International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 05 | May - 2022 Impact Factor: 7.185 ISSN: 2582-3930

THE BLOCKCHAIN TECHNOLOGY: DISCUSSION, CLASSIFICATION, APPLICATION AND AUTHENTICATION

Dr.S.THAVAMANI M.Sc., M.Phil., Ph.D.,

Associate Professor
Department of Computer Applications
Sri Ramakrishna College of Arts and Scince (Autonomous)
Coimbatore.
thavamaniphd11@gmail.com

Abstract - The Blockchain technology has overviwed here based on the discussion of the basics which aslo includes working principle, typical network formation of the blocks, areas of appliation which is has utilized mostly and autentiation of the same from malicious users from this technology adapters.

***Key Words*:**BitCoin, IoT, Cloud Environment, Denial of-Service.

1. INTRODUCTION

The blockchain is a public ledger which operates like a log by having a record of all business or other transactions in a chronological order which was operated by the user, and also secured by an fitting compromise mechanism and providing an absolute record. Satoshi Nakamoto published a brief but groundbreaking paper to a cryptography forum. In it he outlined a way to overcome the double-spend scenario – a problem which plagued previous cryptocurrency: "Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones behind it" (Nakamoto, 2008). Its exceptional characteristics include immutability, irreversibility, decentralization, persistence and anonymity. With these advantages, it has found applications in almost all fields requiring data sharing among multiple parties but with secure authentication, namelessness and durability. It's a short of trending technology not only with bitcoin aslo called as cryptocurrency but also inclludes other fields like Payment processing and money transfers,Monitor supply chains, Retail loyalty rewards programs, Digital IDs, Data sharing, Copyright and royalty protection, Digital voting, Real estate, land, and auto title transfers and so on. It doesnot have limited accesses in few fields.The figure-1 depicts about the characteristic of Transactions & Smart Contracts which is a transaction is an exchange of assets that is managed under the entity service's rules. Such rules are usually Operationalized through scripting languages (e.g. Bitcoin's Forth) and are used for advanced transactions (such as escrow and multi-party signatures) to be performed.

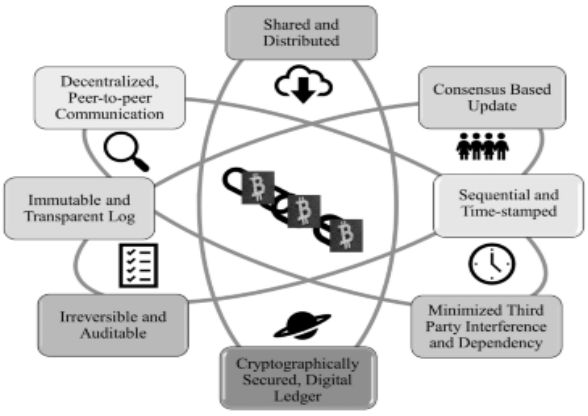

Figure-1. Blockchain Characteristics.

These rules also form the basis for smart contracts. Consensus & Trust In events surrounding nuclear disarmament near end of the cold war, President Regan made a Russian proverb famous: "trust, but verify." The same could be claimed for Blockchain. It is trusted by consensus as all parties must have identical copies of the Blockchain; but each participant is responsible for verifying it. 3 Public and Private Blockchain can be classified as public, private or hybrid variants, depending on their application. Although across from these characteristics the Blockchain method is available with four core characteristics known as Immutable – (permanent and tamper-proof), Decentralized – (networked copies), Consensus Driven – (trust verification), Transparent – (full transaction history)

1.1. Blockchain Functionality

Bitcoin exchange and transfer occur by means of a shared distributed ledger, which records the details of every transaction occurred among the network participants without involving any trusted centralized party. The single copy of the ledger resides in synchronization with all the complicated parties, thus dropping the risk of a single point of failure. Bitcoin works on Public Key Infrastructure (PKI) in the Blockchain for authenticating unnamed users and regulatory access. For source authentication and identification, each

transaction is digitally signed by the owner with the private key. To keep a track of transactions occurring concurrently, multiple transactions are gathered together in a structure called a 'block' uniquely identified by its hash and timestamp. Validation of transactions and the block, among potentially distrusted users is done using a consensus mechanism, The working principle of Blockchain technology is quite significant for all users who have transact using it.

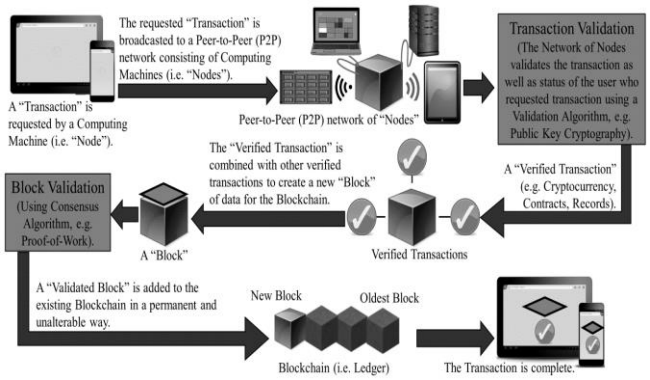

Figure-2: Overview of Blockchain

Basically most famous personalities like Bill Gates and others are using bitcoin which was handled by chain of block (Blockchain) for their huge transactions. When a new transaction or an edit to an existing transaction comes in to a Blockchain, generally a majority of the nodes within a Blockchain implementation must execute algorithms to evaluate and verify the history of the individual Blockchain block that is proposed.

