INTERNATIONAL JOURNAL OF ADVANCED STUDIES
IN COMPUTER SCIENCE AND ENGINEERING
IJASCSE VOLUME 9 ISSUE 3, 2020
03/31/2020

Proof of Behaviour (PoBh):An Enhanced Proof of Stake Blockchain Consensus Protocol.

Damilare Peter Oyinloye
Department of Computer Science
Kwara State University
Malete,Nigeria
damilare.oyinloye@kwasu.edu.ng

Abstract—***Alternative protocols such as proof of stake (PoS) emerged after the drawbacks of proof of work (PoW) consensus protocol had been analyzed by researchers. Bitcon which is powered by proof of work consumes almost the same amount of energy as Ireland yearly among other drawbacks. PoS became the protocol of the moment because it reduces the unimaginable energy consumption in PoW with other enhancements. PoS was not without its shortcomings/drawbacks with respect to its performance, accountability and security. This work proposes a proof of behavior (PoBh) consensus protocol, an enhanced PoS algorithm with a much better performance, enhanced security and accountability.***

Keywords-Proof of Workt(PoW); Proof of Stake(PoS);Consensus ; Blockchain; Protocol; Proof of Behaviour(PoBh).

I. INTRODUCTION

Blockchains are shared and distributed databases that can store digital footprints securely without a centralized control point (Andoni et al., 2019). Blockchains are transparent, tamper-proof and protected systems that can enable unique results, especially when merged with smart contracts (Wang et al., 2019).

Also, blockchain is a decentralized record book for documenting activities of multiple users without a centric control hub using cryptographic program. All participating users validate the block to be appended to the chain, and a consensus mechanism ensures that all participants jointly agree to a specific order at which blocks are added (Sayeed & Marco-Gisbert, 2019).Furthermore, blockchains permits automatic execution of smart contracts in peer-to-peer(P2P) networks (Andoni et al., 2019).

Recently, blockchains has suddenly become an item to interest to developers in the security sphere, with the advent of Bitcoin (Nakamoto, 2008) and Ethereum taking the lead as to what interest investors in the financial space, researchers, developers, enthusiasts and academia. With the increase in its acceptability by major vendors, consortium of banks as a legal exchange, blockchains must continue to improve its security, accountability and throughputs, to achieve a more secure, dependable and reliable system.

However, blockchain usage cut across different sphere of like outside the security space, with different innovations been churned out daily in financial technology, health systems, manufacturing and distribution systems, road maintenance and safety, environmental and disaster management. There are basically two major groups of blockchains: public blockchains, it allows participation by all users in a network, while a private blockchain, only a few users can participate, and it is usually between trusted users (Pungila & Negru, 2020).

II. BACKGROUND

Consensus in a blockchain is a mechanism that ensures and enforces that all the users in the block complies with a specific statute and standard. Also, it ensures that all actions come from a verifiable user by ensuring all participant assent to the distributed database. A variety of consensus mechanism have been invented looking at the huge requirements of a secure payment system. However, proof of work (PoW), proof of stake (PoS), and delegated proof of stake (DPoS) are some of the numerous consensus mechanism implemented by the major cryptocurrencies (Sayeed & Marco-Gisbert, 2019).

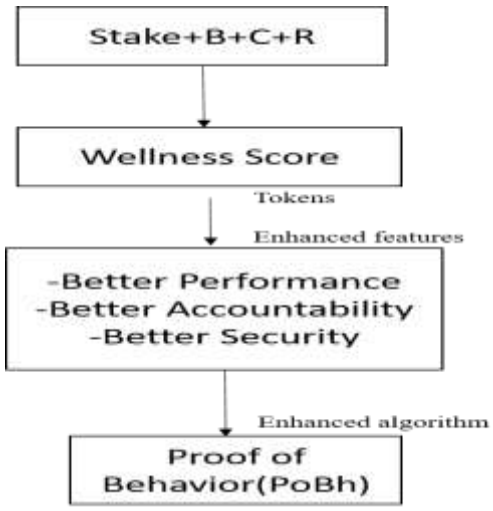
III. LITERATURE REVIEW

Proof of stake (PoS) is a consensus protocol that chooses validator considering the wealth in stakes a participant has in a specific network. Participants that has large volume of coins in their respective possessions has more chances of been selected as a validator above others. Proof of stake (PoS) was first implemented in 2012 with Peercoin. The participant that will create the next block is randomly selected in this type of arrangement. This protocol obtains the volume of the amount of wealth that is kept and the

