Blockchain Technology Adoption and Implementation for Securing IoT Devices

Maha Mohamed Ahmed Al Habsi¹; Smitha Sunil Kumaran Nair²; Said Juma Said Juma Al Sulti³; S. Adarsh⁴

¹Centre for Postgraduate Studies, Middle East College, Sultanate of Oman.
²Centre for Postgraduate Studies, Middle East College, Sultanate of Oman.
³Centre for Postgraduate Studies, Middle East College, Sultanate of Oman.
⁴Kerala Blockchain Academy, IIITMK, India.

Abstract
The rise of connected world is a reality through Internet of Things (IoT) technology and is increasingly changing the way people live, communicate and work. Perhaps, for a continued support to be delivered efficiently and effectively in terms of the services IoT offers, there are some challenges which need attention. This is basically the security aspects pertaining to the data the IoT devices generate, collect and process. In the recent years, blockchain technology gained attention in cutting edge solutions based on securing IoT devices. However, it is observed that adoption of blockchain technology is limited in several countries. The proposed research aims to investigate potential barriers to adopting blockchain technology in smart city applications through a qualitative study. In addition, a stake algorithm to demonstrate the security aspect in IoT device is presented.

Key-words: Blockchain, Internet of Things, Security, Smart Cities.

1. Introduction

The impact of the 4th Industrial Revolution (4IR) technologies brought out positive economic variations and market dynamics in recent years. In the current era of utilizing latest technologies of 4IR, considered to be the new fuel for tomorrow’s business, the proposed research aims to explore the use of blockchain technology in Internet of things (IoT) devices to improve industrial business practices and also from a security perspective. IoT senses the real world through systematized collection and transmission of big data to and from enormous, connected devices for a specific application (IoT Agenda 2021). Secured transactions and exchange of data are equally important, which is proposed to be accomplished by blockchain technology. This kind of integration of
technologies is a must in the current digital era, where technological disruption has become the constant evolution process to succeed as a digitally transformed organization.

Blockchain technology evolved with promising applications in financial domain initially. However, this emerging technology has shown great potential in diverse domains such as healthcare, supply chain and so on. Studies show that blockchain is not just the technology behind bitcoin but something more than that (Arbogast and Eloudhriri 2019) (Conway 2021). Research confirms that blockchain technology is a real way of decentralizing the Internet, hence an ability to make huge positive changes in the industry. Bitcoin and Ethereum are popular architectures of decentralized systems (Anderson 2019). However, generally not many countries have adopted this technology widely (Pawczuk et al 2020). The current research aims to present a stake algorithm to demonstrate how the use of blockchain technology can be used to provide security in IoT devices alongside investigate potential barriers to widely adopting new technologies like blockchain.

2. Literature Review

Automated IoT improves communication within the system, allowing better access and transfer of data. In companies, it increases productivity and allow more controlled monitoring, thus eventually helping to increase revenue. However, IoT lacks security. It is quite easy for a hacker to hack into an IoT system and gain access to all connected devices and obtain confidential information. Also, if a bug or virus infects one device, it will corrupt the whole system. Needless to mention, the more devices connected, the harder it is to manage all the data.

Blockchain is a recent technology evolved as a solution provider to security threats. In a chain of blocks, if an error occurs in one copy of the blockchain, it does not in the majority and thus, is removed. This decentralisation can also secure the data, since any hacker wishing to change it must make sure the change is replicated in 51% of the systems to be acknowledged and considering the millions of networks connected to one blockchain, it is almost impossible. Moreover, the personal data of anyone is not just confidential, but the entire record is also transparent since anyone can view it. It also reduces cost by removing any sort of third-party involvement for carrying out deals and verifying them. However, this technology has certain setbacks. Implementation requires huge investment and work including the necessary programming and related tasks. The process of verifying the transactions is costly for miners depending on where they live and therefore, they would need to be provided certain incentives to continue their work. The amount of confidentiality offered
by blockchain has led to its usage in illegal activities such as making purchases on the dark web which is alarming for the governments (Reiff 2020).

While investigating potential blockchain-based solutions to secure IoT devices, several studies are undertaken that includes potential blockchain solutions for IoT in improving the overall security (Zhou et al 2019). It is important to note that design of protective measures against security threats of an IoT device depends on various features of IoT and hence designing a practical and generic framework is challenging. From an adoption of blockchain technology perspective, the target individual must show a relative amount of interest in the introduced technology. In this case, acceptance occurs only when there is a little undue impression from the environment for groups to accept a specific technique. It must be something unbeaten and, in classical terms, irresistible to ignore. Secondly, it is a fact that there is a need for a framework to support acceptance. For example, when a new technology is introduced, it is not enough just to attract the attention of the consumers. Instead, the most important thing to be made sure of is that there should be a strategy that should maintain the interests in the longer term. This means that there is always a room for improvement, creativity, and innovation according to the changing environment, or else people might not get interested. It is essential to consider such a population who can be helped towards influencing others to adopt a technology that they have not yet been explored (Wintgens 1999).

