An Ethereum Private Network for Data Management in Blockchain of Things Ecosystem

https://doi.org/10.3991/ijoe.v19i01.35261

Abdallah Al-Zoubi[1](✉), Tariq Saadeddin[1], Mamoun Dmour[2]
[1]Princess Sumaya University for Technology, Amman, Jordan
[2]University of Jordan, Amman, Jordan
zoubi@psut.edu.jo

Abstract—The advent of blockchain technology in the development and design of smart internet of things (IoT) systems offers the opportunity to secure and transfer data flow, preserve its integrity, and provide transparent mechanisms for its management. Blockchain has actually attracted applications in vital fields because it provides many advantages over centralized database such as traceability, confidentiality, availability and trust. A private network offers the most secure and peer-restricted environment for big data flow, specifically in IoT ecosystems. An integrated blockchain-IoT ecosystem in which three Raspberry Pi 4 nodes communicate and interact in a closed loop to control smart applications via an Ethereum platform in a secure and an efficiently emulated environment is piloted. The proposed blockchain of things (BCoT) ecosystem adds a new layer to the physical, network and application layers of a typical IoT architecture. The concept of a fully decentralized private Ethereum BCoT network may find applications in several fields that call for the removal of single-point of failure and ensures data integrity and transparency.

Keywords—blockchain, IoT, Ethereum, private, smart system, big data

1 Introduction

The Internet of Things (IoT) has become one of the most powerful emerging technologies that integrate big data, cloud computing and machine learning, into one melting pot that converge the physical and digital worlds together and create a truly data-driven digital society. The size of the IoT market was valued at $190 billion in 2018 and is expected to reach $1.1 trillion by 2026, while the number of IoT connected devices were 8.4 billion in 2017, reached 29 billion in 2021, and expected to rise to 35 billion in 2025, and possibly 500 billion IoT devices in 2030 [1]. A wide range of IoT products and objects such as appliances, furniture, clothes, machines, food packages home security sensors, remote educational labs, wearable medical devices, and industrial IoT devices and systems represent an internet node that interacts with the human environment [2]. In fact, IoT has already been widely adopted in many smart applications, mainly at homes [3], cities [4], factories [5], hospitals [6], farms [7], agriculture [8], transport [9], civil services and governance [10] and weapons [11], to name a few.

However, the nature of IoT centralized infrastructure in which sensors, actuators, devices communicate and exchange data without the need for human intervention makes it vulnerable to attacks and hacks [12]. In addition, it is difficult to ensure security and privacy of the generated big data efficiently. Data sharing between devices in IoT networks may experience falsified authentication and trust due to the heterogeneous sensor types that may lead to increased scope for sharing erroneous, inaccurate, or inconsistent data, and hence inaccurate models built from this data [13]. In addition, the IoT ecosystem faces several challenges such as heterogeneity, diversity of technologies and requirements, limited access to the real devices, protocol fragmentation, releasing regular updates, programming, and handling failures, as well as common pitfalls and bugs that IoT developers and practitioners encounter [14].

In the development and design of smart IoT systems, blockchain technology provides the natural means for secure data management that ensures its transparency and preserves its integrity [15]. In fact, blockchain has emerged in the last decade as one of the most important pillars of the disruptive technologies of the fourth industrial revolution. Its main features have attracted many applications in several fields such as banking, government, business, agriculture, health, transport, logistics, and education, to name a few. In fact, blockchain technology offers many advantages over centralized database solutions such as decentralization, security, transparency, traceability, confidentiality, availability, and trust [16]. According to a Gartner report, the convergence of blockchain and IoT has recently been viewed as the sweet spot of two powerful technologies [17] that were otherwise facing their demise and extinction within 20 years. In fact, issues related to security and management of the massive amount of big data generated by IoT devices rendered the technology inefficient and economically insignificant. However, the integration of the two emerging technologies has led to the launch of a new concept of blockchain of things (BCoT) [18], a term first coined at the IoT Festival 2018 in Australia. The new alliance of BCoT is anticipated to provide proper security infrastructure by leveraging cryptographic blockchain for IoT, which is already showing its limitations and deficiencies, thus, may solve IoT's most pain points [19].

In this paper, a private blockchain of things network, based on Ethereum platform, is developed, and integrated into three IoT sensors and devices units, each connected to Arduino microcontroller and Raspberry Pi 4 minicomputer in order to create a proactive and autonomous ecosystem. Communication and exchange of data between the IoT units is established in an interactive manner where each device makes appropriate decisions independently according to predefined conditions determined by the surrounding environment. The ultimate purpose of system design and adaptation is to demonstrate its viability in strategic, practical and real-life applications.

2 Blockchain and IoT integration

IoT devices are usually susceptible to cyber-attacks because of their limited capacity, storage, and computing processors. In addition, security, privacy, and reliability of big data generated by IoT devices face several challenges that may be resolved using blockchain in complementing the IoT paradigm by providing trusted and secured data and enhancing latency and transparency [20]. Furthermore, IoT may be further

integrated with cloud computing infrastructures to increase systems storage and processing capabilities. One of the main features of blockchain is its ability to eliminate the need for a central authority to store transactions and records in identical copies in decentralized servers within the network. Simultaneously, authentication of data is carried out using a consensus algorithm while analysis is performed using smart contracts [20]. Blockchain further supports communication between IoT units directly, thereby bypassing central servers and allowing faster exchanging of messages and data among nodes. In addition, blockchain guarantees trust and authenticity of IoT information as all nodes keep a copy of verifiable data. Furthermore, security is always ensured, as cryptography is a main pillar of blockchain structure, and the use of hashing algorithms to connect chains forms the basic mechanism of blockchain operation.

The integration of blockchain technology in IoT applications may be traced back to the IBM platform on "Autonomous Decentralized Peer-To-Peer Telemetry" or ADEPT, which advocated for the concept of a decentralized approach that offers greater scalability and security for the IoT [21]. Several surveys were recently conducted on the topic of blockchain and IoT integration, which covered a multitude of methods and models pertaining to many situations and solutions [22–29]. For example, the implementation of a decentralized autonomous organization (DAO) using smart contracts written in Solidity on the Ethereum blockchain to automate organizational governance and decision-making was described for individuals working together collaboratively outside of a traditional corporate form [30].

Xiao, et al introduced a new architecture for IoT task offloading and resource allocation in smart homes, factories, and hospitals. The architecture consists of device layer, a distributed agent controller and a hierarchical edge-computing server that integrates the blockchain in the middle layer to ensure the integrity of transaction data [31]. Sharma et al used a three-layer distributed cloud model utilizing fog computing to manage raw IoT data stream at the network edge and cloud level [32]. On the other hand, Moinet et al presented a security protocol and decentralized model based on blockchain in order to provide cryptographic keys and trusted data storage for wireless networks, thereby enabling various components to authenticate data about every network peer [33].

