Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 199 (2022) 580–588

Procedia
Computer Science

www.elsevier.com/locate/procedia

The 8th International Conference on Information Technology and Quantitative Management (ITQM 2020 & 2021)

Decision Making using the Blockchain Proof of Authority Consensus

Manuel Adelin Manolache*, Sergiu Manolache*, Nicolae Tapus*

[a]Politehnica University of Bucharest, Str.Splaiul Independentei nr. 313, 060042, Bucharest, Romania

Abstract

As the modern world migrates towards an interconnected environment, be it financially, socially, or industrially, the need for distributed systems has become paramount. Emergent paradigms need decentralized solutions to better handle the single point of failure problem, one example is given by the Internet of Things (IoT), in which devices need to be connected to a central hub to function, or the secure decision making process. Blockchain comes with the solution that overcomes some of the shortcomings in existing systems and provides a secure alternative when designing decentralized systems. This paper proposes a decision making system based on the Proof of Authority consensus protocol enabled by the blockchain paradigm.

Keywords: *Integrated Decision Making Environment Using Blockchain, Collaborative Decision Making, Fuzzy Logic Ranking, Proof Of Authority Consensus, Decision Making Blockchain*

1. Introduction

Most existing decision systems require a central management entity to oversee and plan certain details in the decision making process. One example of this is the Internet of Things, which through a fast internet and smart devices, provided a new paradigm, allowing devices that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices, systems over the Internet or with a central management hub. One big caveat of this paradigm is its reliance on a centralized system to manage all the connected devices [1][2].

In the first part of this paper a general overview of the blockchain technology is presented, highlighting the general aspects, but also detailing its use in modern decision making systems, showcasing key concepts and features that can be used in creating a new platform. Going further this paper lists how certain decisional blocks based on the decision blockchain can be improved, incorporating a ranking method which considers the user specialization, relying on fuzzy logic to measure the overall experience and expertise of the participants.

The method proposed in this paper takes key concepts from the blockchain, such as its transparency and incorruptibility and applies them to a decision making system, in which the ranking of a decision is determined

* Corresponding author. Tel.: +4-076-534-0534
E-mail address: manuel2001ro@yahoo.co.uk; manolachesergiu@yahoo.com; nicolae.tapus@upb.ro

10.1016/j.procs.2022.01.071

by all the participants, while providing a superior voting power to the most specialized and experienced participant.[3]

Finally, different results will be analysed, by showcasing some test scenarios which will run in the Quorum network, and detailing performance based on the aforementioned criterion. This paper comes with a new approach when it comes to decision making, using the strengths of different technologies and merging them in a new system.

2. Blockchain in decision making systems

Two of the most important features that lead to the popularization of the blockchain technology, which has applicability to decision making systems, are [4]:

- Incorruptibility - local modifications of the data cannot alter the history and validity of the chain as it will create inconsistency between the altered blockchain and all the other nodes of present in the network
- Transparency - this is provided by the sharing of data between all the nodes of the network, allowing everyone to monitor the validity of the transactions and the whole history of transactions at any moment in time.

Even though at first the blockchain technology was used in the crypto-currency systems, specifically to keep a ledger for transactions, its purpose has steadily migrated to other domains such as decision making. In traditional settings new transaction lists saved in the ledger will contain a reference to the old, hashed transaction list thus validating each other. Different approaches showed how this concept can also relate to decision making as a complete list of decisions can be kept, providing support for future decisions, which can be made by analysing the past data using Artificial Intelligence or Big Data to extract certain patterns, thus providing a better solution.

