Impact of BlockChain Integration with IOT for Payment System

Bhavraaj Singh , Priyabrata Pradhan

Abstract— Blockchain is one of the most anticipated solutions as a decentralized ledger for the Internet of Things. Its decentralized nature makes it one of the best technologies enabling the ideal M2M financial transactions that are important for IoT systems. The Internet of Things has made traditional appliances and devices smart and automatic. Advancement of technology has made this concept into reality. However, there are privacy and security issues making it a challenge for a large-scale implementation. It becomes necessary to build confidence considering the predicted evolution of the Internet of Things in the near future. Blockchain has become an important technology to change the way data is shared between the devices. It is a blockchain which can build trust in distributed ecosystems without intervention of centralized authorities. This technological innovation can revolutionize many industries. IoT leverages cloud computing and big data as disruptive technologies to deal with its limitations. In this paper, we attempt to analyse the impact of blockchain and its benefits for the IoT payment system.

Index Terms— Blockchain, Cloud computing, Decentralized system, Internet of Things, IoT, Scalability, Security issues,

1 INTRODUCTION

The next wave of computing will no longer be limited to laptops or desktops. Most of the objects around us will be connected together in the paradigm of Internet of Things. Radio Frequency Identification and sensor networking technology will get a significant boom in meeting new challenges where communication and information systems will be embedded in the surroundings. It will generate a huge bunch of data that should be processed, stored, and presented in an efficient and smooth way. The Internet of Things will provide all the services and products in the way like traditional mediums. Virtual infrastructure can be created with cloud computing for this utility and it will integrate storage devices, monitoring devices, visualization platforms, and analytical tools. Cloud computing offers the cost based model with end-to-end services for users and businesses to access on-demand applications from any part of the world.

Smart connectivity with context-based computation and existing network is an inseparable part of IoT with network resources. With the increasing use of wireless internet (Wi-Fi) and 4G(LTE) services, the evolution of ubiquitous communication and information is already present. However, for the successful emergence of the Internet of Things, the computing paradigm will be far and beyond traditional scenarios of mobile computing using portables and smartphones, and they can evolve in embedding intelligence in the environment and connecting existing objects in this day and age. The Internet of Things needs pervasive communication and software architecture to convey and process actionable and relevant insights, shared understanding of the situation of appliances and users, and analytical tools for smart and autonomous behaviour in the Internet of Things. It is possible to accomplish context-based computation and smart connectivity with these basic grounds.

Kevin Ashton was the first to bring the term “Internet of Things” in 1999 at Procter & Gamble’s supply chain [1]. Over the years, the term has taken a larger shape and covered a lot of use cases like logistics, healthcare, utilities, etc. [2]. With the evolution of technology, the definition of ‘Things’ would no longer be the same. However, the original objective of making a device sensing information while eliminating human intervention has never changed. The authors at [3] proposed a Cloud-based vision for representing the Internet of Things across the world. The emerging use cases and the key information technologies will open further research paths in the near future. Implementation of Aneka, powered by the interaction of public and private Cloud is proposed in this literature. The authors expanded their need for convergence of distributed and internet computing for their IoT vision at technological research.

Distributed Ledger Technologies (DLT) like Blockchain has a great demand in various fields, especially for IoT Payments. Blockchain is

one of the best technologies for enabling the truly Machine-to-Machine (M2M) financial transactions due to its decentralized nature and it is considered important for the IoT economy. The term "Internet of Things" is also used with "Internet of Everything", the term which consists of the interaction between devices, people, and data. This concept promises to create a world where devices can be connected together and exchange a lot of data [4]. However, the emerging IoT payment technology needs devices and sensors to conduct financial transactions for services without using third parties, such as Peer to Peer (P2P) and Machine-to-Machine (M2M) [5].

These exchanges and transactions will take place especially over the internet network with the advancement of 5G technologies, which are something that payment or billing systems should consider. On the other side, Blockchain is an ever-growing DLT technology that is known for its decentralized nature and it enables anonymous, secure, and immutable transactions. One important matter of argument is the way IoT payment should work when it comes to IoT environments. Due to this lack of clarity, the field of IoT is still lagging behind and the protocols and platforms in lieu of financial rewards for services should be defined in a clear way. IoT services may also sell sensor data as part of Sensing-as-a-Service model [6], or can be used in charging stations for selling power charges to electric vehicles [7]. Automatic micropayments would be very helpful in a pay-per-use model for both services [8]. As discussed in [5], traditional online business models always needed trusted third parties like banks for transactions as intermediaries. Due to this reason, IoT's ability can be limited to make the most of P2P, M2M and even Machine-to-Peer models. Hence, it is important to adapt business processes in a way that they can integrate in the information network for IoT. Blockchain can make it possible thanks to its distributed feature and it can avoid third-party intervention for completely P2P transactions [5].

