Researching the Potential of Blockchain Technology for Securing IoT Networks

Chandrika G. V. [1], Venkatesh A.[2], Naveen Kumar V.[3]
[1]*Selection grade lecturer E & C, Government polytechnic Mulbagal.*
[2]*Lecturer E & C, Government polytechnic, Nagamangala.*
[3]*Lecturer E & C, Government polytechnic Arakere.*

Abstract

Every physical object will soon have an online presence thanks to the "Internet of Things" (Iota), a new form of computer network. These objects may now talk to one another and collaborate thanks to advancements in radio-frequency identification (RFID), wireless networking, and other types of sensors. The major objective of the security concept for the Internet of Things (IoT) is to ensure the confidentiality, integrity, availability (CIA), and privacy of IoT-based systems and data. Block chain (BC) is a trust and security-based mechanism that underpins digital currencies like Bitcoin and Ethereum. BC relies on three pillars: openness, immutability, and a distributed database. Now, Block chain technology is leading the way in establishing new standards for security and privacy in peer-to-peer networks with Iota-like topologies. This article provides a framework for integrating Iota with block chain technology, which would ensure a high degree of security and validation process through the integration between block chain consensus algorithms (PBFT and Tangle). This paper also proposes a direction algorithm to point Iota transactions in the direction of the best BC technique for verification, whether that be PBFT or Tangle. The propose framework improves security, scalability, and high performance by minimising resource consumption and latency time while concurrently lowering data transmission overhead through the use of the proposal direction technique. The experimental findings for the proposed framework demonstrate a 50% reduction in latency time compared to employing each consensus BC technique separately, and the alleviation of Sybil attack worries due to the distribution of work across the consensus algorithms and the dynamic of validation.

Keywords— Bitcoin, Consensus Algorithms, Evidentially Fair Payments, Topology, and the Internet of Everything

I. INTRODUCTION

Improvements in data collecting, processing, and distribution are made possible by the Internet of Things (Iota), which represents the next stage in Internet evolution (think: smart homes, smart cities, etc.). In 2025, there will be 41.6 billion Iota devices, generating 79.4 ZB of data, according to IDC's forecasts [1]. The Internet of Things (Iota) is a hot topic in the field of artificial intelligence; it is not a new technology, but rather a new effective model and strategy that includes all wireless communication technologies and associated ideas, such as wireless sensor networks, mobile networks, and actuators.

The Internet of Things will have a significant impact on our lives now and in the future, altering many facets of society as traditional organizations undergo digital transformations and adopt new business models to boost efficiency, effectiveness, and employee and customer engagement[4]. The Internet of Things plays a crucial part in enabling the notion of Smart cities, with Barcelona serving as an example of a city that began its transition to a smart city in 2012[6]. There is a strong correlation between the success of Iota initiatives and the success of global efforts to better distribute the world's resources to those who need them most [5][7]. To reap the full benefits of Iota systems and ensure their continued, sustainable growth, it's crucial that these networks be as safe as possible. Iota infrastructures are susceptible to attack and have a single point of failure because of their centralized design [21].

DOI : 10.21904/weken/2022/v7/i2/172657

Block chain is a unique technology that underpins the concept of digital currency. A technology with several functions, it was developed to solve a wide range of issues plaguing IoT network nodes. These characteristics include a high degree of scalability, decentralisation, persistence, anonymity, security, scalability, a solid backend, and a high level of efficiency and transparency. Data security and privacy, single points of failure, access control, and preventing the unlawful use of personal data are just a few of the issues plaguing the Iota that may be remedied by implementing blockchain technology [8, 9]. By keeping records in a distributed ledger, block chain removes the possibility of a disastrous data loss. The security of the BC network is provided by the consensus algorithms at the heart of Block chain, some of which are appropriate for Iota and others of which are effective just for financial transactions and digital currencies. [9][10][11].

II. BACKGROUND

A. Getting Things Online

The Internet of Things (Iota) is an umbrella term that encompasses a wide range of applications and technologies, including but not limited to those listed below[2]: wireless sensor/actuator networks; low-power embedded systems; radio-frequency identification; mobile devices that connect to the Internet via Bluetooth; smart homes; connected vehicles; etc. The security architecture for the Internet of Things has to be comprehended. Figure 1 illustrates the typical three-layer IoT architecture. Technologies like RFID and other wireless data sensors make up the perception layer. Data from the perception layer is sent to the network layer, which then forwards it to the appropriate processing systems through wired and wireless connections. The data that has been processed is then used by the programme itself [14].

