EE 424 – DATA COMMUNICATION & NETWORKING

LCL WRITE-UP MID REVIEW II

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

INTRODUCTION:

In order to attempt a thorough and holistic understanding of a technological phenomenon it is fairly crucial to commence by unraveling its intricate *technicalities.* I shall begin by stating that it is a precarious notion that, even though in it's very infancy, *Blockchain* has definitely become a talk-of-the-town —with *technical* experts discussing and dissecting its ramifications and reporting their assumptions and judgements. For instance Stephen Colbert defines Blockchain as *the gold for nerds* whereas Bill Gates calls *technological tour de force.* Perhaps it is evident how various assumptions are engineered about a technology that is solely responsible for causing or generating an ever growing list of records which are linked to cryptology —with each list of records containing cryptographic hash of the previous list of records typified in the form of a *Merkle tree*. If I strictly present the design, Blockchain is resistant to data corruption or alteration, comprised of an *open ledger* that records transaction between two parties. As a *ledger* or record-keeping technology this very Japanese technology is impenetrable and fairly personifies a distributed computing system with high *Byzantine Fault Tolerance*.

STRUCTURE:

A *Blockchain* is typically handled independently using a distributed timestamping server in a peer-to-peer networking landscape and is validated or certified by mass-collaboration which in turn caused by a *shared interest* —on a philosophical fabric it is almost analogous to Rajneeshism of 1970s for it too was a mass-collaboration for a solitary shared interest.

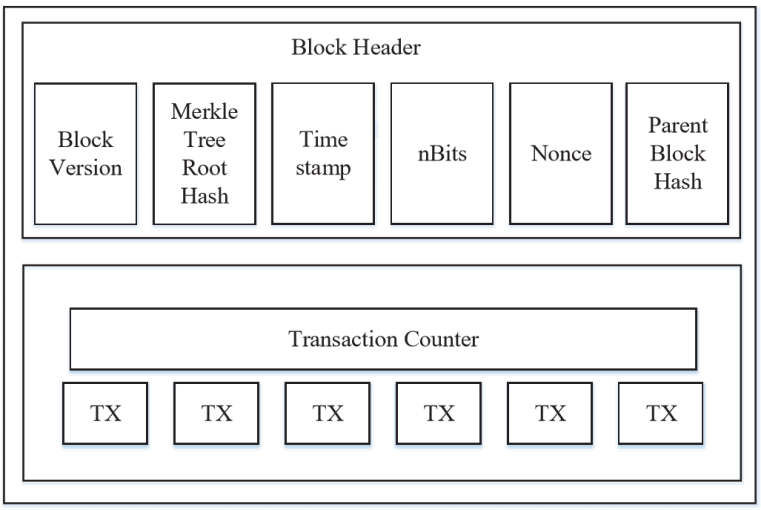

Figure 1: Block Structure of Individual Blocks in the Blockchain.

Perhaps technologically Blockchain constitutes a secure platform of record storage, and its usage exterminates infinite reproducibility for an asset existing digitally by confirming that a single value is transferred only once and therefore responsibly resolving the issue of double-spending. With that it's fairly viable to call Blockchain a platform that keeps *unalterable records* of transactions through a perfectly secure mass-collaboration ―allowing consumers to audit and testify autonomously and also inexpensively.

ARCHITECTURE:

This widely talked-about technological phenomenon is comprised of blocks that hold lists of valid transactions encoded in the hash tree ―with each block consisting of cryptographic hash of the previous block in the chain. With that, making possible for every single transaction data is retrieved in the *Genesis Block* which contains no previous hash and hence ensuring flawless transaction of various nature of digital asset. In a strictly systematic plane this technology is engineered to solve a *proof-of-work* puzzle, a data that is difficult to produce but relatively easier for others to verify. Perhaps in a Blockchain using proof-of-work the chain that consists of most cumulative proof-of-work is deemed valid by the very network.

