An analysis of consensus algorithms for transactions validation in blockchain system

1st Edis Mekic
Depatramnt Technical Sciences
State University of Novi Pazar
Novi Pazar, Serbia
emekic@np.ac.rs

2nd Safet Purkovic
Depatramnt Technical Sciences
State University of Novi Pazar
Novi Pazar, Serbia
spurkovic@np.ac.rs

***Abstract*—Block chain systems and their implementation are in the focus of the it business community. In order to promote and combat technological and economical challenges Blockchain systems adopted different ways to validate effects of the system members. This work will analyze Proof of Work (PoW), Proof of Stake (PoS) and Proof of Burn (PoB) in top blockchain systems.**

Keywords—Block chain, Proof of Work (PoW), Proof of Stake (PoS) and Proof of Burn (PoB)

I. INTRODUCTION

Creating secure ledger system, without third party control over data stored in same, is in the focus of economical, mathematical and computer technologies research. Development of Blockchain technology provided one possible answer for this problem and bonded all those scientific disciplines.

Blockchain technology provided decentralized transaction system for keeping ledger inputs. New inputs in the block chain ledger are possible only after confirmation from majority of network members. Public ledger is accessible to all computers of the network or nodes. Simultaneously nodes are anonymous and system provides higher level of security in process of confirmation of transaction then traditional ledger systems [1].

Transactions in Blockchain system are grouped in blocks. Security of block creation and validation process are based on cryptographic hash function. Hash functions are special class of mathematical function with certain properties suitable for use in cryptography. Hashing is a mathematical algorithm that maps data of arbitrary size to a array of fixed size bits size (a hash). This algorithm is a one-way function, that is, a function which is infeasible to invert.

The only way to recreate the input data from an ideal cryptographic hash function's output is to attempt a brute-force search of possible inputs to see if they produce a match, or use a rainbow table of matched hashes [2].

New block reference older block by solution of hash function and this solution is header of older block. Speed of the calculation of the proper solution is important issue in Blockchain implementation. If we can provide more possible solutions of hash functions in time period provide better chances for acquiring exact solution.

Blockchain systems require also consensus for validation of transaction, as additional level of security. Only after majority validates transaction change in data within Blockchain systems is approved. This consensus is provided by the majority of the machines interconnected in P2P networks. These machines solve hash functions and submit solution to network until successful solution is calculated. Creation of new block into block chain, need considerable calculation power of the computers interconnected in (P2P) network [3].

Several different approaches are proposed for vslidation of the calculation in Blockchain systems. Thre most noticable are Proof of Work (PoW), Proof of Stake (PoS) and Proof of Burn (PoB). We will nalyse adoption measure and energy efficence in the blockchain sytems with highest market capitalisation in the moment of preparing this research.

II. METHODOLOGY

We will define three important proof which are used in top Blockchain systems. first is Proof of work (PoW) which a system that requires a not-insignificant but feasible amount of effort in order to deter frivolous or malicious uses of computing power, such as sending spam emails or launching denial of service attacks. The concept was subsequently adapted to securing digital money by Hal Finney in 2004 through the idea of "reusable proof of work" using the SHA-256 hashing algorithm. Second is Proof of Stake (PoS) concept that states that a person can mine or validate block transactions according to how many coins they hold. This means that the more coins owned by a miner, the more mining power they have. And finally Proof of Burn (PoB) is one of the several consensus mechanism algorithms implemented by a blockchain network to ensure that all participating nodes come to an agreement about the true and valid state of the blockchain network. This algorithm is implementing in order to avoid the possibility of any cryptocurrency coin double-spending. Proof of burn follows the principle of “burning” the coins held by the miners that grant them mining rights.

Than we will analyze top twenty Blockchain systems based on their market capitalization, and which type of the validation systems they support. Also we will analyze energy efficiency of implemented validation systems.

III. CONSENSUS AGLORITHMS

Oldest, and first anticipated consensus protocol was proof of Work protocol presented in Bitcoin whitepaper [4]. Consensus protocol is based on scanning values which when hashed have as result hash starting with zero bits. In order to achieve this we add a nonce to the original value, until we receive hash witch start with requested number of zero bits. Once the nonce is found and PoW satisfied, block cannot be changed without redoing work for that block and all consequential blocks. In this system all blocks are based on first genesis block, they all except first have hash which consist from all previous blocks hashes and nonce required to create zero bits. Genesis block hash have all zero value [5].

Other important consensus algorithm is proof of Stake (PoS). This algorithm was proposed in 2012 as hybrid system [6]. In order to fully implement PoS, initial coin must be created using PoW, and then system is upgraded to PoS. Within PoS coin age is defined as Coin-days. So if someone hold 10 coins per 100 days he have 1000 Coin-days. When coin is used in transaction age of coins is reseted to value zero. In PoW systems chin with most work delivered to system is main chain, in PoS this is system with highest consumed coin age.