At the same time the blockchain technology relies for the consensus mechanism on concepts such as:

1. Proof of Stake (PoS) - where the creator of the next block is chosen via various combinations of random selection. This concept comes with a big caveat known as the “nothing-at-stake” issue, where consensus might not be achieved because there is nothing to lose by voting for malicious blockchain histories.[5]
2. Proof of Work (PoW) - where nodes in the network verify that a specific participant has made a certain amount of computational processing for a purpose. This kind of consensus is used for cryptocurrency, the most representative being Bitcoin, but also comes with a big issue, that of huge energy consumption, thus making it very expensive [6]

One attempt of creating a blockchain decision system was described by [7] in which the PoW consensus was used, but as mentioned above this can lead to huge costs, thus making it somewhat inefficient. An alternative to these two consensus has gained traction in the past few years, the Proof of Authority (PoA), which can be just as secure but computationally cheaper to implement using the identity of the node as a stake.

3. Proof of Authority vs Proof of Stake

PoS can be an expensive and inappropriate option for certain businesses and corporations, and even though PoA can be seen as a form of PoS, its performance and maintenance costs are vastly cheaper than that of any other private blockchain alternative.[8]

When it comes down to advantages over the standard PoS consensus, PoA has an edge due to the fact that block creators can be easily identified (Fig. 1), increasing accountability, and because of “target spacing” predictability is assured, allowing blocks to be issued on fixed time intervals. For it to work, PoA relies on a multitude of factors, such as:

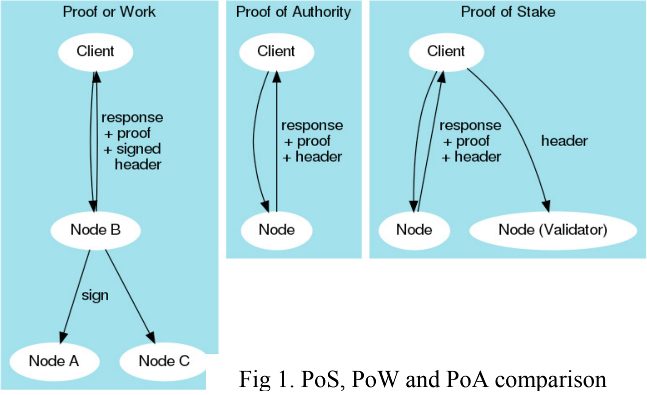

Fig 1. PoS, PoW and PoA comparison

- Validators provide real and accurate data about their identities
- To reduce the risk of malicious agents, money and personal reputation needs to be invested, to ensure a long-term commitment
- The process of validator approval needs to be standardized, so it is common to all candidates

To ensure that new participants in the network are trustworthy, a rigorous validation of their identity needs to occur, and the overall process must be complicated enough to discourage malicious agents, but simple enough so people want to validate. At the base of this system, we find the validators, which with the help of software create block transactions in an automated process that requires the authority node(maintainer) to have an uncompromised computer.[9]

In comparison with PoS, individuals become validators based on the reputation they have gained, as such they are incentivized to respect the validity of the transaction, not doing so negatively affecting the reputation attached to their identities. When it comes down to incentivization, PoA is superior due to the fact that it ignores the individual’s holdings and focuses on their reputation.

As mentioned above, new blocks can be generated by nodes that have proven their authority and have the necessary reputation to do so, but as all protocols it comes with a series of limitations providing malicious actors with way to manipulate the network using [10]:

- Distributed Denial-of-service attacks (DDos) - is an attack to make online services unavailable due to overwhelming traffic, so in this case they would send a large number of transactions and blocks to targeted network nodes in an attempt to disrupt it, making it unavailable.
- 51% attack - is when a user tries to control 51% of the network, which can be a lot harder to do in the case of PoA