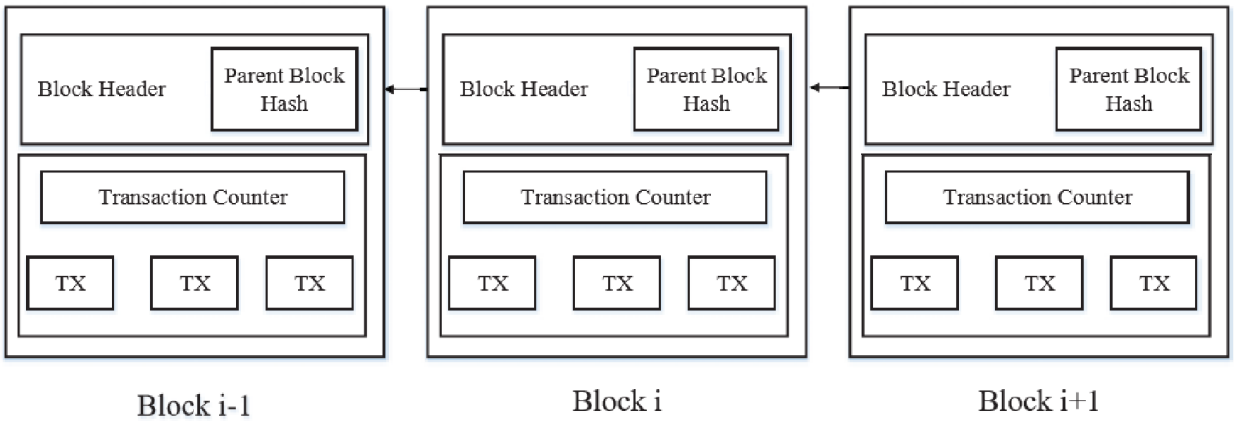

Figure 2: Blockchain Network Architecture; An example of Blockchain which consists of a continuous sequence of blocks.

A number of methods are available and can be employed to present an adequate level of computation —taking place redundantly and not in parallel or segregated manner. In a longitudinal section of block we are exposed to an *index* which contains relevant information useful for locating blocks in the chain, a *timestamp* which is very literal for parameter that records transaction with respective time and date, and *hash* which is a function that converts hexadecimal inputs into a secure and encrypted output of a specified fixed length.

NETWORK:

There are two possible threads in Blockchain with respect to networking, i.e. *networking for Blockchain* and *Blockchain for networking*. Where in order to delve into the former I must put forward a systematic analysis of the same —as previously mentioned Blockchain technology relies on proof-of-work and therefore in order to add a block in the chain mining for the same must be done. Perhaps due to complexities of the algorithms, that are to be crunched to add a block to chain, is relatively very high various nodes contribute to solve a single problem and in the end the reward is too distributed amongst the participant nodes. The entire process of mining, although very difficult and competitive, stirs a fast and reliable communication to take place between the collaborating nodes.

Eventually if I attempt to present the manner in which Blockchain for networking works I shall present an analysis about the same. Which is another potential use of Blockchain which can be used to enable mapping arbitrary addresses or IP addresses. For instance, hierarchical DNS system can be replaced with a Blockchain allowing the user to select URL, check for uniqueness, and can later map the URL to a user desired IP address. These two aforementioned facets of networking through Blockchain completely put forwards a clearer picture of Blockchain.

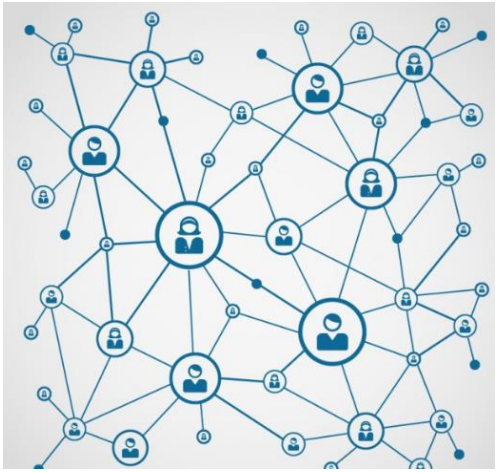

Figure 3: Decentralized Blockchain Network.