duration it has been kept. The major edge of proof of stake (PoS) protocol over proof of work (PoW) is the absence of computationally intensive mining process. Proof of stake (PoS) is not without its draw backs which includes centralization tendency among others. There is also a tendency of a participant who has a large stake to continually increase its stake over time and the probability of taking over 51% of the network can't be overruled. This protocol also encourages the rich to be continue to get richer and probably the poor becoming poorer. Also, malicious participants can take a huge advantage of the 'nothing at stake problem'. Proof of stake (PoS) suffers from lack of accountability and implementation process to be a bit difficult. For a 51% attack to be initiated, an enemy is requested to acquire about 51% of the total wealth of the network. Moreover, the cost of acquiring a 51% of the total wealth of the network can be very difficult but its achievable. It has also be proven that proof of stake (PoS) can be attacked by the long-range attack. The P + epsilon attack may not be easy to execute because it is required that an attacker must achieve a voluminous wealth to contribute as a deposit stake for the participants while voting for the minority. Also , proof of stake (PoS) can be attacked with a DDoS which can cause network disruption and a Sybil attack (Sayeed & Marco-Gisbert, 2019).

The emergence of a decentralized ledger of blockchain eradicates the issue of trust primarily associated with the old energy trading platforms, allowing a decentralized individual to individual energy trading platform which allows the users to set the rules and totally control the operations without government interference. Hence the proposed peer to peer energy trading system strictly controlled by the participants without a central point of call. The ETSB includes a node and data set, consensus protocol and intelligent contract,that are all newly constructed according to the characteristics of energy trading[6].

IV. PROOF OF BEHAVIOR(POBH)



Diagrammatical description of PoBh

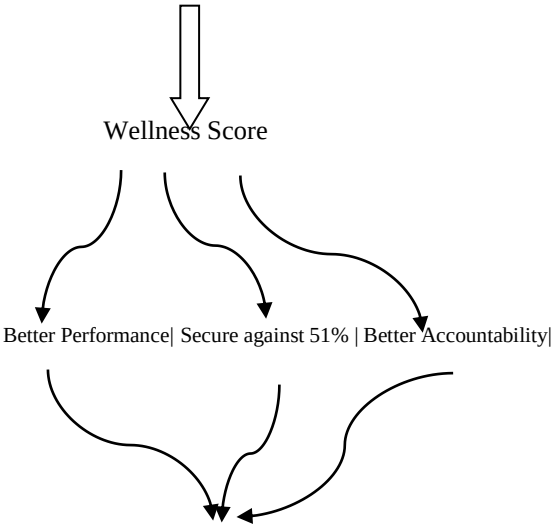
The chances of a validator and block creator to be selected/elected is not solely dependent on the amount of wealth staked in the network but rather, wealth which is represented with W, behavior which is represented by B, contributions which is represented by C and lastly review which is represented by R (Can be positive or negative) which will form the wellness score. The wellness score will form a core component of the enhanced algorithm. It will increase the overall throughput of the network because blocks will be validated earlier and also block creation time will reduce.

Also, the worth of a participant or validator in this enhanced protocol is based on wealth, behavior and contributions, this makes it 3 times more difficult to achieve 51% attack compared to the traditional proof of stake Consensus Protocol.

The addition of behavior, positive/negative review and contributions as metrics cumulating to the overall 'wellness score' of a participant or validator, it adds an extra layer of accountability, where chances/wellness score can't be bought by just a wealthy stake alone.

