IoT and Automation via Blockchain – A Simple Solution

Jéssica M. C. Oliveira*. João V. F. Guedes*
Talita C. Pinheiro*. Mario R. L. Oliveira *
Jonathas T. Neves*. Carlos A. M. Cruz*

** Universidade Federal do Amazonas, Manaus-AM, ZIP 69080-900*
Brazil (e-mails: jsk.mariella@gmail.com, joao.guedes@icomp.ufam.edu.br, agolemar@gmail.com, mario_ruben14@hotmail.com, jonathastn@gmail.com, carlosamcruz@ufam.edu.br).

Abstract: This work introduces a pioneering approach that harnesses the advantages of blockchain technology in a tiny sensor network suit for Internet of Things (IoT), automation, and smart environments application. The proposed solution combines the basic capabilities of an Arduino Uno microcontroller with an Android smartphone equipped with an embedded customized Bitcoin wallet application. By integrating these components, the system capitalizes on the inherent benefits of blockchain, enabling secure and transparent data management within the sensor network. This innovative approach unlocks new possibilities for enhanced data integrity, decentralized control, and seamless integration of the sensor network with the blockchain ecosystem.

Resumo: Este trabalho apresenta uma abordagem pioneira que aproveita as vantagens da tecnologia blockchain em uma pequena rede de sensores para aplicações de Internet das Coisas (IoT), automação e ambientes inteligentes. A solução proposta combina os recursos básicos de um microcontrolador Arduino Uno com um smartphone Android equipado com um aplicativo de carteira Bitcoin personalizado embutido. Ao integrar esses componentes, o sistema capitaliza os benefícios inerentes do blockchain, permitindo o gerenciamento de dados seguro e transparente dentro da rede de sensores. Essa abordagem inovadora abre novas possibilidades para a integridade de dados aprimorados, controle descentralizado e integração perfeita da rede de sensores com o ecossistema blockchain.

Keywords: Blockchain; Internet of Things; Sensor network; Android; Microcontroller.

Palavras-chaves: Blockchain; Internet das Coisas; Rede de sensores; Android; Microntrolador.

1. INTRODUCTION

The features and security attributes of blockchain technology have garnered significant attention due to their desirability for a myriad of applications, including IoT and many ways of automation (Abdi et al. 2022), (Xu et al. 2018), (Zhang et al. 2019), (Islam et al. 2019) and (Nakamura et al. 2020). However, the scalability aspect has remained a persistent hindrance to widespread adoption. In 2008, the birth of Bitcoin's blockchain brought forth a groundbreaking concept that initially eluded full comprehension (Nakamoto, 2008), yet lately in 2017 ultimately demonstrated the potential for building smart contracts and innovative applications. In 2013, Ethereum's blockchain was specifically designed to address the supposed limitations of Bitcoin that were not well understood on its original protocol, such as the support for smart contracts development (Androulaki et al., 2018).

Despite the inherent scalability challenges, Ethereum blockchain has gained widespread adoption in many applications, including IoT and automation, owing to its developer-friendly ecosystem and tools such as the Solidity language for smart contracts (Namane et al., 2022; Novo, 2018; Abdi et al., 2022; Xu et al., 2018; Zhang et al., 2019; Nakamura et al., 2020). The availability of these resources has positioned Ethereum as the most widely used blockchain platform. Additionally, Hyperledger has emerged as another popular choice for building applications (Islam et al., 2019; Xu et al., 2018). However, with the advent of new tools enabling application development on the Bitcoin network, there is now the potential to build applications on a blockchain that is more scalable (Liu, 2023).

The capacity to process a larger number of transactions per second (TPS) in a blockchain is crucial for meeting the scalability requirements of IoT applications. In an IoT ecosystem, numerous devices constantly generate and exchange data, requiring swift and efficient processing. As the number of connected devices and the volume of data they produce increase, the blockchain network must be capable of handling the growing transactional load.

Taking into consideration the average transaction size of 500 bytes, the Ethereum network, with an average block size of 126 kB (EBS 2023) and a block time of 12 seconds (EBT 2023), has the capacity to process up to approximately 21 transactions per second (TPS). Hyperledger, claims to have

achieved a peak of around 3,000 TPS in tests (Kelsey, 2023). However, it's important to note that the actual TPS can vary based on the specific implementation and configuration of the Hyperledger framework being used. Such limitation cripples the scalability of IoT, and automations applications built on blockchain.

