IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received January 21, 2022, accepted February 8, 2022, date of publication February 14, 2022, date of current version February 22, 2022.

Digital Object Identifier 10.1109/ACCESS.2022.3151370

A Secure Blockchain Platform for Supporting AI-Enabled IoT Applications at the Edge Layer

SUBHI M. ALRUBEI[1], EDWARD BALL[1], (Member, IEEE), AND JONATHAN M. RIGELSFORD[2], (Senior Member, IEEE)

[1]Department of Electronic and Electrical Engineering, The University of Sheffield, Sheffield S10 2TN, U.K.
[2]Sensata Technologies, Swindon SN4 8SY, U.K.

Corresponding author: Subhi M. Alrubei (salrubei1@sheffield.ac.uk)

ABSTRACT In this study, a new blockchain protocol and a novel architecture that integrate the advantages offered by edge computing, artificial intelligence (AI), IoT end-devices, and blockchain were designed, developed, and validated. This new architecture has the ability to monitor the environment, collect data, analyze it, process it using an AI-expert engine, provide predictions and actionable outcomes, and finally share it on a public blockchain platform. For the use-case implementation, the pandemic caused by the wide and rapid spread of the novel coronavirus COVID-19 was used to test and evaluate the proposed system. Recently, various authors traced the spread of viruses in sewage water and studied how it can be used as a tracking system. Early warning notifications can allow governments and organizations to take appropriate actions at the earliest stages possible. The system was validated experimentally using 14 Raspberry Pis, and the results and analyses proved that the system is able to utilize low-cost and low-power flexible IoT hardware at the processing layer to detect COVID-19 and predict its spread using the AI engine, with an accuracy of 95%, and share the outcome over the blockchain platform. This is accomplished when the platform is secured by the honesty-based distributed proof of authority (HDPoA) and without any substantial impact on the devices' power sources, as there was only a power consumption increase of 7% when the Raspberry Pi was used for blockchain mining and 14% when used to produce an AI prediction.

INDEX TERMS Edge computing, blockchain protocol, the Internet of Things (IoT), flexible IoT hardware, artificial intelligence (AI), coronavirus disease (COVID-19).

I. INTRODUCTION

Over the years, IoT systems have grown rapidly and increasingly used by many different organizations and users within different sectors, such as healthcare and industry. The presence of IoT in these sectors has offered organizations and governments realistic opportunities to improve economic situations by enhancing its growth over the years and provides an easy way to improve people's lives in general. This is because of the vast amount of useful information provided by IoT systems that can be used for better decision-making. However, organizations often handle this data by creating IoT systems that rely on a central data-processing entity, such as the cloud, for securing and managing IoT devices and processing the data collected by these devices.

This approach of utilizing a central unit, such as cloud computing, has its own drawbacks. For instance, it introduces the risk of a single point of failure, communication overhead, and bottlenecks. This can easily affect the overall performance and security of the system, making user experiences unpleasant. It is essential for many IoT mission-critical applications to obtain secure and reliable solutions that can provide low latency for data processing. In this regard, edge computing has grown rapidly to facilitate this type of solution, providing faster data processing, allowing for near-real-time actionable outcomes. Edge computing allows for location-awareness services that allow IoT applications to produce faster, and more reliable services for users. On the one hand, edge-computing technologies provide IoT systems with these great advantages. On the other hand, as a result of the heterogeneous nature of edge and IoT end devices, the collected data may not be fully secured during transit and while stored [1].

The associate editor coordinating the review of this manuscript and approving it for publication was Jiafeng Xie.

In recent years, IoT systems' implementation has significantly increased (and this will continue in the future). This increase, in turn, has provoked the re-emergence of the AI as the main means of data analysis. These two technologies can easily create a system with capabilities to sense, think, learn, analyze, and produce outcomes in the form of future prediction and in cases where changes can take appropriate actions.

The data collected by IoT systems require security, especially in terms of integrity and availability, and the integration of a distributed and secure system, such as blockchain, can deliver these security features. Blockchain requires additional computational power and storage capabilities that some IoT devices may not have. However, the presence of edge-computing abilities can accommodate such requirements and make it possible to integrate blockchain. Combining the edge technology with blockchain technology can provide a decentralized, robust, and secure solution, offering IoT devices the ability to interact and share data among themselves and with users. The available resources on the edge devices help to provide the required computation and storage resources for the blockchain technology, allowing the end devices to exploit the security offered by the blockchain closer at the edge.

With the integration of a distributed, self-managed, and decentralized network, both the dynamic and distributed IoT systems and the intelligence AI engine will benefit greatly from such integration [2], [3]. With the presence of edge computing, these benefits include: a) providing IoT networks with a reliable ability to control and manage computation-workload distribution among a large amount of distributed IoT hardware, b) strengthening the security posture of the overall IoT system by enhancing its ability to improve data integrity and ensuring its availability and holding all participant nodes accountable for their actions [4]; c) enhancing the AI engine's ability to perform the required analyses and provide the desired outcomes using these trusted data.

A. CONTRIBUTION

- The design and development of an architecture that integrates four different technologies: IoT, AI, edge computing, and blockchain in one system that can monitor and sense the environment, learn, analyze data based on the requirements of the executed task, and produce actionable outcome. The proposed system is based on the integration of low-cost edge devices and takes full advantage of their available storage and all IoT devices' computation power to provide a data-processing and sharing public blockchain platform.
- This architecture was validated experimentally using 14 low-cost, flexible IoT hardware entities. Practical implementation and performance analyses in terms of system latency, system accuracy, and energy consumption of real-world applications in the form of an early warning system for the detection of COVID-19 in sewage water were carried out.
- A new blockchain protocol for handling communication aspects of the system and enhancing its security by providing assurance, ensuring the integrity of the data, and holding nodes accountable for their actions. It is suitable for integration into edge, and IoT devices and can handle the AI-related data.

The remainder of this paper is organized as follows: section II presents related work, followed by the proposed architecture in section III. In section IV, we provide an analysis of the system followed by the security analysis in section V, and then the implementation and testing of the system-example application in section VI. Section VII presents the results, and section VIII presents the discussions, the conclusions, and the directions for future work.

II. RELATED WORK

The integration of blockchain into the edge layer has attracted considerable attention from researchers in recent years. The authors of [5] introduced an architecture that combines the blockchain, software-defined network (SDN), and edge layer in one system. The architecture contains a device layer for collecting data, an edge (fog) for raw data processing utilizing an SDN controller, and a cloud layer for data storage and processing. Another work by IBM [6] proposed autonomous decentralized peer-to-peer telemetry (ADEPT). It is built for coordinating autonomous devices through the use of the Ethereum blockchain network and smart contract.

The framework proposed by [7] is an excellent example of how blockchain and edge layers can be used to secure IoT applications. It is introduced for vehicular communication systems by hosting security managers and blockchain, both of which are utilized to provide key transfer and management at the edge layer. Similarly, the authors of [8] proposed a new control system. It uses the hyperledger fabric blockchain, along with a smart contract, in a micro-service architecture at the edge layer to secure and validate data initiated at the lower layer. Another edge-based framework called EdgeChain was proposed by [9]. Similar to [8], it uses blockchain and smart contracts at the edge, so that devices in the lower layer can access resources at edge servers.

Another research area that has gained similar attention from researchers is the integration of blockchain, edge computing, and AI technologies. The work by [10] using blockchain and machine learning introduced a prediction framework called ModelChain. This allows multiple healthcare institutions to train the same framework for better results in terms of health prediction. The BlockDeepNet framework was proposed by [11] for data analysis within IoT systems. It combines blockchain technology, smart contracts, and deep learning. The authors of [12] introduced a blockchain-based NeuRoNt platform that integrates multiple agents by using smart contracts to solve complex problems. A similar approach utilizing both Ethereum and smart contracts was taken by the authors of [13], who proposed

TABLE 1. Summary of the important related works.

