**Proceedings Paper:**
Alrubei, S. orcid.org/0000-0002-0839-2147, Ball, E. and Rigelsford, J. (2020) A secure distributed blockchain platform for use in AI-enabled IoT applications. In: Proceedings of the 2020 IEEE Cloud Summit. IEEE Cloud Summit 2020, 21-22 Oct 2020, Online conference. IEEE , pp. 85-90. ISBN 9781728182674

https://doi.org/10.1109/IEEECloudSummit48914.2020.00019

# A Secure Distributed Blockchain Platform for Use in AI-Enabled IoT Applications

Subhi Alrubei*, Edward Ball* and Jonathan Rigelsford*
*Department of Electronic and Electrical Engineering
The University of Sheffield,
Sheffield, UK
Email: {salrubei1, e.a.ball, j.m.rigelsford}@sheffield.ac.uk

***Abstract*—The increased implementation of Edge Computing technology has provided The Internet of Things (IoT) with the ability of real-time data processing and tasks execution requested by smart devices. To support this processing the integration of Artificial Intelligence (AI) into IoT is considered one of the most promising approach. While AI helps in the analyses of the data, blockchain technology provides a robust environment within which to create a secure, distributed way to share and store data. This paper proposes an architecture that combines the strengths provided by edge computing, AI, and blockchain technologies to provide robust, secure, and intelligent solutions for secure and faster data processing and sharing. The pandemic created by the rapid spread of the novel Coronavirus COVID-19, as well as the tracking of viruses in water sewage to help control the spread of such viruses, were used as our case study for exploring this architecture. To secure the proposed architecture a new concept for consensus mechanism based on Honesty-Based Distributed Proof of Work (DPOW) were devised and tested.**

***Index Terms*—The Internet of Things (IoT); Edge Computing; Artificial Intelligence (AI); Blockchain; COVID-19;**

## I. Introduction

IoT systems have been used successfully in many different sectors, such as the industrial and health-care, where IoT has the potential to offer organizations and governments enhanced economic growth while improving people's lives in general. IoT can provide vast amounts of useful information, which leads to better decision making. The current approach with regard to data processing is that IoT systems trust a central entity such as a cloud service provider for data processing, security, and system management.

This central entity introduces the risk of a single point of failure that could affect system performance and security and can result in increased latency. In many IoT, especially mission critical ones, it is essential to have a suitable solution that provides reduced latency for data processing. One notable approach is the utilization of edge computing that is able to process data faster than cloud and produce actionable outcomes. Edge computing provides services based on location awareness, with low latency for IoT applications. Nevertheless, the data collected due to the heterogeneous nature of IoT and edge devices may lack adequate security in transit and in storage, which makes it difficult to maintain a heterogeneous and distributed system such as IoT [1].

Blockchain provides a robust, secure, and decentralized platform for secure interactions and information exchanges between devices and humans. Data collected by IoT needs to be secure, and this is easily achieved with a transparent and distributed system such as blockchain. The presence of edge nodes helps in accommodating the computation power and storage that blockchain requires. Since IoT is a distributed and dynamic system, it will greatly benefit from the integration of decentralized, self-managed, and regulated blockchain networks [2] [3]. The integration of blockchain into IoT, especially with the presence of edge computing, can provide reliable control of the IoT network's ability to distribute computation over a large number of distributed devices, improve overall security by improving the data integrity and ensure accountability [4]. It also provides the intelligence system with the ability to perform analyses and forecasting using trusted data.

The ever-increasing implementation and use of IoT have resulted in the re-emergence of Artificial Intelligence (AI). IoT and AI together form a system that is able to sense, learn, think, and take appropriate actions in response to changes. While IoT systems have a significant role in the collection of data, AI has the ability to analyze this data and perform the appropriate action based on each specific situation. Integrating and deploying blockchain and AI in the IoT systems, especially into the edge layer, can provide users and organizations with a platform capable of data processing and provide the desirable analyzed outcome.

