Securing IoT-Blockchain Applications Through Honesty-Based Distributed Proof of Authority Consensus Algorithm

Subhi Alrubei*, Edward Ball,†and Jonathan Rigelsford‡
dept. Electronic and Electrical Engineering, University of Sheffield
Sheffield, Uk
Email: *salrubei1@sheffield.ac.uk, †e.a.ball@sheffield.ac.uk, ‡j.m.rigelsford@sheffield.ac.uk

***Abstract*—Integrating blockchain into Internet of Things (IoT) systems can offer many advantages to users and organizations. It provides the IoT network with the capability to distribute computation over many devices and improves the network's security by enhancing information integrity, ensuring accountability, and providing a way to implement better access control. The consensus mechanism is an essential part of any IoT-blockchain platform. In this paper, a novel consensus mechanism based on Proof-of-Authority (PoA) and Proof-of-Work (PoW) is proposed. The security advantages provided by PoW have been realized, and its long confirmation time can be mitigated by combining it with PoA in a single consensus mechanism called Honesty-based Distributed Proof-of-Authority (HDPoA) via scalable work. The measured results of transaction confirmation time and power consumption, and the analyses of security aspects have shown that HDPoA is a suitable and secure protocol for deployment within blockchain-based IoT applications.**

***Index Terms*—Blockchain, The Internet of Thing (IoT), Cyber Security, Secure Consensus Mechanism, Proof of Authority PoA, Transaction Finality.**

I. INTRODUCTION

Recently, the IoT has been growing rapidly and providing excellent service. However, there are some important issues that need to be addressed. One issue is that IoT systems must trust a centralized entity that are operated and maintained by service providers. This can have an impact on trust, as these providers may have an illegal ability to control IoT devices. Another issue is that organized attacks, such as Distributed Denial of Service attacks (DDoS), can be carried out to disrupt the services provided by IoT data centers, which may also result in compromising their security due to the centralized approach in place. Other important issues are the communication overhead and scalability that can result as a consequence of the centralized topology approach, especially when there is a need to update all connected devices or when dealing with a massive surge of services requests [1]. One possible solution to these unsolved issues is to adapt a more decentralized and distributed approach, such as blockchain technology.

Blockchain has been around for approximately three decades [2], and in 2009 it re-emerged as an attractive technology for financial purposes in the form of Bitcoin [3]. Blockchain possesses desirable characteristics, such as distribution, decentralization, robustness, and security, allowing it to be an ideal solution to the above-mentioned issues. It provides a robust platform for devices and humans to interact with each other and exchange information among themselves securely [4], [5]. By applying blockchain technology to the IoT, the overall security can be improved by ensuring data integrity and accountability, and single points of failure can be eliminated. It can also offer a dependable way for IoT networks to control the distribution of computational tasks over many distributed devices, [6].

Integrating blockchain into IoT systems is a complex task to accomplish, and some challenges may arise when blockchain is introduced into IoT systems. One of these challenges is designing a suitable consensus protocol for implementation in the IoT realm. This is due to the fact that some connected IoT devices may not have adequate resources, such as storage and power capabilities. The design of any IoT-centric consensus protocol should satisfy the security and performance requirements of IoT-blockchain applications [6]. One of the main requirements is that the consensus protocol must be able to utilize the available computation power of devices without major consequences on their overall performance. It should be resilient against attacks such as Sybil and DDoS. Any IoT-blockchain consensus protocol should have the ability to adapt in the case of dishonest and/or faulty nodes by making sure these nodes do not take part in the mining and validation process.

In this paper, we propose a new consensus mechanism based on Proof-of-Authority (PoA) and Proof-of-Work (PoW) called Honesty-based Distributed Proof-of-Authority (HDPoA) via scalable work. In HDPoA, the security capabilities offered by PoW are realized while its long confirmation time is mitigated by combining it with PoA.

The rest of the paper is organized as follows. Section II presents the related work; this is followed by the proposed HDPoA architecture in Section III. Section IV presents the implementation of HDPoA; this is followed by the results and discussions in Section V. Finally, the conclusion and future works are presented in Section VI.