Paper	Application	Solution	Technology-utilized	Limitations
[11]	Deep learning DL for object detection in IoT applications	Secure DL model based on blockchain to support collaborative DL in IoT	DL, blockchain, smart contract, edge, and IoT	Local models only, trained on local private data. Limit models' ability to access all data
[14]	Energy exchange for smart grids	An intrusion detection system (IDS) that employs recurrent neural networks (RNNs) to detect network attacks and fraudulent transactions in the blockchain-based energy network.	Blockchain, RNN, and smart grids	The consensus process is long and this could have a negative impact on the transaction finality and the system latency
[15]	Smart city	Deep learning-based IoT-oriented infrastructure for a secure smart city where blockchain provides a distributed environment at the communication phase of CPS, and software-defined networking (SDN) establishes the protocols for data forwarding in the network.	Blockchain, DL, SDN, fog, cloud, and IoT	The proposed system does not realize the full potential of the decentralization approach provided by the blockchain as it relies on a central cloud entity
[17]	Data-sensitive applications for example, healthcare.	Proposes and implements an Ethereum blockchain based architecture with edge artificial intelligence to analyse data at the edge of the network and keep track of the parties that access the results of the analysis	Blockchain, edge computing, and AI	Scalability can be an issue because gateway can only support a limited number of end-devices. Requires additional scalability analysis.
[18]	Mission-critical applications	Blockchain based edge intelligence (EI) system for improved data security, privacy, and performance. It uses a public blockchain to ensure the communication security of consumer electronic devices (CEDs) and a private blockchain to ensure communication security among EI servers.	Blockchain, smart contract, edge computing, and AI	Lacks analyses in terms of the effect of the overall system latency and scalability on mission critical applications and comparison with other related works.
[19]	AI-envisioned Internet of Vehicles (IoV)-based smart city	blockchain-based batch authentication scheme for IoV.	AI, blockchain, fog, cloud and Internet of Vehicles (IoV)	Network relies on cloud to convert and mine full blocks.
[20]	Healthcare applications (diseases' control)	Blockchain-based AI-empowered pandemic situation supervision scheme in which a swarm of drones embedded with AI is engaged to autonomously monitor pandemic outbreaks	Blockchain, AI, drones, edge computing, and cloud.	While this is a good solution for controlling the spread of diseases or viruses; it introduces the issue of human and data privacy.

a mobile edge system for service sharing and data processing in smart-city IoT applications. The DeepConin framework was introduced in [14] for fraudulent transaction detection and blockchain-attack prevention based on deep learning and blockchain within smart-grid applications. A similar framework based on blockchain was introduced in [15]. It uses deep learning and SDN to allow smart city applications to access and utilize cost-effective and high-performance computing resources.

The authors of [16] provided a practical integration that combines federated learning (FL) and blockchain with the aim of securing big data and preserving privacy within IoT systems. It achieves this by using fuzzy hashing to detect suspicious activities, such as poisoning attacks in FL-trained models. The authors of [17] also proposed an architecture for data analysis at the edge based on blockchain and AI. The aim is to enhance the security of privacy-critical systems, such as healthcare applications, by restricting raw data to producers only. The authors of [18] proposed a blockchain-based edge intelligence (EI) system for improved data security, privacy, and performance. It uses a public blockchain to ensure the communication security of consumer electronic devices (CEDs) and a private blockchain to ensure communication security among EI servers.

The work by [19] introduced a scheme for batch authentication in the Internet of Vehicles (IoV) based on blockchain and AI. The aim is to address the security challenges that result from the communication between different entities within IoV-based smart cities. The scheme provides the IoVs with the secure ability to authenticate themselves when two vehicles are communicating and for a group of vehicles to be authenticated by the roadside unit. The authors of [20] proposed a pandemic situation supervision scheme based on blockchain and AI. It utilizes an AI-equipped swarm of drones to monitor an outbreak in the case of a viral pandemic. This scheme was designed to help control the spread of viruses by ensuring that people follow the guidelines and performing surveillance checks (e.g., face coverings, temperature measurements, and social distancing). Similarly, the work by [21] proposed the use of blockchain technology along with unmanned aerial vehicles (UAVs) for patient data collection within healthcare. It uses UAVs to collect data and a blockchain to store the collected data. It uses tokens and shared keys to establish secure communication with users' body sensors. Table 1 provides a summary of the important related work, including the solution provided, the applications, and the limitations in each work.

III. SYSTEM ARCHITECTURE

The proposed architecture provides a system for collecting data, processing, and analyzing data and produces a sharable outcome among nodes. A general overview of this architecture is presented in Fig.1. The platform operates according to the following three steps:

- The first step is the *Monitoring and Collection* step: the IoT system monitors the environment or situation and utilizes its sensors at the lowest layer to collect the environmental or change data.

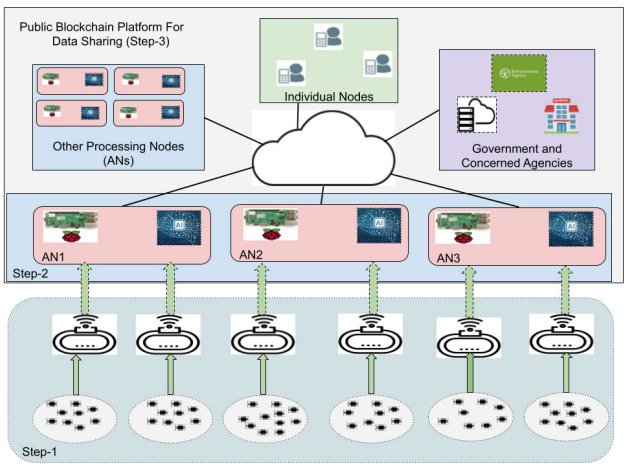


FIGURE 1. General concept of the system architecture.

- The second step is the *Analysis and prediction* step: in this step, the collected data is propagated to the intelligent engine located at the edge nodes for analyses and providing predictions.
- The third and the final step is the *Sharing* step: in this step, the produced outcome from the edge devices are shared among all participant nodes on the freely accessed public blockchain network.

A. ARCHITECTURE DIFFERENT LAYERS

To accomplish the three previously discussed steps and provide free access to the public blockchain platform, we designed an architecture that consists of four different layers. Figure. 2 provides the layout of these layers.

1) SENSING LAYER

This is the lowest layer in the architecture and is the most important layer; it is the data feeder to the sharing platform. In this layer, a wide range of many low-cost, low-power, and small sensor devices are used for monitoring and data collection. The collected sensor data will then be submitted to the gateway, which can be in the form of low-cost devices (e.g., Arduino ESP-32), which can then be validated and prepared and then submitted to the next layer for processing. This aids in achieving the first step of our architecture, which is the *monitoring and collection*.

2) NETWORK LAYER

The data submitted by the gateway is then transferred to the next layer. This is where the network layer takes part. In this layer different communication links can be utilized (for example, wireless connectivity, such as the Wi-Fi, LoRaWAN, or 5G, or a wired connectivity).

3) PROCESSING LAYER

This layer is equipped with the necessary AI engine to perform the required analyses and is responsible for achieving the second step in the architecture, which is the *analyses and prediction*. Devices deployed at this layer can be low in both cost and power, and one example of such a device is the Raspberry Pi (R-pi). The data collected by the sensing layer arrived at this layer. The AI-expert engine located at these edge devices will then be used to process and analyze the data and then provide predictions and necessary outcomes that can be used to help the decision-making process. All nodes located in this layer should be a full clients of the blockchain platform (see Subsection III-B). This means that these nodes will be able to share their collected data and AI outcomes instantly with the rest of the blockchain clients. In doing so, the platform will have a continuous stream of data (collected by sensors and the outcome of the AI), allowing for a better performance of the system.

