miner's reward address.

The types of consensus protocols are by no means restricted to the five most popular ones, new, innovative protocols can be invented any time (Ahmed et al. 2019).

Let us discuss some of the details, starting with the Bitcoin consensus protocol (PoW), as the most frequently used application of the blockchain technology. The set of rules in the protocol among others define the types of changes in the database, the time the changes take place and the participants who are authorized to initiate a change, or to make it simple, how and when a block can be added to the blockchain. The rules ensure that the transaction data will be added to the database in an unambiguous, unchangeable way, and the modification is agreed by all participants and no single node or a small group of nodes have the ability to control the addition of the transactions to the blockchain.

The PoW protocol is operated by those active users who sacrifice significant computing resources to participate in the integration of new blocks. They solve a complex computing problem (called mining) and broadcast the result in a way that any other participants can check the validity of the solution in an easy and quick way and they can verify the solution for the public. The acknowledgement helps in the acceptance of the new block and accepts the successful mining operation and compensation of the miner. The application of the PoW consensus protocol is unavoidable with each block, as it provides unambiguity of the transactions to prohibit double spending of the same coin, and the proper order. If someone wants to tamper with a transaction, the copy of the entire blockchain has to be modified and all the past PoWs recalculated, while all other copies will remain unchanged. Technically, for a successful fraud, at least one half of the full computing capacity of the participants is required. As it was proved by Eyal (2013) that a non-technical "economic" attack is possible, i.e. a profit-oriented cartell of participants can cheat the system even if their resources are smaller, then half of the network's capacities.

The expenses associated with the PoW protocol is clearly a disadvantage and the mining activity is limited in time: when the average expense of mining one bitcoin exceeds its value, the incentive for the miners disappears and the consensus protocol will not work any more.

Another popular protocol, *Proof of Stake,* was introduced for another cryptocurrency, Nextcoin. The PoS type verification does not require either significant computing capacity or sacrifying other resources. It does not require much electric power either. As a result, the system is more decentralized in practice as in Bitcoin's case, where the participants with higher resources are in a privileged position. Even a smartphone is capable of verifying a block with the PoS scheme. The Nextcoin application uses a PoS protocol in the following way. A random number generator selects a Nextcoin every 60 seconds (all coins are supplied with a serial number) and the owner of the selected coin is entitled to carry out the verification. If the selected party's computer is online, it collects all new, non-verified transactions, forms a block and broadcasts it on the network. The participant gets a small recompensation. If the computer is offline, a new verifier is selected by the network, and the originally selected person will not be payed. The driving force behind the continuous operation of the Nextcoin system is that people who own more nextcoins will not switch off their computers, as the probability of being selected for verification and compensation is higher, producing a higher income. The number of Nextcoins is fixed from the launch of the system at 1 billion.

In contrast to the case of the PoW protocol, the verifying capacity of a Nextcoin owner is not defined by their computing capacity, but by the actual balance of their account. PoS experts suppose that participants with higher balance are more exposed, and take better care of their investment, as a successful attack against the system reduces the trust in the currency and, consequently, decreases the value of the investment. If a stakeholder (or group of cooperating stakeholders) acquires 51% of all Nextcoins, they are capable of modifying the blockchain. As the total amount of Nextcoins is limited, the market price of a coin will increase due to increased demand, but the exchange value decreases, and fraud will not pay off in the end. In the case of the PoW protocol, for a successful fraud a high concentration of resources is required, and the unit cost of the resources is decreasing as the concentration is increasing. As a result, the unit cost of increasing one's influence is decreasing in the PoW process, while it is increasing in the case of PoS.

4. POTENTIAL USE OF THE BLOCKCHAIN TECHNOLOGY IN AN ONLINE VOTING SYSTEM

In an online voting system a vote cast is equivalent to a transaction. Each transaction is attached to a blockchain. With the use of a proper consensus protocol (e.g. PoW or PoS), the blockchain cannot be tampered with and if a vote is lost, or added afterwards, it will be evident for all participants. The final result should be accepted by everyone, as everyone can check whether there were illegal votes, or anyone changed the votes, and in addition all votes were counted once and only once.

