Comparative analysis between a Private Network Micro-blockchain IoT and a Public Blockchain in the Data Collection of Decentralized Agents

Jonathas Tavares Neves* Jessica M. C. Oliveira**
Talita C. Pinheiro* Mario R. L. Oliveira**** Carlos Augusto de Moraes Cruz*******

**Universidade Federal do Amazonas, Av. Octávio Hamilton Botelho Mourão - Coroado\\ CETELI-UFAM\\ Manaus, Amazonas, Brasil; (e-mail: jonathastn@gmail.com).*
***Universidade Federal do Amazonas, Av. Octávio Hamilton Botelho Mourão - Coroado\\ CETELI-UFAM\\ Manaus, Amazonas, Brasil; (e-mail: jsk.mariella@gmail.com).*
****Universidade Federal do Amazonas, Av. Octávio Hamilton Botelho Mourão - Coroado\\ CETELI-UFAM\\ Manaus, Amazonas, Brasil; (e-mail: mario_ruben14@hotmail.com).*
*****Universidade Federal do Amazonas, Av. Octávio Hamilton Botelho Mourão - Coroado\\ CETELI-UFAM\\ Manaus, Amazonas, Brasil; (e-mail: carlosamcruz@ufam.edu.br).*

Abstract: In this study, we conducted an investigation into the effectiveness of a private Micro-blockchain IoT (Internet of Things) when contrasted with a public blockchain in the context of decentralized data collection. The results revealed that the private Micro-blockchain exhibited a notable advantage in terms of data privacy and control, surpassing the alternative of the public blockchain. Additionally, the private Micro-blockchain solution demonstrated a reduced demand for hardware resources, enhancing its efficiency. These insightful findings provide valuable guidance for the practical implementation of data collection strategies within the realm of IoT, underscoring the potential for heightened security and improved operational efficiency.

Resumo: Neste estudo, realizamos uma investigação sobre a eficácia de uma microblockchain IoT (Internet of Things) privada quando contrastado com uma blockchain pública no contexto da coleta descentralizada de dados. Os resultados revelaram que o microblockchain privada apresentou uma vantagem notável em termos de privacidade e controle de dados, superando a alternativa da blockchain pública. Além disso, a solução microblockchain privada demonstrou uma demanda reduzida por recursos de hardware, aprimorando sua eficiência. Esses resultados perspicazes fornecem orientações valiosas para a implementação prática de estratégias de coleta de dados no âmbito da IoT, destacando o potencial para maior segurança e eficiência operacional aprimorada.

Keywords: Micro-blockchain; IoT (Internet of Things); Private network; Decentralized agents; Bitcoin SV.

Palavras-chaves: Microblockchain; IoT (Internet das Coisas); Redes Privadas; Agentes Descentralizados; Bitcoin SV.

1. INTRODUCTION

In recent years, blockchain technology has gained prominence as a promising solution for various challenges in different domains (Tapscott and Tapscott, 2018). Its ability to provide security and transparency (Pahlajani et al., 2019), immutability, and decentralization (Nakamoto, 2008) has sparked interest in areas such as finance (Xinyi et al., 2018), supply chain, and energy (Sinha et al., 2019). Simultaneously, the emergence of the Internet of Things (IoT) has facilitated connectivity and collaboration among a wide array of devices (Zinonos et al., 2019).

The convergence of IoT with blockchain technology has sparked scientific interest and holds promise for numerous innovative applications IoT enables connectivity and collaboration among diverse devices, creating an environment conducive to reliable and immutable data collection (Sinha et al., 2019). Additionally, integrating blockchain with IoT addresses fundamental challenges in information security (Anagnostakis et al., 2021). A notable approach in this context is the use of micro-blockchains and decentralized agents (Hao et al., 2018). Micro-blockchains are streamlined versions designed for specific applications with lower hardware requirements. Decentralized agents, on the other hand, are autonomous entities operating on the blockchain network, performing specific tasks and contributing to system functionality.

This scientific article aims to compare public and private blockchains, focusing on determining the minimum hardware requirements for each type. By evaluating their

characteristics and specific requirements, valuable insights will be provided to researchers and developers seeking to optimize the performance and efficiency of their blockchain applications. Understanding the hardware needs, particularly in private blockchains, will facilitate resource selection and efficient deployment in various application areas.

The article's structure includes Section 2, which presents the theoretical foundations of blockchain, IoT, micro-blockchains, and decentralized agents. Section 3 discusses the methodology employed for comparing public and private blockchains, while Section 4 presents the discussion. Finally, Section 5 explores the conclusions drawn from the study and outlines possible future directions.