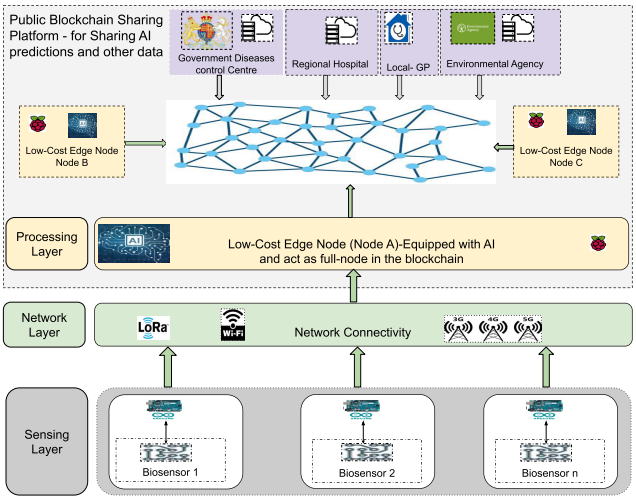


FIGURE 2. Example application - detailed system architecture.

4) SHARING PLATFORM

This is a freely accessible and a public blockchain platform and is responsible for achieving the *sharing* step, which is the final and last step of the architecture. All the devices in the processing layer are part of the public blockchain. This would allow any organizations, users, or other concerned parties to be part of such a platform and have the ability to freely access all processed AI and collected data.

B. BLOCKCHAIN PROTOCOL

Designing a blockchain protocol that has the ability to handle different types of transactions, including those related to AI engines, is an essential part of our proposed architecture. Therefore, a new blockchain platform, including bespoke transaction and block-header formats, has been designed, developed, and implemented. In terms of the consensus mechanism, we utilized our own consensus protocol called honesty-based distributed proof of authority (HDPoA), which we previously published in [22]. The blockchain platform can utilize the resources of all the available IoT devices. Based on this, we categorized these devices into three different classes based on their hash power and storage capabilities, as follows:

- *Full Client (FC)*: These can be low-cost devices that have enough hash power and storage capability. This would allow these clients to play more roles in terms of consensus mechanisms and storage of the full chain. One example of such a low-cost device that can be utilized as a full client is R-pi.
- *Hybrid Client (HC)*: These devices are low in cost and power. They may have limited resources in terms of storage capability, but their available power can be utilized for the purpose of carrying a small number of the hashing task. These devices can act as gateways in which many sensor devices are connected.
- *Participant Client (PC)*: These are the small sensor devices at the sensing layer. Although they cannot be part of the blockchain, they still play an important role in our proposed architecture, as they are the data feeder to the processing layer.

In terms of HDPoA, the roles of the nodes in the consensus mechanism are classified into two types of nodes. *Authority Nodes (ANs)*, these nodes are from the FC class and have enough trust levels to manage and coordinate the mining process. *Worker Nodes (WNs)*, any node that is able to participate in the mining process is classified as WN and can be from both FC or HC; only the current AN that manages the mining process cannot be part of the WNs. All other nodes should make themselves available for the mining tasks. More details regarding how HDPoA works can be found in [22].

IV. SYSTEM ANALYSIS

The proposed system utilizes a free-access public blockchain network where the lowest value of the difficulty D is one—that is, when the value of the target hash h_v is 2^{232}. In the network, the sources of data traffic are broadcast transmission processes of transactions and blocks through the network. The important parameters used are listed in Table 2.

A. TRANSACTIONS CONFIRMATION TIME AND THROUGHPUT

The probability of any transaction (including AI-related transactions) to arrive and confirm on the network can be measured based on the Poisson process, in which the outcome can arrive on a confirmed block with an arrival rate of λ. The following equation is used as the starting point for driving all the equations in this subsection.

$$P(T \leq t) = 1 - e^{-\lambda t} \tag{1}$$

In the proposed blockchain system, as discussed above, the HDPoA-consensus mechanism does not require extra time to confirm the arrived block, as long as none of the authority nodes (ANs) initiate a block rejection process. Based on this, we can define λ as $\lambda = \frac{1}{M_t}$ block/s, where $M_t = \frac{D \times 2^{24}}{h_p}$.

TABLE 2. System parameters and their definition.

Parameters	Definition
M_t	Mining time required to find the correct hash for one block
T_pd	Average time required to propagate a transaction from one node to all other nodes in the network
B_pd	Average time required to propagate a block from one node to all the other nodes in the network
V_t	Average time consumed by a node to validate a new block and all transactions in that block
D	Blockchain mining difficulty
V	Voltage
L	Time from the submission of the AI input values until the final AI output value is confirmed on the blockchain network
h_p	Number of hash/s produced by any node on the blockchain

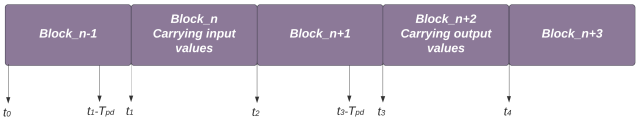


FIGURE 3. Overall system latency and the processing of AI data.

The t parameter (i.e., time) relies on the number of blocks n the user needs to wait before the block carrying the transaction (e.g. AI-expert engine final prediction) is confirmed on the network, B_{pd}, and V_t of the new block. Based on this, the probability ($P(n)$) of the confirmation of any transaction (including AI-related transactions) can be calculated as:

$$P(n) = 1 - e^{-\left[\left(\frac{1}{\frac{D\times 2^{24}}{h_p}}\right)\times n\times\left(\frac{D\times 2^{24}}{h_p}+B_{pd}+V_t+Tpd\right)\right]} \tag{2}$$

Based on this the *confirmation time* C_t of any transaction can be calculated by:

$$C_t = \frac{\ln(1-P(n))}{\frac{-1}{\frac{D\times 2^{24}}{h_p}}} + B_{pd} + V_t + T_{pd} \tag{3}$$

To provide an estimation of the network throughput (i.e., transactions per second), we assume that the block size is B_{size} and the transaction size is Tx_{size}. Then, the network throughput can be calculated by:

$$Throughput = \frac{\frac{B_{size}}{Tx_{size}}}{C_t} \tag{4}$$

B. SYSTEM OVERALL LATENCY (L)

Measuring the overall system latency (L) is an important aspect of the system performance metrics. To calculate (L), we assume that all AI-related transactions arrive at the elected AN transaction pool on time to be included in the next block. As shown by Fig. 3, we assume transactions submitted before the time $t_1 - T_{pd}$ will be included in the next block (Block_n). Another important aspect of the proposed system we need to consider is the fact that we validate the AI input values and the final outcome of the expert engine on the blockchain network. This means that two rounds of confirmation are needed before the arrival of the final outcome. Based on these assumptions and considerations, the overall system latency L can be calculated as follows:

$$L = 2 \times \left[\frac{ln(1-P(n))}{\frac{-1}{D\times 2^{24}/h_p}}\right] + B_{pd} + T_{pd} + V_t \tag{5}$$

C. POWER COST

The energy consumption of both the blockchain and the AI-engine is a significant parameter of the proposed architecture; therefore, it is important to analyze this parameter and identify its impact on the power sources of the devices. Each device is typically in one of the following states:

1) Sleeping state (S): In this state, the device will not perform any task. Instead, it will goes to sleep and wakes up by a timer or event. In this state, power consumption can be identified by p_s:
2) Connectivity state (C): In this state, the device's operating system is active, and it is connected to the available connectivity link (i.e., Wi-Fi link) and does not perform any task. In this state, the power consumption can be identified by p_c. This is our reference state, in which we compare the energy consumption of the other states.
3) Data Exchange state (DX): During this state, the device will indeed be in data transmission or data reception. The power consumed during this state can be defined as p_{dx}.
4) Worker state (W): In this state, the device is engaged in the blockchain-mining activity by performing a small task of the block-mining process, in search of the nonce for the new block. In this state, the power consumption can be identified by p_w:
5) prediction state (PRE): In this state, the device will receive the AI-input values and then will utilize its built-in AI-expert engine to process these values and produce an AI prediction. During this state, the power consumed is defined by p_{pre}:

