A Study on Blockchain Technology and its Applications

Achal R Poonja, Ashish S K, Sagar Ramesh Pujar, Shravan Kini
Department of Information Science and Engineering
Mangalore Institute of Technology and Engineering
Mangalore, India

***Abstract*—Blockchain is a buzzword that has successfully transpired across the information technology industry. Blockchain began as the underlying technology behind the Bitcoin network. Blockchain at its core is a distributed, decentralized and immutable ledger. Due to its extraordinary security features, it has grown prominence in a very short time and there are already research being done on using Blockchain as services. Many businesses are shifting towards Blockchain to enhance the security and provision trust in their networks. Blockchain uses advanced concepts of cryptography like digital signatures, hashes and concepts of cloud computing like distributed computing.**

This paper is a study on the Blockchain Technology, its advantages and a study on where the Technology can be used and where it is going towards. The paper presents an elaboration on various concepts of Blockchain and aims to provide a robust review of the same.

Keywords—Blockchain; Distributed Ledger; Hash; Nodes; Smart Contracts.

I. INTRODUCTION

The inception of the World Wide Web(WWW) began in the early 1990s. The Web was built on the client-server model of the computing where there is a central server that handles the interaction between the system and the user. These systems have been widely adapted in various domains and through advancement in technology, they have evolved extensively. The client-server model is an example for a centralized system. The server is the central authority that handles the interaction with the user. The server is responsible for maintenance, storage and provisioning of the user's data. In critical systems, there is a dire need of having advanced security principles at place that could potentially protect all the data in the system. Through advancements in cryptography, many types of algorithms like RSA encryption, Diffie-Helmann Key Exchange protocol, etc. helped improve the overall security of the system but failed at certain junctures which made them less immune towards cyber attacks. After the web revolution, the cloud revolution began. Cloud computing could potentially provide infrastructure, platform and software as a service using internet across platforms through advanced concepts of virtualization, distributed computing, etc. With the adaption to the cloud paradigm, the need of a secure system became even more important. Blockchain took its birth as a solution to the security issues through its philosophy.

Blockchain took its birth with the introduction of Bitcoin by Satoshi Nakamato. Bitcoin is an electronic payment system based on cryptographic proof instead of trust, allowing any two willing parties to transact directly with each other without the need for a trusted third party[1]. Bitcoin has grown very popular due to its market value and for building a robust system that is almost completely hack-resistant.

Blockchain, the underlying technology controlling the Bitcoin also grew popular over the years. Through inherent research, many organizations have come forward and started to provisioning Blockchain as a service to various businesses. Although, there have been extensive advancements in the last few years, Blockchain is still at the growth stage.

II. WHAT IS BLOCKCHAIN?

Blockchain is a distributed, decentralized and immutable ledger system. A Ledger is a document that keeps track of everything that happens in the network. It keeps records of every transaction that has
happened in the network. Blockchain being distributed means that the computational power required for many actions of the network is rendered through a distributed network between the participant nodes. Decentralized means that the network is not owned by an entity but instead is equally used by all the participants. Immutability is a very important feature of Blockchain that ensures the integrity of data in the Blockchain. In addition to having these features, the Blockchain also consists of smart contracts. Smart contracts have the business logic written in them and they are responsible of provisioning the intended services of the Blockchain.

For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with Blockchain history. If majority of the nodes agree in favor of the transaction, then it is approved and a new block gets added to the existing chain[2]. Each block has a header that contains a hash called as hash pointer. Hash pointer is obtained by using hashing techniques like SHA-256, SHA-1, etc on the previous block. The hash pointers are responsible for creating the connection between individual blocks in the system.

III. TYPES OF BLOCKCHAINS

Blockchain finds its applications across a variety of domains. There are many clients that could benefit from the advanced provisions rendered by the technology. In this light, there are three types of Blockchain networks, namely Public Blockchains, Private Blockchains and Permissioned Blockchains.