There is no doubt that the application of blockchain technology solves a few problems raised in the election practice of quite a few countries. For example, in the year 2000 in Florida the votes had to be recounted, the same event happened in 2016 in a few other states of the USA. Also, it became obvious that hackers can influence the online voting systems or other information resources of the elections. The supposed mistakes or hacker activities did not change the results in 2000 or 2016, but the trust in the fairness of voting systems was challenged, and there are no sure methods to restore perfect trust.

According to the critics of the electronic voting systems, undisputed security is provided only by a paper-based process. In a contemporary society, however, voters do not want to wait weeks for the results, and there is no way to ensure the fairness of the counting process. It is impossible to detect fraud, changing a vote or adding illegitimate votes. The fairness of the system fully depends on the fairness of the participating humans, and a relatively small group of people who are responsible for the counting are in a position to influence the results. The larger the number of voters in a paper based system, the option for cheating is higher because of the growing complexity of the control.

Application of the blockchain technology, however, could ensure the fairness of the voting with a high statistical confidence, with a probability close to 1. Each voter can check that the votes were not manipulated with a probability close to 1, and in this case there is no need for recounting the votes which challenge the trust in the system. Another advantage is the immediate final result. The blockchain technology, however, is a real tool only for an election if it is designed and implemented in a pragmatic way. The remainder of this paper discusses the practical problems of the real applications.

5. TRUSTLESS SYSTEMS

The concept of trustless systems is very intriguing. A trustless system works without the need for confidence in the elements of the system. We discuss the pragmatic aspects of trustlessness. A computerized transaction system as an IT application – e.g. money transfer – is traditionally based on the fact that the source of the transaction, the communication infrastructure and all their elements and networks, and the people working on the system and also all organizations involved are reliable. Reliability means in this context that the risk of deliberate or random mistakes is acceptable by the users. Either the potential impact of an incident is negligible, or the probability of the occurence is small, or there is a third party, e.g. an insurance company, which reimburses the damage.

Traditional money transfers are considered reliable as the banks carry full responsibility for the the infrastructure and the successful transactions. Trust in the banking system is enhanced by the knowledge that not only the bank, but a third party, for example the government or an insurance company warrants the transaction. The error-free, reliable operation is the direct business interest of the operating organization.

The examples of loosing trust in the monetary systems, as it happened in 2008, raised the question of the existence of a real transactional system where trust is not a necessary condition of the operation, where the participants are not supposed to trust each other or the system itself. The blockchain construction is one of the candidate solutions. In the case of Bitcoin, the validity of all transactions can be checked by each participant, everyone can be sure that no errors were made or nobody has tampered with the data. In the Bitcoin system, the initiator of a transaction broadcasts electronically signed transactions and the validity of the signature can be checked by all parties. Unvalidated transactions are simply deleted by the system. The block of transactions are validated by the miners, and the validity can be checked by the parties. If the block is accepted along the consensus protocol, there is little chance of modifying it.

A blockchain system, as it is used for cryptocurrencies, is in fact a distributed trust system rather than a trustless system (Tomaino 2016). The participants actually have to trust several parties: the validators of the transactions, the strength of the applied cryptographic methods, the developers who maintain and improve the code, and the users of the platform. But the trust is distributed, and so no single party is trusted.

In theory, the consensus protocol of Bitcoin or similar mechanisms provide the condition for a distributed trust operation, at least in theory it does not require the participation of a single third trusted party. But the system does not exclude the existence of a third trusted or untrusted single party. The “Hard Fork” operation of the Ethereum cryptocurrency in 2016, however, proved that the past of the blockchain can be changed (Coindesk 2016a). The Hard Fork was carried out by the founders in order to retrieve 60 million USD stolen by hackers who exploited a vulnerability in the software. The controversial action proves that central censorship is not unthinkable and the participants have to trust the founders.

As it is clearly shown by Noizat (2015): “existing electronic voting systems all suffer from a serious design flaw: They are proprietary, that is, centralized by design, meaning there is a single supplier that controls the code base, the database, and the system outputs and supplies the monitoring tools at the same time", which contardicts the idea of distributed trust.