2. LITERATURE REVIEW

2.1 Private blockchain and public blockchain

A private blockchain is a blockchain network limited to a selected group of authorized participants (Wang et al., 2023). This approach is commonly adopted by organizations that aim to maintain greater control over their transactions and confidential data, given the sensitive nature of this information. In this type of blockchain, participation and validation of transactions are carried out by a restricted number of trusted entities. Besides the time-stamping features, the main benefit of private blockchains is data privacy, as transactions are visible only to authorized participants. Additionally, the governance of a private blockchain is centralized, allowing for greater control over network rules and policies.

According to Pahlajani, voting-based consensus algorithms are widely used in private blockchains, where the nodes are known. This is the fundamental distinction compared to proof-based consensus algorithms (Proof of Work – PoW and Proof of Stake – PoS), where nodes are often allowed to join and exit the verification system. In voting-based consensus, it is necessary to exchange results within the network before appending the block to the blockchain. In other words, future consensus values must be established in advance before the initiation of transactions to avoid the need to interrupt the network during consensus execution.

For the case of Hash in a private blockchain (isolated or industrial) without any interaction with external networks, encryption would not be necessary, since only authorized agents would operate the data (Jo et al., 2020). Private blockchains have been successfully applied in the Industrial Internet of Things (IoT) due to their advantages and adaptability to algorithms that optimize scalability (Cao et al., 2020). The majority of industrial organizations working with IoT technologies use private blockchains exclusively or as a priority.

A public blockchain is characterized by being open to anyone or any entity that wants to participate in the network (Gorkhali et al., 2020). It is often associated with cryptocurrencies such as Bitcoin SV and Ethereum. In a public blockchain, as depicted in Fig. 1, any participant can join the network, validate transactions, and contribute to the security and integrity of the system. Transparency and decentralization are the fundamental principles of a public blockchain, meaning that all transactions and information are visible to all participants in the network. In this case, strong encryption is required to maintain data privacy. The governance of a public blockchain is decentralized and based on consensus among the participants. One of the public blockchains that executes a significant number of transactions is Bitcoin SV, as shown in Fig. 2.

Algorithm 1: Connection to a Public Blockchain

```
Data: Generate a unique user ID
Result: Connection to the blockchain
Step 1: Request user authentication
 (username, password);
Step 2: Verify the credentials;
if Credentials are valid then
    Step 3: Open blockchain wallet and
     perform network block operations for
     information storage;
end
else
    Step 4: Terminate connection (Invalid
     credentials);
end
```

Fig. 1: Pseudocode for accessing a public blockchain

One of the consensus algorithms used in a public blockchain, such as Bitcoin, is Proof of Work (PoW) (Gorkhali et al., 2020). Miners compete to solve cryptography problems and find a number called a “nonce” that allows them to add a new block to the blockchain. The majority of participants verify and agree on the new block, achieving consensus. This algorithm is secure but consumes a significant amount of energy and may have scalability limitations.

The hash mechanism in a public blockchain involves the use of cryptography hash functions, such as SHA-256 (Secure Hash Algorithm 256 bits). These functions transform input data into a unique and fixed hash value, which represents a condensed version of the original data. The hash is used to ensure the integrity of blocks and transactions in the blockchain, as any changes to the data would result in a completely different hash (Gorkhali et al., 2020).

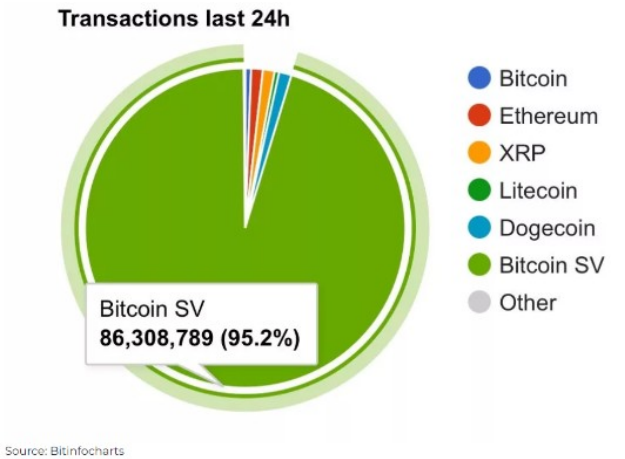

Fig 2: Performance data of a public blockchain- Bitcoin SV (Lucas, Gavin, 2023a)

When implementing encryption, several factors must be considered. In the context of RSA encryption, the size of the RSA key used within a blockchain can vary. Typically, key sizes of at least 2048 bits are employed to ensure a sufficient level of security (Albakri et al., 2019). However, in certain scenarios, larger key sizes such as 4096 bits might be advisable to enhance protection against brute-force or advanced attacks. The selection of a key size depends on the specific security needs of the blockchain and recommendations from cryptography experts. Thus, a comparison of blockchain structures can be illustrated in Fig. 3.