On May 25, 2023, Bitcoin Satoshi Vision (BSV) processed an impressive 4,324,354 transactions in a single block on the mainnet at block 793495 as can be checked on online chain explorer as shown in Fig 1.

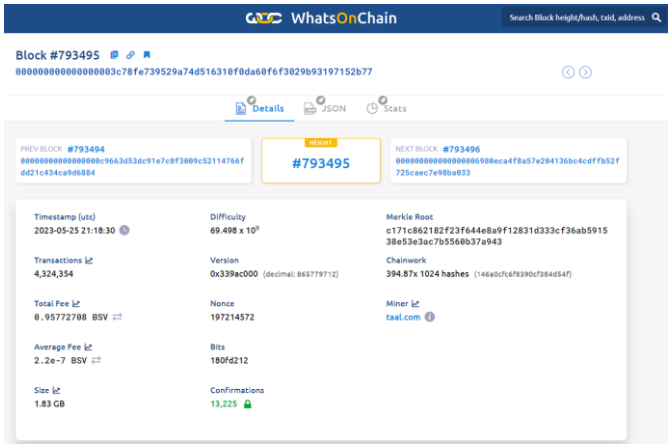

Fig. 1 BSV blockchain with 4M transactions.

This translates to more than 7.2 kTPS, considering the average block time of 10 minutes per block. Furthermore, there are promises of reaching 50 kTPS in the near future (Chan, 2021).

On August 8, 2023, whitin a 24 hour timeframe, the BSV blokchain achieved another remarkable global record with 128.691 milion transactions using the original Bitcoin protocol. This achievement serves as a fact that theoretical limitation on scability are indeed misleading and that the actual potential for expansion is greater than initially expectations (Lucas, 2023).

Fig 2 demonstrates BSV blockchain's capability to power applications and number of transactions processed in 24 hours (Lucas, 2023).

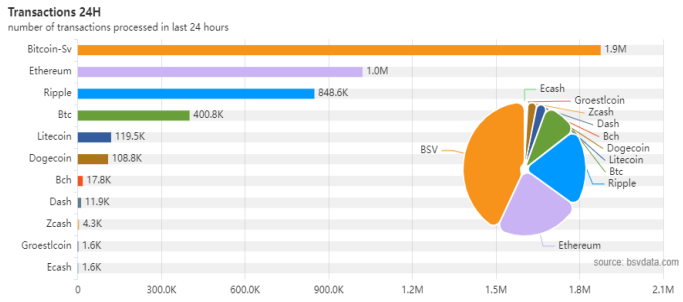

Fig. 2 Blockchain statistics.

Table 1 illustrates an analysis between our methodology using BSV blockchain with two state-of-the art approaches. As evidenced by the information in Table 1, it is clear that the approaches utilize IoT and are easily accessible through mobile devices.

In the research (Haque et al., 2021) used purely decentralized system utilizing Hyperledger Blockchain technology. However, in an alternate approach detailed (Ghorbel et al., 2022), a system was suggested. This system enables farmers to track data from wireless sensor networks using a public Ethereum Blockchain.

The implemented approach introduces a different viewpoint, opting for BSV blockchain technology instead of a distributed system due to its ability to track all transaction made. As a result, no one has the capability to modify, delete or change any data that becomes part of the block.

Table 1. Blockchain comparison

Blockchain	Technology	Embedded	Device
Hyperledger	IoT	No	Mobile
Ethereum	WSN	No	Mobile
BSV	IoT	Arduino	Mobile

In this work, we present a simple solution that enables the communication and synchronization of the two microcontrollers through the BSV networks, such solution is suited for IoT and automation applications. Our approach aims to address the specific requirements and challenges of integrating IoT and automation systems with a robust and scalable blockchain platform. By utilizing the unique capabilities of the BSV blockchain, including its high transaction throughput and promising future scalability potential, we propose a solution that ensures secure and transparent data exchange, decentralized control and reliable automation processes. Through this implementation, we envision unlocking new possibilities for the seamless integration of IoT and automation technologies, enabling efficient and trustworthy systems in various domains.

The work is divided in the following parts: Section 2 presents the proposed implementation using automation and blockchain with its challenges. Subsection 2.1 shows the composition and operation of the system with the arduino microcontroller, two android smartphones communicating via bluetooth and recording each transaction and state change in the blockchain network. Section 3 presents the experimental results and the states stored on the blockchain. Section 4 presents a conclusion about the groundbreaking approach that leverages the power of blockchain technology in a compact sensor network tailored for IoT, automation, and smart environments.