Nevertheless, blockchains can help in the auditability of the voting system, as the changes at least do not remain undetected. But there is a necessity for a proper and practical consensus protocol, accepted by the participants. We shall discuss further the potencial application of consensus protocols for the voting systems. In our opinion, blockchain technology does not fully eliminate the risks associated with voting, but rather rearranges the risk landscape.

6. SYSTEM-LEVEL RISK: ECONOMIC ATTACK

We call this type of risk economic, as the potential for a successful attack was proved in the case of Bitcoin. Eyal and Sirer (2015) demonstrated that a fraudulent, but profitable strategy of a relatively small number of partcipants can motivate others to join the cheater's group and manipulate the blockchain, as the expected profit of the cheating group is higher than that of the honest participants. When the group controls 51% of the resources it can modify the blockchain. The strategy is not perfect (Buterin 2016) but in the case of an election, where a small number of groups are fighting for full control, the risk is clear. As simulation experiments show, 25% of the participants can take over the control of the system.

7. SECURITY RISKS

The blockchain infrastructures are information systems and perhaps they are not free of vulnerabilities. Weak points of Bitcoin for example are discussed in Bitcoin.it (2019), but we can add further risk factors, as the denial of service attack, or a specific Sybill attack, when a computer runs several clients simultaneously for increasing its impact. Another risk factor is the "timejacking", attack, when the hackers tamper with the network time and the transaction timestamps will be invalid. Well known targets are the wallets, protected by relatively weak cryptography, weak signature key exchanges, and signature programs. All known types of attacks can be repelled, but the potentially high profit of a successful attack against Bitcoin is enough motivation for innovative solutions.

8. PRACTICAL PROBLEMS OF THE BLOCKCHAIN APPLICATION IN THE VOTING SYSTEMS

The blockchain technology is clearly not enough for building an end-to-end secure and trusted voting system. In an online voting environment, the voter has to certify their authority for voting, and the electronic documents, certifying the right to vote, must be distributed in a procedure outside the blockchain framework.

This detail is different from the principles applied in the currency systems where the right of spending a coin is certified within the system, as the result of the distributed trust. The external authorization contradicts the principle of trustlessness, or more exactly, distributed trust, when trust is distributed among a large number of participants and thus ensures fair operation. Of course, multiple voting or the loss of votes can be easily prevented by the PoW and PoS protocols in a blockchain framework.

There are a few businesses and nonprofit foundations on the market which develop and offer a blockchain based voting system as a service (FollowMyVote.com 2017). For the time being, however, there are no systems applicable for practical purposes. The blockchain technology might be a promising technological basis of a trusted and fast online voting system in the future, but there are quite a few theoretical and technical problem yet to be solved. For the certification of the voting right of a person, an identity card with a chip might be a solution, as the card contains a tamper-proof personal identifier, and the right to vote might be obviously defined. Of course, there is a need for a central authorization database with the identity data of the legal voters. The voters must trust the owner of this central database, thus the trustlessness or distributed trust of the system does not exist anymore, as the voters must trust the operator of the authorization database.

Consequently, in case the whole system should be fully controlled by the voters, the database of the voters' credentials should be operated on a blockchain. That is, the official voters' registers should be organized on a blockchain and the authorizations assigned in a normative, controllable way. Yet, the problem of concensus protocols needs to be dealt with. Neither the present speed nor the mode of operations are applicable in real voting systems.

In the case of Bitcoin, the use of the PoW protocol assumes that joining a new block of approximately 700 transactions takes 10 minutes, the size of a block is 1 MByte, the number of transactions per second is between 1 and 3.5 seconds when transactions are of average size. These parameters are not controlled by a central computer device or organization, but are determined by the required computing time according to the complexity of the work and the communication time. With the overall growth of computing power, the 10 minute period could decrease, but in this case the complexity of proof is automatically increased by the system. These limitations of course are not very friendly, and the need for an easily scalable consensus protocol arises.