II. RELATED WORK

PoW is a well-known consensus approach within blockchain technology. It was first introduced into the Bitcoin blockchain

[3]. PoW is a permissionless protocol that was designed for securing the public blockchain platform. In PoW, nodes can join and leave the network freely as needed. PoW is one of the most secure algorithms if the majority of nodes connected to the network are honest, but it suffers from one disadvantage, which is its increasing energy consumption due to the increasing demand for computation power [8].

Proof-of-Stake (PoS) is another well-known protocol that can be used for both a permissionless and permissioned blockchain platform. Compared with PoW, PoS uses less energy and might have been introduced to replace the PoW [9]. When a new block is mined, the consensus process is carried out based on coin ownership; the higher the stake of coins the node has, the greater its chance of mining the next block and collecting the reward. Nevertheless, it is vulnerable to the Nothing-at-Stake attack [10] and Coin Age Accumulation attack [11]. PoS is disadvantageous for nodes having a lower coin stake compare with nodes having a higher coin stake. This will result in nodes with a higher coin stake becoming richer.

The Practical Byzantine Fault Tolerance (PBFT) algorithm is designed to tolerate Byzantine faults [12]. In each round, a primary miner is selected to mine the next block. PBFT is suitable for implementation in a permissioned network. The PoA consensus protocol is one of the algorithms in the Byzantine fault-tolerant family [13]. This protocol was designed for implementation in a permissioned and private blockchain platform. PoA is a simple protocol that does not require any extensive computation power, as the network depends on authority nodes (ANs) that are assumed to be trusted to mine blocks, hence it consumes very little energy.

The proof-of-activity consensus protocol is a combination of PoW and PoS [14]. In this protocol, nodes first use the PoW mechanism to search for the right nonce for the next block's hash; validators are then chosen based on PoS to validate the block. Nevertheless, the protocol does not provide the desired solutions needed to solve the issues surrounding both PoW and PoS protocols, in fact it is complex and time-consuming.

The authors of [15] proposed a new consensus protocol based on PoW called proof-of-trust for use within IoT-blockchain applications. The work by [16] also introduced another variant of PoW called credit-based protocol for IoT-blockchain applications. Similarly, the works by [17] introduced the Proof-of-Credit (PoC) protocol, which uses voting-based chain finality (VCF) mechanisms for implementation into IoT systems. However, these protocols [15]–[17] depend on the concept of a few trusted nodes, where nodes with a higher score or value of trust usually mine blocks of lower difficulty. This will eventuality result in a more centralized blockchain platform that is controlled by (maybe) just one node or a small number of nodes.

The authors of [18] used the idea of sub-blockchain to show it is possible to apply PoW to IoT systems. Nevertheless, their works were only intended for a private blockchain platform. Another IoT-blockchain consensus protocol was proposed by [19]. This protocol is called Geographic Practical Byzantine Fault Tolerant (G-PBFT), and it uses the geographic locations of devices to ensure the security of the network. For this consensus to be secure, the IoT devices' locations need to be fixed; this makes it difficult to secure a dynamic and mobile IoT network. The Proof-of-Space (PoSpace) consensus mechanism was proposed by [20]. In PoSpace, a node has to prove that it has competed to mine a new block through the use of the disk storage capabilities.

III. HDPoA Architecture

Within the IoT realm, there are many connected devices that have with different capabilities in terms of resources such as computational power and storage space. While some of these do not have the resources required for them to fully take part in any consensus process within IoT-blockchain applications, other devices possess adequate resources to be part of such a consensus protocol. Based on device resources such as CPU, storage capabilities, and battery power, IoT devices are divided into three classes (see Fig. 1) as follows:

- The first class is called *Full Nodes*, These nodes can be in the form of low-cost IoT devices that have enough CPU, storage capacity, and battery power to allow them to act as miners and validators within the IoT-blockchain, and they can store a full copy of the chain locally.
- The second class is called *Hybrid Nodes*. These hybrid nodes may not have the storage capacity to store a full copy of the chain, but they can store the header of the blocks and use their computational power to take part in the consensus process and carry out small tasks such as finding the right nonce for the next block's hash. These nodes take the form of low-cost and low-power IoT devices that, in addition to taking part in the consensus