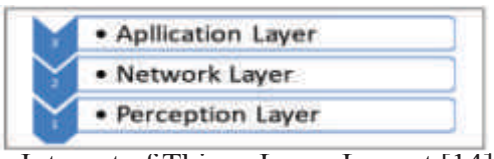


Fig. 1. Internet of Things Layer Layout [14]

Keeping data flow in each application safe from unauthorized usage or assault is a top priority for all Iota applications [5] [19].

1) Consequences of IoT Vulnerabilities for Security: With the introduction of the CIA concept, the security of the IoT has become a top priority. Each component of an IoT's design has its own set of security concerns. Since most IoT devices lack robust security measures in their software and architecture, there has been a lot of recent research into this area. According to Gartner's 2016 IoT Backbone Survey, 32 percent of IT executives see security as the biggest challenge to the expansion of the IoT. The next several years will see a continuing megatrend of research into finding a happy medium between the benefits of Internet of Things connectivity and the security risks that come with it [24]. The Internet of Things (IoT) presents three distinct types of danger: First, designers of products and IoTs could not be aware of dangers that come with using the Internet. Second, dangers particular to Internet of Things devices that arise from a lack of universal security protocols. Third, security measures to prevent harm from accidental or intentional usage, such as improperly operating actuators. Due to user limitations in terms of both power and security, IoT devices' Internet connectivity poses the greatest threat. [13]. Some security flaws can lead to malicious assaults. Default and weak credentials, firmware and operating system updates that are cumbersome, a lack of vendor assistance for fixing vulnerabilities, online interfaces that are susceptible to SQL injection and cross-site scripting, and coding flaws are just a few examples.



Fig. 2. Changes in Blockchain Technology

DOI : 10.21904/weken/2022/v7/i2/172657

Blockchain is a decentralised, autonomous, and anonymous system that meets all of these criteria. By eliminating the single point of failure, the vulnerability to attack, and the isolation of individual nodes, BC mitigates the problems of centralised systems[15],[16]. First, Blockchain can be broken down into public and private blockchains, the latter of which is most commonly associated with digital currencies like Bitcoin and Ethereum but can be used in any system that meets certain requirements, and consortium blockchains, which combine public and private blockchains. For a second category, we may look at how the transactions are handled: buffer overflow attacks that don't ask for permission, protocols that utilise clear text and leave superfluous ports open, distributed denial of service attacks, and distributed denial of service attacks. Theft and tampering by physical means, assaults on authentication and network availability, and attacks via deployed technologies like RFID[22]. Blockchain, which is built on the idea of a peer-to-peer distributed network with hashing cryptography and consensus methods, is seen as an efficient solution for the security problems inherent in Internet of Things (IoT) systems, which arise because of the client-server application paradigm.

B. Blockchain

First conceived and described by an anonymous individual or group going by the name "Satoshi Nakamoto," Block chain technology has now become the backbone of digital currency. As the first real-world use of BC, Bit coin is presented in [23]. In a block chain, data is stored in blocks, and the entire chain is secured using cryptography and hashing techniques. The sender, the recipient, the transaction data, and the timestamp are all stored in a cryptographic hash that is part of each block. Block chain is predicted to be among the top ten trends in data and analytics by Gartner in 2020 [36]. Figure 2 depicts the development of block chain and block chain creation throughout time. Initially, block chain was utilized just for digital money (blockchain1.0). Bit coin, sometimes known as "the internet currency," uses the Proof of Work algorithm as its consensus mechanism, and its average transaction throughput is six transactions per second. In the first stages of its evolution, Block chain 2.0 saw the introduction of the programmable Ethereal platform and the smart contracts enabled by the solidity programming language; it also adopted the proof of stack consensus mechanism and achieved an average transaction throughput of 14 tops. The average transaction pace is increased to 100Ktps and decentralized apps are the focus of Block chain 3.0. As a result, the average transaction rate on Block chain 4.0 rose to 1M tops [25], and it became more flexible in meeting the needs of various industries through the use of a variety of consensus methods. [26].