Eya et al. (2016) define a “next generation” (NG) algorithm, where the delay depends only on the data transfer, and the quantity of transferred data is defined by the processing capacity. If the NG algorithm can prove its advantages in the future in a real environment, the low speed of the blockchain operation will not be an obstacle to practical applications.

Another question to deal with is who will reimburse the costs occured in the verification, who will pay the verifiers for using a considerable amount of computing resources and electric power, even in the case of scalable PoW protocols. The present form of the PoW protocol, even its NG version, is hardly applicable in a voting framework.

Let us discuss other consensus protocols and their practical use. The basic assumption of the PoS protocol is that a great number of participants are continuously active, i.e. they are online. However, if the majority of the voters want to sabotage the system they can go offline and the increasing number of transactions to be verified will slow down the system, and perhaps a specific denial of service situation might occur. The problem of rewards is also an issue. In a voting system each participant has only one vote and thus no one has a greater incentive than the others to use resources for the verification. Thus, the important motivation factor that operates the cryptocurrencies with the PoS disappears.

The PoET protocol was proposed by the Intel Corporation. The algorithm is similar to the PoW procedure, but with much lower energy consumption. The new blocks are created on the specific hardware designed by Intel for this purpose but it does not require computationally intensive solution of mathematical problems (Coindesk 2016b). This is clearly not a trustless or distributed trust solution, as the participants have to trust the hardware manufacturer as a third party. The majority of the blockchain users, however, share the opinion that the blockchain and trustlessness (or at least distributed trust) go together.

The PoC protocol is a form of the “pay for the participation scheme”, similar to PoW. The potential verifier pays with their storage capacity. The bigger the storage capacity offered by the participant, the greater the probability of being selected as a verifier of the next block, and being reimbursed for the work. The cryptocurrency Burstcoin uses the PoC protocol. In a real voting procedure it is hard to suppose that a significant number of voters will offer storage capacity without the reward. A small number of verifiers, however, does not ensure the random distribution of trust.

In case of PoB, someone who wants to participate in the validation procedure has to pay for the activity into a central wallet. The one time payment is “burnt”, as nobody gets back the money, it only ensures the right of participation in a random draw where the winner is entitled to verify a block and be rewarded. Payment is accepted either in the native currency or in currencies external to the system. Those participants paying more have a higher probability in winning, i.e. being selected for the verification and rewarded. As the number of contributors increases, the chances of being selected decrease, and so if one wants to keep their position, they have to make additional payments. The systems was used by the cryptocurrency Slimcoin, with a very moderate success. This protocol clearly contradicts the democratic principles of a contemporary voting system, as you can buy rights for money in this framework. The chances are not equal.

The PoA protocol is a combination of PoW and PoS (Investopedia 2018b). Construction of PoA was motivated by the limitation of the amount of Bitcoins in the future (the limit is approximately 21 million coins). If the limit is reached, the interest in mining and verification disappears, as there will be no reward for the verification of the blocks or, to be more exact, the reward for the verification will be less than the cost of energy used in the mining process, and the system will fail. The combination of PoW and PoS is a potential option for the solution. In the process, the verification is carried out with the PoW protocol, but instead of verifying the real transactions, a sample which does not contain transactional data is verified. The “winning” block contains only the proof of the work and the verifier’s identification. When the winning block is constructed, the system changes to the PoS protocol and randomly selects a group of participants, who are entitled to accept or reject the proof of the work. The probabilty of the selection of a participant is higher if they own more coins on their account, as the random selection is based on the coins rather than the participants. The sample becomes a valid block after the approval of the selected participants. If one or more of the selected nodes are not available, then the next winning block becomes active and a new group of participants will be drawn. The selection iterates until it reaches the requested number of approvals for a winning block. The reward is shared between the verifiers and the participants who approve the verification. As of today, the cryptocurrency Decred uses this protocol. In a voting system, the PoA protocol is not an option, as there are no guarantees in the counting procedure and the cost of the verification is also not covered by the system.