A method to collect, store and retrieve data from IoT devices and sensors using blockchain in a secure, authentic and decentralized fashion was developed as a testbed on private Ethereum along with a low-cost Raspberry Pi in order to test the feasibility and performance of blockchain-based secure IoT system [34]. The encrypted data was stored in Inter Planetary File System (IPFS) or Swarm while PKI provided data authentication and confidentiality and all keys are securely stored in TPM and locked into Raspberry Pi. TPM provides secure key management, cryptographic functions, and disk encryption [34]. Accordingly, Fernando et al carried out experiments with IoT devices and blockchain technology to merge low-cost Raspberry Pi minicomputer devices with Ethereum platform, yielding promising outcomes when applied in pharmaceutical industry [35]. Furthermore, a blockchain-IoT based system was developed to detect the rice stock in orphanages using mobile application. The system was designed to collect data generated from a Raspberry Pi sensors connected to the network, thereby offering service providers, donors and rice suppliers the ability to track system operations such as rice financial transactions and shipping items to the orphanage, and hence reduce transaction manipulation and amplify transparency [36]. On the other hand,

a blockchain-based emergency service was implemented in a smart home system to handle the access control among untrusted public services and smart home IoT devices [37]. The system consisted of a Raspberry Pi as a tool to gather data from the home sensors and Ethereum platform. The solution is supported by web applications for home users and for staff of home service providers supervising the entire operation. In addition, the system incorporates an IPFS database to handle the generated files from the smart home, thus inherently enabled to prevent DDoS attacks. An Ethereum blockchain-based web-interface solution to handle the facilitation of renewable energy transactions in an effortless and efficient way was also proposed as a solution that describes the ability to perform energy transactions in near-real time from a prosumer to consumer without the need of a central authority [38]. On the other hand, Devi et al proposed a design architecture for satellite monitoring by merging IoT and blockchain that resulted in a new architectural framework, which enhanced security and data transparency through the implementation of consensus algorithms to predict various satellite performance parameters [39]. Numerous other applications of the marriage between blockchain and IoT can actually be found in the literature.

3 Standard IoT ecosystem

The basic IoT architecture consists of physical or perception layer, network layer, and application layer as depicted in Figure 1. At the physical layer lies the hardware sensors, actuators and devices that act as an interface with the physical world of the IoT ecosystem. These eventually share information and exchange data with each other using various communication and internet messaging protocols such as radio-frequency identification (RFID), message queuing telemetry transport (MQTT), advanced message queue protocol (AMQP), wireless sensor network (WSN), Bluetooth and ZigBee, and Wi-Fi. Routers, switches, and firewalls are deployed as gateways at the network layer in order to communicate with one another and with application platforms such as computers, remote-control devices, and smartphones as well as to transmit data from IoT devices to cloud servers such as Google, Amazon, IBM and Microsoft Azure for storage and analytics purpose. The communication or network layer performs functions related to gateway, routing and addressing, message, publishing and subscribing, flow control and reliability and QoS, and hosts the IoT web portal. All decisions related to communications and measurements of the flow and its quality and energy consumed are made in this layer. With the advent of 5G technology, faster connectivity makes it suitable for low-powered IoT sensors, while Internet Protocol version 6 (IPv6), which comes with large addressing space, makes it a desirable communication protocol for IP enabled smart devices.

On the other hand, the application layer is responsible for delivery of various applications to different users in different industry segments such as healthcare, manufacturing, smart cities, food, logistics, retail, environment, public safety and drug. In fact, the application layer encompasses specific service support and contains common capabilities that can be used by different IoT applications, where all actions related to the control, security and management of the application are made such as QoS manager, device manager, business process and execution, authorization, key exchange and

management, trust and reputation, identity management. A services layer performs functions such as service storage, composition, organization and orchestration, virtual entity resolution and monitoring. All decisions related to the monitoring, storage, organization and visualization of the received information, including resolving virtual entities created are made. An improved and reliable seven-layers IoT architecture that takes on all functions of the traditional architecture has recently been introduced [40].

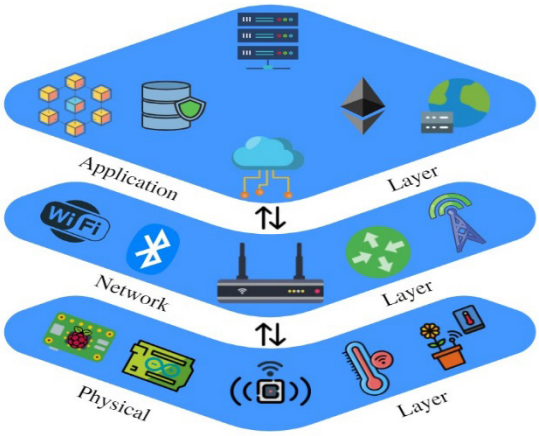

Fig. 1. Basic three-layered IoT architecture

4 Standard blockchain technology

Blockchain is a sequence of blocks linked together in an ecosystem that encompasses a wide range of applications as it employs complicated encryption techniques to verify transactions as shown in Figure 2. When transactions are validated through mining, a new block is added to the chain and the miner is rewarded with the crypto-currency associated with that blockchain. In fact, mining is the process of conducting complex computational mathematics, specifically complicated cryptographic computations that need a significant amount of computing power and capacity to complete [25]. The miners' task is to check the legitimacy of payments and add the approved transactions to the network. The process in which the miner starts working to solve the complicated cryptographic computations is called Proof of Work (PoW), when a miner solves the PoW, other miners tend to check the validity of that solution, and then the blockchain nodes validate the block to be added to the chain.

Ethereum, in particular, is an open-source blockchain platform that can access the data stored in the chain to read and write. An Ethereum network can also run in a private mode to restrict permissions to specific users. Only the nodes with the right permissions will be able to access the blockchain while being isolated from the main network. The Ethereum platform utilizes smart contracts to simplify transactions and to store data. Smart contracts are compiled into Ethereum Virtual Machine (EVM) byte code and ABI definition using Solidity, which supports the characteristics of a modern scripting language, including static typing, inheritance and complicated user-defined data types.

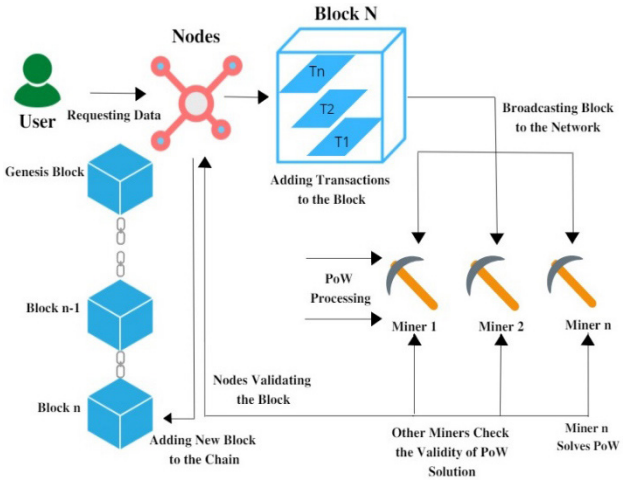

Fig. 2. Transaction block validation and addition flow

Proof-of-Work (PoW) is a consensus algorithm deployed in cryptocurrency transactions in such a way as to calculate a certain hash value of the block header to gain the right to append a new block to the chain [41]. Every block has a unique hash that is used in the calculations of the PoW algorithm. When a block is ready to be appended to the blockchain, every field of the header is filled except the first nonce. The nonce value is the solution of a mathematical problem [42]. One node would broadcast the block to other nodes once it reaches the target value and all other nodes would then mutually confirm the correctness of the hash value. When a miner completes a task, the block is verified by other nodes in the network. The hash function has the property that the verification can be performed fast comparing with PoW calculations. Reducing the complexity of proof of work is needed in IoT systems to obtain a shorter time to achieve consensus. If most of these nodes validate the PoW, the block is inserted in the chain copies of each node within the system. In case that more than one miner completes the PoW at the same time, a fork in blockchain appears. Future-validated block will be inserted in the longest chain and the remaining chain will be lost [43]. The consensus mechanism used in Ethereum is a variant of PoW, which has the same principles as PoW.