There are two types of BC: permission less BC, which allows any user to generate a block of transactions, and permissioned BC, which limits block creation to a select group of authorized users.

1) Using Consensus Algorithms for Blockchain Applications: Among the many possible consensus mechanisms, the most well-known are Proof-of-Work (POW) systems, which rely on computational power, Proof-of-Stake (POS) systems, which rely on the credibility of entities with widespread participation, DPOS (Delegated Proof-of-Stack) systems, which are similar to POS mechanisms but use selected delegates, and Proof-of-Authority (POA) systems (DAG), Private BC[16][17] relies heavily on the verification of blocks and transactions by a small group of trusted users. The logistics industry, which relies heavily on Internet of Things (IoT) sensors, is perhaps the most well-known and influential blockchain user.

III. CONTEMPORARY APPROACHES

Internet of Things (Iota) security and block chain-based application security have been the subject of much study and investigation. Some of the research, future-state vision, and current challenges in achieving adequate block chain-based Iota security are presented here. Although the authors of [27] suggest a smart city security framework layer that makes use of Ethereal, they exclude any discussion of the applicable algorithms.

DOI : 10.21904/weken/2022/v7/i2/172657

Although the authors of [27] suggest a smart city security framework layer that makes use of Ethereal, they exclude any discussion of the applicable algorithms. As Ethereal relies on Pops, which isn't optimal for such Iota systems because of the monetary ideas of stakes, it's not a great fit. IP address exploitation remains an issue despite a proposal to utilize IP addresses of devices in an Iota system as a key to access data stored in block chain by the authors of [28]. From January 2016 onward, the authors of [29] have presented many security techniques for Iota systems, and they emphasize the potential significance of employing block chain. Keep an eye out for intrusions and try to avoid them, but

Despite the challenges posed by the storage requirements and computational burdens of other security methods, block chain is emerging as the gold standard for protecting Internet of Things devices. Block chain architecture, consensus techniques, and Iota applications are all discussed in [30], along with related security and performance concerns, with a focus on large-scale Iota use cases. The consensus procedures of block chain were given by the authors of [31]. The lack of a centralized consensus methodology and the inability to scale are the two biggest obstacles standing in the way of a fully integrated block chain and Internet of Things system. The authors of [32] discussed how Block chain may be adapted to meet the unique requirements of Iota devices, including issues of energy efficiency, scalability, throughput, and latency. In [33][17], the authors present a review of block chain's consensus algorithms for protecting Iota systems and discuss the necessity of utilizing block chain to improve Iota security, dependability, and scalability. Because Proof of Work consensus techniques introduce significant delay and are incompatible with Iota devices' constrained memory, the authors of [35] proposed a hybrid block chain architecture for the Internet of Things. It is clear from these analyses that there is still more work to be done until an efficient and viable block chain solution is developed that can scale to the vast numbers of devices and transactions typical of Iota systems while yet maintaining excellent speed.

IV. PROPOSED FRAMEWORK FOR BLOCKCHAIN-BASED IOT SECURITY

While the Internet of Things relies on a peer-to-peer architecture, it is implemented using a client-server approach in which a central webserver is responsible for managing the network. This central hub, which receives data from all Iota devices, is a potential weak spot. Shortage of security communication standards and protocols; Data confidentiality and privacy issues associated with unsecured Iota networks; inadequate authentication and authorization approaches for devices inside an Iota system all contribute to the system's overall vulnerability. A hacker, for instance, may disrupt service by gaining access to the control center of an interconnected electrical grid. Due to insufficient security procedures, Iota devices are vulnerable to cyber-attacks that aim to steal sensitive information. Block chain has the ability to alter business models across all industries, including Iota, according to Gartner [37]. However, it will take the block chain and Iota industries between five and 10 years to achieve its peak. Iota system security may be improved by using Block chain. Given that Block chain is based on a decentralized distributed ledger system, it provides an efficient means of plugging the security hole in the Internet of Things. As can be seen in Figure 3, the best block chain solution may be selected to meet the needs of the Iota system based on the requirements of the system and the domain in which it operates. The degree of demand for performance, scalability, and reliability in an Iota system should guide the selection of a block chain solution.