Based on these states, we can calculate the total power p_{tot} consumed by any device in the blockchain network as follows:

$$p_{tot} = p_s + p_c + p_{dx} + p_w + p_{pre} \tag{6}$$

The system will be in each state for a certain amount of time, and the time of the sleeping state can be identified as s_t; during connectivity state, it can be defined as c_t; during the data exchange state, it can be defined as dx_t; during the worker state, it can be defined as w_t; and during the prediction state, it can be defined as pre_t. These values, along with the measured power in each state, can be used to calculate the energy consumption EN of any device as follows:

$$EN = (p_s \times s_t) + (p_c \times c_t) + (p_{dx} \times dx_t) + (p_w \times w_t) + (p_{pre} \times pre_t) \tag{7}$$

Based on this equation and the different system states, we can calculate the cost of power (P_{cost}) (J/s) during the worker state (p_w), or the prediction state (p_{pre}), in comparison to when the system is in the connectivity state (p_c), our reference state, using the following equation:

$$P_{cost} = (p_w, p_{pre}) - p_c \tag{8}$$

Battery life (B_{life}): When dealing with the small battery-powered IoT devices, it is essential to utilize them in a way that ensures limited impacts to their batteries. We designed our architecture to ensure a limited impact on the battery life of the devices. Based on the above assumptions and the calculation of the power consumption and cost, the life of a battery with a capacity of $B_{capacity}$ can be calculated by:

$$B_{life} = \frac{B_{capacity} \times V}{EN} \tag{9}$$

V. SECURITY ANALYSES

For security analyses, we performed a qualitative risk assessment of the proposed architecture using the NIST SP-800-30 standard [23]. Table 3 shows the determination of the risk level based on attack likelihood and its impact level. The following subsections discuss the risks associated with the most likely attacks that can target our architecture.

A. DENIAL OF SERVICE (DoS) ATTACK

The architecture was designed to allow nodes to access the services provided by the AI-expert engine; however, a DoS attack against the node hosting the engine is possible. The system was designed to enhance the robustness of the AI engine by utilizing the distributed approach provided by the blockchain. In our experiment, we utilized one node to host the AI engine, which has the ability to allow any of the ANs to host the AI-expert engine, and each node can produce its own prediction value, as all nodes have access to the data in the blockchain. In fact, with the implementation of the blockchain and the bespoke protocol formats, it is possible to implement the AI in a distributed approach, in which each AN can host one layer or more of the engine, allowing for more transparency, as the flow of the data from one layer to another will be validated on the blockchain network. This makes the system robust against any attacks that target the services provided by the AI engine.

Therefore, although the likelihood of a DoS attack is *high*, its impact's level is *low* making the residual risk level of this attack *low*.

B. DATA INTEGRITY ATTACKS

The integrity of the data is very important for ensuring that AI prediction is performed on legitimate and fresh data. Nevertheless, the integrity of the data can be targeted and can be vulnerable to manipulation. In our proposed system, the blockchain platform is utilized to first validate new data before adding them to the system. Second, it ensures that the

TABLE 3. NIST SP-800-30 determination of the risk's level [23].

Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

added data cannot be modified or deleted. This feature of the blockchain enhances the system's ability to ensure that the AI engine accesses only trusted and fresh data. However, there is still the risk that some sensors may feed the system a fabricated or untrue data. This might not be detected; however, once any node is discovered behaving in a manner that could harm the data integrity, our HDPoA consensus algorithm will blocks that node from feeding or accessing the data on the blockchain.

With the presence of our HDPoA-based blockchain platform, the likelihood of any attacks that can harm the data integrity is *low*, and their impact can be *high*. This makes the residual risk level of any attack *low*.

C. MALICIOUS AN

It is possible that one of the ANs can be malicious or that it can be compromises. A malicious AN can harm our architecture in two ways: either by forging a new block or by producing an untrue AI outcome. In both cases, the platform can manages this node. First, the block-mining process is performed by multiple unrelated WNs. Second, other ANs on the network only add and validate a new block produced by the elected miners (see [22] for more details). If such a block is not valid, then the node that produced the block will be eliminated from the AN category, and it will have to build its trust from zero. In terms of the AI prediction, we built the system to allow any trusted AN to host the AI-engine. This would allow the network to utilize more than one node to perform the AI prediction, allowing for more validation and outcome-consensus of any outcome before it is confirmed on the blockchain.

The impact of any attack from any malicious AN *high*; however, the likelihood that ANs can misbehave or become compromised is *moderate*, making the residual risk level of any attack *moderate*.

D. MALICIOUS WN

Similar to the malicious AN, any WN can be malicious, or it can be compromised. Any WN can misbehave, and this can only occur in the form of submitting incorrect solution to any assigned task. The platform can easily address this problem. First, any solution submitted by any WN will be validated by the elected AN. Second, any new block will be validated by other ANs on the network, thus eliminating the collusion between any malicious or compromised ANs and WNs.

Although the likelihood of an attack by a malicious WN is *high*, the impact of such an attack is *low*, which makes the residual risk level of any attack *low*.

E. 51% ATTACK

The traditional 51% attack targets the control of the blockchain network by controlling the majority of the hash power (i.e., 51% or more). This type of attack, if successful, provides the attacker with total control of the blockchain platform. Our consensus mechanism deployed in the blockchain platform eliminates attacks that are associated with controlling the majority of the hash power. This is because the mining process is divided among multiple unrelated WNs, and it also deploys an added security layer by incorporating the AN category along with the PoW process. However, in our blockchain platform, for this attack to be successful, the attacker needs to have control of the majority of the ANs (control more than 50% of ANs). Although this is possible, it is also very time consuming, making it difficult to achieve.

Therefore, the likelihood of this attack is *moderate*, and the impact, if it is successful, is *very high*, making the residual risk level of this attack *high*.

F. ATTACK ON COMMUNICATION LINKS

Attacks on the communication links, such as jamming and DoS are possible. The main focus on this study was to evaluate the performance and security of the a blockchain platform when utilized in supporting AI-enabled IoT applications. Hence, we assume that the network provider will has adequate security mechanisms and protection in place.

Even though attack likelihoods on communication links can be *moderate*; the impact of such attacks is *low* on the assumption that adequate protection is in place, making the residual risk level of this attack *low*.

VI. IMPLEMENTATION AND TESTING OF EXAMPLE APPLICATION: AI-ENABLED SYSTEM FOR TRACKING VIRUSES IN SEWAGE WATER

The worldwide pandemic caused by the novel coronavirus COVID-19 has wreaked havoc among organizations, governments, and businesses. The lack of robust and reliable tracking and early warning systems and platforms has resulted in the loss of many lives and major economic losses. Technologies such as blockchain, IoT, and AI can provide governments with a secure, intelligent, and robust platform for tracking and tracing and for implementing early warning system. Such a system is a desirable solution that can help in tackling the spread of COVID-19 or other future viruses and allows governments to save lives and reduce economic impacts. In this system, the sensing and data-collection ability of the IoT can be combined with the decentralized and secure abilities offered by blockchain and, with the intelligence capabilities of the AI, can provide the best solution that can be utilized to tackle current and/or future pandemics.

