Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7– No. 34, September 2020 – www.caeaccess.org

Securing IoT Systems using Blockchain Algorithms

Osama Emam
Faculty of Computers and Artificial Intelligence
Helwan University, Cairo, Egypt

Hanan Fahmy
Faculty of Computers and Artificial Intelligence
Helwan University, Cairo, Egypt

Menna Mamdouh
Faculty of Computers and Artificial Intelligence
Helwan University, Cairo, Egypt

ABSTRACT
Internet of Things (IoT) is an advanced computing network where all physical objects are connected to the internet. All these objects are able to communicate and interact with each other using many technologies such as radio-frequency identification (RFID) technology, wireless technologies and other sensors technologies. Security concept is the main concern to ensure the sustainable development in IoT and to achieve confidentiality, Integrity, Availability (CIA) and Privacy. Blockchain (BC) is a technology based on the concept of trust and security that is the base of in the cryptocurrency such as Bitcoin and Ethereum. BC has three main pillars of transparency, immutability and distributed DB. Nowadays, Blockchain is paving the way to provide security and privacy in peer-to-peer networks with similar topologies to IoT. This paper proposes an integrated framework for implementing IoT with blockchain technology to guarantee high level of security and validation process based on the integration between consensus algorithms of blockchain (PBFT and Tangle). In addition, this paper proposes a direction algorithm to direct IoT transactions to appropriate BC algorithm to be validated by PBFT or Tangle. The propose framework ensure security, scalability and high performance by optimizing the data transmission overhead and enhancing the validation process by using the propose direction algorithm with reducing both of the resource utilization and the latency time. The conducted experimental results for the propose framework state that the latency time is reduced by 50% than using each consensus BC algorithm separately and mitigate the apprehensive from Sybil attack because of the load balance between consensus algorithms and the dynamic of validation.

Keywords
IoT, IoT Security, Blockchain, Consensus algorithms, PBFT, Tangle

1. INTRODUCTION
IoT represents the next technological evolution of the Internet by upgrading the ability to gather, analyze, and distribute data to get new information and knowledge such as smart home, smart cities,,, etc. By 2025, according to IDC, it is expected to have about 41.6 billion connected devices producing 79.4 zettabytes (ZB) of data [1]. IoT is one of the main subjects related to artificial intelligent and is not defined as a new technology in itself but it is as a new effective model and approach that includes all wireless communication technologies and its concepts such as wireless sensor networks, mobile networks, and actuators [2] [3].

There is a great impact of IoT on the current and future life while changing many aspects by transforming many enterprises into digital businesses and going through new business models for improving efficiency , effectiveness, and increasing employee and customer engagement[4]. One of the most important roles of IoT is that it enables the concept of Smart city; Barcelona is the example of a city that started to become a smart city in 2012[6]. IoT projects are main pillars to improve distribution of the world's resources to those who need them most, and help to understand the planet and help people to be more proactive and less reactive [5][7].Security is a high priority in IoT to get maximum advantage from IoT systems and keep on sustainable development with successful, useful and secured systems. Due to the centralized architecture of IoT systems so IoT systems are vulnerable and are exposed to attacks and single point of failure [21].

Blockchain is a new technology that is the behind concept to digital currencies. It has begun as the technology that has many characteristics to solve different issues in IoT network devices. Some of these characteristics such as decentralization, persistency, anonymity, security, scalability, resilient backend, high Efficiency and transparency [8].Each feature of blockchain can fit to solve IoT issues such as data integrity and privacy, single point of failure, access control and preventing illegal use of personal data [8][9].Blockchain keeps a distributed database of records that solve the issue of single point of failure. Consensus algorithms are the core of Blockchain to ensure the security of the BC network where some of them are applicable to IoT and others only effective on financial transactions and digital currencies[9][10][11].

2. BACKGROUND
2.1 Internet of Things
IoT is an umbrella term that includes multiple different categories and technologies such as : Wireless sensor/actuator networks, Low power embedded systems, RFID, devices that connect via Bluetooth-enabled mobile phones to the Internet, Smart homes, connected cars,...etc.[2].It is important to understand the IoT security architecture. In general, as shown in figure 1, the IoT structure is divided into three layers. The perception layer consists of wireless and data sensors technologies such as RFID. The network layer is responsible for transmitting the received data from the perception layer to processing systems through various network technologies, such as wireless and wired networks. The application layer uses the processed data within application to get actual useful function [14].