In this paper we propose an architecture combining the IoT, AI, and blockchain technologies in a system that is able to sense, learn, and analyze data based on the needs of the task at hand. It integrates low-cost edge nodes and exploits their storage capabilities and the overall IoT devices computation power to provide a public blockchain platform for data processing and sharing. To secure the proposed architecture, DPoW consensus mechanism were created and tested. It is suitable for the implementation in public blockchain-IoT applications and takes advantage of the IoT devices' collective hash powers to share the work of mining a block.

The rest of this paper is organised as follows: Section II presents the related work, and the proposed architecture is discussed in Section III. In Section IV we discuss an example application and Section V presents the DPoW consensus mechanism followed by its implementation in Section VI. Finally, Section VII presents the conclusion and future works.

## II. Related Work

Recently, blockchain has been increasingly integrated into the IoT systems, the authors of [5] proposed an architecture based on blockchain and the Software Defined Network (SDN) controller at the edge. It consists of three layers: the device layer for data collection; the fog layer equipped with an SDN controller for processing received raw data from devices; and finally, the cloud layer receives all processed data. IBM [6] in 2015 introduced the Autonomous Decentralized Peer-to-Peer Telemetry (ADEPT) system based on Ethereum blockchain and smart contracts for coordinating autonomous devices. Another work by [7] proposed a framework for vehicular communication systems based on blockchain. It utilized a second layer similar to edge computing to host a security managers (SMs) and blockchain platform for key transfer and management. Another edge-based implementation is introduced by [8] for systems control. The top layer uses Hyperledger Fabric and smart contracts to ensure the security and validity of transactions and the bottom layer is based on a microservice architecture at the edge nodes and controls devices and processes. Another work by [9] proposed an EdgeChain framework based on blockchain and smart contract that allows IoT devices to access resources provided by the edge servers.

In terms of combining blockchain, AI, and edge computing, [10] proposed a platform named NeuRoNt based on the Ethereum and smart contract. It consists of multiple agents capable of solving complex problems. Ethereum and smart contract–based mobile edge sharing systems were proposed by [11] for data processing and sharing of services in IoT-enabled smart cities. ModelChain proposed by [12], which aims at allowing multiple institutions to train the medical health prediction framework using blockchain and machine learning. The work by [13] proposed the BlockDeepNet framework, which combined the implementation of deep learning, blockchain, and smart contracts for data analyses in IoT. The work by [14] introduced DeepCoin framework for smart grids based on blockchain and deep learning for detecting fraudulent transactions and attacks in the blockchain network. Another framework proposed by [15] based on Deep Learning, SDN, and blockchain for enabling high-performance and cost-effective computing resources for smart city applications. Nevertheless, both [14] and [15] frameworks suffer from centralization issues.

The design of IoT-specific consensus algorithms is one of the important research areas in IoT-blockchain. The authors of [16] proposed Proof of Trust consensuses mechanisms based on PoW for implementation in IoT. The authors of [17] also proposed IoT-centric consensus mechanisms named Credit-Based for IoT applications. Both tend to rely on trusted nodes, the node with higher trust value will mine the block in a lower difficulty. This might result in more centralized network where (may be) just one node controls the network. The authors of [18] showed with the use of the concept of sub-blockchain, PoW can be used within IoT. However, their implementation is for permissioned blockchain system.

Unlike other previous related work, in this paper we produced a novel intelligent, secure, and distributed platform for data sharing within IoT systems. It takes the advantages of the computation power and storage capacity of edge nodes and exploits IoT devices' overall power to implement a secure public blockchain platform based on the PoW consensus algorithm. We utilized the benefits of AI, IoT, and blockchain in a single architecture to provide users with a trustworthy data processing and sharing system.

## III. Proposed Architecture

In this section we provide a description of our system architecture, which provides a platform for data collection, processing, analysis and sharing. Fig.1 provides a general overview of the proposed architecture. This platform is based on three steps. These steps are: 1) IoT devices monitor and collect data, 2) the intelligent edge-devices analyse the collected data and provide AI predictions, and 3) the blockchain platform enables the sharing of these AI decisions. As shown by Fig.2 this Architecture Consists of four different layers.