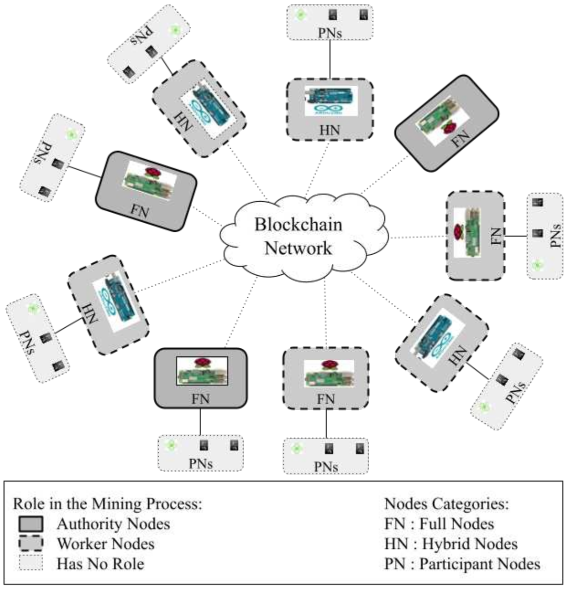

Fig. 1. The different classes of IoT devices and their role in the consensus process.

process, can also create and submit transactions to the blockchain network.

- The third class is called *Participant Nodes*. These nodes do not have the required capabilities to be part of the blockchain or the consensus process. However, they still play an important role in the blockchain, as they are the sensor devices that collect information and they can be connected to other nodes, either full or hybrid. This allows participant nodes to submit their collected data to the blockchain network through connected nodes.

A. HDPoA Design

We have considered different algorithms, such as PoS, PoW, BFT, and its variation PoA. The PoA implemented by [13] is a lightweight consensus algorithm that offers two key advantages: it does not require much energy to mine a block, and it has a lower latency as it does not require confirmation rounds as shown by [21], making it suitable for IoT implementations. However, one disadvantage is that it is intended for permissioned and private blockchain platforms, which goes against the decentralized approach.

PoW is one of the most secure consensus algorithms for a public blockchain, yet it suffers from a long transaction confirmation time, which is approximately six blocks on Bitcoin. Many authors including [15], [16], [18] have shown through their works that it is possible to integrate PoW into blockchain-IoT applications.

In this study, the security advantages provided by PoW are realized while its long confirmation time is mitigated by combining it with PoA in a single consensus mechanism, HDPoA via scalable work. PoA depends on a number of trusted nodes called authorities that are expected to be honest (at least comprise 51% of them) to mine and validate blocks, a. In classical PoA, ANs are assigned and authorized by the owner of the network. In the proposed HDPoA, ANs have to perform works and build their honesty level to earn the privilege of mining and validating blocks. The work can be in any form, such as some work in the mining process. As shown in Fig. 1, we divided the IoT devices based on the roles that each device plays in the consensus mechanisms as follows:

- Worker Nodes (WN): the scalable work concept allows any node to join the network for the first time as a worker regardless of node category. The WN can be utilized within the blockchain network to carry out some tasks, such as a small portion of the mining process. By honestly performing any task assigned to them, these WNs can increase their level of honesty until they reach the required level for promotion to the next category (the Authority category), if they have the required resources to be in that category.
- Authority Nodes (AN): this is the highest category in the HDPoA protocol. Nodes in this category must reach the required honesty level, and they must be full nodes. These nodes are responsible for managing and coordinating the mining process, signing and propagating new blocks, validating WN solutions for any work they carry out, and validating any new blocks propagated to the network by another AN.