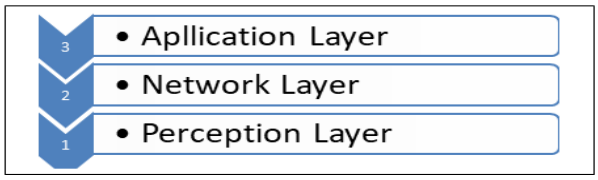

Figure 1: IoT Layer Architecture [14]

The main requirement in all IoT applications is security to keep the data traffic in each application secure and save it from any malicious use or attack [5] [19].

2.1.1 Security Issues in IoT

IoT security becomes the main issue and concern to get successful and secured system with concept of CIA. There are many security issued in each layer of IoT architecture. Most of IoT devices haven't powerful protection level at their software and infrastructure so the current studies in IoT focus on security aspect. The 2016 IoT Backbone Survey by Gartner found that 32 % of IT leaders perceive the security as a top barrier to IoT progress. Understanding how to balance the promise of IoT-connected devices with potential security challenges will continue to be a megatrend in the next years [24].There are three categories of risks in IOT; Firstly, risks that are inherent in any Internet system but that product/IoT designers may not be aware of them. Secondly, specific risks those are unique to IoT devices due to lack of security standards. Third, Safety to ensure no harm is caused by the misuse, for instance, misusing actuators. Internet connection as the most risky aspect of IoT devices due to the constraints of consumer power and security[12] [13].There are some of security issues that cause attacks Such as default and weak credentials, difficult to update firmware and OS, lack of vendor support for repairing vulnerabilities, vulnerable web interfaces that cause SQL injection and XSS, Coding errors that cause buffer overflow, Clear text protocols and unnecessary open ports, DoS / DDoS, Physical theft and tampering, attacks on authentication, network availability ,attacks through used technologies like RFID[22].IoT systems have security issues depending on the concept of client-server applications so blockchain is considered as an effective solution for IoT security issues as it is based on the concept of peer-to-peer distributed network with hashing cryptography and consensus algorithms.

2.2 Blockchain

At the beginning, Blockchain technology is known as main concept of digital currencies developed and defined by person or group known by anonymity Satoshi Nakamotoand. Bitcoin is introduced as first implementation to BC[23].Blockchain is a chain of many blocks each block contain data which are cryptography with hashing function algorithms that is irreversible process. Each block has cryptographic hash that has data about sender, receiver, transaction data and timestamp. According to Gartner, Blockchain is one of top ten trends in data and analytics for 2020 [36].There is an evolution for blockchain and blockchain generation as shown in figure 2. Blockchain started with blockchain1.0 that was just used as digital currency Bitcoin, it was called as internet of money and use Proof of work as consensus algorithm and the average transaction rate is 6 tps. Blockchain 2.0 started with the developing smart contract and Ethereum platform that is programmable by solidity and moving to use proof of stack consensus algorithm and the average transaction rate is 14 tps. In Blockchain 3.0, Blockchain is moving towards decentralized applications and the average transaction rate is raised up to 100Ktps. Then, Blockchain 4.0 become more adaptable in industry requirements by using different consensus algorithms and the average transaction rate increased up to 1M tps [25][26].

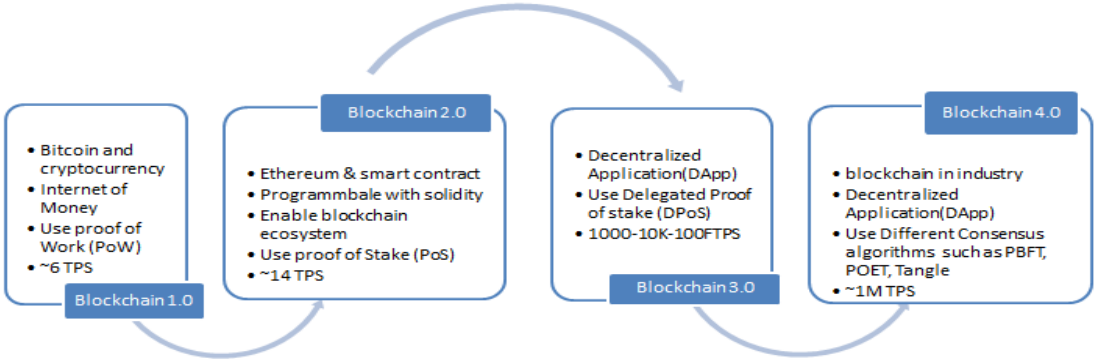

Figure 2: Blockchain Development Stages

Blockchain is a distributed system that is trust, secure, autonomous and anonymous. BC solve the main issues in centralized system that are central point of failure ,easy to attack and each node in the system doesn't know each other or connect with others[15][16].There are two types of classification to Blockchain firstly, classification based on access to data, three types of blockchain: public BC mostly known with digital currencies such as Bitcoin and Ethereum but allowed to use in general system depend on system requirements, private BC that is specific internal network with specific permission and consortium BC that is combination between public and private BC. Second type of classification based on the processing of the transactions: permissionless BC that doesn't have any restrictions for users to create block of transaction and permissioned BC that has predefined list of user with permission to do specific transaction [17].