***Sensing Layer*** is where many small, low-cost sensor devices can be used for monitoring, and data collection, it is responsible in achieving step one of this architecture. This data will be submitted to a gateway device such as Arduino ESP-32, where they will be sent to the processing node. ***Network Layer***, data collected by the sensor's devices will be transferred to the processing node using available communication links. Various connectivity can be utilised in this layer, such as Wi-Fi, LoRaWAN, or 5G.

***Processing Layer*** is responsible in achieving second step of this architecture, it will be in the form of low-cost edge-devices such as Raspberry Pi. In this layer the AI expert engine will process collected data and provide an outcome to help the decision-making process. This layer is part of a blockchain platform, and devices will be able to communicate AI predictions to the sharing platform. This means the continuous stream of collected data will allow the AI engine to ensure continued predictions. ***Sharing Platform*** is publicly accessible blockchain platform of which all devices in the processing layer are a part. Any users, organisation, or other

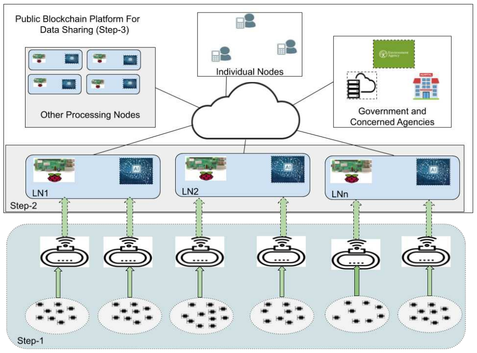
Public Blockchain Platform For Data Sharing (Step-3)
Individual Nodes
Other Processing Nodes
Government and Concerned Agencies
LN1
LN2
LNn
Step-2
Step-1

Fig. 1. Proposed Architecture - General Concept.

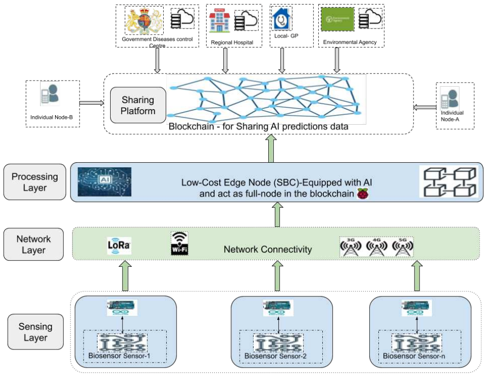

Fig. 2. Protocol Different Layers-AI-Enabled Example Application.

concerned entity can be part of this platform and access the data processed by the intelligence layer. It is responsible in achieving the final and third step of this architecture.

To ensure the security of the platform, it was essential to design a secure consensus mechanisms that is suitable for IoT implementation. The PoW consensus mechanisms implemented by [19] is one of the most secure consensus protocols, however it needs adaptation to ensure it utilises IoT devices resources more efficiently. We have designed a consensus mechanism, suitable for implementation in public blockchain-IoT applications (see section V). Based on this we divided the IoT devices into three categories as follows, based on their CPU and battery power:

- ***Leader Nodes (LN):*** These nodes should have adequate resources to act as leader. Leader nodes can coordinate the mining process and store the full chain locally. The concept of leader nodes is not new as Bitcoin-NG protocol [20] was built around the leader nodes concept as discussed in the background section.
- ***Hybrid Nodes (HN):*** These nodes have less computation capabilities than the LN, so they are only able to store the block's headers but will have more roles as they will participate in the mining process by performing some of the calculations of the block hash.
- ***Participant Nodes (PN):*** These nodes are the small end devices with a very limited capabilities that are not able to perform calculations, they are environment-monitoring sensors.

## IV. Example Application: AI-enabled System for Virus Tracking in Wastewater

The pandemic created by the rapid spread of COVID-19 virus has wreaked havoc among governments, businesses, and people worldwide. Sadly, without a reliable system for tracking and tracing this spread, many people have lost their lives, and many countries have witnessed major economic downturns. Blockchain is well known for its ability to provide a secure platform for tracking and tracing, which in the case of the COVID-19 is a desired solution in helping suppress the spread of the virus and indeed any similar future viral outbreak.