9. CONCLUSION

The consensus protocols are inseparable parts of a practical blockchain system. Without an efficient and secure protocol, the technology is useless. We have discussed the applicability of popular and less popular protocols in a real voting environment. The analysis suggests that the protocols currently in existence are inadequate for direct use in a voting system. With all known protocols, the participants who want to play an active role in the verification of the correctness of transactions have to sacrifice resources (computing time or money), or have to have a certain level of wealth, or open capacities to the public, etc. Besides the right in the verification process, they are also rewarded. In democratic voting, however, all voters must have the same rights in all aspects, their differerentiaton based on their activities is not an option.

If we want to use blockchain for voting, it is necessary to create a new consensus protocol that creates equal rights for everybody. The verification, however, should be rewarded, because the system will not work without this motivation. As of today, all protocols satisfying the condition of equal rights and equal motivation might be operated only outside the system and of course, the consensus protocols and their management must be transparent.

The blockchain technology without a consensus protocol, as a distributed, integration preserving database naturally can be used in an electronic voting system, if an external organization, e.g. a government certfication center validates the transactions (Barnes et al. 2015).

The blockchain as a database and a certification center might comprise a working model of the online voting if the voters trust an organization, which they cannot directly audit or contol. Here the auditing of the blockchain is possible only by a central organization. The online voting in this framework perhaps is more efficient and cost effective than the paper based voting, but the role of central control is unavoidable and on the system level does not rule out manipulation. For millions of Bitcoin and other cryptocurrency users, however, the lack of a central controlling organization – e.g. a bank – is actually the most attractive property of the system.

We have proved that none of the frequently used consensus algorithms fully comply with the requirements of an online voting system. The consensus on the correctness of the blockchain and anonimity of the voters are only necessary, but not sufficient conditions for a real life voting. The blockchain technology has a real potential in developing a secure, trusted and inexpensive voting system, but there are many theoretical and practical issues that have to be dealt with before the technology will be accepted even for testing.

REFERENCES

Ahmed, M. – Kostiainen, K. (2019): Don't Mine, Wait in Line: Fair and Efficient Blockchain Consensus with Robust Round Robin. *arXiv*: 1804.07391v2 [cs.CR].

Antonoupoulos, A. M. (2017): *Mastering Bitcoin*. O'Reilly Media.

Ayed, B. (2017): A Conceptual Secure Blockchain-based Electronic Voting System. *International Journal of Network Security & Its Applications* 9(3): 1–9.

Barnes, A. – Brake, C. – Perry, T. (2015): Digital Voting with the Use of Blockchain. Technology University Plymouth. https://www.economist.com/sites/default/files/plymouth.pdf, accessed 31/01/2019.

Bitcoin.it (2018): Proof of Burn. https://en.bitcoin.it/wiki/Proof_of_burn, accessed 31/01/2019.

Bitcoin.it (2019): Common Vulnerabilities and Exposures. https://en.bitcoin.it/wiki/Common_Vulnerabilities_and_Exposures, accessed 31/01/2019.

BitCongress (2016): BitCongress Whitepaper: Control the World from Your Phone. http://www.bitcongress.org/BitCongressWhitepaper.pdf, accessed 31/01/2019.

Buterin, V. (2016): Selfish Mining – A 25% Attack against the Bitcoin Network, https://bitcoinmagazine.com/articles/selfish-mining-a-25-attack-against-the-bitcoin-network-1383578440/, accessed 31/01/2019.

Caiazzo, F. – Chow, M. (2016): A Block-Chain Implemented Voting System, http://www.cs.tufts.edu/comp/116/archive/fall2016/fcaiazzo.pdf, accessed 31/01/2019.

Coindesk (2016a): The Hard Fork: What's about to Happen to Ethereum and the DAO. https://www.coindesk.com/hard-fork-ethereum-dao, accessed 31/01/2019.

Coindesk (2016b): Intel is Winning over Blockchain Critics by Reimagining Bitcoin's DNA. http://www.coindesk.com/intel-winning-blockchain-critics-reimagining-bitcoins-dna/, accessed 31/01/2019.

Cointelegraph (2018): US: West Virginia Completes First Blockchain-Supported State Elections. https://cointelegraph.com/news/us-west-virginia-completes-first-blockchain-supported-state-elections, accessed 31/01/2019.