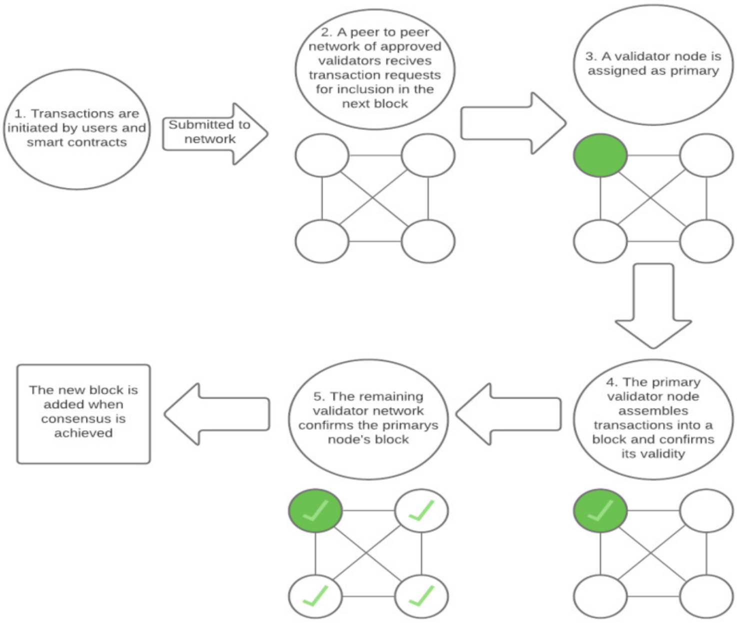
1. Transactions are initiated by users and smart contracts
Submitted to network
2. A peer to peer network of approved validators recives transaction requests for inclusion in the next block
3. A validator node is assigned as primary
4. The primary validator node assembles transactions into a block and confirms its validity
5. The remaining validator network confirms the primarys node's block
The new block is added when consensus is achieved

Fig 2. PoA Consensus Mechanism diagram

The PoA consensus mechanism (Fig. 2) can differ depending on the implementation but in general the following conditions must be met:

- Validators or deciding agents must confirm their real identities.
- Each candidate has to put his reputation at stake and in certain circumstances also invest some money. A candidate that goes through a tougher validation process will more likely be interested in a long term commitment to the decision blockchain and also unsuitable candidates will be filtered out.
- The deciding agents(validators) will go through the same validation process
- In order to assure honest validators, and the integrity of the decision blockchain, their identity must be periodically verified

The main advantages of using PoA consensus [11]:

- high risk tolerance, except the case where 51% of the validators are acting maliciously
- predictable block generation time, in the case of PoW or PoS the generation time varies
- high transaction rate
- no need to waste resources on processing, like in the case of PoW

PoA limitation [12]:

- the deciding agents (DA) have their identities known by everyone so that third parties could try to manipulate them
- the PoA mechanism is not fully decentralized because it relies on the trusted people that activate on the Decision Blockchain network, so in a sense it’s a form of decentralized delegated centralization, this can also make existing centralized systems more efficient

One of the most popular PoA Blockchains is VeChain[13], even though no official list of Authority Nodes exists, and only very few actors have confirmed their status: DNV GL [14], CA Hrenheit [15].

4. Proof of Authority implementation based on VeChain proof of consensus algorithm

For the Decision Blockchain we chose the VeChain proof of consensus algorithm that is described in more detail in the official documentation of VeChain Foundation [16].

The consensus protocol of any blockchain must contain the following mandatory information: the timestamp when the block was produced and the identity of the entity that generated the block. In order for the protocol to be complete it also needs an algorithm for deciding the legitimate branch at any given time that will go into the trunk of the blockchain.

The VeChain Blockchain blocks are produced every Δ seconds. The genesis block being timestamped with t_0. Any block with the height n > 0 at t_n, will have a timestamp that satisfies the following: $t_n=t_0+ m\cdot\Delta$ where $m \in N$ and $m \geq n$.

To satisfy security constraints VeChainThor uses a deterministic pseudo-random process (DPRP) and the concept of "active/inactive" status if a master node is a legitimate option to produce block B(n,t), with height n and timestamp t. Using this method t must satisfy $(t-t0) \bmod \Delta=0$. So to answer who generates the block, a pseudo-random number is generated $\gamma(n,t)$ by:

$$\gamma(n,t) = DPRP(n,t) \triangleq hash(n \circ t); \quad (1)$$

where ∘ is the operation that concatenates two byte-arrays.