Ethash is a Proof of Work (PoW) algorithm based on hashing designed to resist ASIC and to avoid problems of computing power centralization and mining resource centralization caused by the emergence of ASIC in Bitcoin, which to some extent alleviated the problem of mining centralization [44]. The main feature of this algorithm is that it consumes the entire available memory access bandwidth; hence making memory reads the bottleneck of the whole computation process. This high load is based on using a large data structure called DAG, during mining [45]. If the number of correctly calculated Ethash function values for a given clock frequency turned out to be less than the number of correctly calculated Ethash function values for a lower frequency, then the experiment can be considered completed [46]. Ethash includes three main sub-functions: first, Keccak512 with its input is the header and the nonce concatenated

into a string of length 320 bits. The length of the output is 512 bits, and this result will be the input for the next sections. The second is a loop, which consists of two parts; the first consists of 64 loops, each of which consists of fetching data from the DAG file and using the FNV function to compute the required values, while the second part calculates the cmix value from the mix value. The third sub-function is Keccak256 with its input taking the form of hexadecimal string concatenated from the Keccak512 result and the cmix from the loop has a length of 768 bits [47]. However, a proof of authority (PoA) consensus protocol was practically implemented on an existing IoT-blockchain system, followed by a performance analysis based on different solutions procedures [48]. The implementation investigated the issues that affect the integration of blockchain and IoT like latency and network stability, demonstrating an increase stability in the block period of the PoA Ethereum network. Proof of Work (Ethash) consensus algorithm was eventually chosen over Proof of Authority (Clique) because it supports the mining process needed for smart contracts migration and later transactions.

5 Proposed blockchain of things system

There are many forms of architecture to integrating blockchain with IoT. A system is proposed to integrate blockchain technology into an IoT ecosystem in order to deal with big data generated by sensors and devices. Integration of blockchain technology in IoT is useful for data immutability, privacy, transparency, decentralization, authentication, preserving confidentiality, integrity, and availability. In fact, blockchain grants IoT devices independence as they lack autonomy outside of their centrally managed networks. On a blockchain network; however, each node has a unique private and public key pair that identifies it as an independent participant on the network. Specifically, the keys are enforced largely using cryptographic signatures or digital messages that unmistakably recognize the sender. Thus, each node makes its own decisions and uses its own resources independently of other nodes. Consequently, the network becomes secure as it removes the situation of a single point of failure [49]. The system focuses on building a private Ethereum network to benefit from the full transparency, privacy, network restrictions, decentralization, and security features that are also present in public networks but not as fully integrated as in private networks. In addition, private blockchain networks allow IoT communication with the blockchain without restrictions, which is a valuable alternative to all the machine-to-machine protocols [50].

A private Ethereum network was constructed using Go-Ethereum client, forming a blockchain layer on top of the three standard IoT layers as shown in Figure 3. A pilot system which consists mainly of three IoT units as nodes and a windows miner node was constructed, where the blockchain layer plays as a middleware with the application layer [26]. The system consists mainly of three IoT units as nodes and a windows miner node. Each of the IoT units consists of a Raspberry Pi 4, Arduino UNO R3, and multiple sensors connected to the Arduino. The Arduino is connected to the Raspberry Pi serially, where a Python script is used to retrieve the big data generated by these multiple sensors and stored in the Raspberry Pi 4.

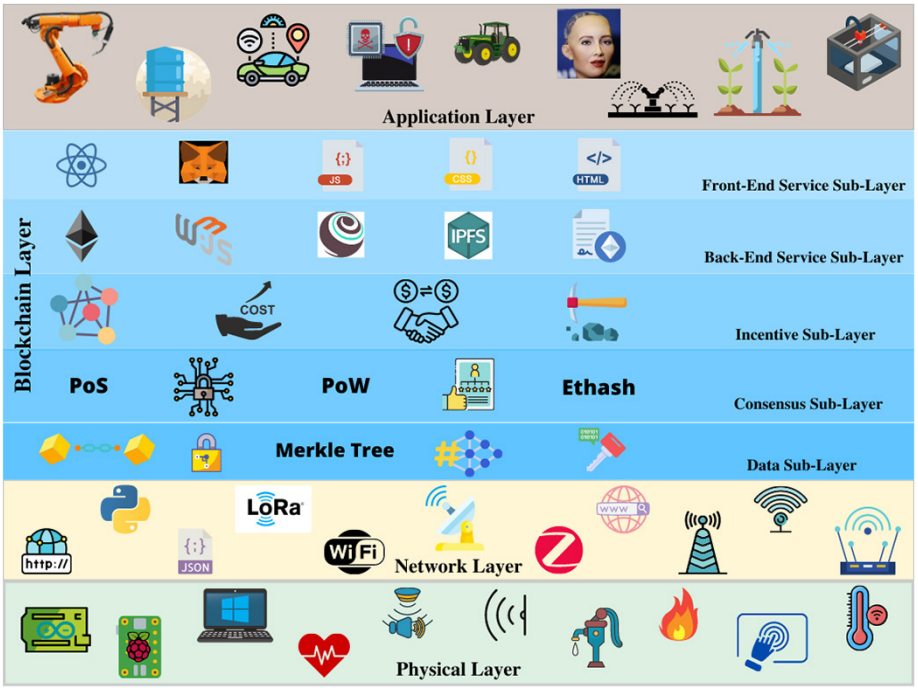

Fig. 3. Private Ethereum blockchain of things ecosystem architecture

The Arduino is connected to the Raspberry Pi serially, in which a Python script is used to retrieve the big data generated by these multiple sensors and stored in the Raspberry Pi. Communication in the physical layer between IoT devices including Raspberry Pi and Arduino is established using a simple Python code as demonstrated in the code below, while a screen shot of implementation of the physical layer is shown in Figure 4.

```
import serial
if __name__ == '__main__':
ser = serial.Serial('/dev/ttyACM0, 9600')
ser.flush()
while True:
   if ser.in_waiting > 0:
      line_s = ser.readline().decode('utf-8')
```

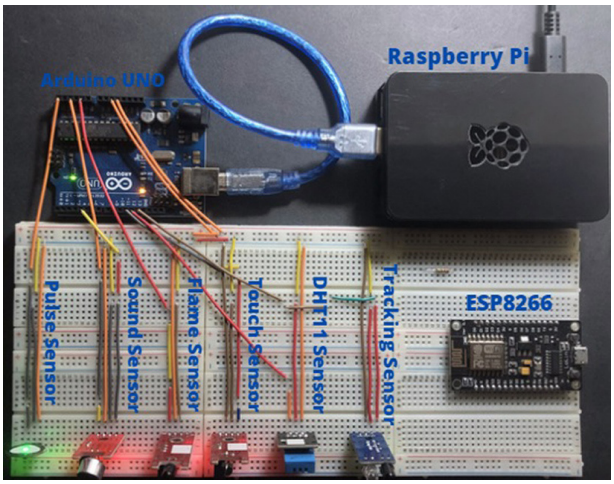

Fig. 4. Screen shot of the physical layer implementation

The blockchain layer actually consists of five sub-layers, which offers services such as application programming interfaces (APIs), data collection from IoT physical layer, and encryption of data with digital signature using various algorithms and hash functions depending on the blockchain platform [26]. For example, BTC blockchain chooses SHA-256 as the hash function and ECDSA as the signature algorithm. The network sublayer is essentially an overlay P2P network running on top of the communication layer. The overlay network consists of either virtual or physical links connecting nodes in the underlying communication networks. One node only simply broadcasts the block of transactions to its connected peers. Once receiving the block of transactions, other peers will verify it locally. If it is valid, the block will be further propagated to other nodes through the overlay network.