According to [21] wastewater-based epidemiology (WBE) can help detect viral infection in its early stages by monitoring the presence of viral genetic markers in wastewater. Our architecture, as shown by Fig.2, can be used to quickly and efficiently forecast the potential spread of such a virus. It provides a cheaper and more practical approach: one in which the continued collection and analysis of data would serve as an early warning notification system for government agencies to make effective decisions to stop the spread of viruses. It can help in evaluating the effects of medical treatment and government interventions (such as social distancing) by monitoring the infection rate curve and whether it is increasing or decreasing. This can help in saving valuable resources and time by reducing the need for mass testing among the population while helping to control the spread of the virus.

First, the sensing layer can utilize sensors that are deployed around the main wastewater locations to collect readings on the level of viral agents in wastewater. An example of a sensor that can be used is the biosensor, a small device with a biological receptor [22]. Then the readings can be submitted to the processing layer at the edge where a trained AI system analyzes collected data and can provide a forecast of how and where the virus is spreading. The processed data will then be shared among different entities through the utilization of our blockchain platform. For example, government disease control agencies can monitor and control the spread of viruses and hospitals can acquire data and be prepared for potential patient visits.

## V. DPoW Consensus Mechanism

We propose a customised honest-based DPoW consensuses mechanism (see Fig.3), where the PoW work is distributed among the IoT devices with each carrying a small amount of the hashing calculations. This means any node can join the network freely and benefits from the available AI services in exchange for a small amount of power.

***Honesty Level:*** The protocol utilizes honesty-based PoW algorithm, which entails a small amount of work performed by different nodes. The first time a node joins the network, it will have a honesty value of zero. We define that node $n$ has honesty level value of $H_n$ and the honesty level will increase as the node behaves honestly. honesty behaviour is when the node obeys system rules, is available to participate in the mining process, and ensures it only submits correct answers to any work it carries. As a node behaves honestly, its honesty value will increase, giving the node the chance to be promoted to the leader nodes category if it has adequate resources. Unlike the works proposed by [16] and [17] we don't decreases the difficulty level of the PoW, which might compromise the security of the network, in fact as more nodes join the network the difficulty can be increases.

In the proposed consensus to reward honest nodes, as the node's honesty level increase the mining work assigned to that node decreases, this helps the node to save energy. On the other hand as the node's honesty level decreases more mining work

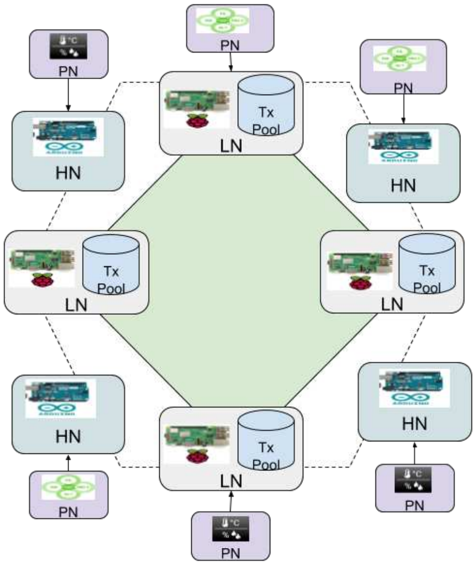

Fig. 3. Consensus Mechanise Architecture.

load will be assigned to it. The target honesty threshold of the network can be defined as $H_T$. Node *n* can be leader only if:

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

Every work has a value of honesty $HV_W$, and any correct answer to any mining work carries a positive honesty value of $H_P$. A wrong answer carries a negative value represented by $H_N$. If the total number of mining works *w* over a time period *t* is *i*, then the node's value of positive honesty at the end of this period can be calculated by:

$$H_P = \sum_{w=0}^{i} HV_W \tag{2}$$

While the node's negative honesty level can be calculated by:

$$H_N = -\sum_{w=0}^{i} HV_W \tag{3}$$

Finally, we can calculate the value of the honesty level for each node by

$$H_n = H_P + H_N \tag{4}$$

Once a node becomes a leader node, it can coordinate the mining process, validate the worker results, and sign and propagate new block when it is its turn to lead.

