Blockchain Approaches to Secure Iot Data

Aditi M Joshi[1], Apexa J Bhavsar[2], Alok B Patel[3]
[1, 2, 3] Assistant professor, Dept of CE
[1, 2, 3]Swarrnim Start up and Innovation University, Gujarat, India

Abstract
In IoT, things process and exchange data without human intercession. Therefore, this full autonomy, these entities need to recognize and authenticate each other as well as to ensure the integrity of their exchanged data. Otherwise, they will be the target of malicious users and malevolent use. Decentralized Blockchian system with various implemetedplatforms which ensures a robust identification and authentication of devices. And protects the data integrity and availability.

Keyword: Blockchain, Decentralized network, Distributed network, Permissionless.

INTRODUCTION

Blockchains are immutable digital ledger systems implemented in a distributed fashion (i.e. without a central repository) and usually without a central authority. [1]

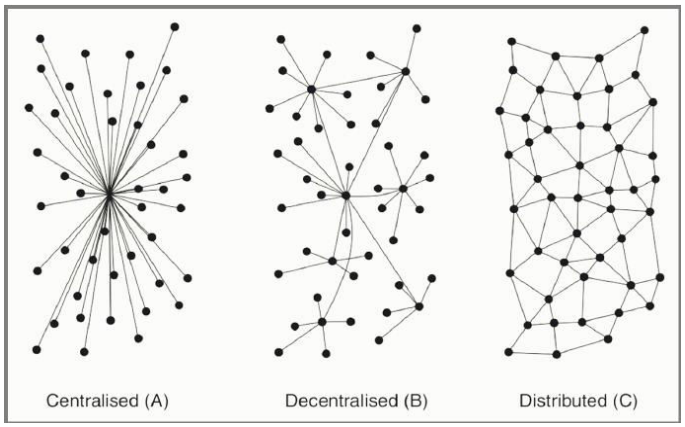

Figure1: Types of Networks

Centralized network—In case of a centralized network, we have a central network owner. The central network owner is a single point of contact for information sharing. The biggest issue with a centralized network is with a single central owner it also becomes a single point of failure. Further, with a single copy stored with the owner, every instance of access to the resource leads to an access issue with time.

Decentralized network—As for the decentralized network, the we have multiple central owners that have the copy of the resources. This eliminates the biggest problem of single point of failure with centralized network. With multiple owners, if a particular central node fails, the information can still be accessed from the other nodes. Further, with multiple owners the speed of access to the information is also reduced.

Distributed network—The distributed network is the decentralized network taken to the extreme. It avoids the centralization completely. The main idea for the distributed network lies in the concept that everyone gets access, and everyone gets equal access.

Background Theory

Types of Blockchain [2]

1. Permissionless (Public)
2. Permissioned (Private)

Bitcoin

Bitcoin is a cryptocurrency and a digital payment system, based on a public Blockchain. Each block of the Bitcoin Blockchain contains a strong hash of its transactions called merkle root stored in the header. Bitcoin uses PoW mechanism for block validation.

Ethereum

Ethereum is a public Blockchain that provides a cryptocurrency called Ether.

Smart contracts are executed by participating nodes using an operating system known as Ethereum

Virtual Machine (EVM)

The block size is shorter than in Bitcoin and the validation time, takes only 14 s compared to Bitcoin which takes 10 min.

Ethereum uses The Ethereum Greedy Heaviest Observed Subtree (GHOST) protocol for consensus and miners reward

For blocks' validation, Ethereum uses a PoW mechanism called Ethash.

Hyperledger Fabric

Hyperledger Fabric is an open-source permissioned Blockchain created by the Linux Foundation,more specifically by IBM.

Does not provide a cryptocurrency.

Hyper-ledger uses the Practical Byzantine Fault Tolerant (PBFT) as a con-sensus mechanism.