Consensus sublayer is mainly involved with the distributed consensus for the trustfulness of a block. Various consensus algorithms like PoW, PoS, PBFT, and DPOS can achieve the consensus. The block propagation mechanisms are the prerequisite for the distributed consensus protocols. The incentive sublayer is responsible for digital currency issuing and distribution; designing reward mechanism especially for miners; and handling transaction cost. The service sublayer provides users with blockchain-based services for various industrial sectors including manufacturing, logistics, supply chains, food industry and utilities. The blockchain as a service (BaaS) can be achieved by smart contracts, which can be automatically triggered when a special event occurs. The network sublayer that is established on top of the communication layer is the abstraction of underneath communication networks, consequently offering a universal network access across different networks as shown in Figure 3.

The second layer, referred to as the backend of the system, is built to handle, store, and manipulate big data generated by the IoT units. A Solidity smart contract was written to retrieve the big data from each Ethereum IoT unit node, and then deployed using truffle framework, to install truffle, node.js and node package manager (npm) are needed. Web3 is the latest version of the web, and it is programmed using JavaScript language. The Web3.js is needed to communicate with the Ethereum IoT unit nodes because the Ethereum nodes only speak JSON RPC language, which is only understood by Web3.js.

On the other hand, Inter Planetary File System (IPFS) is integrated as a decentralized storage for the big data generated. The front end was programmed using ReactJS, JavaScript, HTML, and CSS to be a user-friendly decentralized application. If users request access to that DApp, MetaMask is needed to connect their Ethereum account to the DApp. Zheng et al have actually proposed an IPFS-based blockchain data storage model to solve the problem of high demand on space and bandwidth and to synchronize data with the bitcoin network [51]. Evidently, the data size and compression ratio is greatly reduced, its security performance enhanced and synchronization speed improved because of utilizing the characteristics of the IPFS network and the features of its hash. In addition, Hasan et al proposed an IoT-blockchain based solution using IPFS to transfer large-size streaming data in a decentralized, transparent, traceable, reliable, secure, and trustful manner [52]. In this way, IPFS offers an appropriate alternative for big data storage as the transfer process preserve its privacy and confidentiality through a proxy re-encryption network. In fact, an IoT-IPFS framework was evaluated experimentally and proved feasible utilizing a Raspberry Pi minicomputer, hence demonstrating the advantages of P2P decentralized storage infrastructure [53].

6 Programming smart system applications

The data generated by the sensors connected to Arduino will flow according to a code that controls operations within an infinite loop as shown in Figure 5. The Arduino keeps receiving data as long as the sensors are functioning appropriately. These sensors are distributed over the three IoT test units that monitor and measure a number of physical quantities such as temperature, humidity, pressure, flame, pulse, sound, colour, and tracking in both analog and digital forms. Specific messages are generated and displayed with each corresponding sensor and updated every ten seconds as long as the Arduino is connected to the Raspberry Pi, and both are on, up and running.

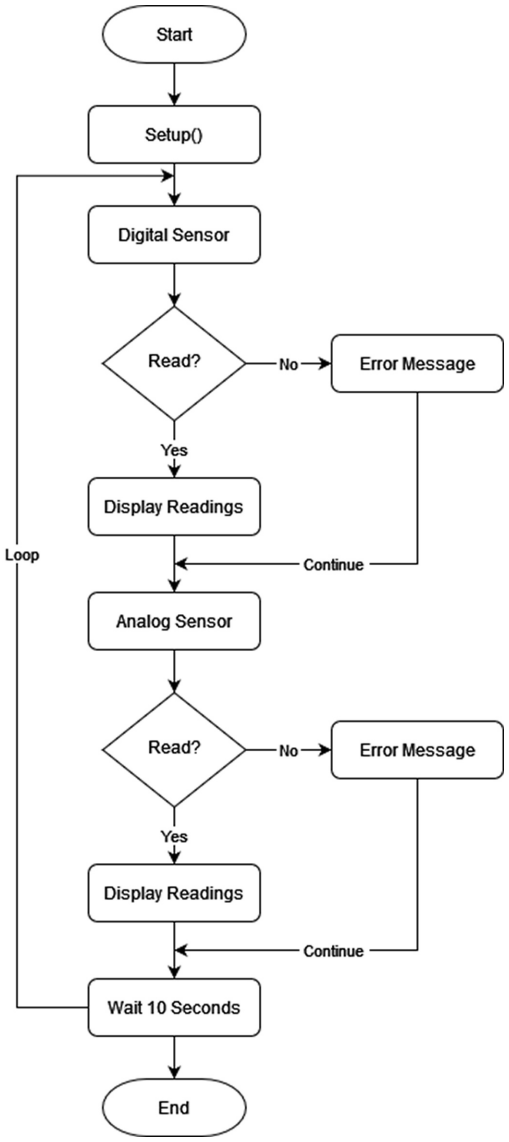

Fig. 5. Flowchart of system operation

The smart contract is migrated and deployed successfully using Truffle framework as depicted in the example of the Solidity code below:

```
contract BlockchainofThings {
  struct IoTUnit {
    string id;
    string hum;
    string temp;
    string touch;
    string fire;
    string pulse;
    string sound;
  }
  mapping(uint256 => IoTUnit) public IoTUnits;
```

When the migration is complete, a message, which indicates that the migration is being saved to the chain and some useful outcome for later use, will appear. The outcome shows the smart contract address in hexadecimal format, node account public address, block timestamp and number. In addition, the cost, Eth balance in that node account, gas used and price which is equal to 1 gwei (according to Ethereum.org glossary: gwei is short for gigawei, a denomination of ether, commonly utilized to price gas. 1 gwei = 109 wei. 109 gwei = 1 ether). This migration can be executed using truffle with the command: pi$ truffle migrate—reset.

> contract address: 0x9F16613350983E57c98F8263D7A3319142c7BbdE
> block number: 193
> block timestamp: 1649136742
> account address: 0xe3FE4957561E7C13614A25ed17fDbed4BA9096D0
> gas used: 929516 (0xe2eec)
> gas price: 1 gwei
> Total deployments: 2
>Final cost: 0.001121459 ETH

The smart contract creation was submitted after deploying it using truffle on the node exhibiting its address, hash in hexadecimal format, and zero nonce value in the node as shown in Figure 6. The figure also shows the peer count participating in this Ethereum private peer-to-peer network, which is the windows miner node. If adding other nodes in the network, the peer count will increase. To add any peer to the network, the java script console command (Admin.addPeer (enode address)) may be used. Consequently, to determine the enode of any specific node, the java script console command (Admin. nodeInfo.enode) is used. The smart contract is then migrated on the Raspberry Pi node, and the submission is reflected on the windows miner node, hence displaying a new sealing work commit, indicating that a potential block was mined, and that the transaction fees to create the smart contract is executed.