2. PROPOSED IMPLEMENTATION

Besides scalability issues, another barrier to build blockchain applications including those in IoT and automation environment is the need to use third party wallets that grant writing access to blockchain. The reliance on third-party wallets to build applications on blockchain introduces a significant burden and potential complexities. When developers need to integrate external wallets into their applications, it adds an extra layer of dependency and requires users to manage separate wallets for different

blockchain interactions. This can create friction and inconvenience, particularly for users who may not be familiar with the intricacies of managing wallets and private keys.

In the proposed application we employ an embed wallet application that reduces the burden to have an additional account on another platform just to run the application. By integrating a wallet directly into the application, users gain the convenience of seamless and unified access to blockchain functionalities. They no longer need to rely on external wallets, streamlining the user journey and reducing potential barriers to adoption.

2.1 System Composition and Operation

The basic composition of the proposed system consists of two Arduino Uno microcontrollers M1 and M2, two Android smart phones A1 and A2, as shown in Fig 3. M1 and M2 connect with A1 and A2, respectively, via Bluetooth in order to communicate the state of the sensors they monitor and to receive instructions of any type of job they must perform.

The Android devices A1 and A2 are responsible to receive the data form the microcontrollers M1 and M2, pack this data in a transaction compliant with the bitcoin protocol and broadcast it to the Blockchain. They are also responsible for retrieving data from the blockchain containing the instructions of tasks that the microcontrollers must perform.

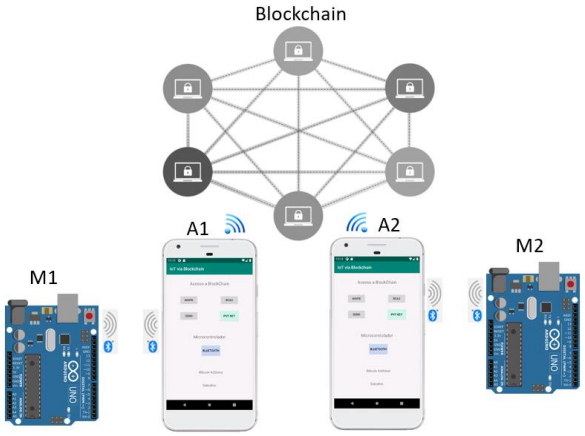

Fig. 3 Interconnection between devices of the system.

The system works as follows: M1 and M2 connects with their respective Android devices, A1 and A2 that enables access to the BlockChain. Each microcontroller has its own private key that allows it to write and store information in a specific address at the blockchain.

In the application herein presented, each microcontroller keeps listening to the address of its peer in order know the instructions of the next task to be performed. The state of the sensors in M1 determines the subsequent tasks for M2 and vice versa. After performing its task, each microcontroller reads the state of their sensors and inform them to the blockchain, and the next cycle of tasks is determined. This mutual exchange of information enables the microcontrollers to synchronize their actions based on the sensor data, facilitating coordinated operations between two devices.

Fig 4 shows a simple scheme on how the process takes place. Suppose at the beginning M1 broadcasts its state to the blockchain, so the last transaction at Address 1 will contain the information State M1(0). Now, M1 keeps listening to Address M2 in order to know what to do next. As M2 is listening to Address M1 it perceives a new transaction containing the information State M1(0), this data brings the instruction of the next task it must perform. Therefore, M2 perform the required tasks, reads the state of its sensors and broadcasts to the blockchain a new transaction to Address M2 containing the information State M2(0). As M1 is listing to the Address M2 it perceives a new transaction and verify that there is a new instruction to be performed and the cycle repeats. In this way tiny network sensor keep synchronized through the blockchain.

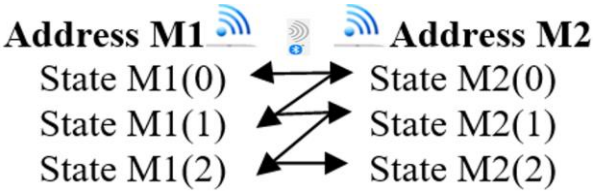

Fig. 4 States Stored on the Blockchain.