***Number Of Workers and Difficulty D:*** We have established the relationship between the hashing power $P_{WN}$ of a worker node *WN*, total number of workers $T_{WN}$, the Mining Time *Tm*, and *D*, where D = 1 is the minimum difficulty with Difficulty Level *DL* (the number of leading zeros at the start of the hash) is 24 by the following equation:

$$Tm = D * 2^{24} / P_{WN} * T_{WN} \tag{5}$$

The increase of the number of workers in the network results in reducing the *Tm*, correspondingly this allows for increasing the difficulty as more nodes join the network.

## VI. Implementation of DPoW

The first phase was to design a suitable blockchain platform using our proposed consensus protocol. We have created our customized blockchain platform that implements our proposed consensus mechanism discussed above. Currently, our network consists of 22 raspberry pi devices. *Leader Nodes (LNs)* as stated above, coordinate and manage the consensus process and and *Worker Nodes (WNs)* perform the mining tasks and can be any nodes from both LN and HN. Leader node selection is based on a round-robin process, and before each block mining process one leader node is elected as a miner. All other nodes apart from the miner will act as WNs and allocate a mining job to perform and reports back to the miner. The consensus process begins with the miner and takes place over four phases. If we assume it is *LN1's* is the miner. We also define transaction as *Tx*, block as *B*, Target Hash as *TH*, *DL*, the Merkle Root of all transactions that will be included in the next block as *MR*, and the target nonce as *TNonce*. Then it will perform the following:

- First, *LN1* will start the process by executing the initiation phase, which includes distributing the mining work among available WNs. A node once receives a mining work will send an reply to LN1 either by accepting or rejecting the work, no reply means node has rejected the task. This might create an overhead in terms of network traffic but it is needed to ensure devices and mining process synchronization, hence a successful mining process.
- Then, multiple Worker Nodes *WNs* ,which can be any of the node type (LN or HN) will conduct the hashing work.
- Next, *LN1* will conduct the validation of the worker-reported results and sign and propagate the next block.
- Finally, other Leader Nodes will validate the propagated block.

Algorithm 1 provides detailed steps of the DPoW consensus process we implemented in our in house built blockchain platform.

### A. Measured Results

We have tested DPoW algorithm using different numbers of workers and only one leader node. As can be seen in Fig.4, by adding more worker nodes, the mining time significantly reduced, until the network consisted of 21 worker nodes managed to mine block every 53 seconds. Figure.4 shows both the Predicted *P* (using 5) and the Measured *M* mining time for both 24 and 25 difficulties for different numbers of worker. Our network is small in its number of workers; nevertheless, within IoT with the presence of thousands of devices, the difficulty can be increased according to the number of available nodes in the network.

Figure.5 shows the Predicted *P* (using 5) and the Measured *M* mining time using 21 worker nodes while increasing the difficulty. Once the level of difficulty reaches 30, the mining time increases to above 25 minutes; however, if more devices were available to us, this time could be easily lowered to under 10 minutes. This makes such consensus mechanisms feasible to implement within IoT, and a network with thousands of available workers can achieve a reasonable difficulty to secure the network and manage the mining work between the workers to save energy.

### *B. System Evaluation*

In this paper we utilised a purpose-built blockchain within our system that provides a distributed platform for data processing and sharing. Our system implementation spans two phases. Currently, we have completed the blockchain platform using our distributed approach to the implementation of PoW with our designed consensus mechanism.Compare to other IoT based consensuses mechanism we provided a public blockchain based on secure DPoW without he need for decreasing the difficulties of the hash mining. Results showed that low-cost devices can be used for performing consensus process without substantial power cost. Because as the number of participated nodes increases, the effect on their individual power will decrease, it was ideal to use a public network for this application, with high levels of security from our consensus mechanism.