Any Block chain relies on consensus methods to determine how transactions are confirmed and kept with a certain level of security [17].

DOI : 10.21904/weken/2022/v7/i2/172657

Various consensus algorithms have been created to validate transactions depending on access restriction or the most appropriate type of block chain (private, public, or consortium) in order to achieve the performance-scalability-reliability required for a given domain. Many consensus methods, like POW, POC, LPOS, and POA, are solely appropriate for financial transactions and are therefore incompatible with IoT systems.

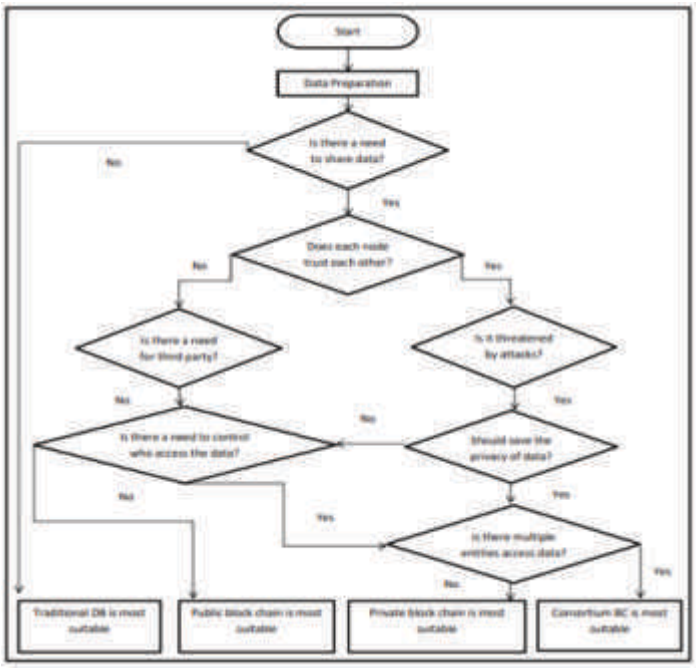


Fig. 3. Procedure for determining which blockchain technology is best suited for Internet of Things applications

Several studies [17–20] explain the theory underlying several consensus techniques. Other consensus algorithms well-suited to the Internet of Things have been explored in this line of work, and each has its own set of limitations. After looking at a wide variety of consensus methods, the suggested framework would rely on PBFT and Tangle, both of which rely on a distributed ledger. In the proposed framework, Iota transactions go through multiple checks before being added to the network: first, an algorithm determines which consensus algorithm is best suited for the task at hand; next, a validation process is carried out; finally, the results of the validation process are confirmed.

Figure 4 depicts the proposed framework's architecture, which consists of the following five parts:

- Internet of Things Sensors
- Computerized Contract
- Inclination Detector
- Networked Block chain
- Distributed Ledger Node

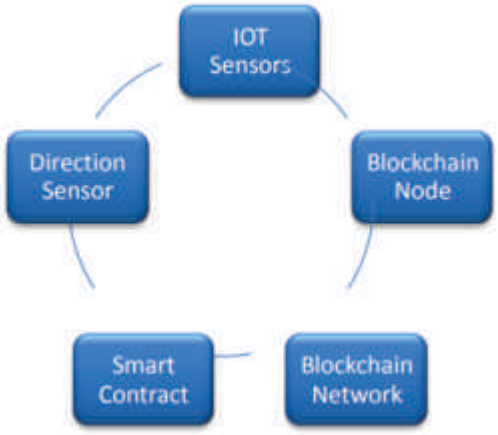


Fig. 4. Constituents of the proposed structure

1 Internet of Things Sensors: The computing and memory capabilities of the Iota devices that make the wireless sensor system are constrained. Through the use of one-of-a-kind IDs and secure channel communication protocols. Numerous transactions and data sets produced by Iota sensors must be verified and managed.

2 A digital agreement or smart contract: One definition of a smart contract is "a script that stores on the chain with a single urn and defines all actions and functionalities." There are permanent references in a smart contract to completed transactions that can't be removed.