The BSV blockchain offers not only scalability features but also the ability to include arbitrary data types within transactions. This means that any kind of data can be inserted into a transaction and subsequently retrieved using the transaction's unique ID through any accessible retrieval service within the network. To illustrate this concept, an example of data retrieval is depicted in Figure 5, highlighting the seamless process of accessing the desired information.

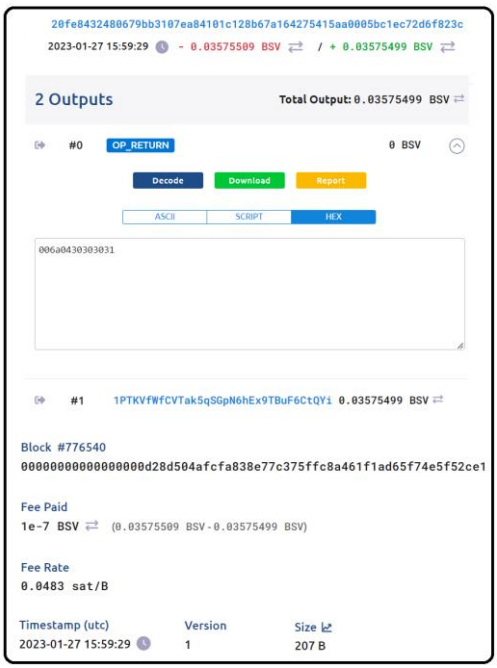

Fig. 5 Sample of timestamped data from the proposed system.

The information retrieved shown in Fig. 5 includes: transaction ID; address of the microcontroller; transaction

output, one of which includes the data of our system in hexadecimal format; the number of the block on which the transaction was included; the hash of the block; and the timestamp on which the block was created by the transaction validators.

To ensure the validation and inclusion of a transaction in a block, it is imperative to include a transaction fee for the validators. These validators, who compete with one another, are responsible for creating blocks within the system. As of the time of writing this paper, the average fee rate on the BSV blockchain stands at 0.05 Satoshi per byte.

For the sake of simplicity and focus on the proof of concept, the employed sensors in this study were limited to on/off detectors. By utilizing these sensors, the emphasis was placed on validating the fundamental principles and functionality of the system. While the choice of on/off detectors may restrict the range of data inputs, it allowed for a clear and concise demonstration of the system's core capabilities.

It is worth noting that one of the challenges associated with blockchain-based system applications is the requirement for a strong and reliable internet connection to ensure optimal system performance. A stable and high-speed internet connection is essential for seamless communication and interaction with the blockchain network. However, it is important to acknowledge that the reliance on a robust internet connection can be considered a downside of such systems. In scenarios where internet connectivity is limited or unreliable, it may result in disruptions or delays in the system's operations.

3. EXPERIMENTAL RESULTS

Table 2 provides an overview of the primary hardware components employed in the project. The model of the microcontrollers and Bluetooth modules are the same for both tiny sensor network, whereas the android device models where different for each node.

Table 2. Components of the System

Devices	Model
Microcontroller M1	Arduino Uno
Bluetooth module M1	HC-05
Android 1	J2 Core
Microcontroller M2	Arduino Uno
Bluetooth module M2	HC-05
Android 2	JPrime 7

To run the system the following steps are required: First, insert the private key of each Arduino device's microcontroller into the embedded wallet application. The main interface will display the microcontroller's address after connecting to the blockchain. Second, input the address of the microcontroller that will be monitored by the first one. Third, connect the Bluetooth device responsible for communication with the microcontroller of each Android device. Finally, synchronize both tiny networks using the designated button, marked as "LED 1."

The user interface appearance for these steps is shown in Figures 6(a), (b), (c), and (d). Figure 6(a) displays the Main UI for the Android IoT Blockchain Application, Figure 6(b) showcases the monitoring address insertion interface, Figure 6(c) illustrates the Bluetooth connection options interface, and Figure 6(d) demonstrates the tiny network state sensor interface. By referring to these figures, you can easily navigate and configure the system, ensuring seamless operation and effective control. A picture of the working system is presented in Fig. 7.