A proof of concept is presented to demonstrate securing medical data by proposing an IoT-Blockchain architecture through smart contract, protocols for data access and publisher subscriber system for the notification (Rifi et al 2018). A set of challenges associated with securing IoT devices with blockchain in terms of storage and computing resources are also addressed (Agoulmine et al 2018). Yet another interesting research that demonstrates promising potential of blockchain in IoT security is the stalker. It aims to preventing one node to publish other blocks on the main chain by acting as a variant of selfish miner (Jesus et al 2018). An architecture based on a network of hyperledger fabric is proposed for securing IoT devices advantaged with minimum resource utilization (Arse and Dubey 2020).

There are some key features and core values any system possesses that brings forth its uniqueness, and that identity then promises its best position among other market technologies. Still, again that core quality is applied conditionally based on its utilization purpose, and if it does not suit the primary purpose of utilization, the very same core value can act as a curse and count as a drawback overall. Blockchain technology is designed for its transparency and openness. It involves a group or chain of people who have access to certain information mutually. Within that chain, there
stands no privacy or confidentiality, which in some firms like in the fabric industry is very helpful. But if the same technology is applied to a bank, the purpose will be severely sabotaged and would be considered a flaw. Therefore, in terms of privacy and protection, this technology has multiple limitations too (Lencioni 2020). The proposed research tries to investigate the potential barriers to adopting blockchain technology in general and also proposes a stake algorithm to demonstrate securing IoT device using this technology.

3. Materials and Methods

To investigate the potential barriers and opportunities for adopting blockchain technology, in general, an interview was conducted with some employees of UK organizations. In addition, potential organizations to use smart city platform were identified since such organizations might be needed to adopt such a huge shift in technology. This included public and private sectors in Oman. Data were collected through an interview with senior level managers to investigate the potential barriers for blockchain technology adoption at a larger scale in the country. Qualitative data gathered were analysed to conclude this study and the same is presented in Section 4.

To demonstrate the stake of algorithm to secure IoT devices using blockchain technology, blockchain has been connected with the physical world over wires as discussed subsequently. It involves checking whether one is allowed to use a service or not. In addition, certain number of tokens that will be assigned to user account identified by its address is checked by retrieving them using Smart Contract (SmartToken), LEDs with a button.

Figure 1 illustrates the flow diagram. Assume there are two users: User A and User B (sender and Receiver). User A initiates bitcoin transaction on Ethereum blockchain connected to web platform. User A transfers a bitcoin to User B, every transaction is represented on network as block. This block will broadcast the transaction to the network. On every transaction, validity can be verified by user, and this is further added to the chain. After that, the verified records can be visible to all users, which is under the transaction of bitcoin. Then the data can be securely moved between User A and User B (Satapathy et al 2018).

Table 1 - Indicates the Hardware and Software Utilized.
Table 1 - Hardware and Software Requirements

| Hardware   | LED          | Bread board | Wires | Button | Resistors | Raspberry Pi |
|------------|--------------|-------------|-------|--------|-----------|--------------|
| Software   | Ethereum Web3| Web3        | Node. Js |        |           |              |

- Hardware includes LEDs (2 Nos. green and red), a button, bread board and wires, 4 resistors (2 x 220Ω, 1kΩ, 10kΩ), Raspberry Pi 3 B+

- Software includes two packages (Web3 and On Off) and Node.js

Step 1: Start with electronics section: Initially Raspberry Pi must be turned off before proceeding. An LED is connected to the RPi’s GPIO17 port. Figure 2 illustrates the schematic diagram. Figure 3 shows the physical connection of the electronic components on a bread board arrangement.

GPIO17 port (port 11) ↔ LED’s (positive) anode pin.

LED’s (negative) cathode pin ↔ resistor ↔ RPi’s GND port (port 6).

Power on the RPi once finished.

Step 2: Make the RPi connection: This is accomplished using the SSH command to make a connection to RPi.

Step 3: Start nodes: Start the miners and RPi node with appropriate commands before the deployment of the Smart Contract.

Step 4: Preparation of RPi: All the operations to be performed on RPi such as installation of software for running the script is done. The script will help in interacting with Smart Contract.