Aspect	Public	Private
Access	Open to anyone	Restricted
Participants	Unknowns	Selected
Consensus Algorithm	Proof of Work	Determined by Voting
Scalability	Many Hindrances	Few Hindrance
Data Privacy	Public visibility	Restricted visibility
Cryptography	Strong encryption	Not required
Immutability	Network dependent	Depend on the safety and security provided by the owner
Governance	Decentralized	Private

Fig 3: Comparison between Public and Private Blockchains

2.2 Micro-blockchains and minimum IoT hardware

According to Anagnostakis, a micro-blockchain is a reduced and simplified version of a traditional blockchain. It is designed to operate in smaller-scale environments such as IoT devices, local networks, or specific systems. A micro-blockchain typically has fewer participants, fewer computational resources, and a simplified consensus structure compared to a full blockchain. This approach aims to provide the basic functionalities of blockchain, such as transaction recording, data security, and integrity, in a more efficient and suitable manner for resource-constrained devices or specific systems.

However, the feasibility of a micro-blockchain relies solely on the hardware it is associated with. Taking into account the operational limits previously discussed in the current section on public and private blockchains, it is evident that a micro-blockchain would not be able to fulfill its functionality in a "public" network, as its hardware would need to have the same storage and processing capacity as that of a regular public blockchain. Therefore, the exclusive use of a micro-blockchain is limited to private environments, such as industrial or isolated settings.

Another issue to be analyzed is the ability of the micro-blockchain, composed of minimal IoT hardware, to communicate in a bidirectional manner (as both sender and receiver). During the execution of transactions in the micro-blockchain, certain codes may require a hybrid architecture that prioritizes certain functions for periodic tasks (rate monotonic) and determines which functions should be executed for aperiodic tasks (deadline first) using scheduling mechanisms addressed in hard real-time systems (Kopetz and Steiner, 2022).

3. METHODOLOGY

For comparison purposes, commercially available microcontrollers adapted for IoT communications, such as Bluetooth or Wi-Fi, will be employed. There will be no direct comparison between the hardware of a private micro-blockchain and that of a public blockchain, due to the differing robustness required to handle high transaction volumes. The satisfiability requirements will be evaluated in comparison with the Bitcoin SV blockchain, alongside the proposed microcontrollers: Arduino Nano 33 IoT, as discussed in Anagnostakis' article, and ESP32-WROOM, as proposed in this paper. The analysis will center on performance, scalability, and efficiency, taking into consideration the resources and capabilities of the selected microcontrollers. The obtained results will determine which microcontroller is better optimized for operation within a micro-blockchain, considering their technical capabilities and specific project needs.

3.1 Performance Evaluation

A public blockchain like Bitcoin SV on May 25, 2023, processed an impressive 4,324,354 transactions in a single block on the mainnet at block 793495, this translate to more than 7.2k TPS, considering the average block time of 10 minutes per block. Furthermore, there are promises of reaching 50k TPS in the near future (Lucas, Gavin, 2023b). When considering hardware capabilities, this transfer capacity directly influences the network's processing and transmission capabilities. To meet these requirements, a

developed node must possess a minimum processing capacity of 10 cores and 20 threads, along with an internet connection of 1Gbit+ (up and down).

For a private micro-blockchain, we conducted an analysis of optimized hardware with specific requirements. In this context, we employed two IoT microcontroller devices as a comparative benchmark. The first device, Arduino Nano 33 IoT, as cited by Anagnostakis, operates at a processing capacity of up to 48 MHz (with a single core). It features the SAMD21 microcontroller based on the ARM Cortex-M0+ architecture. In terms of maximum transmission rate, the Arduino Nano 33 IoT supports Wi-Fi (IEEE 802.11b/g/n) and Bluetooth (BLE), enabling wireless communication. However, for a public micro-blockchain, it would be impractical to utilize hardware with inefficient hash capabilities susceptible to attacks.

Another notable example is the ESP32 WROOM microcontroller, a development module based on the ESP32 microcontroller. It boasts a processing capacity of up to 240 MHz and houses a dual-core Tensilica LX6 processor, providing two independent processing cores.