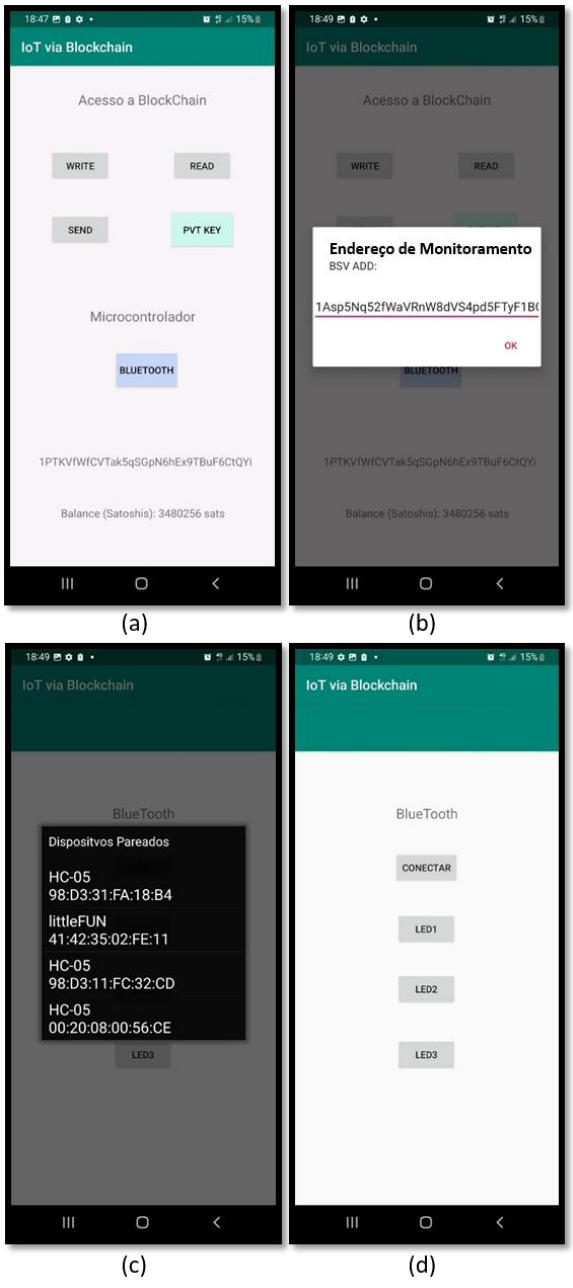

Fig. 6 (a) Main UI for the Android IoT Blockchain Application; (b) monitoring address insertion; (c) Bluetooth connection options; (d) state sensor interface.

It is worth emphasizing that the inclusion of the embedded wallet application significantly simplifies the process. You only need to insert the private key of the microcontroller

linked to each Arduino device. Once connected to the blockchain, the main interface will promptly present the respective device address, streamlining the control and management of your devices effortlessly.

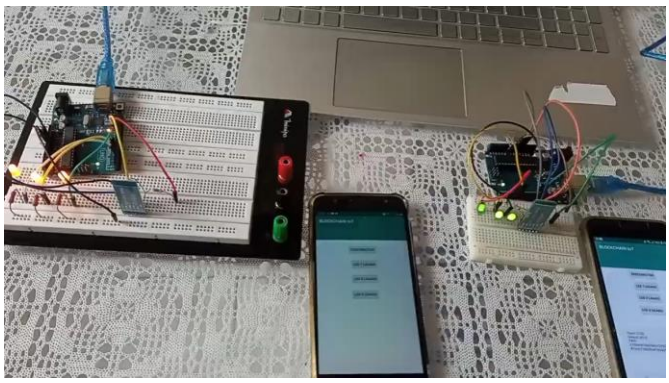

Fig. 7 Tests of the proposed architecture.

In this experiment, each Arduino is responsible for both setting and reading the state of three distinct gates. The status of these gates is visually conveyed through three separate LEDs, which clearly indicate whether each gate is currently active or inactive. The next state of each network will be determined by current state of its peer as presented in Table 3 for microcontroller M1 and Table 4 for microcontroller M2.

Table 3 illustrates all the activities performed by M1 throughout a complete test cycle. The designation ADD M1 represents the specific address that M1 utilizes to transmit data to the blockchain. STATE_0 does not correspond to a state of the sensor network managed by M1. Rather, it means the initial state of the overall system, set directly by the user on the blockchain, conveying the intended starting point for the network under the control of M2. SENT INST ID_0 corresponds to the ID of the transaction sent by user to the address of M1 to state the system.