B. Enhanced Security via HDPoA

PoA is only suitable for permissioned networks, where nodes are authorized to join the network and only a few nodes are allowed to mine and validate new blocks at fixed time intervals. These nodes can easily be targeted by attackers, especially for DDoS attacks. In HDPoA, nodes can freely join the network and build up their honesty level through scalable work, in which nodes perform useful works on the network such as carrying out some of the hash calculations. With the introduction of the scalable work concept, HDPoA would enhance the overall security of the network by:

- By integrating PoA with PoW, HDPoA provides a secure permissionless blockchain, where mining tasks can be divided into small tasks carried out by IoT devices.
- Nodes can increase their honesty level, and if all nodes behave according to the network rules, they can all be included in the AN category, realizing the full potential of the decentralization concept. Hence, more nodes would be available to manage the mining process, thus reducing the risk of DDoS associated with PoA.
- HDPoA eliminates the impact of the 51% attacks associated with PoW, where if a node controls 51% of the network hash power, it can control the network. This is because HDPoA first relies on ANs to manage and control the block generation and mining process. Second, the task of finding the right nonce for the next block's hash is divided into small tasks carried out by different nodes. Hence, in HDPoA, the attacker needs to control 51% of the authority, which is very difficult, as the protocol allows for the number of authority nodes to increase without any limit on the honesty level.

Many authors, including [15]–[17], have tried to integrate PoW into the IoT-blockchain. However, their work relied on the concept of reducing the PoW difficulty for nodes that have a high credit score or trust. This would result in a less secure network, as mining would happen on *low difficulty*. In contrast, in HDPoA, the difficulty can be increased as the number of WNs increases, resulting in a more secure network.

Scalable work is used to increase the security of the network in the case of misbehaving WNs. By majority vote, ANs can penalize these nodes by increasing the work required from them. This can eventually result in the excessive use of the power of these nodes, or in having them empty their batteries doing meaningless work.

IV. HDPoA Implementation

This protocol is a combination of PoA and PoW, where the mining process is divided into small tasks that are executed by multiple unrelated nodes. ANs, described above, manage and co-ordinate the process of generating a new block. The selection of ANs is performed based on a round-robin process. Prior to mining a new block, one AN is elected as a primary and another as a secondary. This is to ensure that a block

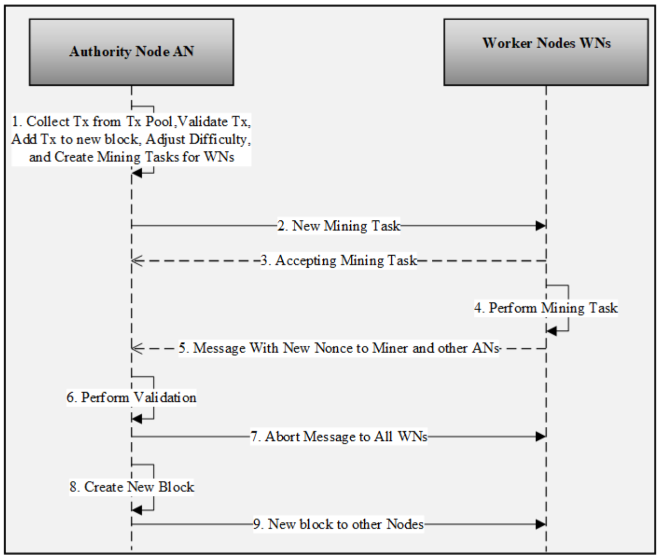
Authority Node AN
Worker Nodes WNs
1. Collect Tx from Tx Pool,Validate Tx, Add Tx to new block, Adjust Difficulty, and Create Mining Tasks for WNs
2. New Mining Task
3. Accepting Mining Task
4. Perform Mining Task
5. Message With New Nonce to Miner and other ANs
6. Perform Validation
7. Abort Message to All WNs
8. Create New Block
9. New block to other Nodes

Fig. 2. The Different Steps of the Mining Process

Algorithm 1 Block Validation by Authority Nodes

```
Input: $Txs$, $BH$,$LH$, and nonce from WN.
Output: Valid Block
  for $Txs$ in Block do
    Calculate $MR$
  end for
  $H = Hash(LH \parallel MR \parallel nonce)$
  if (H != BH) then
    $block \leftarrow notValid$
    Initiate Removal Process
  else
    if (all $Txs \leftarrow Valid$) then
      $block \leftarrow Valid$
      $LocalChain \leftarrow block$
    else
      $block \leftarrow Invalid$
      Start AN Removal Process
    end if
  end if
```

is propagated to the network in each round. All other nodes apart from the elected primary and secondary miners will act as workers.