2.2.1 Consensus Algorithms in Blockchain

The key mechanism for proper functioning in blockchain is called consensus mechanism to determine the conditions to proper blocks in BC, there are many types of consensus mechanism but the most known ones are POW (Proof Of Work) that depends on the power of processing, POS (Proof Of Stack) that depends on the reputation of entity with high participation, DPOS (Delegated Proof Of Stack) like POS mechanism but with selected delegates , and POA (proof Of Authority) that depends on the value of identities that relies on

a limited number of block validators, PBFT depends on the voting process to add the new block , Tangle that depend on the directed acyclic Graph (DAG),Blocks and transactions are verified by pre-approved participants and mostly used in private BC[16][17] . The most important and famous field that apply blockchain is logistics field that by default depend on IoT devices for deployment.

3. STATE OF ART

There are many studies and researches on Internet of Things security and securing IoT applications by using blockchain technology. Here are some of these studies, there visions and issues to be able to get suitable securing IoT systems within using blockchain. In [27], authors proposed smart city security framework layers and mention to using Ethereum without mention the useful algorithms in this case. As Ethereum depend on PoS that not completely suitable for such IoT systems due to the monetary concepts of stakes. In [28], authors proposed to use IP addresses of the devices in IoT system as a key to access data stored in blockchain but still have the issue of IP address exploitation. In [29], authors present different security technique for IoT systems since January 2016 and the importance of using blockchain in the future and Focus on intrusion prevention and detection but Facing a number of computations and the storage overhead in different security techniques and how blockchain is paving the way in securing IoT systems. In [30], the authors present an overview of blockchain architecture, consensus algorithms, and applications in IoT with the security and performance issues, especially for large scale IoT scenarios. In [31], authors presented the consensus protocols in blockchain. The main challenges to get fully integrated blockchain and IoT system is non-availability to centric consensus protocol and scalability issue. In [32], authors presented the adaption of Blockchain to specific needs in IoT systems, the need for different technical requirements like energy efficiency, scalability, throughput and latency to get effective system. In [33][17], authors Presented a survey of using blockchain and its consensus algorithms to securing IoT system and the need to enhance security, reliability and scalability in IoT systems using blockchain. In [35], authors presented a hybrid blockchain architecture for IoT where IoT devices form subgroups which use Proof of Work consensus algorithms that cause high latency and difficult to fit with limited storage capacity for IoT devices .From all of these studies , can find that applying blockchain to IoT require to adapt some of its mechanisms, especially the consensus algorithms implementation and need more work to reach to effective and suitable blockchain solution match the scale of large number of devices and transactions in IoT systems and get high performance.

4. The PROPOSED FREAMEWORK FOR SECURING IOT SYSTEMS WITHIN BLOCKCHAIN

IoT depend on peer -to -peer topology but executed by client-server model that relay on a single point of webserver to control the entire network. All IoT devices transmit their data to this central location, which often can be vulnerable and easily compromised. Vulnerabilities on IoT system can be summarized in shortage on security communication standards and protocols, Confidentiality and privacy of data stored on insecure IoT networks and Ineffective authentication and authorization methodologies for devices in an IoT system. For example, attacker can get access to the central control system of a connected power grid and cause a power outage. As IoT devices don't have enough security protocols to detect whether the data that they receive is normal or has malicious data, they are easy targets for security attacks. According to Gartner [37], blockchain has the potential to transform business models across all industries and one of these industries is IoT and blockchain and IoT industry will take around from five to ten years to reach the plateau of the industry. Using Blockchain is effective way to secure IoT systems .As Blockchain works on the decentralized distributed ledger system it is effective solution to eliminate the security gap in IoT system. According to the IoT system requirement and domain, the best suitable blockchain option can be chosen to fit the system requirements as shown in figure 3. Choosing blockchain solution is based on the percentage need of performance, scalability and reliability on IoT system. Consensus algorithms are the core and ground base of any existing Blockchain and define how transactions are validated to be stored with security level [17]. There are many developed consensus algorithms to validate the transactions also based on the access restriction or suitable type of blockchain (private, public, and consortium) in order to reach the performance-scalability-reliability according to the particular needs of a certain domain. So for IoT systems, must choose the most suitable consensus algorithms as there are many consensus algorithms not compatible for IoT systems only suitable for financial transactions such as POW, POC, LPOS and POA.