According to the author of [24], wastewater-based epidemiology (WBE) offers an effective method for the early detection of possible viral infections before its actual spread by tracking and measuring the presence of viral genetic markers in wastewater. The proposed architecture discussed above is shown in Fig. 2. It provides an affordable and more practical system that can be utilized to efficiently and securely predict the possibility of any viral infections. By continuously collecting and analyzing the data, the system will serve as an early warning notification for concerned entities, such as disease-control agencies, allowing them to take effective and early actions to slow down or stop the spread of such a virus. Additionally, the system's ability to serve as an early warning

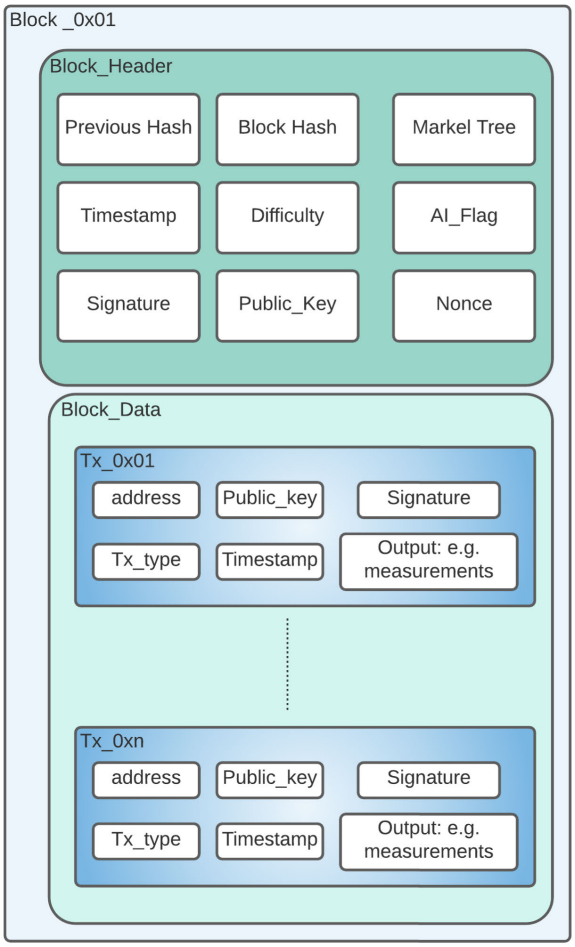


FIGURE 4. Block's header and transaction formats.

notification platform can also help governments evaluate the effectiveness of other virus-control measures, such as social distancing, lockdown, and mass testing.

A. BLOCKCHAIN IMPLEMENTATION

We developed and implemented our own blockchain platform secured by the HDPoA consensus mechanism that we previously developed and tested. This platform is a public blockchain where any node can join in exchange for a small amount of energy through its participation in performing tasks on the network, such as performing a small amount of block mining or AI prediction. For our platform to handle different transaction types on the network, including AI-related transactions, we created and implemented a bespoke transaction and block's header formats, as shown in Fig. 4.

In terms of the consensus mechanism discussed above, there are two types of nodes in the network: ANs and WNs. ANs are responsible for ensuring the security of the blockchain by managing the mining process, validating transactions and blocks, validating any work performed by a WN, and validating each other's work. Any node that joins the blockchain for the first time will join as a WN and then build its own honesty level until it can be promoted to the AN category. Full details of how HDPoA works can be found in [22].

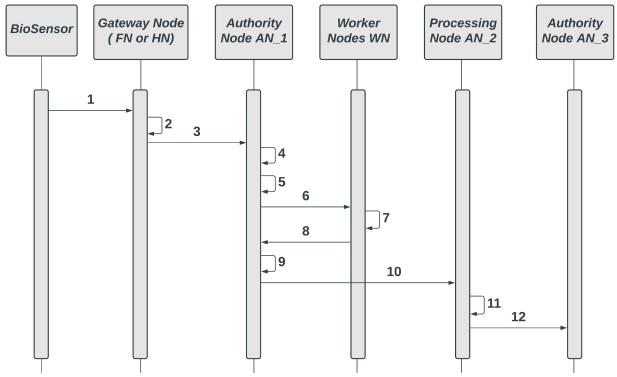


FIGURE 5. Data flow within the different layers of the architecture.

B. DATA FLOW

Figure. 5 shows the different steps of the data flow in the system. These steps are as follows:

1) First, the sensors that are installed in the different sewage-water locations will sense and collect data in the form of readings of any presence of viral agents in sewage water. One sensor that can be used is a biosensor with a biological receptor [25]. These readings are submitted to a gateway that can be either a FC or a HC.
2) The gateway will validate the readings (if it was signed by the sensor), create a transaction, and label the type of this transaction as an AI-input value.
3) Then, the gateway will broadcast the transaction to all ANs on the blockchain network.
4) Assuming node AN_1 is responsible for the mining process of the next block (i.e., $block\_n$), it will collect transactions, validate them, and add them in a new block, and it will set the AI-flag to the appropriate value (0 or 1).
5) Then, in step 5 AN_1 will create mining tasks for all the available WNs and send the tasks to each one of them.
6) Upon receiving the task, any WN will accept it and begin performing the process of searching for the correct nonce that satisfies the current difficulty.
7) If any WN finds the nonce that satisfies the next block difficulty, it will forward it to AN_1 and all other ANs for future validation.
8) AN_1 receives the nonce and then will validate it by executing one hash.
9) If the nonce is valid, then $block\_n$ will be signed and propagated to the network.
10) Once $block\_n$ arrives at the processing node (we assume this node is AN_2), it will extract the relevant AI input values, feed them to the AI-engine,

TABLE 4. Example of our created test dataset, based on information from related work [27]–[29].

Viral proteins S PFU/mL	Viral proteins N PFU/mL	Viral genetic material RNA PFU/mL	Output
1.28	13.12	9.92	1
1.12	8.80	8.00	0
5.92	16.00	10.24	2
6.08	13.12	2.24	1
0.64	0.96	13.12	0
2.72	0.96	1.92	0
12.16	14.40	14.08	2

process them, and produce the final AI outcome (the prediction). This processing of the input values by the AI-engine occurs during the mining process of $block\_n + 1$.

11) AN_2 will then add this outcome to a transaction and propagate it to all ANs on the network.
12) Assuming the node responsible for managing the mining process of the next block ($block\_n + 2$) is AN_3, it will execute the same steps as 4–9, and will then propagate $block\_n + 2$ that carries the final AI outcome to the network. Now, the AI outcome is available on the public blockchain and can be accessed by any interested government entity or organization.

C. EXPERIMENT AND TESTING

To test our system, we deployed a blockchain network and used 16 R-pis. Two were used as ANs and 14 were used as WNs. One AN was used for managing the mining process, and we developed, trained, and deployed an AI-engine on the other AN. The AI-engine consists of three inputs and three outputs. For the hidden layer, we utilized the tenser-flow kerase dense function [26], and for activation functions, we utilized Relu and SoftMax. Figure. 6 shows the architecture of the AI-expert engine.

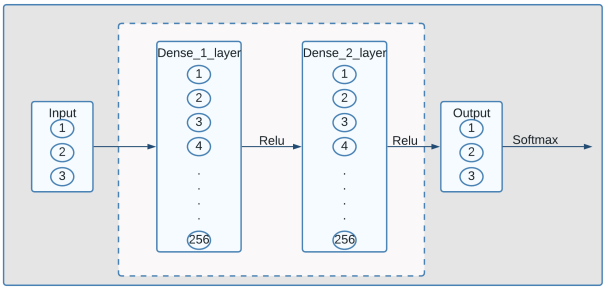


FIGURE 6. The architecture of the AI-expert engine.

It was very difficult to find any COVID-19 dataset related to wastewater, therefore, based on the literature, we created our own test dataset. Based on [27], biosensors, such as electrochemical reaction biosensors, can be utilized to measure and detect the levels of viral nucleic acids, proteins, and small molecular antibodies. Different studies investigated the use of biosensors for detecting COVID-19 in wastewater [27]–[29]. One common way to measure viruses and proteins using biosensors is the plaque-forming units PFL/mL; for COVID-19, this could be up to 16 PFU/mL [27]. The method used to create our dataset is based on the assumption that there are available biosensors to measure three different parts of the virus: viral proteins S, viral proteins N, viral genetic material RNA, and provide readings measured by PFL/mL. We created data based on three input values: viral protein S, viral protein N, and viral genetic material RNA. The higher the PFU of each input, the higher is the COVID-19 infection rate in a certain area. We classified our AI outcomes into three different categories: low risk, medium risk (needs attention), and high risk (needs immediate action). Table 4 presents an example of our test dataset, where the numbers in the table are representative of those found in [27]–[29].