Regarding transmission rates, the ESP32 WROOM supports a variety of wireless communication protocols, including Wi-Fi (IEEE 802.11b/g/n) and Bluetooth (Classic and BLE). The achievable transmission rate depends on the operating environment, specific module configurations, and the protocol being used. Under optimal conditions, the ESP32 WROOM can achieve data transfer rates of up to 150 Mbps for Wi-Fi and 3 Mbps for Bluetooth. Therefore, the second option is chosen considering the evaluated cost-effectiveness.

3.2 Scalability Assessment

Regarding the scalability of the Bitcoin SV network, the information provided by (Lucas, Gavin, 2023b) reveals that as of February 2023, the Scalability Test Network (STN) had grown to approximately 4.5TB in size. Notably, the network continues to expand at a rate of approximately 1.1TB per month. This signifies a commitment to minimizing the frequency of network resets for the STN, emphasizing the ongoing development and expansion of the network.

Proof of Work (PoW) is a consensus mechanism used in blockchains like Bitcoin, providing decentralized consensus, security against tampering, Sybil attack resistance, and fair block creation through puzzle-solving. While PoW has drawbacks like energy consumption and scalability, renewable energy can mitigate energy concerns, and alternative consensus solutions like Proof of Stake (PoS) aim to address scalability. However, it's worth noting that while Ethereum network has not been able do scale after switching consensus from PoW to PoS (Buterin, Vitalik, 2023), scalability can also be achieved by increasing block sizes, as demonstrated by Bitcoin SV (BSV) blockchain, which scales by allowing larger block sizes to accommodate more transactions by working out the appropriate hardware technology.

The main figure to measure scalability is the number of transactions a blockchain can process in a finite period of time.

Therefore, scalability can be measured according to the (1):

$$S = \frac{Blocksize\ x\ Timer\ per\ Block}{Average\ TX\ size\ in\ bytes} \quad (1)$$

It is worth noting that hardware storage and processing capabilities are in any scenario key points toward scalability. When considering a micro-blockchain limited to private applications (such as industrial or isolated use cases), scalability is closely related to processing power. To determine the minimum and most optimized hardware capable of providing scalable capabilities for a micro-blockchain, the following equation described in (2):

$$S_{micro-blockchain} = \frac{PxT}{R} \quad (2)$$

Where:

• Smicro-blockchain: Scalability of the microcontroller for the micro-blockchain.

• P: Processing capacity of the microcontroller.

• T: Transaction rate of the micro-blockchain.

• R: Transfer rate of the microcontroller.

This equation allows for the evaluation of hardware options that meet the minimum processing capacity requirements for achieving satisfactory scalability in a specific micro-blockchain. It is crucial to consider these factors during the configuration of a micro-blockchain, ensuring that the selected hardware can handle the desired transaction rate while maintaining an adequate transfer rate.

In comparative terms, scalability should be associated with transaction throughput, which is described in (3).

$$\frac{S_{micro}}{S_{public}} = \frac{P_{micro}\,xT_{micro}}{R_{micro}}\,x\,\frac{B_{public}}{T_{public}} \quad (3)$$

In this (3), Smicro and Spublic represents the scalability ratio between the micro-blockchain and the public blockchain. The terms Pmicro, Tmicro, Rmicro, Bpublic, and Tpublic are the variables representing the processing capacity, transaction rate, and transfer rate of the micro-blockchain, as well as the transaction rate and maximum block size of the public blockchain, respectively.

This equation allows for a direct comparison of the relative scalability between the two types of blockchains, taking into account the key factors that influence their processing and transaction capabilities. By doing so, it provides a more

comprehensive view of the scalability capacities and limitations of each blockchain type.

3.3 Efficiency Comparison

In the case of a private micro-blockchain, the overall efficiency of the hardware is determined by comparing the capacity of each component, which can be expressed as (4):

$$Efficiency = \frac{Processing\ Capacity}{Transaction\ Rate} \quad (4)$$

To assess the efficiency, the specifications provided in the datasheet of each hardware element are considered, allowing for appropriate substitutions. The benchmark comparison between ESP32 WROOM and Arduino Nano 33 IoT is shown in Table 1.