A_B denotes the set of master nodes with the "active" status associated with B, so to verify if a is legitimate master node for producing B(n,t) the following relation is defined and shown in Fig 3.:

$$A^a_{B(n,t)} = A_{PA(B(n,t))} \cup a; \text{ where PA(.) gives the parent block.} \quad (2)$$

The computed index $i^a(nt)$ is as follows:

$$i^a(nt) = \gamma(n,t) \bmod \|A^a_{B(n,t)}\| \quad (3)$$

A deciding master node produces B(n,t) if and only if $A^a_{B(n,t)}\,[i^a(n,t)] = a$.

In Fig. 3 the status update is illustrated, showcasing four time slots {t1, t2, t3} for block production. The blocks with solid lines mark the unverified blocks produced on time while the dashed ones are the missing blocks. Using equation (3) the system can compute, for each time slot, the index of the responsible master node. As seen from the equation (3) and (4), after the system verifies B(n, t3) the status gets updated.

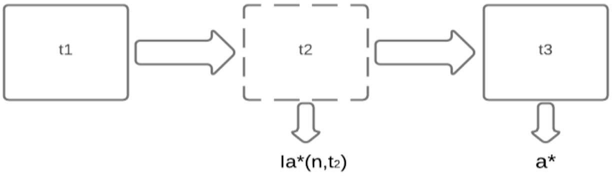

Fig. 3 Status update diagram

$A^{a^*}_{B(n,t2)}\,[i^{a^*}(n,t_2)] \leftarrow$ inactive

$a^* \leftarrow$ active; where a* is the signer of $B(n,t_3)$

The order of master nodes that produce blocks can be completely changed if there is a missing block before a legitimate timestamp t. So, in this case it would be difficult for attackers to predict which master node will produce a number of consecutive blocks at a much later time, VeChain occasionally allowing master nodes to skip block creation, thus increasing unpredictability.

The legitimate branch validation algorithm decides the valid branch that will become the trunk out of two legitimate ones. Because in PoA there is no computational competition, the "longest chain" rule can't be applied. The alternative to this, as implemented by the VeChain Blockchain PoA algorithm, is selecting the branch that is witnessed by the most DAs, which is considered to be better than the two. In order for this to be achieve the algorithm computes a specific value for each branch called accumulated witness number (AWN), for each block B(n,t) using the formula:

$$\pi_{B(n,t)} = \pi_{PA(B(n,t))} + ||A_{B(n,t)}|| \quad (4)$$

$||A_{B(n,t)}||$ computes the number of master nodes that can be active in association with B(n,t) and can be regarded as the number of nodes that witnessed B(n,t). As such the branch with the largest AWN is chosen as the trunk and if they are the same, the VeChain Blockchain selects the branch with the smaller length. So when given two branches B and B' with the latest blocks B(n,t) and B'(n', t'), the protocol first calculates their AWNs πB(n,t) and πB'(n',t'), then the following decision is made: chose B as trunk if πB(n,t) > πB'(n',t') or choose B' if πB'(n',t') > πB(n,t). If πB(n,t) = πB'(n',t'), choose B if n<n' and B' of n'>n. If n=n', keep the current trunk.

5. Decision Blockchain Trust ranking used for PoA

The Decision Blockchain block types and their structure, defined and presented in more detail in a previous article, [6] offer the perfect framework to implement a PoA algorithm suitable for decision making.

The Decision Blockchain contains the following Block Types [17][18][19]:

1) **Definition Block** - this block is considered a primitive block, because using it other block types can be defined but can also define concepts, mechanisms, abstract objects that can be used as reference in other blocks.

2) **Action Blocks** - using this block actions between objects, entities, or other blocks can be defined.