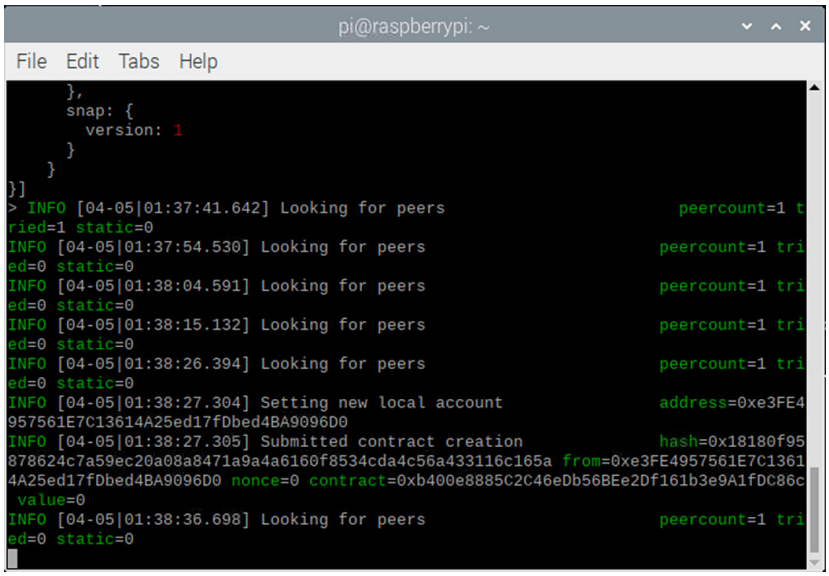

Fig. 6. Smart contract creation reflected on Geth node

Additionally, when running the miner node on Windows using Go-Ethereum (Geth), the command used should specify the database in which the chain data will be stored. Then, enable http, considering http APIs that will be used such as ether, miner, web, and personal APIs, unlock miner account address with its pass phrase, and define the CPU threads will be used in mining. The result will display the block number and hash, seal hash, gas used as shown in Figure 7. The miner node will keep mining and the block number will keep increasing as long as the miner node is running. Eventually, when the block is successfully mined, the miner will be rewarded, thus presume mining a new block.

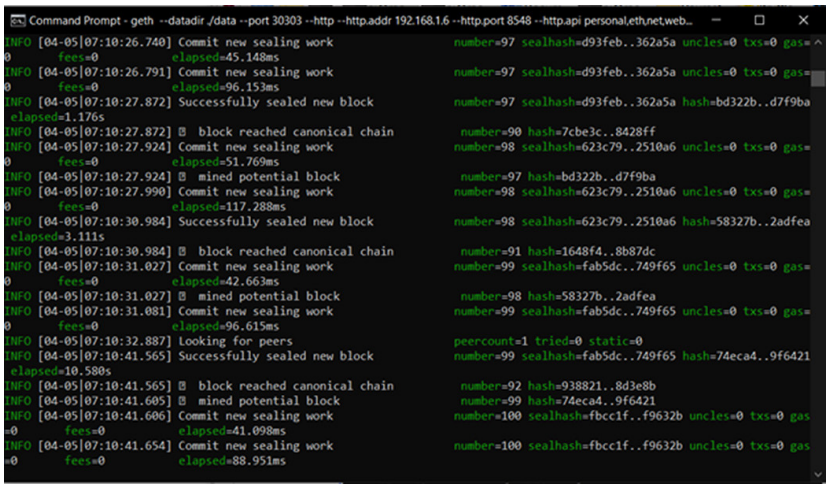

Fig. 7. Data mining procedure on the windows miner node

IPFS was installed on each Raspberry Pi for later use in data storage in a hashed way, a step that will improve the performance of data storage and security mechanism. The data will actually be encrypted and stored in IPFS in a decentralized manner. The official Go implementation of IPFS (Go-IPFS) was configured and initialized as shown in Figure 8, thereby enabling IPFS to function properly on each IoT node using the command $ipfs init daemon. In addition, the command $ipfs swarm peers was used to start looking and communicating with other IoT peers. The IPFS nodes uses bidirectional communication, as they listen (receive) and announce data at the same time using TCP and UDP protocols.

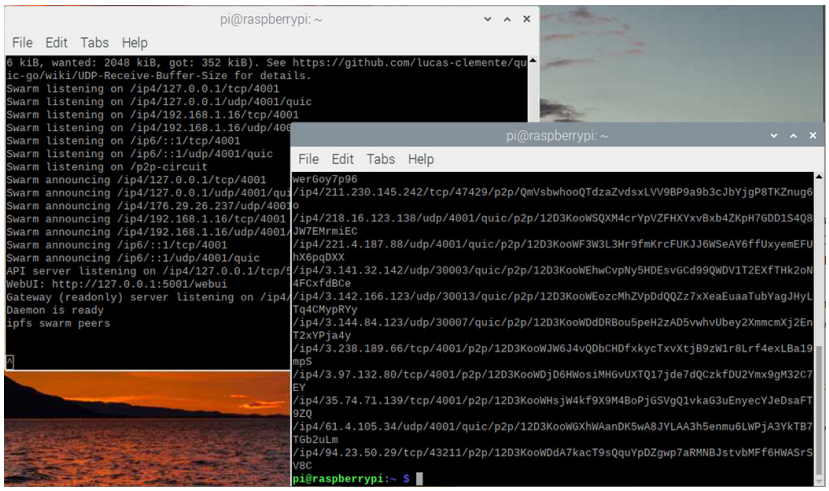

Fig. 8. IPFS running on Raspberry Pi

7 Results and discussion

A full-decentralized private Ethereum network was implemented with three IoT full nodes and one miner node. The network was operated with PoW algorithm which enabled each IoT node to act as an independent entity and to interact and communicate with each other over the blockchain. Appropriate smart contracts were migrated successfully on each IoT node, and the miner node was able to mine the blocks of big data chunks generated by the sensors and devices, hence establishing a holistic high performance decentralized application (DApp). The DApp was initially designed as a public network; however, as IoT devices do not act as independent entities and need a way to connect and communicate with each other using socket programming or message queuing telemetry transport (MQTT) protocol, a private network was eventually chosen to realize the network. In fact, the private Ethereum blockchain network solution gives the DApp full decentralization, transparency and independence features. Consequently, IoT nodes acquire the ability to take independent unilateral decisions based on a predefined set of rules.

A client first converts each IoT unit into a full node in an Ethereum private blockchain network integrated with IoT. Go-Ethereum (Geth), the official Go implementation of Ethereum, was chosen for this purpose for its ease-of-use features. Each IoT unit was integrated with Geth to act as a full node, while connecting nodes together becomes necessary to act all as a private network. This, in turn, necessities the creation of a genesis block where a JSON file is initialized in each node. Puppeth tool was used for creating the genesis block that gives the option to choose between two blockchain consensus algorithms, Proof of Work (Ethash) and Proof of Authority (Clique). The Proof of Work algorithm was chosen as it supports mining, which is needed later for smart contracts migrations with the truffle framework. Puppeth is actually a very useful tool to generate the genesis block with prefunded Ethereum accounts and to determine the difficulty of the mathematical calculations made by the miner.