In terms of security and user trust our architecture, compared to other related frameworks, provides a distributed public blockchain platform that ensures the security of data through our proposed honesty-based DPoW. Users can see the platform's trustworthiness because it relies on an immutable, transparent, and secure blockchain. *Malicious or misbehaving Leader nodes* that try to sign and propagate an invalid block can be dealt with. The network implements a mechanism that only accepts a block from any leader node at every *N* block. If this occurs, the network will address the problem by removing the node from the network. *Dishonest Workers Nodes*, if a nodes that submit non-valid solution to the mining work this easily can be dealt with, because the network implements two rounds of validations before its accepting any new block, first by the selected leader node, then by other leader nodes.

In terms of computation power and storage limitation, we designed a consensus process that will utilise IoT devices

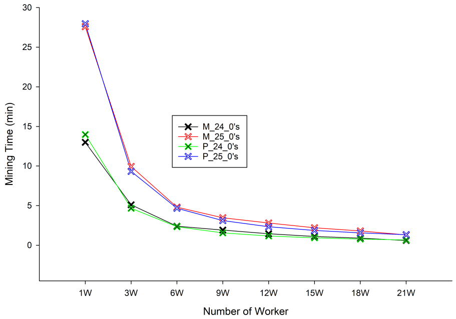

Fig. 4. Predicted *(P)* and Measured *(P)* Mining Time at Different Difficulties.

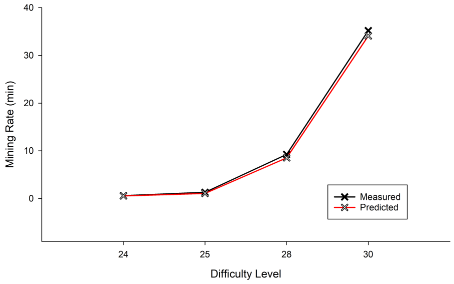

Fig. 5. Predicted and Measured Mining Time using 21 WNs.

**Algorithm 1** DPoW Consensus Process

```
Phase-1:Leader Node Issuing the Mining Work
$LN1 \leftarrow LeaderNode$
Collect all Txs from Tx's Pool
if Tx is Valid then
    $add\ Tx\ to\ B$
else
    $Discard \leftarrow Tx$
Generate MR Hash
Adjust the difficulty level (number of leading zeros)
Adjust work load for each workers
return $LH\ \&\ DL\ \&\ MR\ \&\ nonce\ range$

Phase-2:Worker Performing the Mining Work
Input: $LH\ \&\ DL\ \&\ MR\ \&\ nonce\ Range$
Output: $TNonce\ \&\ TH$
while $TH \leftarrow False$ do
    $H = Hash(LH \parallel DL \parallel MR \parallel nonce)$
    if $H\ leading\ zeros = DL$ then
        $H \leftarrow true$
        $TH \leftarrow H$
    else
        nonce++
return $TNonce\ \&\ TH$

Phase-3: LN1 Validating, Signing and Broadcasting
Input: $Last\ Block\ \&\ Worker\ TNonce\ \&\ TH$
Output: $Next\ Block$
initial: $Validation \leftarrow false\ \&\ Signing \leftarrow false$
$NHash = Hash(LH \parallel DL \parallel MR \parallel nonce)$
if $NHash\ leading\ zeros = DL$ then
    $Validation \leftarrow true$
    $Signing \leftarrow true$
    Broadcast Next Block
    $H_P \leftarrow HV_W$
else
    $TH \leftarrow invalid$
    $TNonce \leftarrow invalid$
    $H_N \leftarrow HV_W$
    Wait for other workers
```

power efficiently. The incorporation of more capable servers and devices into blockchain from government entities, research institutes, and the like, will allow for the storage of processed data on these entities' clouds and servers while the edge smart processing devices store the most recent copy of the blockchain. These intelligent devices can access the complete blockchain copy on the bigger entities mentioned above if needed.