CS Monitor (2012): Could E-Voting Machines in Election 2012 be Hacked? Yes. https://www.csmonitor.com/USA/Elections/2012/1026/Could-e-voting-machines-in-Election-2012-be-hacked-Yes, accessed 31/01/2019.

Eyal, I. – Gün Sirer, E. (2013): Majority Is Not Enough: Bitcoin Mining is Vulnerable. *arXiv*: 1311.0243v5 [cs.CR].

Eyal, I. – Gencer, A. E. – Gün Sirer, E. – van Renesse, R. (2016): Bitcoin-NG: A Scalable Blockchain Protocol. *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation*. Santa Clara, CA, USA.

FollowMyVote.com (2017): Follow My Vote: The Online Voting Platform of the Future. https://followmyvote.com, accessed 31/01/2019.

Friedman, M. (1991): The Island of Stone Money. *Hoover Institution Working Papers in Economics* E-91-3.

Hackernoon (2018): BitcoinBurst, Part 3: Proof-of-Capacity, The Green Alternative? https://hackernoon.com/burst-part-3-proof-of-capacity-the-green-alternative-8e2651211671, accessed 31/01/ 2019.

Hardwick, F. S. – Apostolos, G. – Akram, R. N, - Markantonakis, K. (2018): E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *arXiv*: 1805.10258v2 [cs. R].

Investopedia (2018a): Proof of Elapsed Time (Cryptocurrency). https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp, accessed 31/01/2019.

Investopedia (2018b): Proof of Activity (Cryptocurrency). https://www.investopedia.com/terms/p/proof-activity-cryptocurrency.asp, accessed 31/01/2019.

McCorry, P – Shahandashti, S. F. – Hao, F. (2017): A Smart Contract for Boardroom Voting with Maximum Voter Privacy in International Conference on Financial Cryptography and Data Security. In: Kiayias, A. (ed.): *Financial Cryptography and Data Security. Lecture Notes in Computer Science.* Cham: Springer, pp. 357–375.

Moura, T. – Gomes, A. (2017): Blockchain Voting and Its Effects on Election Transparency and Voter Confidence. *Proceedings of the 18th Annual International Conference on Digital Government Research*. New York, NY, USA.

MSNBC (2011): It Only Takes $26 to Hack a Voting Machine. http://www.nbcnews.com/id/44706301/ns/technology_and_science-security/t/it-only-takes-hack-voting-machine/#.XM1oPGN7nX4, accessed 31/01/2019.

Noizat, P. (2015): Blockchain Electronic Vote. In: Lee, D. (ed.): *Handbook of Digital Currency*. Elsevier, pp. 453–461.

Satoshi, N. (2009): Bitcoin: A Peer-to-Peer Electronic Cash System https://bitco.in/pdf/bitcoin.pdf, accessed 31/01/2019.

Shin, L. (2016): New Initiative Aims to Eliminate Corruption with Blockchain Technology. https://www.forbes.com/sites/laurashin/2016/06/20/new-initiative-aims-to-eliminate-corruption-with-blockchain-technology/#4c7f48413094, accessed 31/01/2019.

Swislow, D. (2016): What the Blockchain could Mean for Democracy in the Digital Age. https://www.demworks.org/what-blockchain-could-mean-democracy-digital-age, accessed 31/01/2019.

Tapscott, A. (2016): Blockchain Democracy: Government of the People, by the People, for the People. https://www.forbes.com/sites/alextapscott/2016/08/16/blockchain-democracy-government-of-the-people-by-the-people-for-the-people/#6fde228c4434, accessed 31/01/2019.

Tomaino, N. (2016): Trustless is a Misnomer. https://medium.com/@ntmoney/trustless-is-a-misnomer-956066661b79, accessed 31/01/2019.

Zdnet (2018): South Korea to Develop Blockchain Voting System. https://www.zdnet.com/article/south-korea-to-develop-blockchain-voting-system/#ftag=RSSbaffb68, accessed 31/01/2019.