Blockchain can also be helpful in dealing with other issues in IoT monetary transactions caused by third parties, such as security risks and lack of privacy for the end users. A customer will just not allow access to their bank account and risk their financial data by storing their transaction history in hundreds of devices [8]. Especially in this age when surveillance and data collection scandals are rising, it can be especially uncomfortable. The ability of users to maintain some sort of anonymity is one of the best parts of blockchain. In addition, the dependence on third-party intermediaries also causes higher transaction fees and it is also undesired in micropayments. Only a few people would like to finish a transaction where there would be a higher transaction fee than the amount for transfer [9]. It goes without saying that transaction fees are the next common issues for blockchain but it can still be improved [10].

This paper is aimed to determine the impact of Blockchain with IoT payments and the compatibility of the same, especially in terms of IoT transactions. We will discuss all the important features making Blockchain the best solution for IoT security and whether it can provide scalability, privacy and security to the users.

2 Literature Reviews

Reyna et al. (2018) explored challenges and opportunities on blockchain and its integration with IoT. In this day and age of the Internet of Things, traditional devices have become autonomous and advanced. Technological advances are turning this vision into reality but there are several challenges we need to address, especially in data reliability. Considering the predicted evolution of IoT in the next few years, having confidence in this emerging field is very important. Blockchain has come up as an advanced technology to turn the way information is shared. It is very important to build trust in distributed environments without authorities' intervention and this technological advancement can change a lot of industries and IoT is one of them. Cloud computing and big data are the disruptive technologies that IoT has leveraged to deal with its limitations since inception and blockchain is considered to be the best technology. The authors focus on the relationship between IoT and blockchain, investigate challenges in IoT applications and survey the most relevant studies to analyse the potential of blockchain in IoT.

Makhdoom et al. (2018) analyse some of the consensus protocols in Blockchain while evaluating challenges in Transaction validation and why they are still not sufficient in Blockchain-implemented IoT

- *Bhavraaj Singh is currently pursuing bachelor's degree program in computer science engineering in Vellore Institute of Technology, India, PH-9930380717. E-mail: singhbhavraaj@gmail.com*
- *Priyabrata Pradhan is currently pursuing bachelor's degree program in electronics and computer engineering in Vellore Institute of Technology, India, PH-7809178745. E-mail: priyabrata237@gmail.com*

solutions. Bitcoin has played its part to change the decentralized payment mechanism without third party intervention and by saving the time and transaction fee in verification in comparison to traditional banking systems. Blockchain is the original technology of bitcoin and designed only for financial transactions. Cryptographic security and fault tolerance benefits of decentralized architecture like data integrity, anonymity, and authentication have led to improved focus on blockchain from security experts and researchers globally to resolve privacy and security problems of IoT. But scalability issues due to huge blockchain size, network expansion, and latency in confirmation are some of the limitations. It is important to address the issues like lack of IoT-oriented validation standards, insecure integration, and absence of consensus protocols.

Panarello et al. (2018) present a complete survey on Blockchain integration with Internet of Things. This study is aimed to analyse the recent research trends about the use of Blockchain technologies and approaches in its implementation on IoT. Considering the related work, this paper has found different novelties like – (1) It consists of several application domains while organizing the literature available as per the categorization, (2) There are two usage patterns – data management and device manipulation, and (3) It covers the development status of some current solutions. The authors also cover some of the major challenges of the research community in integrating Blockchain smoothly into IoT and explain the next research path and open issues. Finally, they also explain a survey on recent use cases of Blockchain. This research is based on a complete survey on IoT and Blockchain.

3 RESEARCH QUESTIONS

- Can Blockchain Provide the Security, Scalability & Privacy IoT Needs?
- How to secure IoT with Blockchain?
- Is Blockchain The Right Solution For IoT Security Challenge?