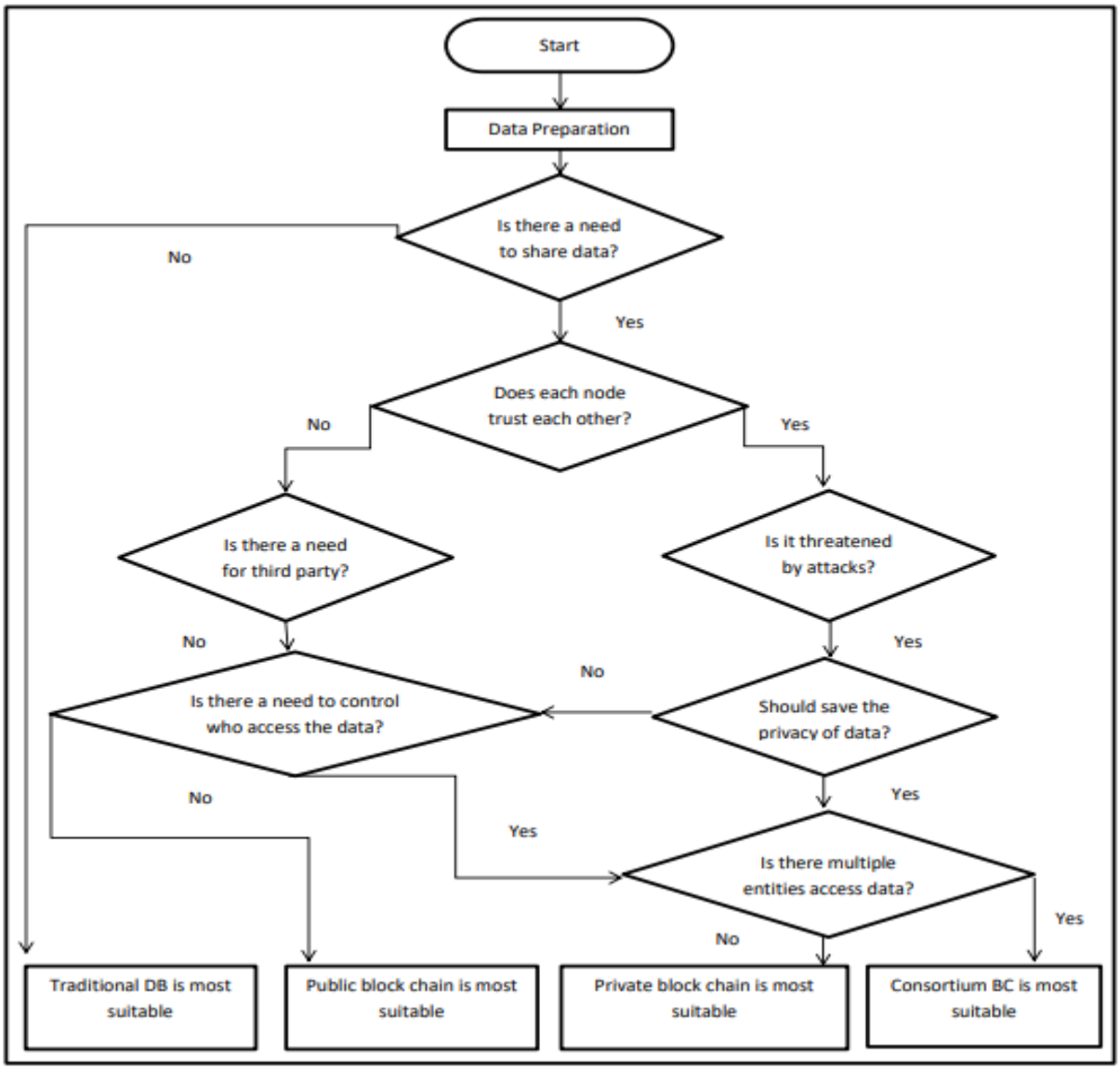

Figure 3: Flowchart of selecting the suitable blockchain type for IoT systems

There are many researches show the concept behind each consensus algorithms [17] [18] [19] [20].In these researches, there are other consensus algorithms suitable for IoT system and also each one has some constrains. After reviewing many consensus algorithms, the proposed framework will depend on PBFT and Tangle that depend on DAG. In the proposed framework; transactions of IoT system pass through many processes to be validated starting with direction algorithm process to select the appropriate consensus algorithm then validation process and confirmation process to be executed and added in the network.