SECURITY:

All forms and sorts of information systems, computational tasks and data storage are taking place in distributed manner these days for reliability, accessibility, parallelism and at times for geographical purposes. Perhaps an advantage of data duplication is that it minimizes the latency and precludes the loss. Additionally, when on one hand distributed technologies have many advantages on another they also encounter several problems and ensuring security is a strange mix of both. Therefore I shall attempt to illume the security facet of Blockchain which is based on keys management over the network and depends on cryptographic schemes. With each transaction pointing towards the previous one, the authenticity of every single transaction is validated by digital signatures when broadcasted between the peers.

In turn permits adversary to delay the communication of delivery and hence cause a double-spending error and another possible problem can be denial of transaction delivery. Although with a high Byzantine Fault Tolerance, Blockchain does possess a loophole and a spam attack is another example of a viable security breach to validate the argument. It comprises of pledging transactions that bear how peers handle data, deceleration of network and dilation blocks creation while losing gas and computation power ―resulting in decrement in the number of reachable peers and the entire network outage. Perhaps, instead of being so perfectly operational and secure Blockchain has its vulnerabilities and that makes it a not-bulletproof technology for adversary. In the digital world although namelessness or anonymity is an overwhelming blessing but it sometimes acts as a curse because metadata exposure disturbs anonymity of the peers and therefore reduces confidentiality and causes an identity exposure risk.

All aforementioned weaknesses in the Blockchain network are capable of causing serious monetary damages but there are present precautionary measure which can be employed to dodge the bullet. Usage of address recently timestamped and that too once, filtering the used connection, adding timeout to queries, and regular audits can be considered as possible countermeasures to avoid serious risks or loss.

CONCLUSION:

As discussed in the paper before Blockchain technology is very efficient for storing unalterable records of transactions and also allows a viable network between nodes. With that, this very Japanese technology also is popular for its security and rightfully so.

REFERENCES:

[1] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.
[2] R. Wattenhofer, Distributed Ledger Technology - The science of Blockchain. Forest Publishing, 2017.
[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] S. Underwood, “Blockchain beyond bitcoin,” Commun. ACM, vol. 59, no. 11, pp. 15–17, 2016.
[5] Blockchain in Logistics – Perspective on the upcoming impact of blockchain, Powered by DHL Trend Research, DHL Solutions and Innovations, 2018.
[6] C. Holotescu, “Understanding Blockchain Technology and How To Get Involved”. 14th International Scientific Conference E-learning and Software for Education, Apr. 19-20, 2018.
[7] 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.
[8] M. Castro and B. Liskov, “Practical Byzantine fault tolerance,” in OSDI, 1999, vol. 99, pp. 173–186.
[9] J. Bonneau, A. Miller, J. Clark, A. Narayanan, J. A. Kroll, and E. W. Felten, “Sok: Research perspectives and challenges for bitcoin and cryptocurrencies,” in IEEE Symposium on Security and Privacy, pp. 104– 121, May 2015.
[10] G. Karame, “On the security and scalability of bitcoin’s blockchain,” in Proceedings of ACM SIGSAC Conference on Computer and Communications Security (CCS’16), pp. 1861–1862, New York, NY, USA, 2016.
[11] G. O. Karame, “Two bitcoins at the price of one? Double-spending attacks on fast payments in bitcoin,” in Proceedings of Conference on Computer and Communication Security, pp. 1–17, 2012.
[12] “State of blockchain q1 2016: Blockchain funding overtakes bitcoin,” 2016. [Online]. Available: http://www.coindesk.com/ state-of-blockchain-q1-2016/
[13] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, “A system view of financial blockchains,” in IEEE Symposium on Service-Oriented System Engineering (SOSE’16), pp. 450–457, Mar. 2016.
[14] M. Rosenfeld, “Analysis of hashrate-based double spending,” CoRR, vol. abs/1402.2009, 2014.