3 Networked Block chain: In this setup, the block chain is a consortium block chain, which blends public and private block chains based on the usage and need of the IOT system needs. The consortium block chain may be thought of as 'semi-private' and is managed by a select group of users. Smart contracts specify the protocols for any and all actions inside a block chain network.

DOI : 10.21904/weken/2022/v7/i2/172657

4 Inclination Detector: is in charge of the planning stage, where each transaction is routed to be validated using a consensus method (either PBFT or Tangle) that will help this framework reaches its goal of providing a high degree of security, performance, and scalability.

5 Node in a Block chain: For the purposes of an Iota system, a BC node can be anything from a standard desktop or laptop computer to a massive server farm. The unique address of each smart contract in the block chain network is stored in each BC node, allowing them to follow all network instructions and participate in the validation procedure. Each node is linked to the others, and each node has a complete copy of the block chain's history and is responsible for validating transactions and storing related data.

Figure 5 shows a recommendation architecture that relies on merging PBFT and Tangle consensus on a consortium block chain in order to achieve high security, scalability, and speed. Once the system requirements have been established, each device on the Iota system will be assigned a unique device identifier (DID), and the number of transactions per second (TPS) expected from a typical device will be predefined. In the Direction algorithm, depicted in Figure 6, new transactions ("Ts") are generated by users, sensors, and connected devices and added to the "transaction data set" ("TDS") based on the device id ("TDID"), and then the "transaction checker" ("Checker") checks the "device data set" ("DDS") to get "TN," and then compares "TN" with "n," and if "TN" for a given device is "less.

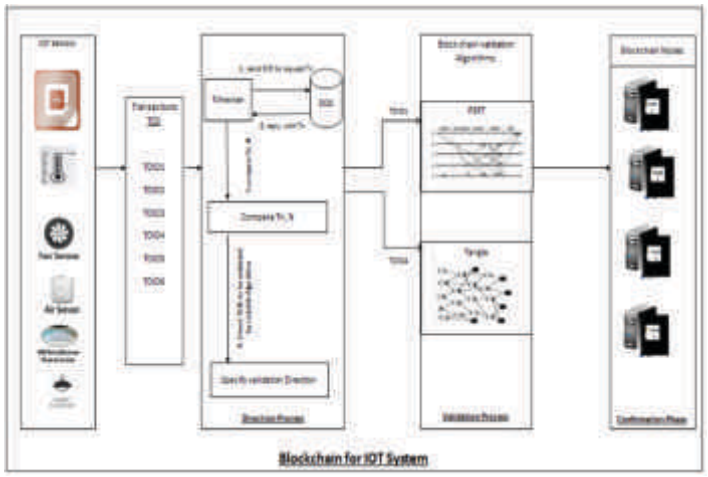


Fig. 5. An infrastructure for the Internet of Things based on blockchain technology is suggested.

Direction Algorithm

Input: A set of IoT transactions Ts need to be validated where Ts are from different sensors and devices on (Transactions Data Set) TDS where each device has its identifier DID predefined on Device Data Set 'DDS' and predefined Tn will validated based on expected n transaction per sec 'TPS' on the system

Output: A set of validated and confirmed transactions VTs

1. TDS ← data set for all transactions from each device
2. DDS ← Predefined Tn for each device DID where
3. **If** TDID ∈ DID where Tn<=n **then**
4. Validate TDID by PBFT Algorithm
5. **Else**
6. Validate TDID by Tangle Algorithm
7. **End If**
8. **If** DID transactions become > n **then**
9. Update DDS database

Fig. 6. To that end, we suggest a new direction algorithm.

V. CONCLUSION AND RESULTS OF EXPERIMENT

The performance of a framework can be evaluated in a variety of ways, including its level of security, transaction rate (where high throughput of more than 1000 TPS is most required in Iota systems), transaction validation time (how long it takes to place a transaction, route it to the validation algorithm, and receive a response), scalability, and latency (how many milliseconds it takes for the validation process to complete).

DOI : 10.21904/weken/2022/v7/i2/172657

Figure 7 shows an anticipated evaluation of the proposal framework's performance until more precise data can be obtained from more trials in future work, based on the research of different models, frameworks, and consensuses algorithms, with an emphasis on PBFT and Tangle (DAG).

