Decentralized Blockchain Based ISP Networks

[1]Rahul Mishra and [2]Pallavi K V
[1,2]Department of CSE AMC Engineering College, Bangalore, India.
[1]robom460@gmail.com, [2]pallu.gani@gmail.com

Article Info
Jenitta J and Swetha Rani L (eds.), *International Conference on VLSI, Communications and Computer Communication*, Advances in Intelligent Systems and Technologies,
Doi: https://doi.org/10.53759/aist/978-9914-9946-1-2_1

Abstract - This paper aims to point out the potential use, of Blockchain based decentralized computer networks in ISPs and how they promote a secure and privatealternative to today's centralized ISP networks.

Keywords - Computer Networks, Blockchains,Networking

I. INTRODUCTION

The current landscape of computer networking consists of a centralized model of operation i.e a centralized architecture. Some of the common pitfalls of centralized architecture are bottlenecks, difficulty in maintenance, high node failure rates etc.[1]

Most modern ISPs utilize this centralized network architecture to provide most of the internet services commonly seen today which also seem to encounter similar pitfalls in the form of outages, bandwidth issues etc. To overcome these pitfalls and provide better services to users the utilization of decentralizedBlockchain based solutions seem quintessential and which are further explored in this paper namely split into two sections: (1) Security in Blockchain based networks, (2) Censorship and Privacy.

II. SECURITY IN BLOCKCHAIN BASEDNETWORKS

How Security works on the Blockchain

To speak more on the secureness of Blockchain based decentralized networks we must delve into the complex cryptographic algorithms that it employs in order to encrypt data. The most popular and well-known algorithms to be utilized in prominent blockchains like the Bitcoin and Ethereum chainsare the Fig.1 shows SHA256 [2] algorithm and Keccak-256 [3] respectively. These algorithms make it nigh impossible or at the very least monumentally difficultfor reverse engineering stolen data from the chain, because decrypting alone requires magnanimous computing prowess to even attempt such a task.

Relevance with respect to ISP's & Networking

There have been many cases where traditional ISP's utilizing the centralized architecture have been compromised in the recent past, one such recent case is the Optus [4] data breach, which rendered almost 2.1 million entries of customer data exposed to malicious actors. The utilization of Blockchain based networks in ISP's could have easily prevented such an attack, even in the case of a data breach, decrypting the data by the hackers would be tough due to the power of the mentioned suite of encryption algorithms, that are by design irreversible. Thus rendering ISP's utilizing Blockchain based networks secure.