OPEN ISSUES ABOUT BLOCKCHAIN INTEGRATION WITH IOT

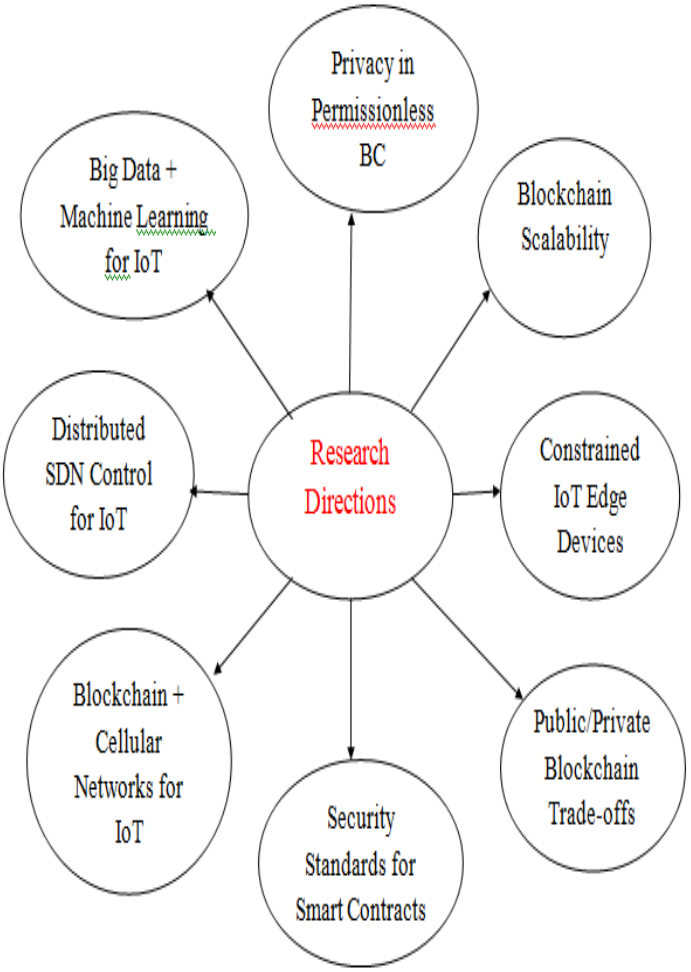

Figure: 2 Open Research Direction in Decentralizing the IoT through Blockchains. [8]

BLOCKCHAIN CHALLENGES

- Blockchain scalability
- Privacy in permissionless Blockchain
- IoT edge device constraints
- Security standards for smart contracts

CONCLUSION

Blockchains achieve immutable and secure records through distributed consensus algorithms. Therefore, Blockchains provide a “trustless" environment for record keeping, where no trust is required to be placed on any individual centralized entity.

Blockchains (with Ethereum/Hyperledger) are hailed as the potential solution to decentralizing the IoT.

REFERENCES:

I. Dylan Yaga (NIST), Peter Mell (NIST), Nik Roby (G2), Karen Scarfone "Blockchain Technology Overview" https://doi.org/ 10.6028/ NIST.IR. 8202, October 2018.

II. Mohamed Tahar, BadisHammia, Patrick Bellota,Ahmedserhrouchni "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT", Computers & Security , https://doi.org/10.1016/j.cose.2018.06.004 , Elsevier, June 2018.

III. SiamakSolat,Engie Lab Paris, France,“ RDV: An Alternative To Proof-of-Work And a Real Decentralized Consensus For Blockchain",2018 ACM ISBN 978-1-4503-6050-0/18/11,November 2018.

IV. Ming, Z., Yang, S., Li, Q., Wang, D., Xu, M., & Xu, K. Blockcloud: Empowering IoT Through a Service-centric Blockchain, https://icorating.com/ upload/whitepaper /V8ZSfbexTx6vkgbIahtBj1KA6k65jLG59j GSbDTT.pdf February 2018.

V. N. Rifi, E. Rachkidi, N. Agoulmine and N. C. Taher, "Towards using blockchain technology for IoT data access protection," 2017 IEEE 17th International Conference on Ubiquitous Wireless Broadband (ICUWB), Salamanca, 2017, pp. 1-5.doi: 10.1109/ICUWB.2017.8251003.

VI. MatevzPustiseka, Andrej Kosa, "Approaches to Front-End IoT Application Development for the Ethereum Blockchain" Selection and peer-review under responsibility of the scientific committee of the 2017 International Conference on Identification, Information and Knowledge in the Internet of Things (IIKI2017).10.1016/j.procs.2018.03.017

VII. Vaughan Emery-Founder and CEO, David Fragale-Co-Founder, Andrii Zamovsky - CTO and VP of Engineering, Peter Kinnaird-Chief Scientist, “The Secure Ledger of Things", v0.9.2, © 2019 Atonomi.

VIII. Muhammad Salek Ali, Massimo Vecchio, Miguel Pincheira,KoustabhDolui, Fabio Antonelli, and Mubashir Husain Rehmani,"Applications of Blockchains in the Internet of Things: A Comprehensive Survey", IEEE Communications Surveys & Tutorials, DOI 10.1109/COMST.2018.28869322018.

IX. Ethereum whitepaper, [Online] Available: github.com/ethereum/wiki/wiki/White-Paper.

X. Embark Framework, [Online], Available: https://github.com/iurimatias/embark-framework.

XI. Solidity Introduction to Smart Contracts, [Online], Available: http://solidity.readthedocs.io/en/develop/introduction-to-smartcontracts.html.

XII. Olivier Alphand, Michele Amoretti, Timothy Claeys, Simone Dall ’Asta, Andrzej Duda, et al..IoTChain: “A Blockchain Security Architecture for the Internet of Things”. IEEE Wireless Communications and Networking

Conference, Apr 2018, Barcelona, Spain. 2018. <hal-01705455>

XIII. M. Vucini˘c,´ B. Tourancheau, F. Rousseau, A. Duda, L. Damon, and R. Guizzetti, "OSCAR: Object Security Architecture for the Internet of Things," Ad Hoc Networks, vol. 32, pp. 3 – 16, 2015.

XIV. L. Seitz, G. Selander, E. Wahlstroem, S. Erdtman, and H. Tschofenig, "Authentication and Authorization for Constrained Environments (ACE)," Internet Engineering Task Force, Internet-Draft draft-ietf-ace-oauth-authz-07, Aug. 2017, work in Progress. [Online]. Available: https://datatracker.ietf.org/doc/html/draft-ietf-ace-oauth-authz-07.

XV. Chao Qu, Ming Tao ,Jie Zhang, Xiaoyu Hong, and Ruifen Yuan, "Blockchain Based Credibility Verification Method for IoT Entities", Hindawi Security and Communication Networks Volume 2018, Article ID 7817614, 11 pages https://doi.org/10.1155/2018/7817614, June 2018.