The implementation of a private blockchain network has actually been proven to be a very cost-effective solution because it leads to a decrease in the difficulty of calculations carried out by the miner compared to a public blockchain, thereby lowering CPU usage and reducing power consumption. At the same time, the utilization of a Raspberry Pi to act as a full Ethereum node is also cost effective, as it requires low power to operate efficiently, costs less than an actual computer yet acts as one. In addition, transaction fee is much lower in private Ethereum networks compared to public ones due to the reduced pressure on nodes requesting transactions. In addition, private Ethereum networks nodes perform tasks efficiently and rarely take up extra resources that slow down the platform, which is the case in public Ethereum network. Hence, private Ethereum networks enjoy attractive features such as stability and efficiency.

However, integrating blockchain in IoT is not a straightforward process because of high resource consumption, scalability, and processing time. Privacy and security in IoT are also challenging due to low resource capabilities and lack of standardization [54–55], which pose as a serious limitations for the proposed system. Consequently, security measures and practices were applied to the physical system, specifically to the Raspberry Pi by installing uncomplicated firewall (ufw) and Fail2ban software to configure each unit. In fact, Fail2ban software acts as an Intrusion Prevention System (IPS), which blocks any suspicious activity. Another limitation is power consumption of the PoW consensus algorithm, specifically when using Graphics Processing Unit (GPU) for mining. Fortunately, the proposed system utilizes CPU for mining, hence consumes less energy [56].

In IoT, one of the most popular integrated blockchain platform is Ethereum, although it was not designed especially for IoT. A private blockchain is a preferred option over a public one for implementation within a single organization due to its high efficiency, fast transaction speed, low cost, permissioned consensus and easy data handling and access [57–58]. In addition, Ethereum supports the use of private blockchain, which can be modified and utilized to fit in different IoT scenarios.

However, IOTA is another blockchain platform designed specifically for implementation in IoT devices. It is an open-source DLT that intends to provide a trust layer for IoT devices. IOTA has a unique data structure called Tangle, structured by directed acyclic graphs (DAG), which does not have blocks, only transactions, different from other DLTs such as Ethereum. IOTA has demonstrated its advantages in enhancing IoT applications' security and privacy. IOTA also adopts the PoW consensus algorithm,

which allows issuing transactions by approving previous transactions, then confirms their consistency and prevent spamming from malicious clients. A transaction with a proper nonce is allowed to attach to the Tangle, indicating that the PoW algorithm in IOTA is more lightweight than in Ethereum [59]. Both Ethereum and IOTA maintains a stable memory space usage. However, IOTA has a smaller memory usage than Ethereum while consuming more CPU resources and hence executing a smaller number of transactions than IOTA does.

8 Conclusions

A cost-effective and power-efficient private Ethereum network based on a number of Raspberry Pi nodes that control a smart application was designed and deployed in securely managed BCoT ecosystem. The private blockchain network was integrated with IoT devices to stream big data chunks generated by a large set of sensors connected to Arduino development board microcontroller and serially passed to the Raspberry Pi. The main purpose of this BCoT environment is to benefit from its features, including decentralization, transparency, privacy, and security. The BCoT concept may find applications in several fields that ensures data integrity and transparency and demand the removal of single-point of failure.

9 References

[1] N. Ahmad, P. Laplante and J. F. DeFranco, "Life, IoT, and the Pursuit of Happiness," IT Professional, Vol. 22, No. 6, pp. 4–7, 2020. https://doi.org/10.1109/MITP.2019.2949944

[2] G. Singh, S. Srivastav, A. Gupta and V. Garg, "Companies Adoption of IoT for Smart Retailing in Industry 4.0," 2020 International Conference on Intelligent Engineering and Management (ICIEM), pp. 487–492, London, UK, 17–19 June 2020. https://doi.org/10.1109/ICIEM48762.2020.9160272

[3] S. K. Sooraj, E. Sundaravel, B. Shreesh and K. Sireesha, "IoT Smart Home Assistant for Physically Challenged and Elderly People," 2020 International Conference on Smart Electronics and Communication (ICOSEC), pp. 809–814, Trichy, India, 10–12 September 2020. https://doi.org/10.1109/ICOSEC49089.2020.9215389

[4] S. S. Hajam and S. A. Sofi, "IoT-Fog Architectures in Smart City Applications: A survey," China Communications, Vol. 18, No. 11, pp. 117–140, Nov. 2021. https://doi.org/10.23919/JCC.2021.11.009

[5] V. Bhatt and A. K. Bindal, "Smart Hardware Development under Industrial IOT (IIOT) 4.0: A Survey Report," 6th International Conference on Signal Processing, Computing and Control (ISPCC), 2021, pp. 262–265, 2021. https://doi.org/10.1109/ISPCC53510.2021.9609399

[6] S. Jing, R. Xiao, T. Shan, Z. Wang and Y. Liu, "Application Practice of Smart Hospital Based on IoT Cloud Platform," IEEE International Conference on Consumer Electronics-Taiwan (ICCE-Taiwan), pp. 1–2, Taoyuan, Taiwan, 28–30 September 2020. https://doi.org/10.1109/ICCE-Taiwan49838.2020.9258204

[7] T. M. Bandara, W. Mudiyanselage and M. Raza, "Smart Farm and Monitoring System for Measuring the Environmental Condition Using Wireless Sensor Network-IOT Technology in Farming," 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA), pp. 1–7, Sydney, Australia, 25–27 November 2020. https://doi.org/10.1109/CITISIA50690.2020.9371830

[8] N. Kumar, A. K. Dahiya, K. Kumar and S. Tanwar, "Application of IoT in Agriculture," 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), pp. 1–4, Noida, India, 3–4 September 2021. https://doi.org/10.1109/ICRITO51393.2021.9596120

[9] M. K. Deore, D. B. Raj, S. N, V. P and V. M, "Smart Bus and Bus Stop Management System Using IoT Technology," International Conference on Design Innovations for 3Cs Compute Communicate Control (ICDI3C), pp. 197–202, Bangalore, India, 10–11 June 2021. https://doi.org/10.1109/ICDI3C53598.2021.00047

[10] N. Tewari and G. Datt, "Towards FoT (Fog-of-Things) Enabled Architecture in Governance: Transforming e-Governance to Smart Governance," 2020 International Conference on Intelligent Engineering and Management (ICIEM), pp. 223–227, London, UK, 17–19 June 2020. https://doi.org/10.1109/ICIEM48762.2020.9160037

[11] A. Singh, T. Anand, S. Sharma and P. Singh, "IoT Based Weapons Detection System for Surveillance and Security Using YOLOV4," 6th International Conference on Communication and Electronics Systems (ICCES), pp. 488–493, Coimbatre, India, 8–10 July 2021. https://doi.org/10.1109/ICCES51350.2021.9489224

[12] Mohd F. M. Sam, Albert F. M. F Ismail, Kamarudin A. Bakar, Amiruddin Ahamat and Muhammad I. Qureshi, "The Effectiveness of IoT Based Wearable Devices and Potential Cybersecurity Risks: A Systematic Literature Review from the Last Decade", International Journal of Online and Biomedical Engineering, Vol. 18, No. 9, pp. 56–73, 2022. https://doi.org/10.3991/ijoe.v18i09.32255

[13] J. Byabazaire, G. O'Hare and D. Delaney, "Using Trust as a Measure to Derive Data Quality in Data Shared IoT Deployments," 29th International Conference on Computer Communications and Networks (ICCCN), pp. 1–9, Honolulu, USA, 3–6 August 2020. https://doi.org/10.1109/ICCCN49398.2020.9209633