The architecture of the proposed framework that is described in figure 4 can be divided into five components:

- IOT Sensors
- Smart Contract
- Direction Sensor
- Blockchain Network
- Blockchain Node

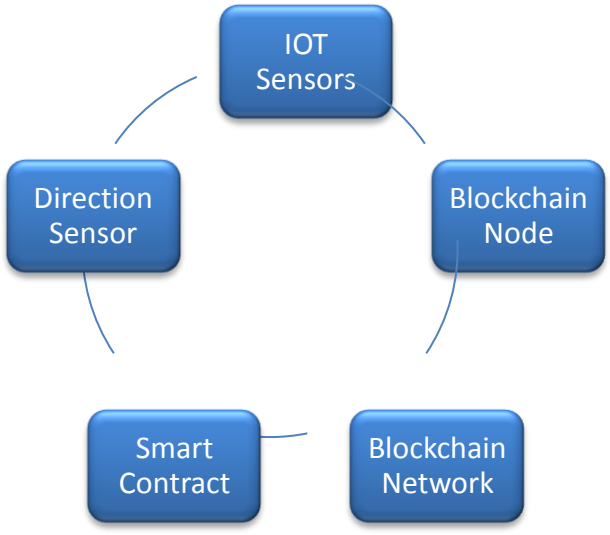

Figure 4: The components of proposed framework

1) IOT Sensors: the IoT devices belonging to the wireless sensor network are limited in their computational power, memory. With unique identifiers with communication protocols that support level of secure channels. IoT sensors generate a huge amount of transaction and data that need to be validated and coordinated.

2) A smart contract: smart contract can described as a script that is stored on the blockchain with a unique address and all operations and functions are defined in it. Smart contract contains references to transactions that are executed and cannot be deleted from the system.

3) Blockchain Network: The blockchain network in this framework is consortium blockchain that combines public and private blockchain according to the usage and the need of the IOT system requirements , The consortium blockchain is most likely as 'semi-private' and is controlled by specific user group. All instructions or operation steps in blockchain network are defined in smart contract.

4) Direction Sensor: is responsible for direction phase to each transaction to be validated with appropriate consensus algorithm either PBFT or Tangle that support the target of this framework to achieve high level of security and performance and scalability.

5) Blockchain Node: BC node is any kind of devices according to the IOT system requirements, starting from normal PC or laptop till huge servers. Each BC node has the identifier address for smart contract in the blockchain network to be aware with all instruction in the network or interact with the validation process. All nodes are connected to each other that responsible for validate and store the valid transactions and information and contain a full copy of the history of blockchain

The suggestion framework that is shown in figure 5, is depending on integrating between PBFT and Tangle consensus on consortium blockchain to get more features with high security, scalability and performance by depending on direction algorithm. Firstly, understanding the system requirement then define each device on IoT system with specific device id 'DID' where each normal device with expected 'Tn' normal transaction per sec 'TPS' and based on predefined transactions per second n then the system will be able to direct the transaction to right way to be validated by PBFT or Tangle .In Direction algorithm, as shown in figure 6, after users, sensors and connected devices generate new transactions 'Ts' that will be added in transaction data set 'TDS' by depending on device id 'TDID' then transaction checker 'Tchecker' check DID in device data set 'DDS' to get Tn after that compare Tn with n, if Tn for specific device is smaller than or equal n then validate the transaction TDID by PBFT algorithm else validate TDID by tangle algorithm, and if Tn for any device become greater than n then update DDS which help to get more secure and scalable network.