VII. RESULTS

A. SYSTEM LATENCY

We tested the system while mining using different numbers of WN (1 to 12 WNs). We then measured the overall latency of the system for each test. Figure. 7 shows the average L. From the figure, we can see that as the number of WNs participating in the block mining process increases, the average L decreases. We managed to lower the overall latency from over 40 min when we were using only one WN to approximately 4.3 minutes when the total WN utilized to mine one block was 12. If we had more WN at hand, this time could have been reduced to less than one minute.

B. AI-ACCURACY

In terms of the AI engine accuracy, the system was first trained on 70% of the dataset, using R-pi, and produced a

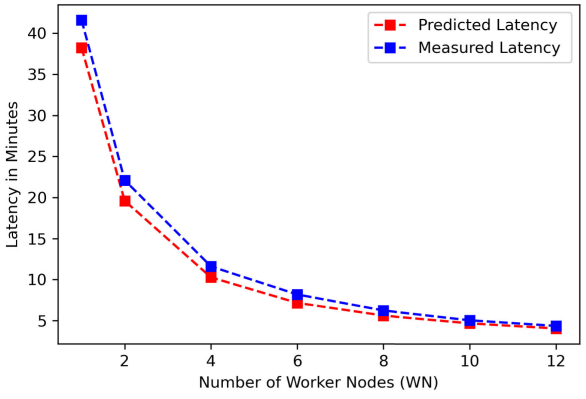


FIGURE 7. Measured and predicted system overall latency.

prediction accuracy of 97%. We then tested the system on a stand-alone R-pi device, not connected to the blockchain network, using 15% of the dataset, resulting in a prediction accuracy of 95%. In the final test, we deployed the system on the blockchain network using one AN. We then tested the system in three rounds. With each round, we used 5% of the remaining dataset (the data were sent over the network as blockchain transactions, as described by the data flow in Fig. 5). All three rounds of the unseen dataset resulted in the same prediction accuracy of 95%, which is the same as when testing using the stand-alone system. This shows that utilizing blockchain for better data security did not affect the AI-engine accuracy; Fig. 8 shows the accuracy for both tests compared to the training.

C. POWER COST

An important aspect of the proposed system is the impact on the battery and power sources of devices. To investigate this impact, we measured the power consumption during different system states, including connectivity (C), data exchange (DX), worker (W), and prediction (Pre). Figure. 9a shows the consumed power by the R-pi during each of these states. It is clear that the impact of using the device for mining or hosting the AI engine is minimal, as most of the power is consumed when the system is running and connected to the Wi-Fi without performing any task. This is clear in Fig. 9b, as it shows the percentage of the power increase when the system is utilized to perform blockchain mining, data exchange, or AI prediction. When using the R-pi for AI prediction, the power increase was 14%, and this increase was 7% when utilized for blockchain mining. However, in a network where the available number of WNs and ANs is a few hundred or even thousands, such an impact can be eliminated, as we would have more than enough nodes to perform different tasks in the network. This means that a device may spend a day without performing any task.

Battery Life is an important factor in our proposed system. We designed our architecture with the aim of protecting the battery-powered IoT devices. We predicted the impact on the battery life of such small devices [using (9)], and, as can be seen in Fig. 10, these small devices can participate on the network without substantial impacts to their batteries. For example, in a network of 3,000 WN a battery with a capacity of 600 mA has an expected life of more than two months. This expected life is well above three months, when the number of WN is increased to up to 5,000. This shows that these battery devices can access the service of the blockchain network by performing small tasks with limited impact on their battery life.

D. THROUGHPUT AND BLOCK SIZE

The block size is an important aspect when calculating the network throughput (transactions per second); as the block size increases, the throughput increases, and vice versa. Our experiment was conducted using a reliable connectivity in the form of Wi-Fi, which connects nodes to each other. In [30], an intensive study of the impact of the block size on IoT-blockchain applications was performed, and it was found that a block size of less than or equal to 1 MB should be used. Conversely, in our work, we limited the block size to a maximum of 500 kB for better energy efficiency, and to limit the impact of the block size on the network synchronization. This allows the number of WNs to increase, and hence, a lower mining time, while maintaining high network synchronizations among nodes. We tested the network throughput when the block size was 500 kB while varying the number of WNs that participated in the block-mining process (4–14 WNs). Table 5 lists the throughput. Clearly, as the network grows in terms of the number of WNs, the throughput increases. This is because the block-mining time decreased.

We had only a limited number of devices at hand to conduct large-scale experiments. However, to investigate the impact of the number of WNs that are available on the network to participate in the mining process, we calculated that impact in terms of the number of WNs, transaction confirmation time, difficulty, and throughput, using (3, 4). Figure. 11 shows the predicted throughput for different network setups. It is clear in the figure that as the number of WNs increases, the throughput can be increased. For example, a network

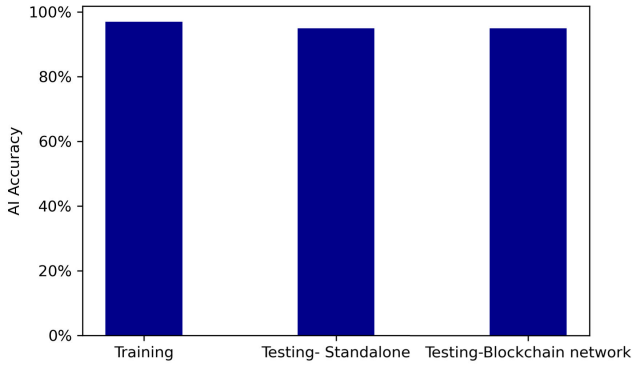
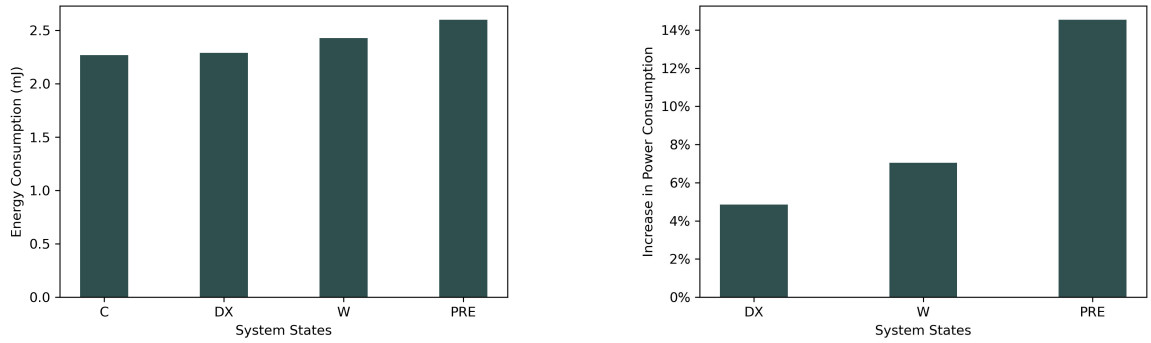


FIGURE 8. Accuracy of the AI-expert engine.

