IOT Ecosystem with Blockchain and Smart Contracts

Maneesha Poluri, Abhishek Kumar, Sunandha Allam , K.V.D.Kiran

Abstract— An engaging element of blockchain technology is smart contracts. A smart contract is a piece of code that keeps running over the blockchain upon execution to encourage and authorize an understanding between any unknown entities without the concept of trust and intrusion of a third party. Internet of Things(IOT), basically communication among digital devices gains more security by using smart contracts concept which indirectly relies on blockchain technology. This publication will direct an orderly mapping examination to gather a complete exploration significant to the concept of smart contracts in a specialized point of view. The point of doing as such is to distinguish ebb and flow investigation on themes and difficulties for lateral examinations when this concept is explored. We explored 26 publications from various logical databases. The outcomes demonstrate that around 66% of the papers center around recognizing and handling smart contract issues. Four key issues are distinguished, to be specific, systematizing, security, protection and execution issues. The remaining paper centers around applications or other subjects which are related to smart contracts. Holes that should be tended to in future research investigations are mentioned.

Keywords: Internet of Things, Blockchain, Smart contracts

INTRODUCTION

Smart contracts based on the technology, blockchain has provoked enthusiasm among different ventures and shareholders, bringing about the technology being received because of the focal points it showcases, by taking into account the mechanization of certain, executable advanced procedures among the gatherings included. Previous decade had shown a huge technological achievement in IOT as the Internet of Things (IoT) encountered a comparable flood in enthusiasm because of the mechanization utilities it encourages. Incorporating such Iot with latest advances like blockchain and smartcontract technologies[1], we can empower an evident and executable robotization of physical procedures. For instance, look into the utilization instance of some landowner who might want to: (I) robotize a way towards giving access to land and different products; (ii) screen inhabitants' use of wares and administrations; and (iii) mechanize works and assignments to look after the land. It is beneficial for the proprietor to characterize smart contracts with distinctive gatherings required to guarantee that they would certify to keep their finish of the ascension. For example, consider that a contract may express that if lease is not paid on time, at that point the inhabitants are consequently bolted out. For this the smart contracts needs the cooperation of the IoT gadgets included (e.g. a smart bolt). Besides, the proprietor and diverse occupants may, occasionally, likewise need to change certain usefulness. For instance, the landowner might need to execute a vast bolt out on a measure of time for every smart bolt if various endeavors are not useful. The arrangement along with these lines should take into account the end IoT rationale to be settled and characterized inside the contract, to reinvent with no human intercession on the gadgets when smart contract enters the play. Utilization case like this could turn into a real scenario, once IoT gadgets are coordinated with blockchain frameworks and give re programmability dependent on the substance of these contracts.

1.1 Key Contribution

In recent years, many researchers who are keen about this integration started digging deeper and found some interesting facts. Konstantinos Christidis[1] opined that the combination of blockchain and Internet of Thing is powerful and this combination will be responsible for invention of many innovative distributed applications. Doug Simon[2] used wireless devices such as Sun ™ Small Programmable Object Technology (SPOT) to verify this security and G Wood[3] had introduced a protocol where one can implement a node on ethereum network. K. Bharghavan[7] in his work outlined a verification based framework for achieving secured runtime and appropriate functioning of smart contracts belonged to ethereum whereas M.Samaniego[5] verified the performance of blockchain on virtual digital devices. J. Yli-Huumo [15] in his review paper put forward that till date, 80% of the research work is carried out on the things that rely on blockchain like bitcoin, smart contracts and only 20% of the work actually focussed on the true blockchain technology.

Revised Version Manuscript Received on March 08, 2019.

Maneesha Poluri, Students, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh.

Abhishek Kumar, Students, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh.

Sunandha Allam, Students, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh.