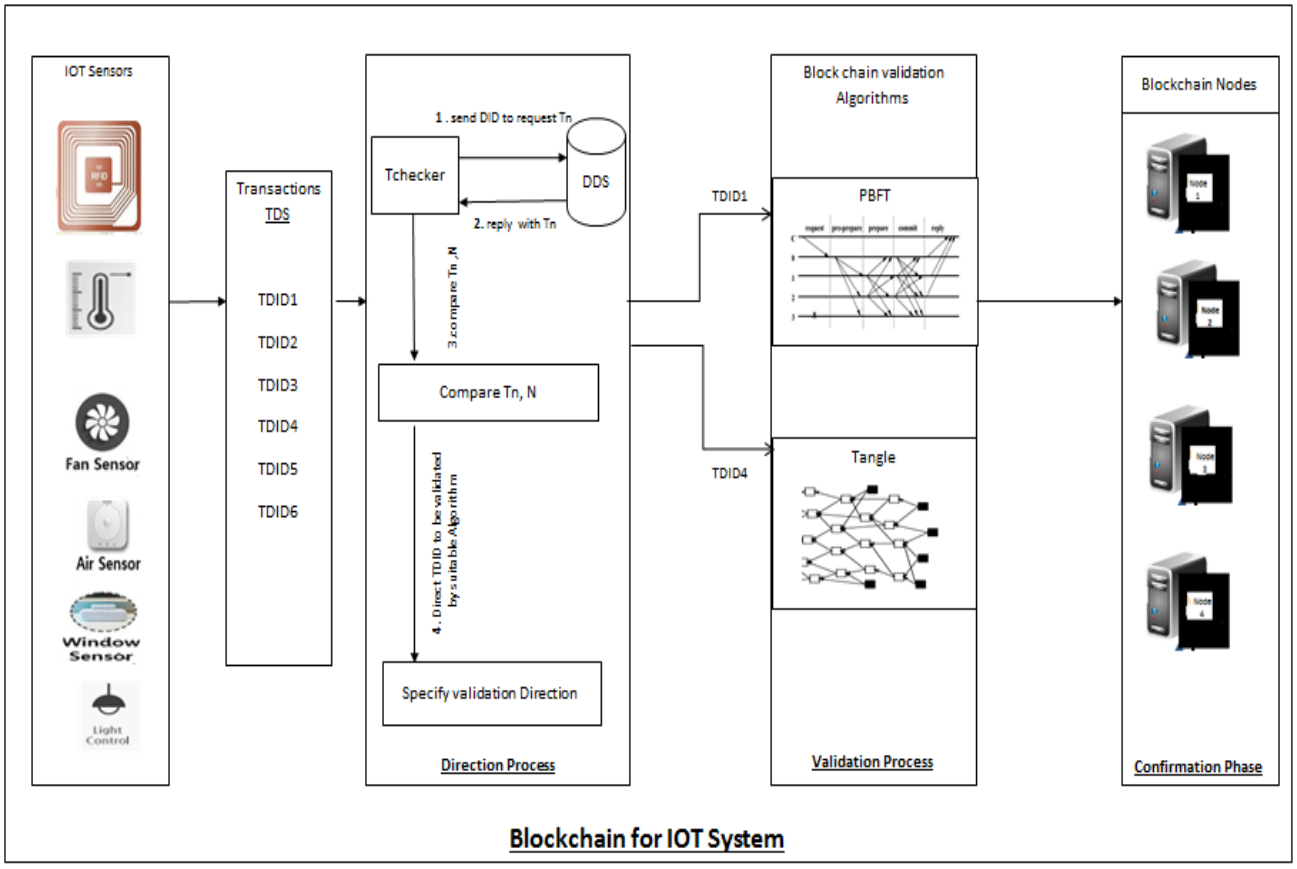

Figure 5: The proposed IoT Blockchain framework

Communications on Applied Electronics (CAE) – ISSN : 2394-4714
Foundation of Computer Science FCS, New York, USA
Volume 7– No. 34, September 2020 – www.caeaccess.org

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

DDS	
DID	Tn

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

Figure 6: The proposed direction algorithm

5. EVALUATION AND EXPERIMENTAL RESULT

There are many factors that measure the performance of the framework such as security level, transaction rate where high throughput is greater than 1000 TPS is most required in IoT systems, scalability and latency that is the time to between placing a transaction, direct it to validation algorithm and to be validated and low latency equal number of milliseconds. According to the previous studies of other models, frameworks and consensuses algorithms and focusing on PBFT and Tangle (DAG) to reach to the propose framework, figure 7 presents the expected evaluation of the performance to the propose framework till get accurate data from more experiments as future work.

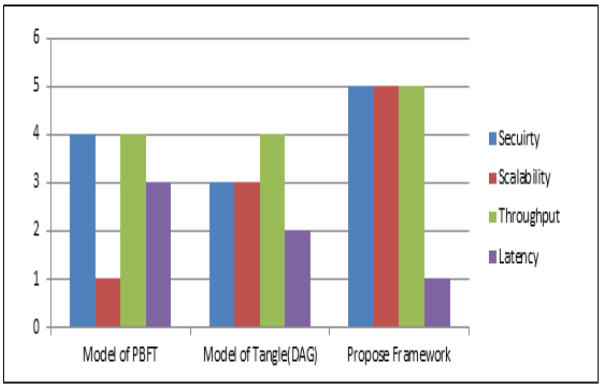

Figure 7: Evaluation of proposed framework compared to PBFT and Tangle

The simulation using CASAS dataset which are smarthome-based data sets [38]and using Netsim simulator and emulator to evaluate the performance. The proposed framework based on a consortium blockchain using the Hyperledger Fabric which is a blockchain platform uses the PBFT algorithm as consensus algorithm and using a private Tangle based on the IOTA architecture. By using four server machines as validation nodes, each node has a two-core Intel Core i7 2.2GHz CPU with 16GB DRAM and 256GB SSD, with operating system Ubuntu 16.04 as. And simulate other four server machines as IoT devices with predefined expected TPS for each one to deploy on them. Implement direction process algorithm in the smart contract to work as gateway to each transaction to be validated by PBFT or tangle. The evaluation of the performance to the propose framework depend on the metrics of latency, Scalability and security by generating and sent number of transactions by the APIs provided by Hyperledger Fabric and to test the latency and the scalability of the system. As shown in figure 8,while the number of sensors increase which mean increasing in the number of transactions; the latency in the proposed framework the time decrease while comparing using PBFT or Tangle only as the load of validation is balanced between PBFT and tangle depend on direction process and generated device for transactions. Figure 9 show that the performance of scalability as a result of number of transactions per second is better in the proposed framework compared to each algorithm separately.