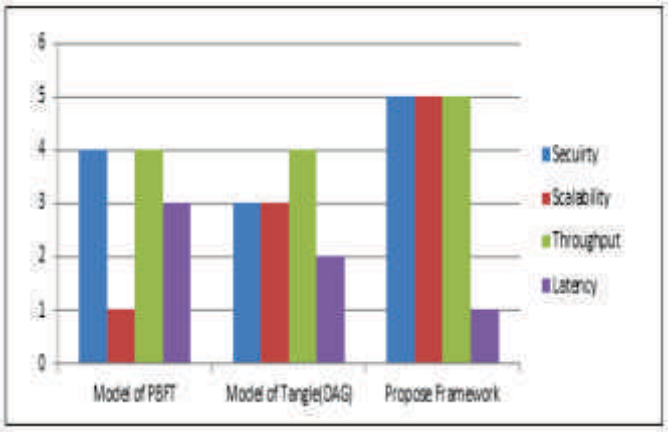


Fig. 7. Using PBFT and Tangle as benchmarks, we assess the merits of the proposed framework.

Using the CASAS dataset [38], which is comprised of smart-home-based data sets, and the Netcom simulator and emulator, we simulated the system and analyzed its performance. The proposed framework is based on an IOTA-inspired consortium block chain built on top of the Hyper ledger Fabric block chain platform, with the PBFT algorithm serving as the consensus mechanism and the Tangle serving as the private ledger. Using four server computers, each with a two-core Intel Core i7 2.2GHz CPU, 16GB DRAM, and 256GB SSD running Ubuntu 16.04 as the validation nodes. And treat the other four virtual servers as if they were Internet of Things gadgets, complete with their own set of projected throughput rates (TPS). Use a gateway algorithm in the smart contract that directs traffic to the PBFT or tangle for transaction validation. With the APIs offered by Hyper ledger Fabric, we were able to generate and send a large number of transactions to evaluate the system's latency and scalability, and we could also simulate a large number of potential attacks. Since the proposed architecture divides the weight of validation between PBFT and tangle based on the direction of the processing and the device that generates the transactions, latency decreases as the number of sensors increases (and hence the number of transactions), as illustrated in Figure 8. Scalability, measured by the number of transactions processed per second, performs better in the proposed framework than it does in any of the individual algorithms (see Figure 9).

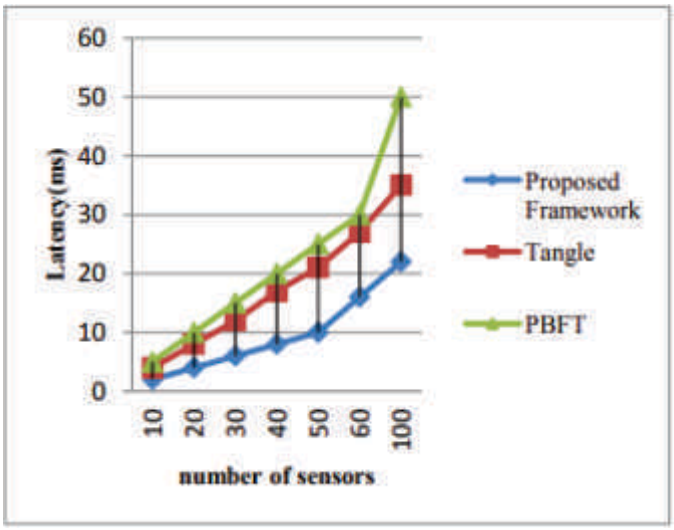


Fig. 8. Latency distribution as a function of sensor count on average.

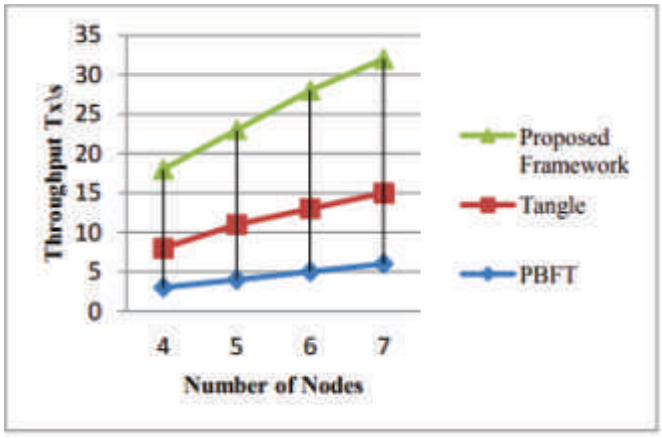


Fig. 9. Any and all suggested algorithms and frameworks must be scalable.