Public Blockchains work on an anyone can join basis. Anyone can clone the Blockchain client and run it in their systems. Participants of the Public Blockchain have access to the entire history of transactions that have transpired in the network. Private Blockchains are more suitable for business applications as only trusted participants have access to the network. The network is maintained between multiple nodes and kept secretive. Permissioned Blockchains are a special type of Blockchains where some participants are allowed in the system and permissions to manipulate the data can be altered. Permissioned Blockchains also pave way for creating Blockchain solutions for business problems.

IV. APPLICATIONS

It is important to understand the applications of a particular technology. Blockchain finds it applications across various types of industry. Through its enhanced security features and a robust trust system, Blockchain has proved to be competent enough to solve a

few common businesss problems. Blockchain can help maintain huge amounts of data securely and produce the same whenever required. Blockhain coupled with Internet of Things (IoT) could render robust services. Blockchain will enable the sharing of key relevant data captured from the IoT using a distributed, decentralized, shared ledger that is available to participants in the business network[3]. It could also help the Data Science community since it could hold immutable data that could help make better prediciton models. The hype for Blockchain technology has grown adamantly in the current year. The fig.1 represents hype cycle for emerging technologies,2018. It potrays blockchain as a game changer in various sectors of business.

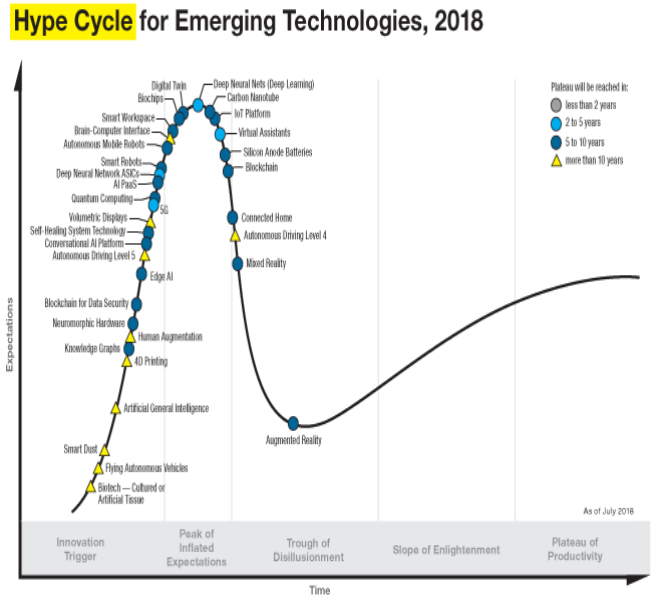

Fig.1 Gartner Hype Cycle for emergent technologies 2018[4].

The Gartner hype cycle clearly views Blockchain as a potential technology that could affect various business and economic sectors. Some of the real world applications of Blockchain are discussed in the subsections.

A. *SUPPLY CHAIN MANAGEMENT*

Supply Chain Management is the management of integrated activities that procure materials and services, transforming them into intermediate goods and final products, and delivering the products through a distribution system [5]. It is used in various E-commerce organizations as a way of tracking the product to be delivered. Supply chain process has many stakeholders as a part of the system. The current norm in the supply chain process is to isolate the parties from each other. This isolation is practiced to provision data confidentiality among the stakeholders. But the isolation affects the trust of the system. Blockchain coupled with Internet of Things(IoT) solves this problem by rendering a robust service to provision a competent trust among the stakeholders and necessary isolation. The Blockchain would capture key shipment data emitted from IoT devices attached to products or components as the shipment moves from source to destination. The IoT platform would invoke a transaction for the blockchain that contains the shipment container location and timestamp. The transactions captured in the blockchain would serve as proof of shipment and proof of delivery for container shipments[3].

Blockchain can reduce transparency in the supply chain. It helps every stakeholder see important data regarding the shipment being transferred across. Since stakeholders also have a copy of the ledger, it is easier to do so. In addition, by using permissioned blockchains, the stakeholders could moderate what data is to be shown to whom. Thus it provides necessary data confidentiality.