3) **Resource Block** - this type of block allows for resources of all types to be tracked using the blockchain network (money, staff, materials, etc)

4) **Deciding Agent Block** - this block stores personal information of deciding agents, so this is the identity block for the PoA mechanism. To become a DA an individual must voluntarily disclose their identity in order to receive the rights to generate and validate decision blocks.

5) **Vote Block** - using this block type we store different types of votes made by the deciding agents. These are the vote types supported:

   a) **Vote of Trust Block** - this vote type is given by an existing Deciding agent to another Deciding Agent in order to increase their trust rank, each Deciding Agent has only one vote of trust that they can give out or keep for themselves.

   b) **Vote of Validation Block(up-vote)** - this vote type is used on all types of Decision Blocks, you can either validate a certain decision or a new Deciding Agent.

   c) **Vote of Invalidation Block (down-vote)** - this type of vote opposes a certain Decision Block.

6) Feedback Block - this type of block can be added by any type of users of the Decision Blockchain Network to offer feedback on a certain Decision Block.

The example below (Fig 4) shows the relationships before different block types for a transfer resource use case. In this example DA with ID 4

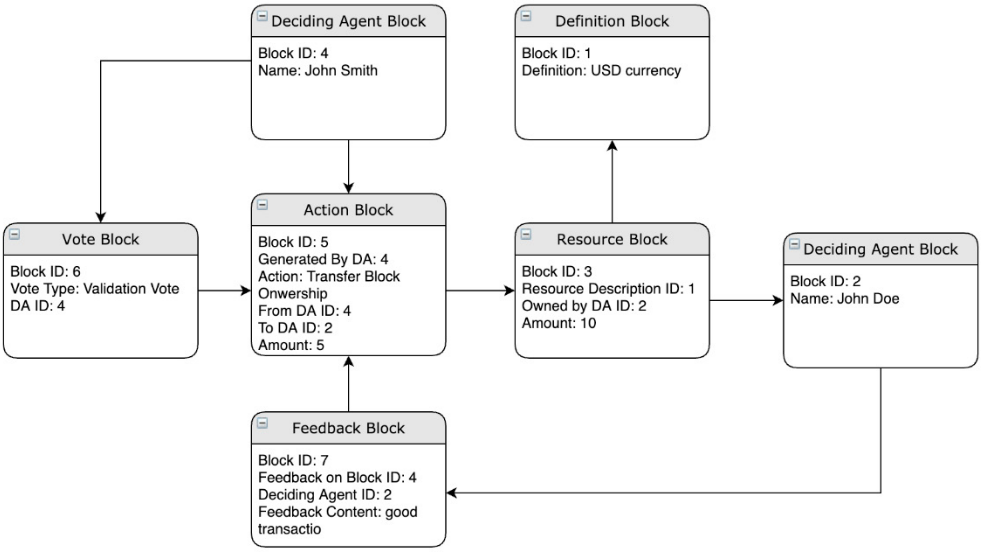

Fig 4. Resource transfer use case and relationships between different block types

The Vote Block is crucial to the overall performance of the system, because inside it fuzzy logic is used to calculate the impact that each user has on the overall decision. Using fuzzy logic [3], the rank of each decision can be calculated based on the up votes and down votes, while at the same time determining the vote weight of each deciding agent by calculating the distance between the domain of the problem and the expertise of the participant. So, we have the following equations to determine the rank:

$$R = U-D \qquad (5)$$

$$U=D= \Sigma \log10\ 200 * di * Ei \qquad (6)$$

Where the general ranking function (R) is defined as the difference between upvotes and downvotes (5). Subsequently the upvotes and downvotes will be directly influenced by the individual specialization (d) and experience (E) adding the votes of all participants. (6) This relation is logarithmic so controversial decisions who might receive a large number of votes do not rank as high as non-controversial ones.