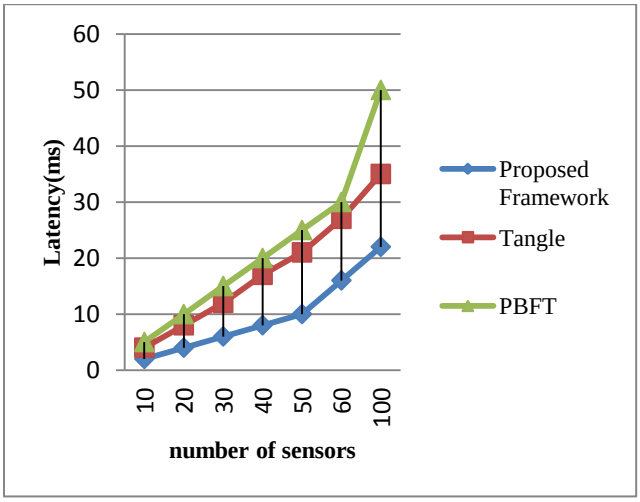

Figure 8: Average of latency time for numbers of sensors

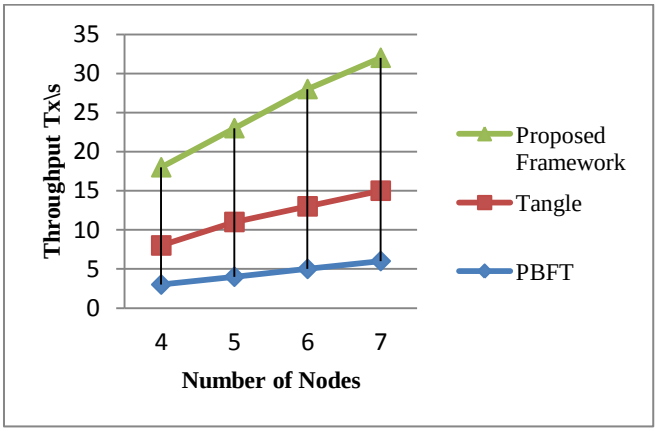

Figure 9: Scalability in each algorithm and proposed framework

Security is the most required in any system especially by using blockchain where the Sybil attack is the most apprehensive but by this framework can mitigate this apprehensive because of the load balance between consensus algorithms and the dynamic of validation. Table 1 summarizes

a comparative evaluation for each algorithm and proposed framework.

Table 1: Comparative evaluation for each algorithm and proposed framework

	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

6. CONCLUSION AND FUTURE WORK

Using Blockchain technology is an effective way to enhance IoT systems where there are a huge number of transitions and data within resource constrains and low computational power to keep the efficiency of the scalability, security and latency in IoT systems. There are many types of blockchain where the core in blockchain is consensus algorithms. This paper presents method to how the selection of an appropriate BC type based on system requirement. In additionally, proposes a new framework for securing IoT systems using blockchain algorithms based on the integration between consensus algorithms of blockchain (PBFT and Tangle) by using the propose direction algorithm to enhance the validation process. The propose framework ensures a high level of performance by enhancing security level, latency time and scalability. The future work will aim to conduct more experiments to investigate the impact and feasibility of this framework to get security and scalability network in IoT systems.

7. 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=prUS45213219.

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

[3] [Online]. Available: http://www.gartner.com/it-glossary/internet-of-things/.

[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.e-zigurat.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-datacom-cyberscitec.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.

[11] M. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges", Future Generation Computer Systems, vol. 82, pp. 395-411, 2018. Available: 10.1016/j.future.2017.11.022 .

[12] P. Kumar and R. Kunwar, A Survey Report on : Security & Challenges in Internet of Things. 2016.

[13] D. Das and B. Sharma, "General Survey on Security Issues on Internet of Things", International Journal of Computer Applications, vol. 139, no. 2, pp. 23-29, 2016. Available: 10.5120/ijca2016909113.

[14] K. Zhao and L. Ge, "A Survey on the Internet of Things Security", 2013 Ninth International Conference on Computational Intelligence and Security, 2013. Available: 10.1109/cis.2013.145.