B. *HEALTHCARE*

Healthcare is one of those fields which has heavily improved due to advancements in technology. The field has benefited thoroughly from the Clinical Data Management System (CDMS). CDMS helps in maintenance and storage of information related to a particular patient in a centralized system. It promotes digitization of clinical data and provides securiy modules that helps in keeping the data secure. CDMS is a web-based and platform-independent system with relational database management system as back-end. The client tie is mainly different browsers, such as IE, firefox. Core frameworks of the system include Apache Struts, Velocity, and JBoss. All the business logics are implemented in business tie with EJB3.0, mainly including session bean and entity bean. Back-end relational database is open-source based postgreSQL which is widely used enterprise level database[6]. This system has evolved thoroughly after its proposal but all the subsequent proposals still follow the method of centralization for storing information.

Blockchain could help store information in a decentralized manner. There can be a Blockchain running between all the clinics where all the patient information is stored in the form of blocks. Since Blockchain is built for security and robustness, it can help drastically help in the CDMS. We can choose to use permissioned blockchains and moderate the permissions for viewing and editing information accordingly. Any clinic could get access to the information required with reduced overhead unlike previously used CDMS.

C. *ELECTRONIC VOTING*

Electronic Voting or E-Voting is one of the sectors that has been scrutinized thoroughly throughout years. The level of trust required in the system is very high. Blockchain immutability could help assure that the votes cast could not modified. By implementing additional authentication protocols over it, Blockchain E-voting could be implemented. The systems inbuilt feature of decentralization could reduce burden on a single party. Through hashing, Blockchain also helps maintain the anonymity of the voter while allowing audit of votes. It is nearly impossible for one entity to control and moderate the votes as the intended actor has to have access to all the nodes in the system. Through powerful consensus algorithms, the system could be improved thoroughly and real world implementations can be thought of.

Blockchain E-voting can ensure security and transparency and reduce electoral violence. It can also produce more mathematically accurate election results. Because doesn't require management from a central authority, voting related costs will decrease. Finally, Blockchain E-Voting should reduce the cost of paper-based elections and increase voter participation[7].

V. CHALLENGES

Although Blockchain has grown as a powerful and robust system, it still has a lot of challenges. Some of the major challenges noticed are discussed below:

1) Storage: The entire ledger in the Blockchain ecosystem is replicated among all the nodes, meaning that every node in the system stores a copy of the ledger. This may not seem like a problem for a small ledger but as the size of the ledger increases, it could cement for a need of high storage systems.

2) Efficiency: The nodes run a consensus algorithm and then decide on addition of blocks to the ledger. Many consensus algorithms like Proof-of-Work, Proof-of-Stake,etc require multiple nodes to compete and successfully help in consensus. The time

taken for an approach of competing, adding and synchronization of the ledger across the network is very high and thus enacts as a disadvantage.

Blockchain does have its share of challenges. It is still at its infant stage of development and adequate research is required for it surpass its challenges.

VI. CONCLUSION

Blockchain is on the brink of growth and there is a long way to go. Research is being everyday to improve the philosophy of Blockchain. In the recent past, there has been considerable improvements in the sector in terms of security and efficiency. Platforms like *Ethereum, Hyperledger, etc.* have provisioned robust modules that help in developing blockchain based applications. Blockchain aims at providing a decentralized future where an individual's data is given more security and user is given more control.

Blockchain could foster growth of decentralization as a solution to various real world problems. Scandals related to data can be reduced considerably with adaption to blockchain technology. There is still a lot of room for research in this domain and with daily improvements in cryptography and cloud computing, the goal of a decentralized future could be reached.

VII. REFERENCES

[1] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", 2008.
[2] Singh, S., & Singh N, "Blockchain: Future of financial and cyber security", 2016 2nd International Conference on Contemporary Computing and Informatics (IC3I).
[3] Miller, D., "Blockchain and the Internet of Things in the Industrial Sector", IT Professional, 20(3), 15–18.
[4] Kasey Panetta, "5 Trends emerge in the Gartner Hype Cycle for EmergentTechnologies,2018"- https://www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/
[5] Ismail, H.-P. M., & Alina S, "Understanding collaboration and supply chain process: A critical review", 2008 4th IEEE International Conference on Management of Innovation and Technology.
[6] Lingli Fu, Sheng Ding, Tao Chen, "Clinical Data Management System", 2010.
[7] Kshetri N. & Voas J. (2018), "Blockchain-Enabled E-Voting" IEEE Software, 35(4), 95–99.