Finally Proof-of-burn (PoB) is algorithm in which we can destroy cryptocurrency in a verifiable manner. Despite its well known use, the mechanism has not been previously formally studied as a primitive. It consists of two functions: First, a function which generates a cryptocurrency address. When a user sends money to this address, the money is irrevocably destroyed. Second, a verification function which checks that an address is really unspendable.

Important issue is energy consumption of blockchain systems, since they use huge amount of calculation power. Exact nature of saving are hard to calculate since we have different computational machines energy efficiency. Design of the validating algorithm provide information that PoW require most energy. Proof PoB, is variation of PoW without energy vaste. Miners who decide to burn coins are in the game for acquiring new one without additional calculation. And PoS is comparable with this two highly energy efficient [8].

IV. RESULTS AND DISCUSSION

From analysis we expect clear overview of the level of acceptance and dominance of the validation methods in the top 12 Blockchain systems. We will analyze different implementation of PoW, PoS and PoB. Especially we will analyze trends in the systems which changed validation method. We will analyses Hash rate change and impact on market capitalization. Exemplar model will be Ethereum network since usage of this system is basis for DeFi systems and smart contract implementation. Etherum network change validation system from PoW toward PoS.

First we will present overview of the validating algorithms in the Blockchain systems with highest market capitalization.

Blockchain systems	Validating algorithm
Bitcoin	PoW
Ethereum	PoW - PoS
Cardano	PoS
Binance Coin	PoS
XRP	RPCA
Dogecoin	PoW
Polkadot	PoS
Uniswap	PoS
Bitcoin Cash	PoW
Monero	PoW
Litecoin	PoW
Stellar	SCP
SlimCoin	PoB

It is obviously that more and more leading Blockchain systems use PoS over PoW algorithm. We will overview presented algorithms in terms of security, scalability and power consumption.

Security of blockchain depend on the number of calculating power or stake holders level in order to successfully attack Blockchain system. Different attack modes are well researched for the PoW systems. Most common is 51% attack were compromising party achieve majority calculating power in system. While this type of attack is feasible in early stage of Blockchain implementation, after some period of time this type of attack become overly expensive.

Ways to compromise are based on generating a block in PoS. In other words, in order to maximize the benefits, validators could generate conflicting blocks on all possible forks with nothing at stake. This problem is commonly referred to as the nothing at stake attack. This attack slows down the consensus time in the network and thus reduces the efficiency of the system. Moreover, it results in blockchain forks which weaken the ability of the blockchain to resolve double spending attacks and other threats.

The “Long Range” Attack Long range attacks on PoS (also known as history attacks) refer to the case where an attacker tries to alter the blockchain history by creating a fork from an already generated block. While this attack in theory requires an attacker that controls the majority of stake in the network, long range attacks can be practically instantiated if the attacker controls/compromises accounts that have no stake at the moment, but have a large stake at some past block height. For example, an account that had 30% stake at block height and no stake at block height+ 1 can still use his 30% stake to re-generate another block at height. This allows an attacker to create forks from past blocks that can overtake the current chain with (past) majority stake.

maximal number of transaction per second is important issue in usability of Blockchain systems. Transactions within PoW systems are limited by block size. Measuring TPS are limited, we do not have verifiable sources for this, and only way to presume exact value of TPS is from tests and whitepapers. Author of this resources are usually form creators of cryptocurrencies.

Other important issue for Blockchain systems is energy efficiency, since well established Blockchain systems like Bitcoin based on PoW demand extremely high calculation power. This demand increased low energy efficiency and high power consumption. We will compare energy efficiency of the PoW, PoS and PoB system and try to put in line for future implementation.

V. PRELIMINARY CONCLUSIND

Preliminary analysis showed that PoW algorithm which is most popular consensus algorithm, slowly showed sings of age and list of different limitation. Most promising validating algorithm is PoS, which will in future replace PoW. Most important reason are better security, better scalability and higher energy efficiency.

REFERENCES

[1] Zyskind, G., & Nathan, O. (2015, May). Decentralizing privacy: Using block chain to protect personal data. In Security and Privacy

[2] Chen, R. Y., & Tu, J. F. (2019). The Computer Course Correlation between Learning Satisfaction and Learning Effectiveness of Vocational College in Taiwan. Symmetry, 11(6), 822.

[3] Mekić, E., Purković, S., &Lekpek, A. (2018). COST BENEFIT ANALYSIS OF COMPROMISING LEDGER SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY. BizInfo (Blace) Journal of Economics, Management and Informatics, 9(2), 27-38. http://dx.doi.org/10.5937/bizinfo1802027M

[4] S. Nakamoto, "Bitcoin: A Peer-to-peerr Electronic Cash system" 2008 [online] https://bitcoin.org.bitcoin.pdf

[5] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO) (pp. 1545-1550). IEEE.

[6] King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. self-published paper, August, 19, 1.

[7] Karantias, K., Kiayias, A., & Zindros, D. (2020, February). Proof-of-burn. In International Conference on Financial Cryptography and Data Security (pp. 523-540). Springer, Cham.

[8] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. In 2017 IEEE international congress on big data (BigData congress) (pp. 557-564). IEEE.