A. Consensus Process

The consensus process, as shown in Fig. 2, begins with the ANs and takes place over the following steps:

1) The first AN in the round-robin (e.g., AN1) collects all transactions (Txs), validates them, and adds them to a new block.
2) Next, AN1 creates mining works using the hash of the parent block (LH), the Difficulty (D), and the Merkle Root (MR) of all (Txs). It adjusts the workload based on the honesty level of the assigned WNs and sends the new tasks to the WNs.
3) When a WN accepts work, it conducts the mining until either it finds a solution, or it receives an abort message from AN1, or it completes the iteration through all of the nonces assigned to it. If it finds a solution, it will submit its finding to all the authority nodes.
4) When AN1 receives the WN solution (i.e., the nonce) to the task, it will validate the work by calculating just one hash to create the new block hash (BH) according to the current difficulty.
5) If the new BH is valid, AN1 sends an abort message to all WNs.
6) AN1 then signs the new block and propagates it to the other ANs on the network.
7) Finally, after the other ANs receive the new block, they validate it according to algorithm 1.

B. Honesty-Level and Workload

The HDPoA consensus protocol was designed for deployment within a public IoT-blockchain platform, allowing any node to join and leave the network freely and as needed. When nodes join the network for the first time, they have a zero-honesty level, where the honesty level of node *i* is defined as H_i. Over time, and with the introduction of the scalable work concept, the node will start building up its H_i, as long as it correctly provides solutions to any tasks it carries out and obeys the network's rules. In return, the node's honesty value will continue to increase, allowing it to be added to the AN category if it is from a full node class. The blockchain network has a target honesty threshold of H_T. Node *i* can be included in an AN category only if:

$$H_i > H_T \tag{1}$$

All the work a node performs will have a value for honesty. If the node provides a correct solution to the work, its honesty level will increase by a positive value of P_v, and if its solution is wrong, its honesty level will be decreased by N_v. For a total number of works *w* equal to *k*, the positive honesty value H_p for node *i* can be calculated by:

$$H_p = \sum_{w=1}^{w=k} P_v(w) \tag{2}$$

Similarly, the negative honesty value H_n for node *i* can by calculated by:

$$H_n = \sum_{1=1}^{w=k} N_v(w) \tag{3}$$

Finally, we can calculate the node's honesty level H_i by:

$$H_i = H_P - H_n \tag{4}$$

After becoming an AN, the node will be allowed to manage and coordinate the process of generating new blocks, signing and propagating new block, ensuring WNs submit correct solutions to the tasks they perform, and validating any new block propagated by other ANs.

Confirmation Time: The relationship between the mining time T_m, any WN hash power P_{WN}, the total number of WNs T_{WN}, and the difficulty D (minimum D = 1; this is when the number of leading zeros at the beginning of the hash is 24) can be established by:

$$T_m = \frac{D * 2^{24}}{P_{WN} * T_{WN}} \tag{5}$$

If the number of WNs is increased in the network, the T_m can be reduced. This would allow for the difficulty to be increased, as more WNs are now available on the network to participate in the mining process.

Using Poisson probability $P(T \leq t) = 1 - e^{-\lambda t}$ to estimate the probability of transaction confirmation after n blocks, where λ represents the rate in terms of adding blocks to the blockchain network, means $\lambda = 1/T_m$ block/sec. We can also define the block propagation delay as (b_{pd}), the transaction propagation delay as (t_{pd}), and the block validation time as (b_{vt}). Based on this, we can calculate the transaction confirmation time (CT) by:

$$CT = \frac{\ln(1 - P(n))}{\frac{-1}{\frac{D \times 2^{24}}{hp(i) \times N}}} + t_{pd} + b_{pd} + b_{vt} \tag{6}$$

Work Load can be defined as W_L; the node computation or hash power factor can be defined as HPF, and the total work is defined as W_T. The node's honesty factor HF can be calculated by:

$$HF(i) = \begin{cases} \frac{H_T - H_n}{HPF} & \text{if } H_T > H_n \\ \frac{1}{HPF} & \text{if } H_T \leq H_n \end{cases} \tag{7}$$

The assigned W_L to any node i can be calculated by:

$$W_L(i) = W_T \times \frac{HF(i)}{\sum_{k=1}^{k=N} HF(k)} \tag{8}$$

As the node's honesty level increases, the work assigned to that node decreases, helping the node save energy. Conversely, if the node's honesty level decreases, more mining work will be assigned to it.