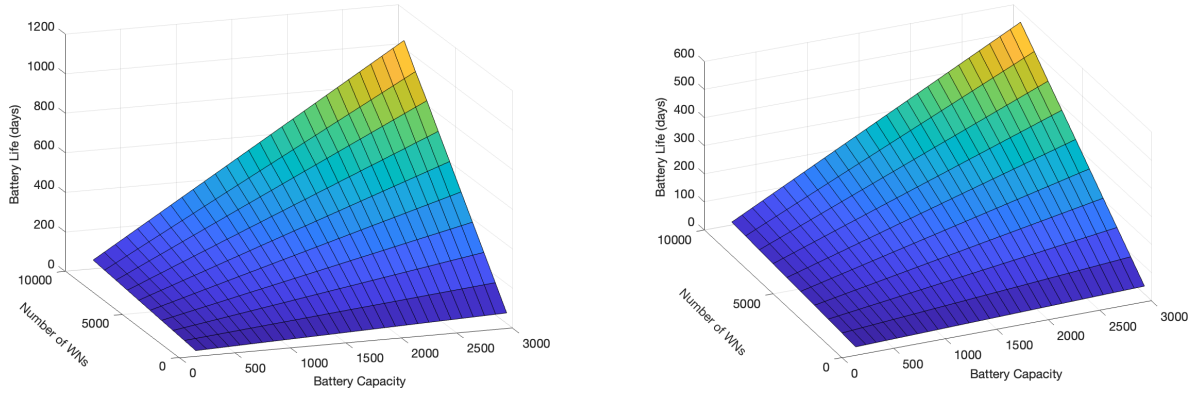
TABLE 5. Measured throughput (Tx/s) for different network with varying number of WNs.

Available WN	Tx confirmation time (s)	Throughput (Tx/s)
4	264	11
6	177	16
8	134	21
10	106	26
12	88	32
14	74	38



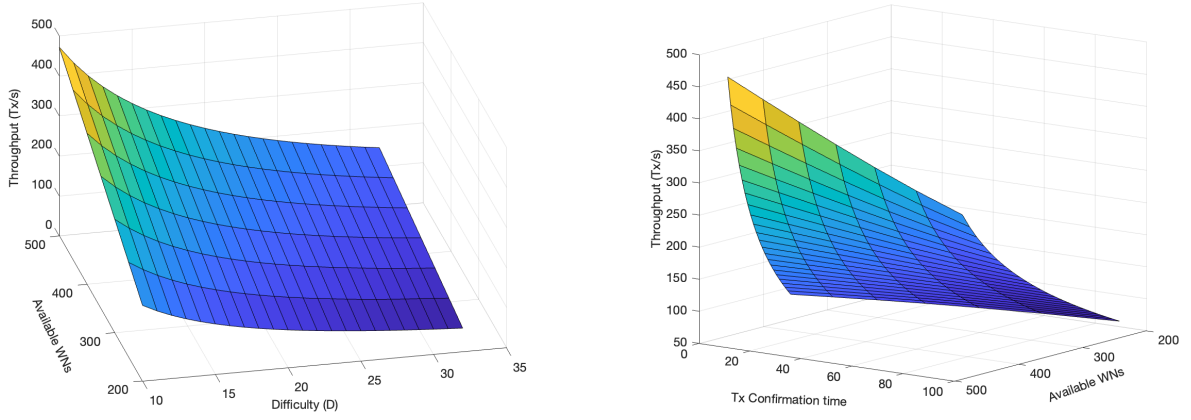
(a) (b)

FIGURE 9. Energy and power measurements. (a) Average energy consumption of the system states. (b) Power cost when the system is in the DX, W, and PRE states compared to when the system is in the C state, that is, the reference state.



(a) (b)

FIGURE 10. Predicted battery life for battery powered IoT devices. (a) Network with mining difficulty of 4. (b) Network with mining difficulty of 8.



(a) (b)

FIGURE 11. Calculated throughput for different network's setups. (a) The number of WNs, difficulty, and throughput. (b) The number of WNs, transaction's confirmation time, and throughput.

of 500 WNs and mining difficulty of $D = 10$ can achieve a network throughput of 471 Tx/s. This shows the flexibility and scalability of our blockchain platform, where HDPoA can enhance the network's security by increasing the difficulty when the number of nodes increases and simultaneously achieves higher throughput.

TABLE 6. Performance comparison between this paper and important related works.

Paper	AI data integrity through validation and transparency.	AI engine Robustness and Redundancy	Blockchain Throughput	AI accuracy	Power Cost	
					AI performing prediction	Blockchain mining
This Paper	Yes. All input data and AI outcomes were validated and added to the blockchain	Yes. The AI can be deployed across different ANs, and each node can produce its own outcome.	Measured up to 38 Tx/s Predicted up to 450 Tx/s.	95%	Increase of power cost by 14%	Increase of power cost by 7%
[11]	Not all the data are validated. Local model trained on local data.	Partially. IoT devices rely on edge servers and the cloud.	Not given	Over 70%	CPU usage of 30%. No power consumption measured	CPU usage of 30%. No power consumption measured
[14]	No. Only trading data are recorded in the blockchain.	Yes	About 3000 Tx/s, not considering the long transaction confirmation time.	Up to 99%	Not given	Not given
[15]	Yes	Partially. Used centralized deep learning-based cloud	Not given	Not given	Not given	Not given
[17]	Partially. Only processed AI data validated on the blockchain	Yes	Not given	Not given	Not given	Not given
[18]	Partially. Some local processing at the consumer electronic device layer	Yes	Not given	Not given	Not given	Not given
[19]	Yes	Partially. It relies on the cloud to convert and mine full blocks.	Not given	Not given	Not given	Not given
[20]	Yes	Yes	Not given	95.18%	Not given	Not given

VIII. DISCUSSION AND CONCLUSION

The proposed architecture provides a platform that is secure, robust, and effective in terms of power and throughput to support AI-enabled IoT applications at the edge. The system is able to ensure continuous AI prediction, thus eliminating a signal point of failure, providing governmental entities and organizations with processed data and outcomes for better decision-making. It ensures data integrity by validating and securing all AI data (inputs and outcomes) using a secure, decentralized, and transparent blockchain platform. Compared with other related studies, the proposed architecture provides a platform that is capable of ensuring AI data integrity through validation and transparency, allowing the deployment of a robust and redundant AI-engine without any impact on its accuracy. It achieves this by utilizing edge devices and IoT end devices without a substantial impact impact on the power of these devices. Table 6 shows a performance comparison with the important related works. The authors acknowledge the difficulty of direct comparisons to other work due to differences in the presented assessment criteria. Furthermore, individual blockchain solutions can be tuned to enhance performance for a specific application.

In conclusion, we proposed, designed, developed, and implemented a system that has the capability to combine the advantages of three important technologies—edge computing, blockchain, and AI—in one platform. This system incorporates the security advantages provided by blockchain to offer a publicly available platform that integrates the intelligence advantages provided by AI into an edge layer to facilitate a secure architecture capable of sensing, analyzing, thinking, and producing actionable outcomes.

Our results showed that the system provided reliable accuracy in terms of the AI prediction of COVID-19 occurrence in sewage water at an acceptable system latency for such an application. The results and analyses of the impact on the devices' power sources showed that it is possible to use low-cost and low-power devices to accommodate the requirements of AI and blockchain in a network of a few hundred nodes.

In future work, the integration of biosensors into the system is needed to further study their impact on the overall system performance and the security of the collected data. Future work will include full deployment of the system around different sewage water sources to collect and analyze real-world data.

REFERENCES

[1] W. Yu, F. Liang, X. He, W. G. Hatcher, C. Lu, J. Lin, and X. Yang, "A survey on the edge computing for the Internet of Things," *IEEE Access*, vol. 6, pp. 6900–6919, 2018, doi: 10.1109/ACCESS.2017.2778504.
[2] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, 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," in *Proc. IEEE Int. Congr. Big Data (BigData Congress)*, Jun. 2017, pp. 557–564.
[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," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 2, pp. 1508–1532, Feb. 2019, doi: 10.1109/COMST.2019.2894727.
[5] P. 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 Inst. Bus. Value, New York, NY, USA, White Paper, 2015, pp. 1–18.
[7] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "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," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4719–4732, Jun. 2019, doi: 10.1109/JIOT.2018.2878154.
[10] T.-T. Kuo and L. Ohno-Machado, "ModelChain: Decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," 2018, *arXiv:1802.01746*.
[11] S. Rathore and J. H. Park, "DeepBlockIoTNet: A secure deep learning approach with blockchain for the iot network," *Trans. Ind. Inf.*, vol. 11, no. 14, p. 3974, 2019.
[12] W. Rouwer and M. Borda. (2017). *NeuRoN: Decentralized Artificial Intelligence, Distributing Deep Learning to the Edge of the Network*. [Online]. Available: https://s3-us-west-1.amazonaws.com/ai.doc.static/pdf/whitepaper.pdf
[13] 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," *IEEE Access*, vol. 7, pp. 18611–18621, 2019, doi: 10.1109/ACCESS.2019.2896065.