Dr.K.V.D.Kiran, Professor, Department of Computer Science and Engineering, Koneru Lakshmaiah Educational Foundation, Vaddeswaram, Guntur District, Andhra Pradesh.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

W. Egbertsen [13] in his work proved that paper contracts are not at all recommended as the alternative of ethereum smart contracts and also identified the importance of blockchain technology on which smart contracts rely on.

2. SMART CONTRACT CONCEPT

The term was coined by Nick Szabo, a computer scientist and cryptographer, in 1996. Szabo claimed that smart contracts can be realized with the help of a public ledger. Blockchain can be a pioneering technology to realize these smart contracts. Indeed, Blockchain 2.0 came into existence exclusively for smart contracts.

Szabo correctly anticipated the necessity of smart contracts and his idea approximately matches to the right use of crowdfunding platforms without trust.

2.1 Bitcoin

Bitcoins are completely decentralized, peer-to-peer, permission less cryptocurrency put forth in 2009. Decentralization refers to no central party for ordering or recording anything, peer-to-peer means software that runs on machines of all stakeholders to form the system and permission less means that anyone can join the bitcoin network and perform transaction. But the question arises when multiple people joining into network and how to ensure security in transaction. Bitcoin also considers smart contract concept where we need not to trust on others. But we call this smart contract as Rootstock and we can consider it as bitcoin's blockchain.

2.2 Ethereum

Initially, before smart contracts crowdfunding platforms are in existence. The major disadvantage of this is we need to trust third party service like 'KickStarter' and the major reason why blockchain is evolved is due to lack of trust. So smart contracts are invented, and these platforms perform everything without third party interference. One such great reputed platform for smart contracts is the Ethereum. Generally, here contract is written in a code which is available to all the stakeholders, the supporters and the product team. If we imbibe the code in hash functions, everyone can verify the code, but no one can tamper the code. If certain goals of the project are reached, then the code automatically transfers the money from supporters to the production team. If the project goals(contracts) fail, then the code can transfer the money back to the supporters.

3. BLOCKCHAIN

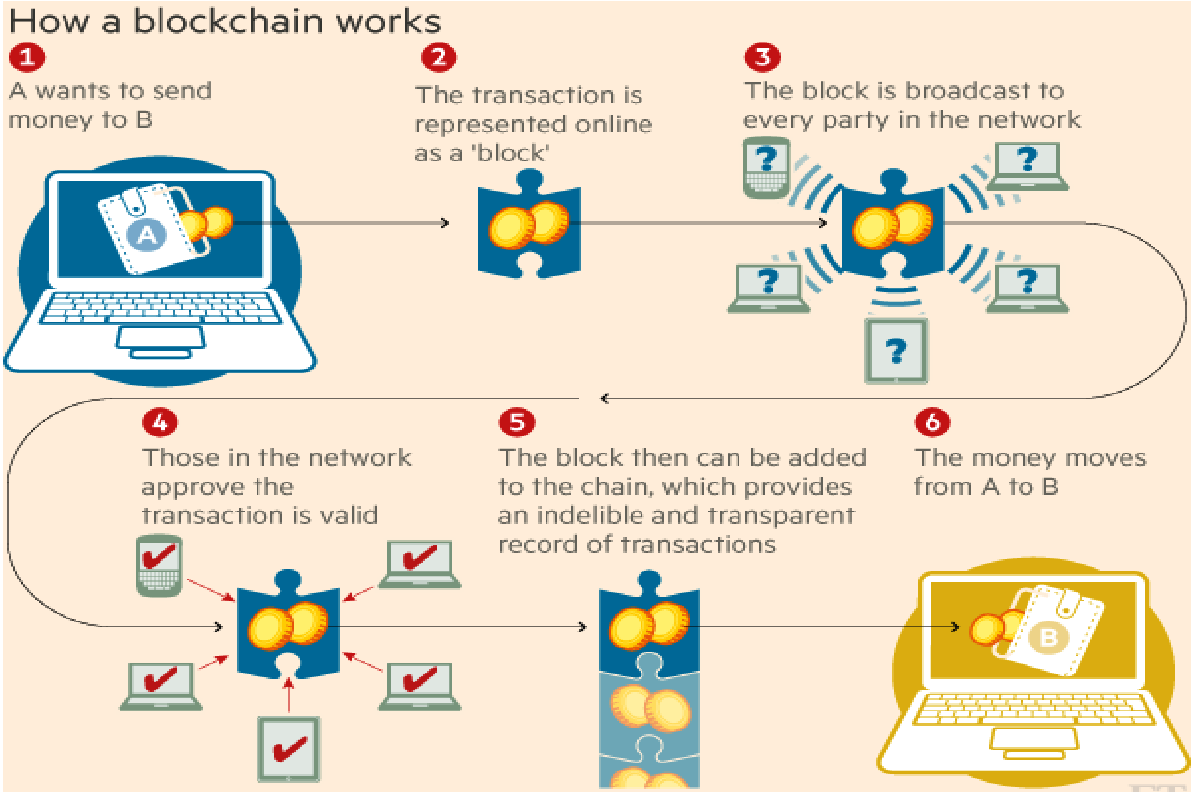
How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B