6. Results and Discussion

The Decision Blockchain model can be simulated using the Quorum network [20]. Quorum offers a similar and simple to use environment, like Bitcoin and Ethereum. Because Quorum supports Decentralized Applications that run on the blockchain and is also more effective than the bitcoin network when it comes to validated transitions per second, it can be used to easily simulate applications running in the form of smart contracts, which can be written in the Solidity Javascript framework.

In order to simulate smart contracts Remix IDE can be used, which is a programming environment running on the web browser that allows the user to implement and execute smart contracts.

For authentication we can use the blockchain based platform Truffle, that assigns virtual identities to nodes for executing smart contracts. Truffle stores a unique address for each account and also performs the needed mining process in order to authenticate and add a transaction to the Blockchain.

Metamask is a browser extension that allows Truffle and Remix connectivity but also networking services to local hosts and blockchain networks.

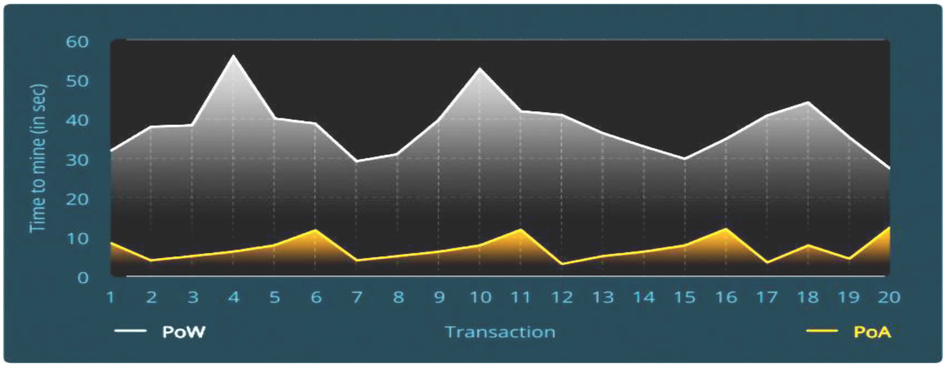

Fig 5. PoW vs PoA transaction speed results

To run the simulation, we set up a system with the following specs: Intel Core™ i7-7700HQ (6M Cache, up to 3.80 GHz), 16GB DDR4, 1TB 7200 RPM + 256GB SSD, GeForce GTX 1070 8GB, Ethereum (Web3J), Quorum v2.5.0, Truffle 5.2.27, Solidity 0.8.1 and CLI Tool Geth.

As seen from the simulation results (Fig 5) the PoW algorithm takes up to 5 times longer to mine a single block compared to the more efficient PoA algorithm used in the Decision Blockchain. Another advantage of the PoA algorithm is the reduced power consumption needed for validating nodes as can be seen from the results in Fig. 6. In PoW the mining is done using a lot of processing power, that translates into a lot of energy consumption, in the case of PoA we don’t validate the blocks using computing power, so we have hardly any energy consumption.

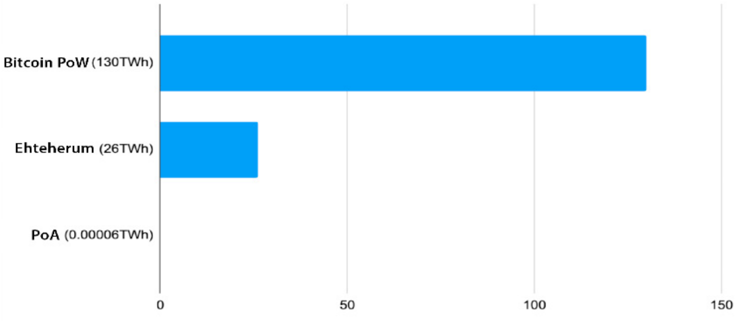

Fig 6. Estimated annual power consumption for PoA vs PoW algorithms

7. Conclusions and Future Work

As seen from the above results, that recommend PoA as a viable and efficient technological solution for Blockchain Decision Making, but also from the global trends that influence the evolution of the technology and ideologies involved in Decision Making in general, we are migrating towards a decentralized or hybrid model for decision making, where the deciding agents, but also the ones involved or affected, directly or indirectly, by the decisions being made take active part by either investing financially(Proof of Stake) or by investing their own reputation which is attached to their identities (Proof of Authority). “Neither a total centralization nor a total decentralization would be the correct answer, but a comprise and balance of both would.”[16]