PoBh Algorithm

1 Join the network by connecting to known peers;
2 Deposit in the stake pool;
/* Main loop */
3 while running do
/* election */
4 if new block cycle then
5 Check WellnessTable;
6 Get WellnessScore;
7 Participate in Election ();
8 end
/* Block proposing & broadcast */
9 if topmost on the WellnessScore
10 Collect transactions and generate block;
11 Write block to blockchain;
12 Broadcast block to the network;
13 end
/* Longest-chain&validation rule */
13 if block is received & is valid & extends the longest chain then
14 Write block into blockchain;
15 Relay blocks to other network members;
16 end
/* PoS-based committee election */
17 Function Election():
18 Fetch the current blockchain state and the Wellness Score(Stake+B+C=R) of all participants; use them as the MPC input;
19 Participate in the MPC that produces BlockGenSeq, a pseudo-random sequence of block generation opportunities;
20 return BlockGenSeq;
21 end
Stake + B+C+R



Proof of Behavior (PoBh)

Diagrammatical enhancement in PoBh

V RESULT AND DISCUSSION

TABLE I Comparism between Proof of Behavior (PoBh) and Proof of Stake (PoS)

S/N	Algorithm	Node Identity Management	Miners election	Tolerated Adversary	51% Attack	Pool Staking
1	PoS	Public	Stake owned	<51% stake	No	Yes
2	PoBh	Public	Stake + Wellness Score	<51% stake + Wellness score	No	No

Security

PoS can tolerated an enemy taking over <51% of the stake in the network and still maintain the integrity of such network. But it has been suggested in several submissions that it is possible for a privileged few to have in their possession more than 51% of the stake in a network, hence the enhancement embedded in PoBh. In PoBh an intending intruder or enemy will not only try to get over 51% of the stake but must also top with the wellness score, which indeed is built over time.

Election of Miners

Both PoS and PoBh consumes lesser power compared to PoW because of the lack of harshing. Miners in PoBh are elected considering not just the coins staked in the network, but also the overall behavior of such node which is evaluated to deduce the wellness score (Stake+ Behavior + Contribution + Review) which makes it a bit difficult for miners who are just in the network to for dubious reasons.

Immune against pool staking

It is two times difficult to take over a PoBh network compared to PoS. It takes just more than wealth and coins to be able to be totally in charge of a PoBh network as it is in PoS. A node must show a significant amount of staked coins and also be one of the topmost node on the wellness table which will culminate into a reasonably high wellness score.

VI CONCLUSION

PoBh consensus algorithm tries to enhancement some of the draw back areas of PoS. It enhances the security of the network by the addition of the overall behavior ranking and the derivation of the wellness score. Also it brought in better accountability and better performance. The wellness score makes it difficult for rich participating nodes to literally take over the network with their wealth.

Further researches can be done in implementing this algorithm in a practical situation and through evaluation and comparism with PoS be highlighted.

ACKNOWLEDGMENT

Tertiary Education Trust Fund (TETFUND) Nigeria.
Dr. Je Sen Teh

REFERENCES

[1] Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., … Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*(February 2018), 143–174. https://doi.org/10.1016/j.rser.2018.10.014

[2] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., … Kim, D. I. (2019). A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks. *IEEE Access*, *7*(May),22328–22370. https://doi.org/10.1109/ACCESS.2019.2896108

[3] Sayeed, S., & Marco-Gisbert, H. (2019). Assessing blockchain consensus and security mechanisms against the 51% attack. *Applied Sciences (Switzerland)*, *9*(9). https://doi.org/10.3390/app9091788

[4] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. *Journal for General Philosophy of Science*, *39*(1), 53–67. https://doi.org/10.1007/s10838-008-9062-0

[5] Pungila, C., & Negru, V. (2020). Improving Blockchain Security Validation and Transaction Processing Through Heterogeneous Computing. In *Conference on Computational Intelligence in Security for Information Systems (CISIS 2019) and 10th International Conference on EUropean Transnational Education (ICEUTE 2019)* (Vol. 951, pp. 132–140). https://doi.org/10.1007/978-3-030-20005-3_14.

[6] Dong, X., Zaoyu, W., Hua, M., Jing, X., Debo, Y., Fanjin, W., & Wei, B. (2020). ETSB: Energy Trading System Based on Blockchain. In *Advances in Intelligent Systems and Computing* (Vol. 895). https://doi.org/10.1007/978-3-030-16946-6_55

[7] Y. Yorozu, M. Hirano, K. Oka, and Y. Tagawa, "Electron spectroscopy studies on magneto-optical media and plastic substrate interface," IEEE Transl. J. Magn. Japan, vol. 2, pp. 740–741, August 1987 [Digests 9th Annual Conf. Magnetics Japan, p. 301, 1982].