figure 1.1 : Working of a Blockchain

Blockchain can possibly drastically increment both the security and level of computerization of specific information exchanges (figure 1.1). The technology takes into consideration the formation of individual squares of information in a type of a chain. As each new square is added to the last, it frames what is, generally, a computerized record containing all the data at any point added to the blockchain.

Since the information on each new square is halfway ascertained from data hung on the past square in the blockchain, with the end goal to adjust a square, an unapproved individual would need to change the data on every one of the squares connected to it to keep the change from being quickly taken note. On account of a cryptocurrency blockchain, for instance, this may well mean changing each and every square on the chain.

The extremely energizing thing about blockchain technology is that it works as a shared decentralized system. In that capacity a system, blockchains don't require any controlling gathering to work. This has tremendous ramifications for huge numbers of the business forms we as a whole depend on today.

More than some other precedent, bitcoin and has demonstrated that it is conceivable to make blockchain based arrangements that enable us to circumnavigate intense organizations, which as of not long ago have had a restraining infrastructure on these procedures.

Another key factor in this decentralized methodology is that every one of the associates or 'hubs' engaged with the system must concede to whatever progressions are to be made. So should a programmer or other unapproved party endeavor to roll out an improvement to the computerized record without authorization, alternate hubs will oppose this change and keep the information from being modified.

The principle way somebody would be able to modify the blockchain is gain command over most of the hubs on the system in the meantime with the end goal to effectively total the change. While examining how troublesome this would be simply remembering that every hub has its very own remarkable access key code too.

Just to give you a thought of the monstrosity of the assignment, as of May 2016, Ethereum's system had 25,000 dynamic hubs implying that any endeavor to change information along these lines would be beside incomprehensible.

4. THE FUTURE RESULT OF SMART CONTRACTS AND INTERNET OF THINGS ON BLOCKCHAIN

According to Solely, there is no ambiguity that IOT along with smart contracts on blockchain will be useful in mechanical utilize cases. Also, keeping that in mind, the Industrial Internet Consortium combined with Object Management Group is taking a gander at conceivable institutionalization of appropriate contract systems.

He said that at present there are no proper standards however, what these standards could do is understood. Likewise, he said that he knows of a few ventures which are trying out different things with IoT smart contracts, they are not yet in an affirmed trial platform inside the Consortium. However, he expects that day is ahead.

"Effects are intense than you might suspect," Soley supposed. "Contemporary time, one anticipates to understand some fascinating proving grounds with subjective frameworks, artificial intelligence and Deep learning. I ponder to witness main blockchain measures in the following year and a dispersed agreement platform coming forth."

5. TROUBLE BY SMART CONTRACTS ON BLOCKCHAIN

Decentralized autonomous organization, a transparent shareholders corporation has established interest around blockchain. In that occurrence, the DAO was attempting to give investment subsidize to all the participants and this was propelled by the Ethereum blockchain and also crowd funded by means of tokens deal in May 2016.