3.1 METHODOLOGY

Blockchain is known for its integrated security in its design to fulfill important security needs of IoT. Its features like transparency, immutability, data encryption, auditability, and operational resilience are capable of solving a lot of architectural issues of IoT. On the other side, the IoT connects smart devices together to gather data and make smart decisions. But there are security issues making it vulnerable to security breaches. In order to find the answers of above research questions and potential solutions of current privacy issues with IoT payment systems, we had to do a detailed research on the concerned subject matters. To find the reliable solutions and current trends in the field of blockchain and IoT, we used trusted sources like news portals, current research papers, journals, studies conducted by the researchers, etc.

3.2 Can Blockchain Provide the Security, Scalability & Privacy IoT Needs?

According to Garner, there would be over 20.4 billion IoT devices to be installed by 2020, while BI Intelligence predicted around 24 billion devices. IDC forecasted around 30 million connected devices to be installed by 2020. To further increase optimism about IoT devices, HIS Markit expected over 125 billion IoT devices by 2030 after surveying over 5000 industry experts, data scientists, financial experts, and analysts. IDC expected the revenue from IoT devices much earlier to cross $537 billion by 2019 end, and McKinsey & Co. predicted the IoT revenue to cross $11.1 trillion worldwide by the year 2025.

All those industry experts expected IoT platforms to analyse data for important information which can be transmitted between devices for smart actions before making all such predictions. They expected improved efficiency, unmatched user experience, and greater automation at the end. Along with the manual process, the IoT is also optimizing and translating them as per the digital world and being able to transfer a huge volume of data. Several smart apps have been developed for sharing of information and they have improved the quality of life and management of services with the help of digitization.

IoT growth has been improved to a great extent thanks to its centralized architectures like the ones in cloud computing. But there are some challenges related to privacy and transparency come forward

as centralized network users don't have any idea about where and how the data they share is going to be used. It is important to address such challenges for IoT to reach the acceptance levels predicted by some research reports.

In a centralized architecture, traditional IoT systems simply relay the data from a device to the cloud where data is analysed and processed and then sent to the IoT device back.

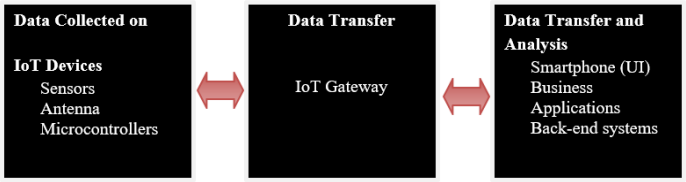

Fig 1 – Data Collection and Transfer Process in IoT Systems

The problems will arise when billions of devices are connected in IoT networks which will make the connection very slow and costly while compromising security at the same time. It will happen for checking and authenticating each of billions of micro-transactions to be processed across connected IoT devices.

Blockchain networks have already been through this problem where transaction verifications have been delayed significantly due to scalability issues. For example, Ripple has the limit of only 1500 transactions per second and Bitcoin is even worse, with only 7 tps. The data these networks can process is not even a part of data that current IoT devices produce. There is always a risk of vulnerability to hacking attacks and data leaks when such a huge volume of information is at stake. It might happen especially when devices are at stake of cyberattacks and where a device is connected to a network. According to NEC [14], a robust blockchain solution is needed to address all these challenges.

3.3 Is Blockchain the Right Solution for IoT Security Challenge?

Digital transformation is such a big leap for any business but it comes with its challenges. Adopting IoT for payments is a part of the process but there are several security issues that come as hurdles to make it a smooth transition. Blockchain is one of the emerging solutions for IoT payments and has become one of the important IoT trends of the modern area as it becomes a trusted security measure. Here are some of the solutions Blockchain can provide for IoT security challenges [15] -

Design – Blockchain is the synonym of security as it is designed on cryptographic algorithms. Every block is hashed in a network to the succeeding block and one cannot replace an intermediate block. Hence, this technology is the best solution for data security on IoT networks and devices in terms of design.

Tracking IoT devices – Blockchain technology can record and monitor communication between the devices which have been connected. It provides access to the data on IoT's activity log. In addition, it tracks and blocks unauthorized access or suspicious login attempts to the records.

Data Storage – Since IoT devices and networks handle a huge amount of business data, data security is a major concern. Because of decentralized nature, blockchain keeps an unalterable data record and it can easily protect and control communication in the system. With this technology, data protection consists of IoT networks and is no longer limited to cryptocurrency.

Secure messaging – Blockchain ensures security in IoT device messaging with smart contracts and robust security standards. Blockchain also provides the same security for ecommerce and online transactions.