[14] M. A. Ferrag and L. Maglaras, "DeepCoin: A novel deep learning and blockchain-based energy exchange framework for smart grids," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1285–1297, Nov. 2020, doi: 10.1109/TEM.2019.2922936.
[15] S. K. Singh, Y.-S. Jeong, and J. H. Park, "A deep learning-based IoT-oriented infrastructure for secure smart city," *Sustain. Cities Soc.*, vol. 60, Sep. 2020, Art. no. 102252, doi: 10.1016/j.scs.2020.102252.
[16] D. Unal, M. Hammoudeh, M. A. Khan, A. Abuarqoub, G. Epiphaniou, and R. Hamila, "Integration of federated machine learning and blockchain for the provision of secure big data analytics for Internet of Things," *Comput. Secur.*, vol. 109, Oct. 2021, Art. no. 102393, doi: 10.1016/j.cose.2021.102393.
[17] A. Nawaz, T. N. Gia, J. P. Queralta, and T. Westerlund, "Edge AI and blockchain for privacy-critical and data-sensitive applications," in *Proc. 12th Int. Conf. Mobile Comput. Ubiquitous Netw. (ICMU)*, Nov. 2019, pp. 1–2, doi: 10.23919/ICMU48249.2019.9006635.
[18] R. Gupta, D. Reebadiya, S. Tanwar, N. Kumar, and M. Guizani, "When blockchain meets edge intelligence: Trusted and security solutions for consumers," *IEEE Netw.*, vol. 35, no. 5, pp. 272–278, Sep. 2021, doi: 10.1109/MNET.001.2000735.
[19] P. Bagga, A. K. Sutrala, A. K. Das, and P. Vijayakumar, "Blockchain-based batch authentication protocol for Internet of Vehicles," *J. Syst. Archit.*, vol. 113, Feb. 2021, Art. no. 101877.
[20] A. Islam, T. Rahim, M. Masuduzzaman, and S. Y. Shin, "A blockchain-based artificial intelligence-empowered contagious pandemic situation supervision scheme using internet of drone things," *IEEE Wireless Commun.*, vol. 28, no. 4, pp. 166–173, Aug. 2021, doi: 10.1109/MWC.001.2000429.
[21] A. Islam and S. Y. Shin, "A blockchain-based secure healthcare scheme with the assistance of unmanned aerial vehicle in Internet of Things," *Comput. Electr. Eng.*, vol. 84, Jun. 2020, Art. no. 106627.
[22] S. Alrubei, E. Ball, and J. Rigelsford, "Securing IoT-blockchain applications through honesty-based distributed proof of authority consensus algorithm," in *Proc. Int. Conf. Cyber Situational Awareness, Data Analytics Assessment (CyberSA)*, Jun. 2021, pp. 1–7, doi: 10.1109/CyberSA52016.2021.9478257.
[23] *Guide for Conducting Risk Assessments*, document NIST SP-800-30, Rev.1, NIST, 2012.
[24] K. Mao, H. Zhang, and Z. and Yang, "Can a paper-based device trace COVID-19 sources with wastewater-based epidemiology?" *Environ. Sci. Technol.*, vol. 54, no. 7, pp. 3733–3753, 2020.
[25] Z. Yang, B. Kasprzyk-Hordern, C. G. Frost, P. Estrela, and K. V. Thomas, "Community sewage sensors for monitoring public health," *Environ. Sci. Technol.*, vol. 49, no. 10, pp. 5845–5846, May 2015.
[26] TensorFlow. *Module Tf.Keras*. Accessed: Nov. 15, 2021. [Online]. Available: https://www.tensorflow.org/api_docs/python/tf/keras
[27] D. Barceló, "Wastewater-based epidemiology to monitor COVID-19 outbreak: Present and future diagnostic methods to be in your radar," *Case Stud. Chem. Environ. Eng.*, vol. 2, Sep. 2020, Art. no. 100042.
[28] K. Mao, H. Zhang, Y. Pan, and Z. Yang, "Biosensors for wastewater-based epidemiology for monitoring public health," *Water Res.*, vol. 191, Mar. 2021, Art. no. 116787.
[29] O. M. Abdeldayem, A. M. Dabbish, M. M. Habashy, M. K. Mostafa, M. Elhefnawy, L. Amin, E. G. Al-Sakkari, A. Ragab, and E. R. Rene, "Viral outbreaks detection and surveillance using wastewater-based epidemiology, viral air sampling, and machine learning techniques: A comprehensive review and outlook," *Sci. Total Environ.*, vol. 803, Jan. 2022, Art. no. 149834.
[30] G. Sagirlar, B. Carminati, E. Ferrari, J. D. Sheehan, and E. Ragnoli, "Hybrid-IoT: Hybrid blockchain architecture for Internet of Things–PoW sub-blockchains," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1–10.

SUBHI M. ALRUBEI received the Bachelor of Engineering degree in communication systems engineering from the University of Portsmouth, Portsmouth, U.K., in 2003, and the Master of Science degree (Hons.) in networks and security from the University of Kent, Canterbury, U.K., in 2012. He is currently pursuing the Ph.D. degree with the Department of Electronic and Electrical Engineering, The University of Sheffield, Sheffield, U.K. He worked for over ten years as a Communication Engineer in Saudi Arabia, where he has managed and executed many communications systems projects. He investigates the integration of blockchain and AI into the future IoT applications for improved security, privacy, and performance. His research interests include blockchain technology, the Internet of Things (IoT), cybersecurity, and AI.

EDWARD BALL (Member, IEEE) was born in Blackpool, U.K., in November 1973. He received the Master of Engineering degree (Hons.) in electronic systems engineering from the University of York, York, U.K., in 1996. After graduating, he worked in the industry for 20 years, first spending 15 years working as an Engineer, a Senior RF Engineer, and finally a Principal RF Engineer at Cambridge Consultants Ltd., Cambridge, U.K. He then spent five years as a Principal RF Engineer and a Radio Systems Architect at Tunstall Healthcare Ltd., Whitley, U.K. In November 2015, he joined the Department of Electronic and Electrical Engineering, The University of Sheffield, Sheffield, U.K., where he currently works as a Reader in RF engineering. He has a particular passion for RF hardware design. His research interests include radio technology, from RF system design, RF circuit design (sub-GHz to mm-wave), and the application of radio technology to real-world industrial and commercial problems. He is a member of the IET. He is a Chartered Engineer.

JONATHAN M. RIGELSFORD (Senior Member, IEEE) received the M.Eng. and Ph.D. degrees in electronic engineering from the University of Hull, Hull, U.K., in 1997 and 2001, respectively. From 2000 to 2002, he worked as a Senior Design Engineer at Jaybeam Ltd. From 2002 to 2014, he was a Senior Experimental Officer with the Communications Group, Department of Electronic and Electrical Engineering, The University of Sheffield, Sheffield, U.K. He then became a Senior Research Fellow at The University of Sheffield. In 2019, he moved to Sensata Technologies as an RF Engineering Lead and maintains a visiting position in Sheffield. His research interests include RF propagation, biomedical electromagnetics, adaptive antennas, RFID, and cybersecurity.