## VII. Conclusion

In this paper we provided an intelligence architecture that leverages three current, captivating technologies: IoT system with edge layer, AI, and blockchain, which make this architecture secure, intelligent, and distributed. The main goal of this architecture is to provide a system that is able to monitor, collect, and analyse data, and provide predictions based on these data within the system coverage using AI analytic tools. Currently, the architecture is in its early implementation stage, in which we have developed DPoW consensus mechanism suited to use within IoT.

The future work will see the completion of all entities of this architecture, which will include an AI analytic and decision system and the integration of several IoT sensors. The aim is to deploy the system in different geographical areas and run a long-term field trial. Additionally, we will work toward the implementation of a distributed AI approach and an increase of deployed use cases.

## References

[1] W. Yuet al., "A survey on the edge computing for the Internet of Things," IEEE Access, vol. 6, pp. 6900–6919, 2017.

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

[3] 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.

[4] 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, Secondquarter 2019, doi: 10.1109/COMST.2019.2894727.

[5] K. Sharma, M. Y. Chen, and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," IEEE Access, vol. 6, pp. 115–124, 2018.

[6] S. Panikkar, S. Nair, P. Brody, and V. Pureswaran, ADEPT: An IoT Practitioner Perspective, IBM, Armonk, NY, USA, 2015.

[7] A. Lei et al., "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," IEEE Internet Things J., vol. 4, no. 6, pp. 1832–1843, Dec. 2017.

[8] A. Stanciu, "Blockchain based distributed control system for edge computing," in Proc. IEEE CSCS, Bucharest, Romania, May 2017, pp. 29–31.

[9] J. Pan, J. Wang, A. Hester, I. Alqerm, Y. Liu and Y. Zhao, "EdgeChain: An Edge-IoT Framework and Prototype Based on Blockchain and Smart Contracts," in IEEE Internet of Things Journal, vol. 6, no. 3, pp. 4719-4732, June 2019, doi: 10.1109/JIOT.2018.2878154.

[10] W. Rouwer, and M. Borda, "NeuRoN:Decentralized Artificial Intelligence, Distributing Deep Learning to the Edge of the Network," (2017), [Online]. Available: https://s3-us-west-1.amazonaws.com/ai.doc.static/pdf/whitepaper.pdf.

[11] M. A. Rahman, M. M. Rashid, M. S. Hossain, E. Hassanain, M. F. Alhamid and M. Guizani, "Blockchain and IoT-Based Cognitive Edge Framework for Sharing Economy Services in a Smart City," in IEEE Access, vol. 7, pp. 18611-18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[12] Kuo, T.T. and Ohno-Machado, L., 2018. "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks". arXiv preprint arXiv:1802.01746.

[13] S. Rathore, J.H. Park, "DeepBlockIoTNet: A secure deep learning approach with blockchain for the iot network," Trans. Ind. Inform. (2019).

[14] M. A. Ferrag and L. Maglaras, "DeepCoin: A Novel Deep Learning and Blockchain-Based Energy Exchange Framework for Smart Grids," in IEEE Transactions on Engineering Management, doi: 10.1109/TEM.2019.2922936.

[15] S. Singh, Y. Jeong, J. Park, "A deep learning-based IoT-oriented infrastructure for secure smart City," Sustainable Cities and Society, Volume 60, 2020,102252,ISSN 2210-6707, doi:https://doi.org/10.1016/j.scs.2020.102252.

[16] 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.

[17] 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.

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

[20] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," 2015.

[21] K.Mao,H.Zhang,and Z.Yang,"Can a Paper-Based Device Trace COVID-19 Sources with Wastewater-Based Epidemiology?,"Environ.Sci.Technol.pp.3733-3753 54, 7,2020.

[22] Z.Yang,B.Kasprzyk-Hordern,C.G.Frost,P.Estrela,and K.V.Thomas,"Community sewage sensors for monitoring public health,"Environ.Sci.Technol.pp. 5845–5846, 49, 2015.