Table 1. Benchmark comparison between ESP32 WROOM and Arduino Nano 33 IoT

Hardware	ESP32 WROOM	Arduino Nano 33 IoT
Memory (RAM)	520KB	32KB
Memory (Flash)	4MB	256KB
Processing Power	Up to 240 MHz	48 MHz (single core)
Power Consumption	80 mA	35 mA
RSA Algorithm Capability	4096-bit RSA	2048-bit RSA

When it comes to a public blockchain, efficiency is typically assessed based on its ability to process transactions quickly and efficiently, taking into account factors such as transaction rate and block size. Efficiency can be measured in various ways, but a common metric is scalability, which reflects the blockchain's capacity to handle an increasing number of transactions without compromising its performance.

One way to evaluate the efficiency of a public blockchain is by calculating its transactions per second (TPS) rate, which indicates how many transactions the network can process in a second. The higher the TPS, the more efficient the blockchain is considered to be. Another metric is the average transaction confirmation time, which represents the time it takes for a transaction to be confirmed and included in a block. A more efficient blockchain will have a shorter average confirmation time.

4. DISCUSSION

The aspect of discussion in this article is an analysis of Anagnostakis' paper on applying Arduino IoT as an IoT hardware solution by implementing it in a blockchain. In the case under discussion in this study, a feasibility study of applying hardware that provides better cost-effectiveness and real-world implementation in an industry is carried out. To achieve this, it is considered that using microcontroller hardware for blockchain nodes, as proposed by Anagnostakis, becomes unfeasible when transaction levels exceed the transmission rate capacity. However, combining this hardware with sensor networks and a public or private micro-blockchain, as being proposed by the current study, is appealing. Private micro-blockchains offer robust node execution, limited connectivity to decentralized agent networks, and enhanced security for sensitive data on public platforms. This provides an efficient solution with control and security.

To calculate the node operability limit for the Arduino Nano 33 IoT, substituting the corresponding values in (5):

$$NodeLimit = \frac{Proc.Cap.\ x\ Mem.Cap.}{Node\ Size\ x\ Proc.Rate} \quad (5)$$

Performing the value replacements for the Arduino Nano 33 IoT, which was discussed by Anagnostakis, we find in (6):

$$NodeLimit = 12.600.000 \text{ Possible nodes} \quad (6)$$

Now, making the proper substitutions with the values for the ESP32, we have in (7):

$$NodeLimit = 125.400.000 \text{ Possible nodes} \quad (7)$$

Therefore, the node operability limit for the ESP32 is approximately 125.4 million nodes.

Taking into consideration that the calculated values are based on unit cycles and small nodes, we can determine the node operability limits for the Arduino Nano 33 IoT and the ESP32.

For the Arduino Nano 33 IoT, with a processing rate of 48 MHz and a memory capacity of 32 KB, the node operability limit is approximately 12.6 million nodes. Similarly, the ESP32, with a processing rate of 240 MHz and a memory capacity of 520 KB, has a node operability limit of approximately 125.4 million nodes. It is important to consider that these calculations assume specific node requirements and idealized conditions.

However, in real-world scenarios, factors such as varying node sizes, complex operations, and specific implementation details can affect the actual node operability limit. Consequently, the application of Anagnostakis' approach with the hardware discussed in potential "micro-blockchain" networks becomes unfeasible. Nevertheless, these results provide a rough estimate and should be interpreted cautiously when considering the practical implementation of IoT systems. Consequently, hardware like the ESP32 could potentially carry out significant data transactions collected through IoT devices and transmit them to a private blockchain network or even a micro-blockchain, as illustrated in Figure 4, depicting the block diagram of a private micro-blockchain. In other words, a blockchain applicable in the

real world and customized for a specific type of use within an industry.

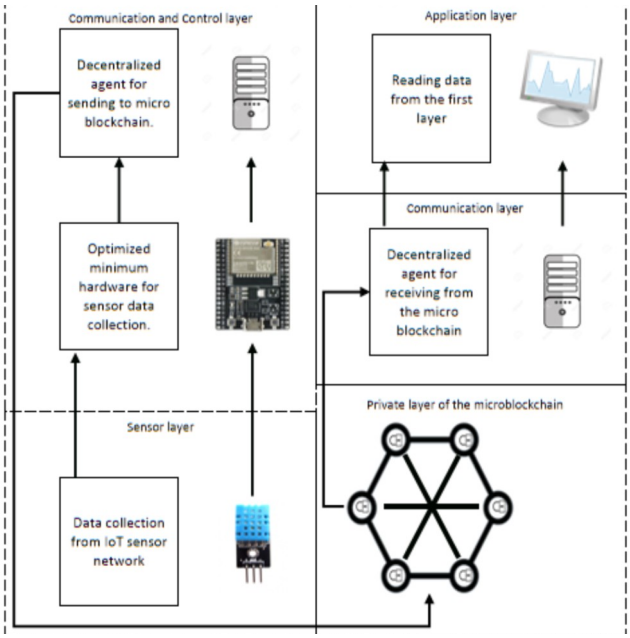

Fig 4: Block diagram for a private micro-blockchain with decentralized agents.