C. Experiment Setup

For the deployment and validation of the HDPoA consensus mechanism, we created a proof-of-concept blockchain network consisting of 11 Raspberry Pi 3 Model B+ (1.4 GHz 64-bit quad-core processor) and two ESP32 microcontrollers. The nodes were deployed in different locations within a small area and connected as a peer-to-peer network. We tested our proposed consensus protocol utilizing different numbers of WNs and one AN over Wi-Fi connectivity.

V. Results and Discussion

A. Confirmation Time

The confirmation time CT is an essential part of our design objective, as one of our aims is to lower the CT compared to the traditional PoW used by Bitcoin. We measured the CT with different numbers of WNs (one to ten WNs) for difficulty $D = 1$. As shown in Fig. 3, by distributing the mining process among more WNs, the confirmation time was significantly reduced, until a network containing 12 WNs managed to achieve a CT of 2.1 minutes.

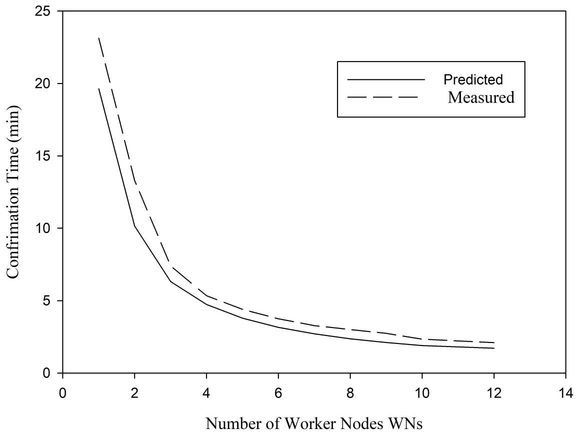

Fig. 3. Overall Confirmation Time of Transactions

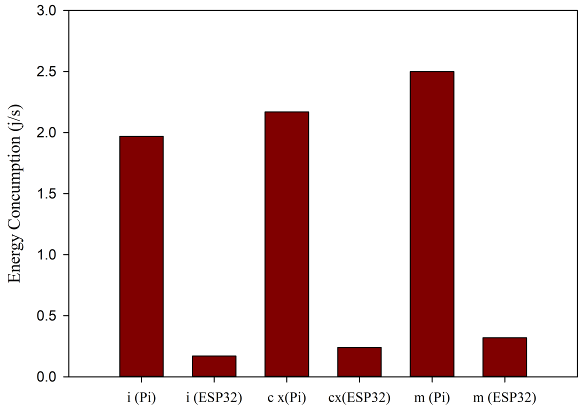

Fig. 4. Energy Consumption during different system states: (i) when devices are idle, (cx) during Wi-Fi connection, (m) when device perform mining task

B. Energy consumption

Energy consumption is a vital aspect of this system; the system was designed to allow low-power devices to be part of the blockchain and benefit from the services offered. This is done in exchange for a small amount of power, where these devices participate in the mining process and ensure blockchain security. The energy consumption was measured for different system states (idle state (i), connection state (cx), and mining state (m)) when the system was implemented on different devices: a Raspberry Pi 3 Model B+ and an ESP32. Fig. 4 shows the average energy consumption of both devices for different states. Most of the energy consumed was due to running the device's operating system (idle state). The difference in energy consumption between the mining state and the idle state was 0.53 j/s for the Raspberry Pi and 0.15 j/s for the ESP32. That is a small amount of energy that the node has to provide in exchange for joining the network and benefiting from the services offered.