Table 3. Activities of M1 during the Tests

ADD M1	1PTKVfWfCVTak5qSGpN6hEx9TBuF6CtQYi
STATE_0	(read) *** → (set) *** → (sent) 0001
SENT INST ID_0	bab2bb8a73901316dab3870bcdc24bdb129245c2f7102c90463dd966ee33d874
STATE_1	(read from State 1 M2) 0100 → (set) 100 → (sent) 0010
SENT INST ID_1	5cb9fda5bff2752f516dd196acb64f1011e7db0e27bb86ff739f5c480a856ae1
STATE_2	(read from State 2 M2) 0001 → (set) 101 → (sent) 0100
SENT INST ID_2	2219074d7d82acf48cae6bc77905686a6aca9b61c78c12861dfac4749667a498
STATE_3	(read from State 3 M2) 0010 → (set) 111 → (sent) 0001
SENT INST ID_3	20fe8432480679bb3107ea84101c128b67a164275415aa0005bc1ec72d6f823c
STATE_4	(read from State 4 M2) 0100 → (set) 011 → (sent) 0010
SENT INST ID_4	a9ed34d209fc6cf7688e226ca50c85261b3cf149ce6752d71cc2d07e21a5a11d
STATE_5	(read from State 5 M2) 0001 → (set) 010 → (sent) 0100
SENT INST ID_5	54f6ae717409f18ef2bdd9d8b229ae5dd2dddc3bbab90ebf5a6fa225bc5da7cc
STATE_6	(read from State 6 M2) 0010 → (set) 000 → (sent) ***

Once the system is initiated, M1 and M2 start monitoring each other's addresses to detect any instructions indicating a change in their respective network states. In this test, M2 detects the first instruction, marked as "SENT INST ID_0," within the address of M1 as shown in Table 3. Consequently, M2 updates its own network state from 000 to 001. Subsequently, M2 transmits a transaction to the blockchain, notifying M1 of the next intended state. This action generates the entry "SENT INST ID_0" in Table 4. M1 responds by modifying its network state from 000 to 100 and generates a new state specific to M1. This synchronized process continues through the blockchain until both networks back to the null state 000.

Table 4. Activities of M2 during the Tests

ADD M2	1Ar5eHdaeuAKLxrSM2WjCSFPfT3gZh8n9J
STATE_0	(read from State 0 M1) 0001 → (set) 001 → (sent) 0100
SENT INST ID_0	057d8456b8f7f9f7d89b5cc82973f5db428ac692587a1387b53603480d558ef4
STATE_1	(read from State 1 M1) 0010 → (set) 011 → (sent) 0001
SENT INST ID_1	8714df30c6c3124e79004d3f64a12dfbaa05a0ef30936f381eba0e4f5f27af0a
STATE_2	(read from State 2 M1) 0100 → (set) 111 → (sent) 0010
SENT INST ID_2	c7db4dd10e944b132357d7d4b9b422458441cc6716025b41898e578c01a32422
STATE_3	(read from State 3 M1) 0001 → (set) 110 → (sent) 0100
SENT INST ID_3	fd0269b004103af50842c82db36e330d3beb898f30e042b57446f4304b629fbc
STATE_4	(read from State 4 M1) 0010 → (set) 100 → (sent) 0001
SENT INST ID_4	3a23364db9b03927a7dd75bd973da354c13502dc8a4ae8196d10b393d7025018
STATE_5	(read from State 5 M1) 0100 → (set) 000 → (sent) 0010
SENT INST ID_5	8056c5d86989fb69f35267ba0aa38332069b206c3a0add573b4d7b81ff9eeed7
STATE_6	(read) **** → (set) *** → (sent) ***

The entire chronicle of system operations is perpetually recorded on the blockchain, enabling the comprehensive history of the system's functioning to be retrieved. This retrieval can be accomplished by referencing the transaction IDs transmitted by the microcontrollers to the blockchain. While the history of transactions can be obtained through the microcontroller's address, it is advisable to maintain a custom database that preserves the IDs of significant transactions for ease of reference and analysis. The addresses and transaction IDs on Table 3 and Table 4 can be employed in searches on a BSV explorer to get additional details of these transactions.

It is crucial to highlight the following scenario: if the system aims to scale and handle a significant and continuous volume of transactions, it is essential for the system to operate its own full node within the blockchain. However, if the transaction volume does not warrant the need for a full node, managing one may not be justified, and instead, the system can leverage the services provided by existing network nodes. Careful consideration of the transaction volume and associated costs will help determine whether deploying a dedicated full node is necessary for efficient scalability or if

relying on the services of other network nodes is a more viable option.