In later part of 2016, obscure hackers attacked and took away more than 30% of the resources by finding an overlooked vulnerability in algorithms. That was the time a questionable "fork" of the Ethereum blockchain was incited. Another fork moved back the record, reorganizing it letting it to show up the occasion never occurred and ostensibly reestablishing the subsidizing to that organization. Nonetheless, the individuals who couldn't help contradicting the move kept up a forked blockchain known as Ethereum Classic. The bug that is popularised as ICON’s 2018 bug enabled all the users including the inventor of smart contracts to enable and disable any transactions. This caused an unimaginable loss of approximately $800+ millions but is considered as little when compared to 2016 crisis. But people think smart contracts faced only 3% failure in its tenure and usage but the fact is only percentage is small and the loss associated with it is some thousands of million dollars.

6. CONCLUSION

Blockchain, an upcoming technology being a distributed database stores all the transactions which will happen in a system. The principle highlight of blockchain is that it provides path without the concept of mutual trust for gatherings to convey information between one another without intrusion of an outsider. Diverse appropriated applications past digital forms of money can be sent over blockchain. One of these applications is smart contracts. Smart contracts are executable codes which execute and authorize a communication between any untrusted parties. Ethereum is at present in the highest position among the widely recognized blockchain stages involved in the creation of smart contracts. To comprehend current points on smart contracts, we chose to lead a deliberate mapping study. The principle point of this orderly mapping examination was to recognize and delineate regions identified with smart contracts. Thusly, we were capable recognize inquire about holes that should be tended to in future investigations. The focal point of this investigation was on smart contracts from a specialized perspective. Accordingly, we avoided thoughts with alternate points of view (e.g., publications with a financial viewpoint). We extricated 26 publications searching in various databases. We found that most papers were based on exploring the new concept of smart contracts and dealing with its concerns.

We assembled the concerns in the form of some classifications, to be specific, classifying, security, protection and execution issues. Whatever is left of the papers center around proposing applications or examining other related themes regarding smart contracts.

7. FUTURE SCOPE

IOT will continue growing and may reach 30 billion by 2022 and these communicate through internet. Therefore security and privacy of the data is the major challenge that is going to hit by all the humans in the near future and blockchain technology servers a solution in terms of its distributed environment and the simplicity in its public ledger, a record where each user in the network can look after. Another challenge the world facing today is lack of trust in paper contracts and smart contracts does it better without relying on trust and third party interference. If the platforms such as Ethereum are economical then these smart contracts will have high impact on digital devices.