TABLE I
PERFORMANCE COMPRESSION BETWEEN HDPOA AND OTHER CONSENSUS MECHANISMS

Consensus algorithm	Computation Complexity	possibility of Forks	Nodes Scalability	Vulnerability	Type of access	Transaction Finality	Suitability for public IoT-Blockchain
PoW	High	Yes	High	51% attack	Permissionless	High	No
PoA	Low	Yes but dealt with efficiently	Low	- Faulty nodes (total node-1/3) - Heavily depends on validators honesty -DoS attacks	Permissioned	Low.	No
PoS	Less than PoW	Yes	High	-51% attack -Collusion of rich stakeholders -Nothing at stake attack.	Permissionless and Permissioned	High	Probably
Proof of Activity	High	No	High	-51% attack -Collusion of rich stakeholders	Permissionless and permissioned	High	No
PBFT	High	yes	High	Faulty nodes (total node-1/3) -DoS attacks	Permissioned	Low.	No
HDPoA	Less Than PoW	Rarely, but dealt with efficiently	High	51% attack	Permissionless	Low.	Yes

C. Discussion

The energy consumption results indicate that low-cost devices have the computation ability to be part of this consensus without having a substantial impact on its energy and computation power. As HDPoA allows for an increase of the number of participating WNs, the impact on the individual power of these WNs will decrease. In a network with a few thousand IoT devices, a node may spend a day without executing tasks. This is because the implemented consensus mechanism was designed based on sharing the computational power among IoT devices, and it is able to efficiently utilize the power from these devices.

In HDPoA, if the transaction is submitted at the start of the mining period of the current block being mined, it will take up to twice the mining time (i.e., $2xT_m$). This means that only one block confirmation is required for ***Transaction Finality*** (transactions cannot be modified or deleted) on the network, compared with about six blocks in Bitcoin PoW, and this provides lower latency for IoT applications.

The consensus mechanism is able to adjust the mining difficulty according to the available mining power on the network and the required mining rate (interval between blocks). As the number of nodes in the network increases, mining power will also increase as more WNs participate in the mining process. Accordingly, the difficulty will increase. A performance comparison between some of the well-known consensus mechanisms and HDPoA is provided in Table. I. Table. I.

D. Security Analyses

Malicious ANs: There is a possibility that an AN can be malicious, misbehaves, or is compromised. In such a case, the HDPoA protocol has the capability to deal with these nodes and defend the network and ensure its security. First, the HDPoA protocol implements a mechanism that only accepts a block from an AN after every N block. Second, each new block in the network will be validated by every AN in the network, both the hash of the block and all the transactions in it (see algorithm 1). If any AN attempt to propagate a malicious block, then the network would address this by removing it from the AN category and its honesty level becomes 0.

Dishonest WNs: there is also the possibility that a WN can be malicious, misbehaves, or compromised. This can be in the form of submitting an invalid solution to a task, which HDPoA can easily deal with. The protocol implements two rounds of validations before it accepts any new block, first by the elected primary AN, and then by other ANs (see algorithm 1).

51% attacks: In the case of PoW, this attack can be successful when an attacker controls 51% of the network's overall hash power. HDPoA eliminates this type of attack, which is associated with controlling the majority of the hash power, by introducing an extra security layer in the form of ANs and the distribution of the hash work. However, to be successful, an attacker needs to control 51% of the HDPoA authority nodes. It is still possible for an attacker to do that, yet quite difficult.

Forking or concurrent blocks: There is a small possibility that a fork can occur on the network, similar to the original PoA [12]. In such a case, HDPoA can solve it efficiently. First, the blocks mined and propagated by the primary elected ANs will have a higher weight than other blocks that are mined and propagated by the secondary elected authority nodes. Second, when ANs on the network receive more than one block, they will always add to their local chain the block with the higher weight if it was mined by one of the elected ANs. Third, the secondary elected authority will always add a small offset to allow for the block mined by the primary to reach the secondary before it releases its block.

VI. CONCLUSION AND FUTURE WORK

In this paper, a new consensus mechanism suitable for deployment in IoT-Blockchain systems called HDPoA was designed, implemented, and validated. HDPoA is a secure consensus protocol that has the ability to ensure that the network is resilient against some well-known blockchain attacks, as shown by the security analysis. It achieves a lower energy consumption than does PoW. It also reduces the required confirmation rounds that are needed for transaction finality on the network.

Our future works will include the utilization of more and diverse low-cost and low-power IoT devices having different capabilities. Any future deployment will include the testing of the protocol over a large area and for longer periods of time for better evaluation in terms of computation capabilities. It will also include the deployment of the network over different connection protocols, such as LoRa, to evaluate the ability of the protocol to perform in different environments.