5. CONCLUSIONS

A comparative analysis was conducted between a Private Network Micro-blockchain IoT and an Open Blockchain in the Data Collection of Decentralized Agents. The results provide valuable insights into different aspects of blockchain technology and minimum hardware requirements. The analysis highlights the advantages of using minimal hardware as data collecting nodes in the network, followed by sending this data to a Micro-blockchain in a private network. These data to create a micro-blockchain are addressed in Table 1. It's worth noting that a private micro-blockchain is designed for a personalized and controlled environment, such as an industry. Thus, this approach offers greater efficiency, privacy, and control compared to an open blockchain, particularly in terms of data privacy and security. It is important to consider trade-offs, such as reduced connectivity and limitations in integrating external data, when choosing between private and open blockchain networks.

REFERENCES

Albakri, Ashwag, Harn, Lein, & Maddumala, Mahesh. (2019). Polynomial-based lightweight key management in a permissioned blockchain. In 2019 IEEE Conference on Communications and Network Security (CNS), pages 1-9. IEEE.

Anagnostakis, Aristidis G, Giannakeas, Nikolaos, Tsipouras, Markos G, Glavas, Euripidis, & Tzallas, Alexandros T. (2021). IoT micro-blockchain fundamentals. Sensors, 21(8), 2784. MDPI.

Buterin, Vitalik. (2023). Ethereum Fails Without These 3 Changes, Says Vitalik Buterin. Available at: https://decrypt.co/143991/ethereum-fails-without-these-3-changes-says-vitalik-buterin. Accessed on: June 11, 2023.

Cao, Bin, Wang, Xuesong, Zhang, Weizheng, Song, Houbing, & Lv, Zhihan. (2020). A many-objective optimization model of industrial internet of things based on private blockchain. IEEE Network, 34(5), 78-83. IEEE.

Gorkhali, Anjee, Li, Ling, & Shrestha, Asim. (2020). Blockchain: A literature review. Journal of Management Analytics, 7(3), 321-343. Taylor & Francis.

Kopetz, Hermann, & Steiner, Wilfried. (2022). Real-time systems: design principles for distributed embedded applications. Springer Nature.

Lucas, Gavin. (2023a). This is What Teranode Is About: 50K TPS. Available at: https://coingeek.com/this-is-what-teranode-is-about-50k-tps/. Accessed on: June 11, 2023 at 10:00 AM.

Lucas, Gavin. (2023b). Over 86 Million BSV Blockchain Transactions in 24 Hours as Another World Record Is Set. Available at: https://coingeek.com/over-86-million-bsv-blockchain-transactions-in-24-hours-as-another-world-record-is-set/. Accessed on: June 11, 2023 at 10:00 AM.

Nakamoto, Satoshi. (2008). Bitcoin: A peer-to-peer electronic cash system. Decentralized Business Review, 21260.

Pahlajani, Sunny, Kshirsagar, Avinash, & Pachghare, Vinod. (2019). Survey on private blockchain consensus algorithms. In 2019 1st International Conference on Innovations in Information and Communication Technology (ICIICT), pages 1-6. IEEE.

Sinha, Upamanyu, Hadi, Abdullah A, Faika, Tasnimun, & Kim, Taesic. (2019). Blockchain-based communication and data security framework for IoT-enabled micro solar inverters. In 2019 IEEE CyberPELS (CyberPELS), pages 1-5. IEEE.

Wang, Minghao, Zhu, Tianqing, Zuo, Xuhan, Yang, Mengmeng, Yu, Shui, & Zhou, Wanlei. (2023). Differentially private crowdsourcing with the public and private blockchain. IEEE Internet of Things Journal. IEEE.

Xinyi, Yang, Yi, Zhang, & He, Yulin. (2018). Technical characteristics and model of blockchain. In 2018 10th International Conference on Communication Software and Networks (ICCSN), pages 562-566. IEEE.

Zinonos, Zinon, Christodoulou, Panayiotis, Andreou, Andreas, & Chatzichristofis, Savvas. (2019). Parkchain: An IoT parking service based on blockchain. In 2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS), pages 687-693. IEEE.