EE 424 – DATA COMMUNICATION & NETWORKING

LCL WRITE-UP MID REVIEW I

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

Topic:

Peer-to-Peer Connection Security in Blockchain Technology

Introduction:

The invention of block chain technology dates back to the year 2008. It was to record the transactions made by through the crypto currency, bitcoin. It is defined as an undeniably ingenious invention in a recent article [1]. The same article outlines and gives evidence of how this technology has become the main foundation of a new internet. That being said, it is worth mentioning that via Blockchain technology, the information can no more be copied instead it can only be distributed digitally [2]. Blockchain technology is distinguished in a way that it is a centralized operating technology where each node or network contributes in the transaction regardless of its computing power. The figure shows how the technology is decentralized. The Blockchain is made up of computing nodes. “Together they can create a powerful second-level network, a wholly different vision for how the internet can function.” [1]

The decentralization feature is advantageous because it doesn’t let the bitcoin be managed by one central authority; it works on a user to user basis thus giving power to its customers, as they can use and access the data while also being a part of the system.

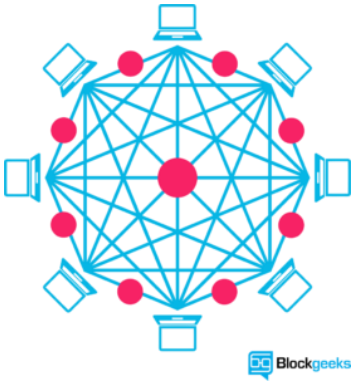

Figure 1: Blockchain network [1]

Blockchain Architecture & Fast Peer-to-Peer Transactions:

In Blockchain technology, user has the power to make the transaction and a copy is received not only by the person who the transaction is for but also people in bitcoin known as the bitcoin minors. This mechanism ensures that the transaction is taking place smoothly without any errors. The transaction records are public and thus, anyone can access it. This is called the Blockchain. This technology contains every single transaction going back to the first one called the 'genesis block'. The bitcoin minors look at all the transactions which have taken place, and have not been yet recorded, and make a block of those transactions and add it to the end of the transaction chain. As they do this they have to solve what is called as a "proof-of work puzzle". The bitcoin is made in a way that one minor can solve one puzzle in ten minutes on average.

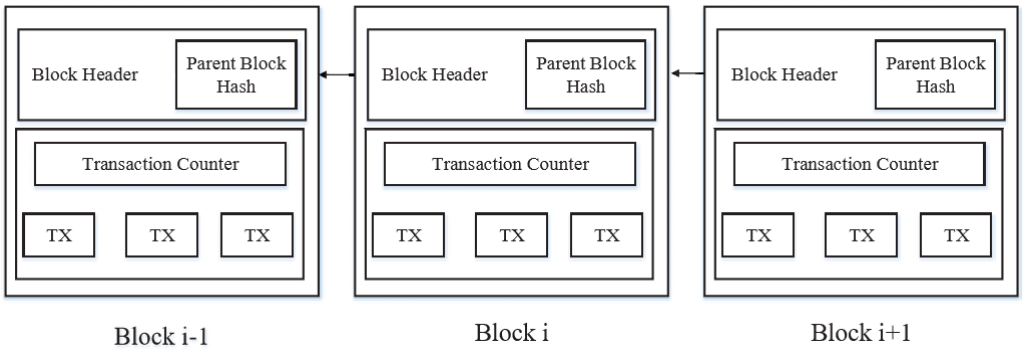

Figure 2: Blockchain Network Architecture; An example of Blockchain which consists of a continuous sequence of blocks.

The above specified figure is the illustration of Blockchain architecture. From the first block which is also called a Genesis block is the block from where the transaction starts and it has no previous blocks hence no associated information of previous hash. The block header which stores the protocols and instructions for every single transaction is the binding notion of the Blockchain. Which however if altered in any way, would result in all the information lost.

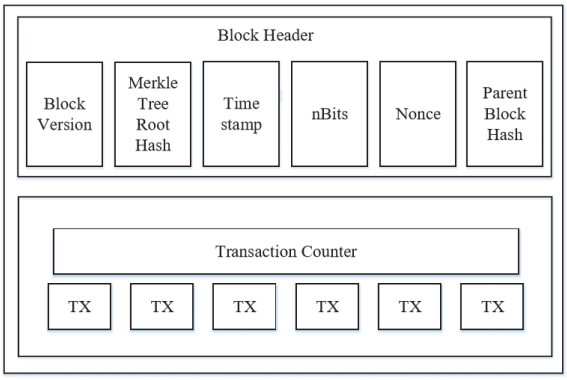

Figure 3: Block Structure of Individual Blocks.