Necessary instructions are followed to install Node.js 7.x on the RPi. Subsequently, project folder is prepared by utilizing Web3 installation via Git. Ethereum Web3 package is utilized. Web3 module is a node module that provides a JavaScript API and this will help in interacting with the Ethereum blockchain. Fetching the Smart Contract’s status is possible through the JS script in this
module. An earlier version is used here due to compatibility issues with the 1.0 beta version. An easy interaction to the RPi’s GPIO pins to On or Off is made possible through the On Off module. To create the client application, JS script is created called “smart_token.js” which are used for interacting with the Smart Contract and RPi.

First, the variable’s value “contractAddress” is changed with the contract’s address being deployed on the private blockchain. Consequently, the ABI of the SmartContract is provided by replacing variable ABI’s contents. Finally, the client application can be executed. Before testing the application, there is a wait period for the change to happen on SmartContract. Eventually, testing is done using Mist by dropping tokens to Pi node’s coin base address. Accordingly, LED gets lit based on the remaining token. By pressing the button, the number of tokens can be obtained.
4. Results and Discussion

Based on the analysis of qualitative data collected, the first and foremost barrier to adopt blockchain is that not many companies and organizations are willing to shift to the new technology. Most of the organizations are either distrustful of the new technology or simply too comfortable in their old practices to be willing to make an effort and exhaust the resources that would be required in making the change. Secondly, every country should have a national strategy for blockchain which is a guiding principle to adopt this technology. Lack of awareness about the technology is yet another barrier. This lack of knowledge automatically means most of the organizations will not be motivated to adopt new technology and might even be distrustful of it. Another problem is lack of relevant expertise and experience, finding people who are specialized in this field and experienced is extremely difficult, especially considering that the majority is not even aware of the technology. Without sufficient expertise, managing the implementation process and the technology upon adoption
is highly risky to adopt an entirely new system. Many problems can arise which no one will know how to deal with.

Another major problem is the lack of proper infrastructure in organizations and inadequate government policies concerning the matter. Most organizations do not have the systems and infrastructure that is necessary to accommodate the integration of such complex technology in their existing systems. The lack of government policies in regard to implementing new technologies and using them means that most organizations do not have a framework they can follow to enable the adoption of blockchain in their systems. Insufficient rules and regulations also demotivate organizations from fear of breaking the law or ethics that might exist out of their knowledge and policies. This is further complicated by fragmentation in organizations. The divide and extreme hierarchies mean there are constant disputes and disagreements which can present a hurdle to any new policy or action being implemented, much less a change of this magnitude.

Another factor which demotivated many organizations from adopting this technology is the lack of potential uses in their company for the technology. No company is willing to waste their resources and time on a technology which eventually will prove to be of little to no use for them and their work. For most organizations, this technology has limited practical applications which are not
worth the resources and effort needed to implement this technology. A simple cost-benefit analysis, the costs outweigh the benefits.

On the other hand, the main ones being the commitment of the government to the cause and their provision of adequate resources for the procedure; since this technology is highly costly and the cost can be a barrier for many (Zmudzinski, 2018). However, adoption of blockchain technology is not too far since smart city realization is already in progress. Several IoT devices play a key role in smart city applications. Security is of course a great concern. Therefore, blockchain adoption to implementation will be a requirement in the near future.

Regarding the results of proof of stake algorithm, Rasperry Pi OS and BlueJava IDE have been used. The web page for bitcoin transaction utilizing blockchain technology is shown in figure 4. Several functions such as deposit token, withdraw token and balance enquiry are provided. Initially deposit token is chosen to deposit a token via this network. Click Execute button as shown in figure 4 and a bitcoin is deposited. Ethereum platform is used for performing this transaction. In every bitcoin transaction, there is a need of encryption. In this, a double encryption method is used namely password and security code as seen in figure 5. Submit button is clicked.

When a bitcoin is deposited using blockchain technology, it implies the transaction is executed. This is indicated through the green LED. As shown in figure 6, the transaction is in the

![Figure 4 - Bitcoin Transaction](image-url)
processing stage. When the bitcoin transaction is fully completed, the notification is obtained as in figure 7. At the same time, the red LED in the circuit blinks which also shows that the bitcoin transaction is fully completed, and the bitcoin is deposited successfully. Transaction information can be found in the database (figure 8). This contains the transaction id, password, and the timestamp. A prototype of a blockchain network application using Ethereum platform to secure IoT devices is implemented that will track the device by storing the identity of those devices on a ledger making it easy not to track the devices.