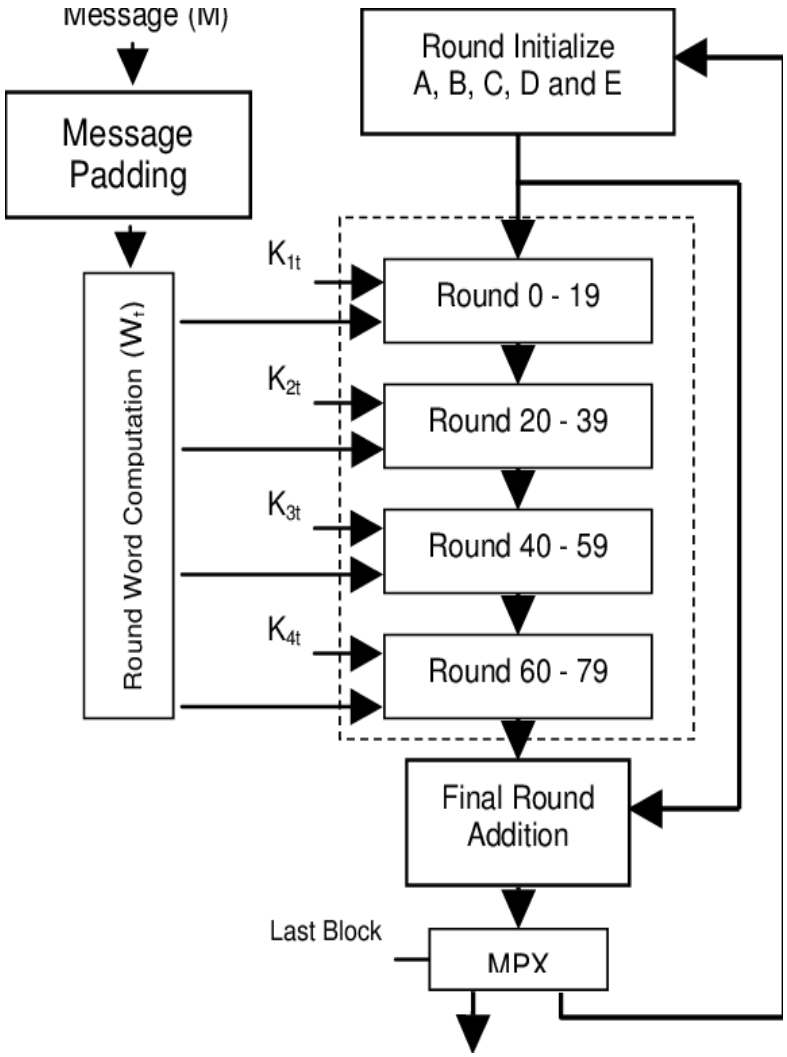

Fig 1. SHA Architecture

III. CENSORSHIP AND PRIVACY

Why is data availability important to ISP's?

To operate an ISP within any region or country, the provider must comply with certain government regulations. One such example is maintenance of activity logs to see what the users are doing on the network. Such regulations sometimes call for censorship of malicious data/information. Under an centralized architecture achieving censorship of data is very easy since all the data is available in centralized systems. This poses a risk to the privacyof consumers.

How Blockchain based ISP services can overcomecensorship and promote freedom of information, privacy

To explain more about this we must delve into howdata is stored inside a block that is a part of the chain. Data is stored as transactions within the blockchain [9]. This data can contain relevant information like name, IP, location etc. each block starting right from the Genesis i.e the first block contains information about all previous transactions or in this case network interactions. Hence to manipulate or censor data one must go through all the blocks in the network and change the data one-by-one. Even if one of the blocks is modified to display data that is censored, for example, blocking access to certain websites, the chain utilizes a consensus algorithm [10].

How Consensus Algorithms help preventcensorship

Most Prominent consensus algorithms are based onthe Fig.2 shows Two Generals [5] problem or the Fig.3 shows Byzantine Fault Tolerance [6] problem.