Minimal human intervention – The human intervention increases the risk of errors in data inputs, data thefts, data loss, and unauthorized changes in any IoT device. Blockchain can eliminate human intervention even for logins and passwords. Instead, it can generate an encrypted identity for every device that can be verified on its distributed ledger.

Transparency

Due to decentralized features, blockchain improves transparency and trust while tracking all the connected IoT devices. It can help create a completely resilient system which is not easy to compromise.

3.4 How to Secure the Internet of Things (IoT) with Blockchain?

Blockchain technology is a revolutionary solution for privacy, reliability, and scalability issues of IoT devices. Blockchain can track billions of connected IoT devices, process transactions and coordinate between devices, and provide great savings to the manufacturers of IoT devices. The decentralized nature of blockchain could bring a more resilient IoT ecosystem without any single point of failure. Consumer data can be more secured with cryptographic algorithms in blockchain.

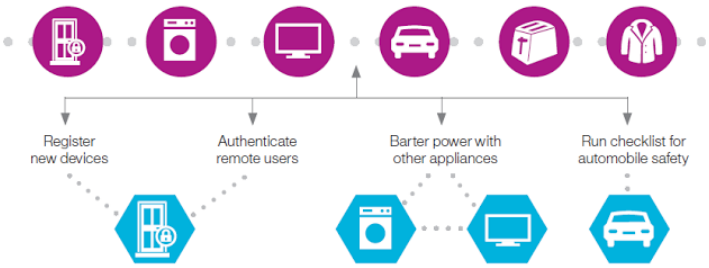

Fig. 2 – Blockchain as Distributed Ledger for IoT transactions [16]

The malicious files and attackers cannot manipulate tamper-proof ledger as it is not placed in any central location. So, it is not possible to plan man-in-the-middle attacks because of absence of any single thread of communication. Hence, blockchain makes P2P, trust less messaging that has really proven its worth in financial services with cryptocurrencies. It eliminates third-party brokers for guaranteed P2P payment services. The autonomous, decentralized, and trust less natures of blockchain are the reason why it is the best solution for IoT security issues. It is obvious that industrial IoT technologies have been the first to adopt blockchain.

Blockchain can store immutable records of smart devices in an IoT network. This feature eliminates centralized authority with autonomous smart device functionality. This way, blockchain serves several purposes of IoT that were once difficult or even impossible. Blockchain provides trust less, secure messaging between IoT devices. Blockchain exchanges messages between the devices just like the bitcoin network processes financial transactions. Smart contracts will be used to verify the transaction between two parties to proceed with message exchanges.

Similarly, in the agriculture sector, it is possible to detect crop conditions to control the irrigation system and flow of water. In oil platforms, smart devices can adjust functioning on the basis of data given on weather conditions. Autonomous smart devices can conduct financial transactions or exchange data without having a centralized broker. Blockchain nodes verify transactions without having to depend on any centralized authority to make this autonomy possible.

In a manufacturing unit, smart devices can place orders to repair its parts when needed, without any centralized party or human intervention. In a truck fleet, smart vehicles can send timely reports of the parts which need immediate replacement after coming back to the workshop. Since blockchain can hold a completely trusted and decentralized ledger of all genuine transactions that are taking place in the network, it can fulfil several regulatory and compliance needs in industrial IoT devices without dependence on any centralized body [16].

4 RESULTS

Considering the above solutions, blockchain comes with great expectations to revolutionize the current IoT solutions. It is the right time to address the challenges in integration of Blockchain with IoT devices. The adoption of regulations is important for the inclusion of IoT and blockchain in government infrastructures. The adoption of blockchain would enhance the interaction between companies, governments, and the common public. Consensus will also be important for including IoT in distribution and mining processes. Along with the storage and scalability implications, there is also a lack of research to ensure the privacy and security of blockchain and IoT.

The use of IoT devices will greatly increase with the integration of blockchain due to its decentralized nature and improved confidence about its security measures. This paper presents an in-depth analysis of major challenges and solutions of blockchain in IoT and the ways to make them work together. We found some important points on how blockchain can improve IoT solutions. We have also evaluated the feasibility of blockchain integration on IoT.

It is evident that blockchain and IoT integration is a relatively new concept but there have been several studies conducted on the use of this technology to improve IoT security in different ways [11]. IoT can also be secured with blockchain in many use cases. The IoT de-

vices can help virtually every traceability application. For example, sensors can provide data about the distribution of the product. Similarly, blockchain can empower many applications to digitize the world by giving recorded data. Blockchain can provide data reliability, authenticity, distributed identity, and authorization options while eliminating central authorities. Blockchain can even make cities smart while ensuring security. Despite so many benefits, there are still some challenges with blockchain like compliance issues, storage, scalability, etc. that should be addressed.

