



Habib University
Fall Semester 2018

EE 424 - Data Communication & Networking

LCL Write-up Proposal

Choudhry Bilal Mazhar
Dhanani School of Science & Engineering
Electrical Engineering Department
Habib University, Karachi, Pakistan
cm00326@st.habib.edu.pk

Topic:

Enhancing Peer-to-Peer Connection Security in Blockchain Technology

Context:

Blockchain is a DLT – Digital Ledger Technology whose primary purpose is for book keeping against the traditional methods making the process cheaper, faster, secure and efficient. It is emerging as a secure form of advanced technology in order to ensure security and privacy in networking systems. The current research on Blockchain technology is being carried out for even more secured peer-to-peer connection and transaction. In Blockchain technology, a combined record of all the communication that is being done among two peers is recorded in the form of blocks, where each block stores the identification means of the previous block, time stamp as well as the transaction data. This sort of peer-to-peer connection is considered relatively more secure because upon once the block is build, no alterations can be done to the data that is stored in the blocks, unless more than half of the preceding blocks are modified.

Problem Statement:

As technology is immersing rapidly when it comes to Blockchain; cryptocurrency, smart tokens, smart contracts, smart property, financial services, energy transactions etc. Its security leakage opens rooms for many more work to be done in the same niche maintaining its security. On the one end, Blockchain technology is considered way securer than any given conventional peer-to-peer connection system, but at the same time, upon modifying more than half of the preceding blocks, the data in the succeeding block can be altered which breaches the security of any given peer-to-peer connection. In this paper, it will be pondered that how might we ensure the secure connection between two connections in the succeeding blocks.

Literature Review & Investigation Methodology:

Since Blockchain technology has wide applications in cryptocurrency, hence an example of cryptocurrency can be taken into account to study the performance of Blockchain. The Blockchain technology itself was invented by the inventor of first ever cryptocurrency Bitcoin, it is heavily misused for artificial pumping of various cryptocurrency prices by various investor groups.

To understand the connectivity mechanism, figure 1 can be referred below where it can be observed that it is a public Blockchain network where anyone can get involved in the transaction and can contribute to the computing/hashing power.

It can be understood by now that how the interest of majority contributors can affect the data in the network blocks and can be drawn artificially as per their networking desires.

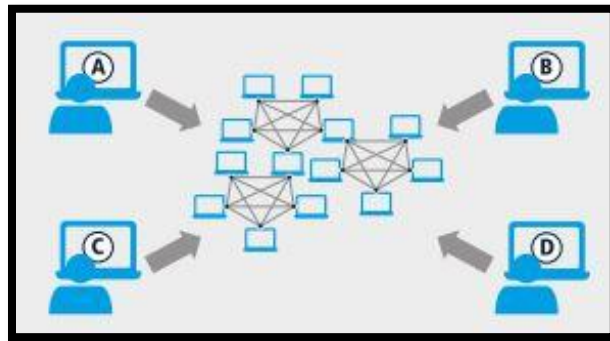


Figure 1: Blockchain network [2]

The architecture of Blockchain network is presented below, where there is a hash of a previous block in the succeeding block which enables the individual blocks to build a chain of blocks hence making it securer. But the problem still stays there, in-case if the data of first two preceding blocks is modified sequentially then, the whole data of all three blocks can be modified, which is a major drawback of Blockchain technology.

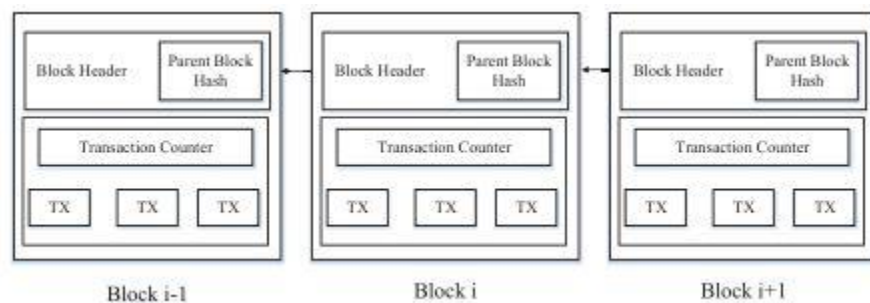


Figure 2: Architectural representation of Blockchain [4]

The individual block involves block header and block body. Block header includes a set of protocols that is to be followed. It also includes the threshold value of the potential hash code for comparison. Whereas, the block header involves a transaction counter which keep track of all the transactions.

The application of Blockchain technology does not only revolve around cryptocurrency in fact this technology is rapidly expanding in various sectors, including digital citizenship related data storage and access, logistical trade, retail, energy sector and in automobile industry [2].



Given its huge potential it is simultaneously important to address the key challenges, specifically the globally acknowledged '*51 percent attack*' that Blockchain technology faces at the current stage. In this paper, potential revision in the architecture of Blockchain's individual blocks would be done to ensure securer technology.

Reference:

- [1] J. Kogure, K. Kamakura, T. Shima, T. Kubo, "Blockchain Technology for Next Generation ICT". FUJITSU Sci. Tech. J., Vol. 53, No. 5, pp-53-61, Sept. 2017.
- [2] Blockchain in Logistics – Perspective on the upcoming impact of blockchain, Powered by DHL Trend Research, DHL Solutions and Innovations, 2018.
- [3] C. Holotescu, "Understanding Blockchain Technology and How To Get Involved". 14th International Scientific Conference E-learning and Software for Education, Apr. 19-20, 2018.
- [4] Z. Zheng, S. Xie, H. Dai, H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus and Future Trends". 6th IEEE International Congress on Big Data, 2017.
- [5] <https://pdfs.semanticscholar.org/f61e/db500c023c4c4ef665bd7ed2423170773340.pdf>