Each block in the Blockchain contains some parameters which are as follows:

1. **Index:**

   It contains the relevant information in order to locate the blocks in the chain. For example it possess the entry of each block corresponding to its hash and other header data.

2. **Timestamp:**

   All transactions being recorded on the Blockchain includes the respective date and time, this trusted timestamping is the process of secure book keeping and track of the creation and modification that occurs.

3. **Previous Hash vs Hash:**

   Hash is a function that converts the hexadecimal input into an encrypted output of a specified fixed length. It works on using an algorithms which is an essential part of the data management in the Blockchain.

   "Hashing requires processing the data from a block through a mathematical function, which results in an output of a fixed length. Using a fixed length output increases security, since anyone trying to decrypt the hash won't be able to tell how long or short the input is simply by looking at the length of the output." [7]

   Hash that defines previous block i.e. previous hash in the Blockchain is the hash of the current block header. This works as a key identifier for that block and is also used to refer to the next block in the chain similar to the way in unique transactions IDs in IBFT – interbank funds transfer is used to refer to a particular transaction.

DLT – Digital Ledger Technology Tempering:

The block header that keeps iterating following track of all the transactional records is also a potential harm and can be used as a triggering point by the majority networks to manipulate the transactional records. Among these parameters, a few possesses the risk of unauthorized alterations such as time stamp and hash that may eventually lead to the alteration in the last parameter, i.e. information.

In order to make Blockchain technology securer, either the security of these five parameters need to be enhanced or more parameters need to be incorporated, i.e. the architecture of the individual blocks has the potential for advancement to ensure security of the information being flowed via Blockchain technology.

Although it is said that the technology maintaining the transactions are perfect and cannot be hacked into, there are some limitations with it. The technology is complex; it uses 'an entirely new vocabulary'. However, it responds to attacks very well and grows stronger. Still, it has an unavoidable security flaw. It is called a "51 percent attack". This is when more than half of the computers which are working as nodes promote a lie; the lie is then seen as a truth.

The architectural structure of Blockchain network involves a chaining mechanism in such manner that the hash of a previous block is located in the succeeding block. However as specified earlier, in a chain of three blocks, if the information in the preceding two blocks is altered, then the whole information can be altered resulting in the loss of actual information/transaction. Blockchain technology is operated using various platforms however to avoid potential attacks on the network, the security of the hash rate of corresponding network is very important. The Blockchain network is however vulnerable to the attack especially if the network is operated in a unified manner and/or if the network has enough computational power. If this is the case, then not only the information can be altered but also the information/transaction that can communicated can also be controlled.

Scientific Journals on the Usability of Blockchain Technology:

The Blockchain phenomenon demonstrates the potential of distributed consensus application on various system's architectures. Blockchain technology is disrupting society by enabling new kinds of disintermediated digital platforms in order to remove middlemen such as retailers from a supply chain by providing goods and services directly to the consumer. Therefore, the use of Blockchain technology in key sensitive sectors such as digital citizenship's data storage, and other important sectors including but not limited to retail, energy sector, logistical trade etc. could be a risky task.

Reference:

[1] "What are Blockchain's Issues and Limitations? - CoinDesk", CoinDesk, 2018. [Online]. Available: https://www.coindesk.com/information/blockchains-issues-limitations/. [Accessed: 05- Nov- 2018].

[2] "What is Blockchain Technology? A Step-by-Step Guide For Beginners", Blockgeeks, 2018. [Online]. Available: https://blockgeeks.com/guides/what-is-blockchain-technology/. [Accessed: 04- Nov- 2018]

[3] 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.

[4] Blockchain in Logistics – Perspective on the upcoming impact of blockchain, Powered by DHL Trend Research, DHL Solutions and Innovations, 2018.

[5] C. Holotescu, “Understanding Blockchain Technology and How To Get Involved”. 14th International Scientific Conference E-learning and Software for Education, Apr. 19-20, 2018.

[6] 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.

[7] https://www.investopedia.com/terms/h/hash.asp