5. Conclusion and Recommendation

In this research, an extensive study has been carried out to understand the impact of securing IoT devices using blockchain technology by presenting a stake algorithm. This technology has the potential to bring in positive impact from a social-economic perspective after exploring the advantages of using it in various business processes. When a country urges to build smart cities, use of IoT devices is obvious and hence the security of data that flows in and out of IoT devices is significant. A 2020 global blockchain survey conducted by Deloitte to know the security level offered by blockchain in comparison to conventional IT systems conclude that the former technology offers more (around 64%) (Pawczuk et al 2020).

Figure 5 - Send and Receive Token
The research study confirms that presently this concept is not widely popular in several countries. However, the countries which adopted blockchain technology has a strategy in place which includes the benefits, focus areas and sectors as to where and how this disruptive technology could be adopted for the benefit of society.

Cybersecurity challenges comes alongside the use of computer systems. From the review, it was observed that every organization faces challenges not only in the cybersecurity but also security in IoT devices, locally as well as globally and hence appropriate measures must be undertaken. Some barriers identified in not adopting new technologies like blockchain included lack of awareness among the private and public organizations, limited infrastructure, old policies, no expertise related to these technologies etc as detailed under Section 4.
As per the findings of this research, it is recommended that every government should take necessary steps to educate the people about blockchain technology and its benefits. More importantly, the government should focus on creating new policies and strategies according to the needs of implementing these technologies to make it easier for organisations to focus on implementation.
The new policies should address the organisational concerns as well as public concerns which includes confidentiality. It also must provide appropriate infrastructure in organisations which would be capable of accommodating the integration of this complex new technology such as better communication channels, faster internet connections, etc. Lastly, the government needs to provide sufficient resources in terms of budget and knowledge of the technology, and problem-solving facilities through conferences and purpose-built guide teams or private organizations to implement this new technology into their businesses and start getting benefited from it. This step will revolutionize the whole country system and will produce some great revenue for the country. Undoubtedly, blockchain technology is a potential bridging factor between IoT and security which can still be enhanced with the convergence of these technologies with Artificial Intelligence providing additional layer of security.

Acknowledgements

The research leading to these results has received funding from The Research Council (TRC) of Oman under the Block Funding Program (TRC Block Funding Agreement No. BFP/GRG/ICT/19/051). The authors would like to acknowledge Kerala Blockchain Academy, IIITMK, India for the training support.

References

Anderson, M., 2019. Exploring Decentralization: Blockchain Technology and Complex Coordination. *Journal of Design and Science*. https://jods.mitpress.mit.edu/pub/7vxemtm3

Arbogast, S. and Eloudrhiri, S., 2019. *Become a Blockchain Developer with Ethereum and Solidity*.

Arse, M. and Dubey, J., 2020. A Mechanism to Secure the Transaction of IoT Devices Using Blockchain Technology. *SSRN Electronic Journal*.

Conway, L., 2021. *Blockchain Explained*. Arbogast Pedia. https://www.investopedia.com/terms/b/blockchain.asp

IoT Agenda. 2021. *What is IoT (Internet of Things) and How Does it Work?* https://internetofthingsagenda.techtarget.com/definition/Internet-of-Things-IoT

Lencioni, P.M. 2020. *Make Your Values Mean Something*. https://hbr.org/2002/07/make-your-values-mean-something

Jesus, E., Chicarino, V., De Albuquerque, C. and Rocha, A., 2018. A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack. *Security and Communication Networks*, 2018, 1-27.
Pawczuk, L., Holdowsky, J., Massey, R. and Hansen, B., 2020. Deloitte's 2020 Global Blockchain Survey from Promise to Reality. Deloitte, 1(1).

Reiff, N. 2020. Blockchain Explained. https://www.investopedia.com/terms/b/blockchain.asp

Rifi, N., Agoulmine, N., Chendeb Taher, N. and Rachkidi, E., 2018. Blockchain Technology: Is It a Good Candidate for Securing IoT Sensitive Medical Data? Wireless Communications and Mobile Computing, 1-11.

Satapathy, S.C., Bhaveja, V. and Das, S. 2018. Smart Computing and Informatics. Proceedings of the First International Conference on SCI 2016, 2.

Wintgens, L., 1999. The Law in Philosophical Perspectives. 1st ed. Springer, Dordrecht, XIX, 274.

Zhou, W., Jia, Y., Peng, A., Zhang, Y. and Liu, P., 2019. The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. IEEE Internet of Things Journal, 6(2), 1606-1616.

Zmudzinski, A. 2018. Nebula-AI (NBAI): The convergence of AI and Blockchain. https://www.fxempire.com/education/article/nebula-ai-nbai-the-convergence-of-ai-and-blockchain-513273