[15] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 2017 IEEE International Congress on Big Data (BigData Congress), 2017. Available: 10.1109/bigdatacongress.2017.85.

[16] W. Gao, W. Hatcher and W. Yu, "A Survey of Blockchain: Techniques, Applications, and Challenges", 2018 27th International Conference on Computer Communication and Networks (ICCCN), 2018. Available: 10.1109/icccn.2018.8487348.

[17] M. Salimitari and M. Chatterjee, A Survey on Consensus

Protocols in Blockchain for IoT Networks. arxiv.org, 2019.

[18] "Blockchain consensus for the Internet of Things | IEEE Standards University", IEEE Standards University. [Online].Available: https://www.standardsuniversity.org/e-magazine/may-2019-volume-9-issue-1-blockchain-standards/blockchain-consensus-for-the-internet-of-things/.

[19] M. Maroufi, R. Abdolee and B. Tazehkand, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies", Journal of Strategic Innovation and Sustainability, vol. 14, no. 1, 2019. Available: 10.33423/jsis.v14i1.990.

[20] S. Zoican, M. Vochin, R. Zoican and D. Galatchi, "Blockchain and Consensus Algorithms in Internet of Things", 2018 International Symposium on Electronics and Telecommunications (ISETC), 2018. Available: 10.1109/isetc.2018.8583923.

[21] L. Hang and D. Kim, "Design and Implementation of an Integrated IoT Blockchain Platform for Sensing Data Integrity", Sensors, vol. 19, no. 10, p. 2228, 2019. Available: 10.3390/s19102228.

[22] F. Jindal, S. Mudgal, V. Choudhari and P. Churi, "Emerging trends in Internet of Things", 2018 Fifth HCT Information Technology Trends (ITT), 2018. Available: 10.1109/ctit.2018.8649535.

[23] S. Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System.

[24] "Survey Analysis: 2016 Internet of Things Backbone Survey", Gartner, 2020. [Online]. Available: https://www.gartner.com/en/documents/3563218.

[25] M. Miraz, "Blockchain of Things (BCoT): The Fusion of Blockchain and IoT Technologies", Studies in Big Data, pp. 141-159, 2019. Available: 10.1007/978-981-13-8775-3_7 .

[26] A. Srivastava, P. Bhattacharya, A. Singh and A. Mathur, A Systematic Review on Evolution of Blockchain Generations. 2018.

[27] K. Biswas and V. Muthukkumarasamy, "Securing Smart Cities Using Blockchain Technology", 2016 IEEE 18th International Conference on High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/SmartCity/DSS), 2016. Available: 10.1109/hpcc-smartcity-dss.2016.0198

[28] K. Prabhu and K. Prabhu, Converging blockchain technology with the internet of things. International Education and Research Journal, 2017.

[29] M. Banerjee, J. Lee and K. Choo, "A blockchain future for internet of things security: a position paper", Digital Communications and Networks, vol. 4, no. 3, pp. 149-160, 2018. Available: 10.1016/j.dcan.2017.10.006.

[30] A. Zorzo, H. Nunes, R. Lunardi, R. Michelin and S. Kanhere, "Dependable IoT Using Blockchain-Based Technology", 2018 Eighth Latin-American Symposium on Dependable Computing (LADC), 2018. Available: 10.1109/ladc.2018.00010 .

[31] I. Makhdoom, M. Abolhasan and W. Ni, "Blockchain for IoT: The Challenges and a Way Forward", Proceedings of the 15th International Joint Conference on e-Business and Telecommunications, 2018. Available: 10.5220/0006905605940605 .

[32] T. Fernandez-Carames and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things", IEEE Access, vol. 6, pp. 32979-33001, 2018. Available: 10.1109/access.2018.2842685.

[33] H. 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. Available: 10.1109/jIoT.2019.2920987 .

[34] M. Ferdous, K. Biswas, M. Chowdhury, N. Chowdhury and V. Muthukkumarasamy, "Integrated platforms for blockchain enablement", Advances in Computers, pp. 41-72, 2019. Available: 10.1016/bs.adcom.2019.01.001

[35] Sagirlar, G.; Carminati, B.; Ferrari, E.; Sheehan, J.D.; Ragnoli, E. Hybrid-iot: Hybrid blockchain architecture for internet of things-pow sub-blockchains. arXiv 2018, arXiv:1804.03903.

[36] [Online]. Available: https://www.gartner.com/smarterwithgartner/gartner-top-10-trends-in-data-and-analytics-for-2020. [Accessed: 10- Aug- 2020].

[37] Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years", Gartner, [Online]. Available: https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows. [Accessed: 10- Aug- 2020].

[38] Cook D. CASAS smart home project, 2017, http://www.ailab.wsu.edu/casas/