This paper comes with an alternative for computer supported collaborative decision-making systems, describing a more efficient way to reach decisions, minimizing cost and performance requirements, when compared to classical approaches, such as the Proof Of Stake.

Going forward it is vital for a global protocol to be established that allows the general population to interactively cooperate, using existing devices and technologies, so that problems for which solutions are scattered among many individuals or institutions can be easily solved, for this to be achieved the solution proposed in this article offers a good starting point, implementing the best solutions from multiple technologies and techniques such as blockchain and fuzzy logic.

References

[1] Rouse M.. “Internet of things (IoT)”. IOT Agenda. August 2019.

[2] Hendricks D.. ”The Trouble with the Internet of Things”. London Datastore. Greater London Authority. August 2015

[3] Manolache S., Popescu N “Bio-Receptor Signal Hierarchy Model for Decision Making Agents”, The 8th IEEE International Conference on E-Health and Bioengineering - EHB 2020

[4] Nakamoto S., “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, 2008

[5] Chinchilla C., “GitHub - ethereum/wiki: The Ethereum Wiki”. August 2019

[6] European Parliament, “Cryptocurrencies and blockchain”. https://www.europarl.europa.eu/cmsdata/150761 July 2018.

[7] Manolache MA, Tapus N., Manolache M. A., “Integrated Decision Making using the Blockchain”, Information Technology and Quantitative Management (ITQM) 2019

[8] Binance, “Proof of Authority Explained”, https://academy.binance.com/en/articles/proof-of-authority-explained, Jan 2021

[9] Wood G., "PoA Private Chains", https://github.com/ethereum/guide/blob/master/poa.md, November 2015

[10] Kaur S., Chaturvedi S., Sharma A., Kar J., “A Research Survey on Applications of Consensus Protocols in Blockchain”, Security and Communication Networks 2020

[11] S. De Angelis, “Assessing security and performances of consensus algorithms for permissioned blockchains,” 2018

[12] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, “A survey on the security of blockchain systems,” Future Generation Computer Systems, vol. 107, pp. 841–853, 2020

[13] Team, V. , “Vechain Whitepaper”, https://whitepaper.io/document/578/vechain-whitepaper, August 2020

[14] Medium “DNV GL Buys Stake in VeChain and Announces Authority Masternode Status Medium” , https://medium.com/@bsc44/dnv-gl-buys-stake-in-vechain-and-announces-authority-masternodestatus-c42992a16a2e , August 2020

[15] Medium, “Introducing Cahrenheit”, https://medium.com/@Cahrenheit/introducing-cahrenheit-cb017bf5dd6b, August 2020

[16] VeChain Foundation, “Defining the VeChainThor Blockchain Consensus — Proof of Authority”, https://vechainofficial.medium.com/defining-the-vechainthor-blockchain-consensus-proof-of-authority-8cf3f51a5fa0, May 2018

[17] Manolache MA, Integrated Decision Making Platform, 21st International Conference on Control Systems and Computer Science, 2017

[18] Manolache MA, Tapus N, Universal resource management and logistics using blockchain technology, 22nd International Conference on Control Systems and Computer Science, 2019

[19] Manolache MA, Organic integrated decision making platform, swarm intelligence using blockchain technology, Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies, 2018

[20] Y. Amir and A. Wool. “Optimal availability quorum systems: theory and practice”. Inf. Proc. Lett., 65(5):223--228, 1998