REFERENCES

1. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things,” IEEE Access, vol. 4, pp. 2292–2303, 2016.
2. D. Simon, C. Cifuentes, D. Cleal, J. Daniels, and D. White, “Java™on the bare metal of wireless sensor devices: The squawk java virtual machine,” in Proceedings of the 2Nd International Conference on Virtual Execution Environments, ser. VEE ’06. New York, NY, USA: ACM, 2006, pp. 78–88. [Online]. Available: http://doi.acm.org/10.1145/1134760.1134773
3. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger,” Ethereum Project Yellow Paper, vol. 151, 2014.
4. J. Ellul and K. Martinez, “Run-time compilation of bytecode in sensor networks,” in Sensor Technologies and Applications (SENSORCOMM), 2010 Fourth International Conference on. IEEE, 2010, pp. 133–138.
5. M. Samaniego and R. Deters, “Hosting virtual iot resources on edge-hosts with blockchain,” in 2016 IEEE International Conference on Computer and Information Technology (CIT), Dec 2016, pp. 116–119.
6. S. Huh, S. Cho, and S. Kim, “Managing iot devices using blockchain platform,” in 2017 19th International Conference on Advanced Communication Technology (ICACT), Feb 2017, pp. 464–467.
7. K. Bhargavan, A. Delignat-Lavaud, C. Fournet, A. Gollamudi, G. Gonthier, N. Kobeissi, N. Kulatova, A. Rastogi, T. Sibut-Pinote, N. Swamy, et al., “Formal verification of smart contracts: Short paper," in Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security, pp. 91-96, ACM, 2016.
8. K. Delmolino, M. Arnett, A. Kosba, A. Miller, and E. Shi, “Step by step towards creating a safe smart contract: Lessons and insights from a cryptocurrency lab," in International Conference on Financial Cryptography and Data Security, pp. 79-94, Springer, 2016.
9. V. Morabito, “Smart contracts and licensing," in Business Innovation Through Blockchain, pp. 101- 124, Springer, 2017.
10. A. Lewis, “A gentle introduction to smart contracts," Available online at: https://bitsonblocks.net/2016/02/01/a-gentle-introduction-to-smart-contracts/
11. G. Wood, “Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, 2014.
12. K. Christidis and M. Devetsikiotis, “Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292-2303, 2016.
13. W. Egbertsen, G. Hardeman, M. van den Hoven, G. van der Kolk, and A. van Rijsewijk, “Replacing paper contracts with ethereum smart contracts," 2016.
14. W. Banasik, S. Dziembowski, and D. Malinowski, “Efficient zero-knowledge contingent payments in cryptocurrencies without scripts," in European Symposium on Research in Computer Security, pp. 261-280, Springer, 2016.
15. J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, “Where is current research on blockchain technology?” a systematic review," PloS one, vol. 11, no. 10, p. e0163477, 2016.
16. K.V.D.KIRAN, “MULTI CROSS PROTOCOL WITH HYBRID TOPOGRAPHY CONTROL FOR MANETS”, Journal of Theoretical and Applied Information Technology, 2017. Vol.95. No.3, ISSN: 1992-8645.
17. K.V.D.KIRAN, “Integrated Distributed Architecture to Integrate Wireless Sensor Networks (WSN) with Grid for Healthcare,” International Journal of Bio-Science and Bio-Technology”, Vol.7, No.3 (2015), pp.243-250, ISSN: 2233-7849 IJBSBT.
18. K.V.D.KIRAN, “A Critical study of information security risk assessment using fuzzy and entropy methodologies,” International Journal on Computers and Communications”, Pages: 17-22, Vol1, Issue1, Dec-,12, ISSN: 2319 – 8869.
19. K.V.D.KIRAN, “Literature Review on RisK Literature Review on Risk and their Components” International Journal for Research in Emerging Science and Technology (IJREST) “,Volume-1, Issue-6, November 2014”, (e-ISSN 2349-7610).
20. K.V.D.KIRAN, “Performance Analysis of Layered Architecture to Integrate Mobile Devices and Grid computing with a resource scheduling algorithm”, IEEE CS’07, SIVAKASI, TAMIL NADU,India.
21. K.V.D.Kiran, “Risk Assessment in Distributed Banking System,” International Journal of Applied Engineering Research(IJAER)”, ISSN 0973-4562 Volume 9, Number 19 (2014) pp. 6087-6100.
22. K.V.D.Kiran, “Analysis and Classification Scheme of Risk Assessment Miniatures placed on Different Criteria for Reducing the Risk”, International Journal of Applied Engineering Research” pp.12069-12085, ISSN 0973-4562 Volume 9, Number 22 (2014).
23. K.V.D.Kiran, “Information Security risk authority in critical informative systems”,CSIBIG 2014.
24. K.V.D.Kiran ,"Survey on mobile malware analysis and detection", Volume 7, Issue 2.32 Special Issue 32, 2018, Pages 279-282, ISSN:2227524X.
25. K.V.D.Kiran ,"Authorization of data in Hadoop using Apache Sentry", Volume 7, Issue 3.6 Special Issue 6, 2018, Pages 234-236, ISSN:2227524X.