[14] A. Makhshari and A. Mesbah, "IoT Development in the Wild: Bug Taxonomy and Developer Challenges," 2021 IEEE/ACM 43rd International Conference on Software Engineering: Companion Proceedings (ICSE-Companion), pp. 225–226, Madrid, Spain, 25–28 May 2021. https://doi.org/10.1109/ICSE-Companion52605.2021.00103

[15] C. K. Da Silva Rodrigues and V. Rocha, "Towards Blockchain for Suitable Efficiency and Data Integrity of IoT Ecosystem Transactions," in IEEE Latin America Transactions, Vol. 19, No. 7, pp. 1199–1206, July 2021. https://doi.org/10.1109/TLA.2021.9461849

[16] A. Y. Al-Zoubi, Mamoun Dmour and Rakan Aldmour, "Blockchain as a Learning Management System for Laboratories 4.0", International Journal of Online and Biomedical Engineering, Vol. 18, No. 12, pp. 16–34, 2022. https://doi.org/10.3991/ijoe.v18i12.33515

[17] https://www.computerworld.com/article/3489503/blockchainiot-integration-accelerates-hits-a-sweet-spot-for-the-two-technologies.html

[18] F. A. Abadi, J. Ellul and G. Azzopardi, "The Blockchain of Things, Beyond Bitcoin: A Systematic Review," IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1666–1672, Halifax, Canada, 30 July–3 August 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00278

[19] Mahdi H. Miraz, "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies", Kim, S., Deka, G. (eds) Advanced Applications of Blockchain Technology, Studies in Big Data, Vol. 60, Springer, Singapore, 2020. https://doi.org/10.1007/978-981-13-8775-3_7

[20] A. A. Sadawi, M. S. Hassan and M. Ndiaye, "A Survey on the Integration of Blockchain with IoT to Enhance Performance and Eliminate Challenges," IEEE Access, Vol. 9, pp. 54478–54497, 2021. https://doi.org/10.1109/ACCESS.2021.3070555

[21] IBM, "ADEPT: An IoT Practitioner Perspective," 2015. www.ibm.com/downloads/cas/QYYYV9VK

[22] S. Aich, S. Chakraborty, M. Sain, H. Lee and H. Kim, "A Review on Benefits of IoT Integrated Blockchain Based Supply Chain Management Implementations across Different Sectors with Case Study," 21st International Conference on Advanced Communication Technology (ICACT), pp. 138–141, 2019. https://doi.org/10.23919/ICACT.2019.8701910

[23] A. Al Sadawi, M. S. Hassan and M. Ndiaye, "A Review on the Integration of Blockchain and IoT," 2020 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), pp. 1–6, 2021. https://doi.org/10.1109/ICCSPA49915.2021.9385757

[24] Elham A. Shammar, Ammar T. Zahary and Asma A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective", IEEE Access, Vol. 9, pp. 156114–156150, 2021. https://doi.org/10.1109/ACCESS.2021.3129697

[25] Alfonso Panarello, Nachiket Tapas, Giovanni Merlino, Francesco Longo and Antonio Puliafito, "Blockchain and IoT Integration: A Systematic Survey", Sensors, Vol. 18, 2575; 2018. https://doi.org/10.3390/s18082575

[26] H. N. Dai, Z. Zheng and Y. Zhang, "Blockchain for Internet of Things: A Survey," IEEE Internet of Things Journal, Vol. 6, No. 5, pp. 8076–8094, 2019. https://doi.org/10.1109/JIOT.2019.2920987

[27] M. Conoscenti, A. Vetrò and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature review," 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA), pp. 1–6, 2016. https://doi.org/10.1109/AICCSA.2016.7945805

[28] Ali Dorri, Salil S. Kanhere and Raja Jurdak, "Blockchain in Internet of Things: Challenges and Solutions". https://doi.org/10.48550/arXiv.1608.05187

[29] Hany F. Atlam, Ahmed Alenezi, Madini O. Alassafi and Gary B. Wills, "Blockchain with Internet of Things: Benefits, Challenges, and Future Directions", International Journal of Intelligent Systems and Applications, Vol. 6, pp. 40–48, 2018. https://doi.org/10.5815/ijisa.2018.06.05

[30] C. Jentzsch, "Decentralized Autonomous Organization to Automate Governance," White Paper, pp. 1–30, 2016.

[31] Kaile Xiao, Zhipeng Gao, Weisong Shi, Xuesong Qiu, Yang Yang and Lanlan Rui, "EdgeABC: An Architecture for Task Offloading and Resource Allocation in the Internet of Things", Future Generation Computer Systems, Vol. 107, pp. 498–508, 2020. https://doi.org/10.1016/j.future.2020.02.026

[32] 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. https://doi.org/10.1109/ACCESS.2017.2757955

[33] A. Moinet, B. Darties and J.-L. Baril, "Blockchain Based Trust and Authentication for Decentralized Sensor Networks," arXiv:1706.01730, 2017.

[34] V. K. C. Ramesh, Y. Kim and J. Y. Jo, "Secure IoT Data Management in a Private Ethereum Blockchain", IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC), pp. 369–375, 2020. https://doi.org/10.1109/COMPSAC48688.2020.0-219

[35] E. Fernando, Meyliana and Surjandy, "Blockchain Technology Implementation in Raspberry Pi for Private Network," International Conference on Sustainable Information Engineering and Technology (SIET), pp. 154–158, 2019. https://doi.org/10.1109/SIET48054.2019.8986053

[36] A. P. Junfithrana, E. Liani, M. Z. Suwono, D. Meldiana and A. Suryana, "Rice Donation System in Orphanage Based on Internet of Things, Raspberry-Pi, and Blockchain," International Conference on Computing, Engineering, and Design (ICCED), pp. 235–238, 2018. https://doi.org/10.1109/ICCED.2018.00053

[37] T. Tantidham and Y. N. Aung, "Emergency Service for Smart Home System Using Ethereum Blockchain: System and Architecture," IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), pp. 888–893, 2019. https://doi.org/10.1109/PERCOMW.2019.8730816

[38] C. H. Park, I. Mejia Barlongo and Y. Kim, "A Market Place Solution for Energy Transaction on Ethereum Blockchain," IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), pp. 1–5, 2019. https://doi.org/10.1109/IEMCON.2019.8936157

[39] M. S. Devi, R. Suguna and P. M. Abhinaya, "Integration of Blockchain and IoT in Satellite Monitoring Process", IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), pp. 1–6, Coimbatore, India, 20–22 February 2019. https://doi.org/10.1109/ICECCT.2019.8869185

[40] Rashmi. "IoT (Internet of Things) Concept and Improved Layered Architecture", International Journal of Engineering Development and Research, Vol. 6, No. 2, pp. 481–484, April 2018. http://www.ijedr.org/papers/IJEDR1802083.pdf

[41] S. Zoican, M. Vochin, R. Zoican and D. Galatchi, "Blockchain and Consensus Algorithms in Internet of Things", International Symposium on Electronics and Telecommunications (ISETC), pp. 1–4, Timisoara, Romania, 8–9 November 2018. https://doi.org/10.1109/ISETC.2018.8583923