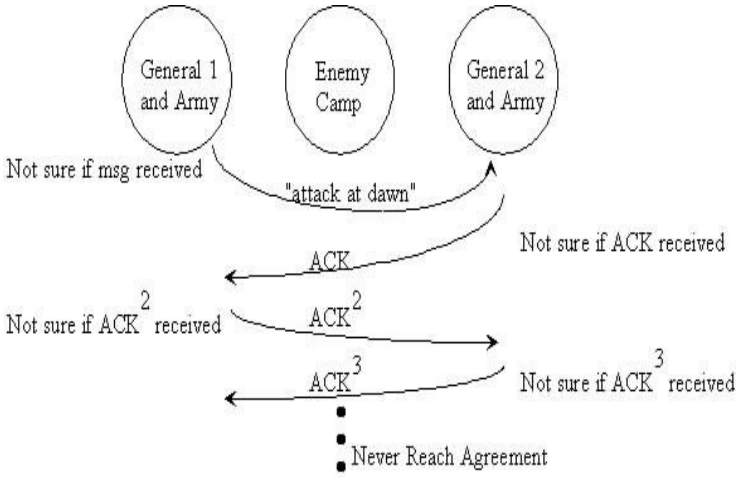

Fig 2. Two Generals Problem

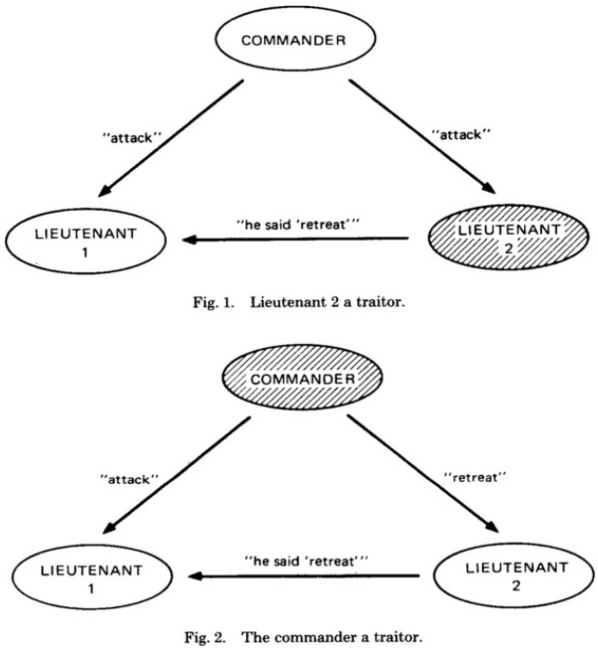

Fig 3. Byzantine Fault Tolerance Problem

Such algorithms or better known as consensus algorithms call for polling of data with all the respective nodes present in the network to check whether the data in a certain node matches with or is the same as data present in other nodes [7]. Suppose one node has a block with tampered data, the consensus algorithms will poll all the other nodes present in the ISP network which has adopted the Blockchain basednetwork architecture, if there is any inconsistency found within one of the nodes, the polling algorithm will consider the data present in the majority of the nodes to be valid i.e it will ignore the tampered node and replace the tampered node's data with the correct data from the valid nodes [8]. If there is such a case where the algorithm cannot reach consensus the faulty or tampered block will be discarded/ignored entirely.

IV. CONCLUSION

Efforts to make web services as well as the computer networks that support them secure has been going on since the dawn of the concept of computer networks. Security is one of the cornerstones of any system agnostic of what type of system it is, hence through the innovations that have taken place recently in the field of Distributed Systems, Networks and Blockchain technologies, a reliable and secure architectural model can be designed which helps tackle the ever-growing problem of privacy and security of data with 3rd parties such as ISPs. With the help of decentralized and disruptive distributed technologies like the Blockchain, the integrity of the data being produced/shared can be checked as well as the privacies of all parties involved in the network can be maintained with the help of the numerous Consensus algorithms. The benefits of such decentralized networks not only promote accountability of all parties involved, but also promote freedom of information and helps regulate unnecessary censorship of data (ex: Banned websites in certain regions). At the same time keeping the data secure by utilizing cutting edge Encryption algorithms. Which prevent malicious actors from reverse engineering/decrypting data stolen from such networks.

References

[1]. https://en.wikipedia.org/wiki/Centralized_database#Disadvantages

[2]. https://en.bitcoin.it/wiki/Block_hashing_algorithm

[3]. https://www.oreilly.com/library/view/mastering-ethereum/9781491971932/ch04.html#:~:text=Ethereum% 20uses%20the%20Keccak%2D256,Institute%20of% 20Science%20and%20Technology.

[4]. https://www.bleepingcomputer.com/news/security/opt us-confirms-21-million-id-numbers-exposed-in-data- breach/

[5]. https://en.wikipedia.org/wiki/Two_Generals%27_Problem

[6]. https://en.wikipedia.org/wiki/Byzantine_fault

[7]. M. H. Amini, “Decentralized operation of interdependent power and energy networks: Blockchain and security,” Blockchain-based Smart Grids, pp. 61–73, 2020, doi: 10.1016/b978-0-12-817862-1.00004-x.

[8]. B. S. Reddy and G. V. V. Sharma, “Optimal Transaction Throughput in Proof-of-Work Based Blockchain Networks,” The 3rd Annual Decentralized Conference on Blockchain and Cryptocurrency, Oct. 2019, doi: 10.3390/proceedings2019028006.

[9]. M. Hassan, D. Pesavento, and L. Benmohamed, “Blockchain-Based Decentralized Authentication for Information-Centric 5G Networks,” 2022 IEEE 47th Conference on Local Computer Networks (LCN), Sep. 2022, doi: 10.1109/lcn53696.2022.9843631.

[10]. F. Funk and J. Franke, “Matching in decentralized two-sided markets via Blockchain-based deferred acceptance,” 2021 3rd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), Sep. 2021, doi: 10.1109/brains52497.2021.9569823.