4. CONCLUSION

In conclusion, this work presents a groundbreaking approach that leverages the power of blockchain technology in a compact sensor network tailored for IoT, automation, and smart environments. By combining the functionalities of an Arduino Uno microcontroller with a customized Bitcoin wallet application on an Android smartphone, the proposed solution harnesses the inherent advantages of blockchain for secure and transparent data management within the network. The integration of these components opens up new opportunities for improved data integrity, decentralized control, and seamless integration with the larger blockchain ecosystem. It is important to acknowledge that a notable drawback of this system lies in its reliance on a stable and reliable internet connection. Nonetheless, overall, this pioneering approach paves the way for advancements in sensor network applications empowered by blockchain technology.

ACKNOWLEDGMENTS

The authors would like to acknowledge the Universidade Federal do Amazonas (UFAM) and the Graduate Program in Electrical Engineering (PPGEE) for support on their research. This work was supported by Fundação de Pesquisa do Estado do Amazonas - FAPEAM under POSGRAD program EDITAL N 008/2021. We greatly appreciate the CAPES, National Council for Scientific and Techno-logical Development - CNPq.

REFERENCES

Abdi, A.I.; Eassa, F.E.; Jambi, K.; Almarhabi, K.; Khemakhem, M.; Basuhail, A.; Yamin, M. Hierarchical Blockchain-Based Multi-Chaincode Access Control for Securing IoT Systems. Electronics 2022, 11, 711.

Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.D.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric. In Proceedings of the Thirteenth EuroSys Conference. ACM, Porto, Portugal, 23–26 April 2018.

Chan, Jerry. This is what Teranode is about (+50k TPS). TECH 9 JUNE 2021. https://coingeek.com/this-is-what-teranode-is-about-50k-tps/.

EBS. Ethereum Average Block Size (I:EBS). Jun 04 2023. https://ycharts.com/indicators/ethereum_average_block_size.

EBT. Ethereum Average Block Time (I:EBT). Jun 04 2023. https://ycharts.com/indicators/ethereum_average_block_time.

Ghorbel, O.; Frikha, T.; Hajji, A.; Alabdali, R.; Ayadi, R.; Elmasry, M.A. Blockchain-Based Supply Chain System for Olive Fields Using WSNs. Comput. Intell. Neurosci. 2022, 2022, 9776776.

Haque, B.; Hasan, R.; Zihad, O.M. SmartOil: Blockchain and smart contract-based oil supply chain management. IET Blockchain 2021, 1, 95–104.

Islam, M.A.; Madria, S. A Permissioned Blockchain Based Access Control System for IOT. In Proceedings of the 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 14–17 July 2019; pp. 469–476.

Kelsey, Dave Kelsey. Benchmarking Hyperledger Fabric 2.5 Performance. February 16, 2023. https://www.hyperledger.org/blog/2023/02/16/benchmarking-hyperledger-fabric-2-5-performance.

Liu, Xiaohui. Introducing the sCrypt development platform on Bitcoin. https://xiaohuiliu.medium.com/introducing-the-scrypt-development-platform-on-bitcoin-4c5bcfa04b88.

Lucas, Gavi. BSV blockchain sets new world record with 128M transactions in 24 hours. BUSINESS 10 AUGUST 2023. https://coingeek.com/bsv-blockchain-sets-a-new-world-record-with-128m-transactions-in-24-hours/.

Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf.

Nakamura, Y.; Zhang, Y.; Sasabe, M.; Kasahara, S. Exploiting Smart Contracts for Capability-Based Access Control in the Internet of Things. Sensors 2020, 11, 1793.

Namane, S.; Ben Dhaou, I. Blockchain-Based Access Control Techniques for IoT Applications. Electronics 2022, 11, 2225. https://doi.org/10.3390/electronics11142225.

Novo, O. Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT. IEEE Internet Things J. 2018, 5, 1184–1195.

Xu, R.; Chen, Y.; Blasch, E.; Chen, G. BlendCAC: A BLockchain-Enabled Decentralized Capability-based Access Control for IoTs. In Proceedings of the 2018 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), Halifax, NS, Canada, 30 July–3 August 2018.

Zhang, Y.; Kasahara, S.; Shen, Y.; Jiang, X.; Wan, J. Smart Contract-Based Access Control for the Internet of Things. IEEE Internet Things J. 2019, 6, 1594–1605.