[42] B. Lucas and R. V. Páez, "Consensus Algorithm for a Private Blockchain", 9th IEEE International Conference on Electronics Information and Emergency Communication (ICEIEC), pp. 264–271, Beijing, China, 12–14 July 2019. https://doi.org/10.1109/ICEIEC.2019.8784500

[43] Y. Hao, Y. Li, X. Dong, L. Fang and P. Chen, "Performance Analysis of Consensus Algorithm in Private Blockchain", IEEE Intelligent Vehicles Symposium (IV), pp. 280–285, Changshu, China, 26–30 June 2018. https://doi.org/10.1109/IVS.2018.8500557

[44] C. Su and X. Li, "A Review of Blockchain Consensus," International Conference on Intelligent Computing, Automation and Applications (ICAA), pp. 598–604, Nanjing, China, 25–27 June 2021. https://doi.org/10.1109/ICAA53760.2021.00110

[45] P. V. Sukharev and D. S. Silnov, "Asynchronous Mining of Ethereum Cryptocurrency", IEEE International Conference on Quality Management, Transport and Information Security, Information Technologies, pp. 731–735, St. Petersburg, Russia, 24–28 September 2018. https://doi.org/10.1109/ITMQIS.2018.8524929

[46] P. V. Sukharev, "Hardware Overclocking to Improve the Efficiency of Ethereum Cryptocurrency Mining", IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering, pp. 1873–1877, St. Petersburg and Moscow, Russia, 27–30 January 2020. https://doi.org/10.1109/EIConRus49466.2020.9039491

[47] D. V. Hieu and L. D. Khai, "A Fast Keccak Hardware Design for High Performance Hashing System", 15th International Conference on Advanced Computing and Applications (ACOMP), pp. 162–168, Ho Chi Minh City, Vietnam, 24–26 November 2021. https://doi.org/10.1109/ACOMP53746.2021.00029

[48] S. Alrubei, J. Rigelsford, C. Willis and E. Ball, "Ethereum Blockchain for Securing the Internet of Things: Practical Implementation and Performance Evaluation", International Conference on Cyber Security and Protection of Digital Services (Cyber Security), pp. 1–5, Oxford, UK, 3–4 June 2019. https://doi.org/10.1109/CyberSecPODS.2019.8885029

[49] T. Ncube, N. Dlodlo and A. Terzoli, "Private Blockchain Networks: A Solution for Data Privacy", 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), pp. 1–8, Kimberley, South Africa, 25–27 November 2020. https://doi.org/10.1109/IMITEC50163.2020.9334132

[50] Abdelzahir Abdelmaboud, Abdelmuttlib I.A. Ahmed, Mohammed Abaker, Taiseer A.E. Eisa, Hashim Albasheer, Sara A. Ghorashi and Faten K. Karim, "Blockchain for IoT Applications: Taxonomy, Platforms, Recent Advances, Challenges and Future Research Directions", Electronics, Vol. 11, No. 4: 630112022. https://doi.org/10.3390/electronics11040630

[51] Q. Zheng, Y. Li, P. Chen and X. Dong, "An Innovative IPFS-Based Storage Model for Blockchain," 2018 IEEE/WIC/ACM International Conference on Web Intelligence (WI), pp. 704–708, 2018. https://doi.org/10.1109/WI.2018.000-8

[52] H. R. Hasan, K. Salah, I. Yaqoob, R. Jayaraman, S. Pesic and M. Omar, "Trustworthy IoT Data Streaming Using Blockchain and IPFS," in IEEE Access, Vol. 10, pp. 17707–17721, 2022. https://doi.org/10.1109/ACCESS.2022.3149312

[53] S. Muralidharan and H. Ko, "An InterPlanetary File System (IPFS) Based IoT Framework," 2019 IEEE International Conference on Consumer Electronics (ICCE), 2019, pp. 1–2, https://doi.org/10.1109/ICCE.2019.8662002

[54] Zeinab Shahbazi and Yung-Cheol Byun, "Integration of Blockchain, IoT and Machine Learning for Multistage Quality Control and Enhancing Security in Smart Manufacturing", Sensors, Vol. 21, No. 4, pp. 1–21, 1467, 2021. https://doi.org/10.3390/s21041467

[55] A. Dorri, S. S. Kanhere and R. Jurdak, "Towards an Optimized Blockchain for IoT," 2017 IEEE/ACM Second International Conference on Internet-of-Things Design and Implementation (IoTDI), pp. 173–178, Pittsburgh, PA, USA, 18–21 April 2017. https://doi.org/10.1145/3054977.3055003

[56] Parul Agarwal, Sheikh Mohammad Idrees and Ahmed J. Obaid, "Blockchain and IoT Technology in Transformation of Education Sector", International Journal of Online and Biomedical Engineering, Vol. 17, No. 12, pp. 4–17, 2021. https://doi.org/10.3991/ijoe.v17i12.25015

[57] S. M. Kolekar, R. P. More, S. S. Bachal and A. V. Yenkikar, "Review Paper on Untwist Blockchain: A Data Handling Process of Blockchain Systems", International Conference on Information, Communication, Engineering and Technology (ICICET), pp. 1–4, Pune, India, 29–31 August 2018. https://doi.org/10.1109/ICICET.2018.8533868

[58] P. B. Dongre and P. Verma, "IOTDMS Blockchain Framework for Secure Data Exchange Between IoT Devices", Innovations in Power and Advanced Computing Technologies (i-PACT), pp. 1–8, Kuala Lumpur, Malaysia, 27–29 November 2021. https://doi.org/10.1109/i-PACT52855.2021.9696501

[59] X. Chen, R. Nakada, K. Nguyen and H. Sekiya, "A Comparison of Distributed Ledger Technologies in IoT: IOTA versus Ethereum", 20th International Symposium on Communications and Information Technologies (ISCIT), pp. 182–187, Tottori, Japan, 19–22 October 2021. https://doi.org/10.1109/ISCIT52804.2021.9590601

10 Authors

Abdallah Al-Zoubi is member of the Institute of Data Science and Artificial Intelligence, International Journal of Data Science and Big Data Analytics, fellow of the International Engineering and Technology Institute, Associate Editor-in-Chief of the International Journal of Instruction, Technology and Social Sciences, Member of ICT Committee of the Arab Engineering Association. He acted as Vice President of the International Association of Online Engineering, Vice President of the International e-Learning Association, and Co-Editor of the International Journal of Emerging Technologies in Learning, International Mobile Learning Association, and International Journal for Online Engineering, European Association for International Education,

International Association of Universities, Mediterranean Universities Union, Higher Education Reform Expert, European Commission, and IEEE.

Tariq Saadeddin is a bachelor student in Networks and Information Security Engineering at Princess Sumaya University for Technology. He is an experienced designer of IoT, blockchain and data storage systems, as well as implementation of a Sumo Robot, and malware analysis. (email: tar20160230@std.psut.edu.jo).

Mamoun Dmour received his MSc degree in computer information systems from Arab Academy for Banking and Financial Sciences, Jordan in 2004, and BSc degree in computer science from Mutah University, in 2000. He is an experienced Web developer and designer as well as a certified trainer in many technologies, and is currently with the computer science department at Staffordshire University, UK. (email: a030236k@student.staffs.ac.uk).

Article submitted 2022-09-10. Resubmitted 2022-11-03. Final acceptance 2022-11-05. Final version published as submitted by the authors.