Due to the load balancing between consensus mechanisms and the dynamics of validation, this framework can reduce the fear of the Sybil attack, which is the biggest concern when adopting block chain. Every suggested framework and algorithm is compared and contrasted in Table 1.

DOI : 10.21904/weken/2022/v7/i2/172657

Table I. Evaluate each suggested framework and algorithm individually.

	PBFT	Tangle	Proposed Framework
Accessibility	Private	Public	Consortium
Decentralization	Medium	Medium	High
Scalability	Low	Medium	High
Latency	Medium	Medium	Low
Network overhead	High	Medium	Low
Storage overhead	High	Medium	Low
Security	51% attack or Sybil attack	51% attack or Sybil attack	Mitigate 51% or Sybil attack due to dynamic of validation process

A systems, but limited resources and processing capacity, using Block chain technology is an efficient solution to improve their scalability, security, and latency. Consensus algorithms provide the backbone of several different block chain implementations. This paper outlines a process for determining which BC model is most suited to a given setup. It also integrates block chain consensus algorithms (PBFT and Tangle) with the propose direction algorithm to strengthen the validation process, suggesting a new framework for protecting Iota devices using block chain technology. Improved security, reduced latency, and scalability are just a few of the ways in which the proposal framework guarantees top performance. More work is needed to test the impact and viability of this framework to achieve network security and scalability in Iota systems.

REFERENCES

[1] "The Growth in Connected IoT Devices Is Expected to generate 79.4ZB of Data in 2025, According to a New IDC Forecast", IDC: The premier global market intelligence company, 2019. [Online]. Available: https://www.idc.com/getdoc.jsp?containerId=prUS45213 219.

[2] R. Minerva, A. Biru and D. Rotondi, Towards a definition of the Internet of Things (IoT), 1st ed. IEEE, 2015.

[3] [Online]. Available: https://www.idc. com/getdoc.jsp? containerId =prUS45213 219.

[4] INFSO D.4 Networked Enterprise &RFIDINFSO G.2Micro &Nanosystemsin co-operation with theWORKING GROUP RFID OF the ETPEPOSS, Internet Of Things in 2020, Roadmap for The future, Version 1.1 (27 May, 2008)

[5] D. Evans, The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Cisco IBSG, 2011.

[6] "Barcelona Smart City: most remarkable Example of Implementation", Engineers & Architects, 2019. [Online]. Available: https://www.ezigurat.com/blog/en/smart-city-barcelona-experience/.

[7] S. Bhattacharjee, M. Salimitari, M. Chatterjee, K. Kwiat and C. Kamhoua, "Preserving Data Integrity in IoT Networks Under Opportunistic Data Manipulation", 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress(DASC/PiCom/DataCom/CyberSciTech) ,2017. Available: 10.1109/dasc-picom-datacomcyberscitec.2017.87

[8] A. Sultan, M. Mushtaq and M. Abubakar, "IOT Security Issues Via Blockchain", Proceedings of the 2019 International Conference on Blockchain Technology - ICBCT 2019, 2019. Available: 10.1145/3320154.3320163 .

[9] K. Christidis and M. DevetsikIoTis, "Blockchains and Smart Contracts for the Internet of Things", IEEE Access, vol. 4, pp. 2292-2303, 2016. Available: 10.1109/access.2016.2566339 .

[10] S. Huh, S. Cho and S. Kim, Managing IoT Devices using Blockchain Platform.ICACT, 2017. G. Eason, B. Noble, and I. N. Sneddon, "On certain integrals of Lipschitz-Hankel type involving products of Bessel functions," Phil. Trans. Roy. Soc. London, vol. A247, pp. 529–551, April 1955. (references)

DOI : 10.21904/weken/2022/v7/i2/172657