REFERENCES

[1] B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, et al., ”When internet of things meets blockchain: Challenges in distributed consensus”, IEEE Network, vol. 33, no. 6, pp. 133-139, Nov.-Dec. 2019, doi: 10.1109/MNET.2019.1900002.

[2] W. S. Stornetta and S. Haber, "How to Time-Stamp a Digital Document," J. Cryptol., vol. 3, no. 2, pp. 99–111, 1991.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Manubot, Tech. Rep., 2008.

[4] N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” Secur. IT, no. August, pp. 68–72, 2017.

[5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp.557–564, 2017.

[6] R.Yang, F.R.Yu, P.Si, Z.Yang, and Y.Zhang, “Integrated Blockchain and Edge Computing Systems: A Survey, Some Research Issues and Challenges,” in IEEE Communications Surveys and Tutorials, vol. 21, no. 2, pp. 1508-1532, Second quarter 2019, doi:10.1109/COMST.2019.2894727.

[7] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, “Blockchain's adoption in IoT: The challenges, and a way forward,” J. Netw. Comput. Appl., vol. 125, pp. 251-279, Jan. 2019.

[8] K. J. O'Dwyer and D. Malone, “Bitcoin mining and its energy footprint,” 25th IET Irish Signals & Systems Conference 2014 and 2014 China-Ireland International Conference on Information and Communications Technologies (ISSC 2014/CIICT 2014), Limerick, 2014, pp. 280-285, doi: 10.1049/cp.2014.0699.

[9] S. King and S. Nadal, “PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake,” self-puplished paper, 2012.

[10] Li, W.; Andreina, S.; Bohli, J.; Karame, G. Securing proof-of-stake blockchain protocols. In Data Privacy Management, Cryptocurrencies and Blockchain Technology; Springer: California, America, 2017; pp. 297–315.

[11] .P. Vasin, Blackcoins proof-of-stake protocol v2, 2014, [online] Available: https://blackcoin.co/blackcoin-pos-protocol-v2-whitepaper.pdf.Accessed on: Aug. 30, 2020.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557–564, 2017.

[13] P. Szilágyi “EIP-225: Clique proof-of-authority consensus protocol,” (2017), [Online]. Available:https://eips.ethereum.org/EIPS/eip-225. Accessed on: Feb. 13, 2021.

[14] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, “Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake,” ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, 2014.

[15] L. Bahri and S. Girdzijauskas. 2018. “When Trust Saves Energy: A Reference Framework for Proof of Trust (PoT) Blockchains”. In Companion Proceedings of the The Web Conference 2018 (WWW '18). International World Wide Web Conferences Steering Committee, Republic and Canton of Geneva, CHE, 1165–1169. DOI:https://doi.org/10.1145/3184558.3191553.

[16] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, “Towards Secure Industrial IoT: Blockchain System with Credit-Based Consensus Mechanism,” IEEE Trans. Ind. Informatics, vol. 15, no. 6, pp. 1–1, 2019.

[17] R. Xu, Y. Chen, E. Blasch, and G. Chen, “Microchain: A Hybrid Consensus Mechanism for Lightweight Distributed Ledger for IoT,” Dec 24, 2019. [Online]. Available: https://arxiv.org/pdf/1909.10948.pdf

[18] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, “Hybrid-IoT: Hybrid Blockchain Architecture for Internet of Things - PoW Sub-blockchains,” pp. 1–10, 2018.

[19] L. Lao , X. Dai, B. Xiao, S. Guo, “G-PBFT: A location-based and scalable consensus pro-tocol for iot-blockchain applications.” In: IPDPS. pp. 664–673 (2020).

[20] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, “Proofs of space,” in Advances in Cryptology – CRYPTO 2015. Springer, 2015, pp. 585–605.

[21] S. M. Alrubei, E. A. Ball, J. M. Rigelsford and C. A. Willis, “Latency and Performance Analyses of Real-World Wireless IoT-Blockchain Application,” in IEEE Sensors Journal, vol. 20, no. 13, pp. 7372-7383, 1 July, 2020, doi: 10.1109/JSEN.2020.2979031.