5 CONCLUSION

With distributed network design, ability to sustain fault tolerance, self regulations, and autonomy, and decentralized nature, blockchain has become a revolutionary technology for IoT payment systems. But there are some open challenges in recent research that should be considered and resolved to make the most of Blockchain. A financial platform is much needed for IoT to expand and complement its support for Machine-to-Machine and Peer-to-Peer communication with decentralization part of blockchain.

Blockchain is a platform that is secure, anonymous, and immutable which enables instant micro-transactions with minimal transaction fees. In this paper, we examine the ways blockchain can provide scalable and trusted platforms to IoT payment systems and also evaluate their optimization opportunities and advantages. It is true that further improvements are needed for blockchain to be completely effective for IoT. But it is still a promising technology with several existing use cases.

REFERENCES

[1] Ashton, K., 2009. That 'internet of things' thing. *RFID journal*, *22*(7), pp.97-114.

[2] Sundmaeker, H., Guillemin, P., Friess, P. and Woelfflé, S., 2010. Vision and challenges for realising the Internet of Things. *Cluster of European research projects on the internet of things, European Commision*, *3*(3), pp.34-36.

[3] Gubbi, J., Buyya, R., Marusic, S. and Palaniswami, M., 2013. Internet of Things (IoT): A vision, architectural elements, and future directions. Future generation computer systems, 29(7), pp.1645-1660.

[4] Miraz, M.H., Ali, M., Excell, P.S. and Picking, R., 2015, September. A review on Internet of Things (IoT), Internet of everything (IoE) and Internet of nano things (IoNT). In *2015 Internet Technologies and Applications (ITA)* (pp. 219-224). IEEE.

[5] Zhang, Y. and Wen, J., 2017. The IoT electric business model: Using blockchain technology for the internet of things. *Peer-to-Peer Networking and Applications*, *10*(4), pp.983-994.

[6] Sheng, X., Tang, J., Xiao, X. and Xue, G., 2013. Sensing as a service: Challenges, solutions and future directions. *IEEE Sensors journal*, *13*(10), pp.3733-3741.

[7] Strugar, D., Hussain, R., Mazzara, M. and Rivera, V., 2018. M2m billing for electric autonomous vehicles. *arXiv preprint arXiv:1804.00658*.

[8] Rykowski, J. and Cellary, W., 2020. Anonymous Pico-Payments for Internet of Things. In *Securing the Internet of Things: Concepts, Methodologies, Tools, and Applications* (pp. 1299-1311). IGI Global.

[9] S. Popov, "The Tangle," IOTA, Oct. 2017. [Online]. Available: https://iota.org.

[10] Ensor, A., Schefer-Wenzl, S. and Miladinovic, I., 2018, December. Blockchains for IoT payments: a survey. In *2018 IEEE Globecom Workshops (GC Wkshps)* (pp. 1-6). IEEE.

[11] Reyna, A., Martín, C., Chen, J., Soler, E. and Díaz, M., 2018. On blockchain and its integration with IoT. Challenges and opportunities. *Future generation computer systems*, *88*, pp.173-190.

[12] Makhdoom, I., Abolhasan, M. and Ni, W., 2018, January. Blockchain for IoT: The challenges and a way forward. In *ICETE 2018-Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*.

[13] Panarello, A., Tapas, N., Merlino, G., Longo, F. and Puliafito, A., 2018. Blockchain and iot integration: A systematic survey. *Sensors*, *18*(8), p.2575.

[14] NEC, 2020. *Can Blockchain Provide the Security, Scalability & Privacy IoT Needs?* Available at - https://www.nec.com/en/global/insights/article/2020022523/index.html

[15] OrangeMantra. (2019) *Is Blockchain The Right Solution For The IoT Security Challenge*, *Orangemantra.com*. Available at: https://www.orangemantra.com/blog/is-blockchain-the-right-solution-the-for-iot-security-challenge/ (Accessed: 22 April 2021).

[16] Banafa, A. (2016). *How to Secure the Internet of Things (IoT) with Blockchain*. DATAFLOQ. Retrieved 22 April 2021, from https://dataflog.com/read/securing-internet-of-things-iot-with-blockchain/2228.