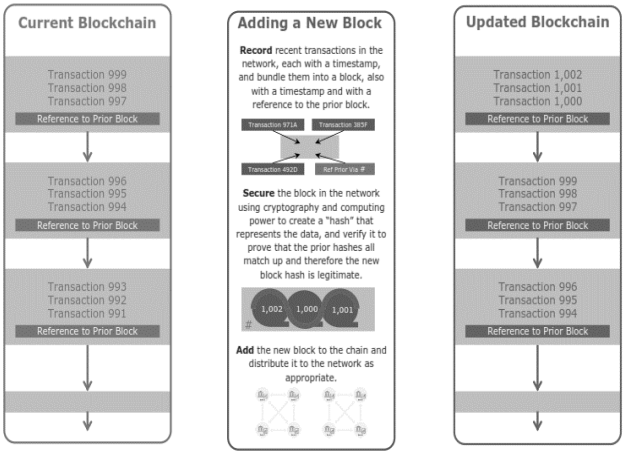

Figure-3: The working way of Blockchain

If a majority of the nodes come to a consensus that the history and signature is valid, the new block of transactions is accepted into the ledger and a new block is added to the chain of transactions. If a majority does not concede to the addition or modification of the ledger entry, it is denied and not added to the chain. This distributed consensus model is what allows Blockchain to run as a distributed ledger without the need for some central, unifying authority saying what transactions are valid and (perhaps more importantly) which ones are not.

2. Classification of Blockchain

Blockchain has been classified into three types as *Public, private and consortium.*

2.1 Public Blockchain

A public Block chain delivers an open platform for people from various organizations and backgrounds to join, transact and mine. There aren't any restrictions on any of these factors. Therefore, these are also called 'permission-less' block chains. Every user is having full rights to read/write transactions, and also to perform auditing in the Blockchain or review any part of the Blockchain at any time. The Blockchain is open and translucent and no such 'validator nodes'. All users can collect transactions and begin with the mining process to earn mining rewards. The availability of the copy of the entire Blockchain synchronized with all the nodes makes it immutable. With complete decentralization, the vastness of existing networks, and an open platform for anyone to join, consensus is achieved by any of the decentralized consensus mechanisms such as proof-of-work, proof of-stake, etc

2.2 Private Blockchain

It is a type of Blockchain system which is setup to enable private sharing and exchange of data among a group of individuals who comes under in a single organization or among multiple organizations with mining controlled by one organization or selective individuals. It is also called a permissioned Blockchain since unknown users cannot get access to it, unless they receive a special invitation. Nodes' participation is decided either by a set of rules or by the network in-charge, to control access. This inclines the network more towards centralization, while derogating the basic Blockchain features of complete decentralization, and openness as defined by Satoshi.

2.3 Consortium Blockchain

A consortium blockchain can be considered as a partially private and permissioned blockchain, where not a single organization but a set of pre-determined nodes are responsible for consensus and block validation. These nodes decide who can be part of the network and who can mine. For block validation, a multi-signature scheme is used, where block is considered valid, only if it signed by these nodes. Thus, it is a partially centralized system, owing to the control by some selected validator nodes, unlike the private blockchain which is completely centralized, and the public blockchain which is completely decentralized. It is decided by the consortium whether read or write permissions wouldbe public or limited to the network participants. Also, the restriction of consensus to a set of nodes doesn't guarantee immutability and

irreversibility, since control of the consortium by a majority can lead to tampering of the Blockchain.

4. Major Blockchain application

Bitcoin is just atypical use of the Blockchain. Blockchain is considered to be a unique revolution in the domain of computing enabling limitless applications such as storing and verifyinglegal documents including deeds and various certificates, healthcare data, IoT, Cloud and so on.

In the *cloud environment*, the history of creation of any cloud data object and its subsequent operations performed thereupon are recorded by the data structure mechanism of 'Data Provenance', which is a type of cloud metadata. Thus this is very important to provide the paramount security to the data provenance for ensuring its data privacy, forensics and accountability. Liang et al. puts forward a Blockchain based trusted cloud data provenance architecture, 'ProvChain', which is fully decentralized.

In an *IoT ecosystem* most of the communication is in the form of Machine-to-Machine(M2M) interactions. Thus establishing trust among the contributing machines is a big challenge thatIoT technology still has not been met widely. However, Blockchain may act as a substance in this regard by enabling enhanced scalability, security, reliability and privacy [9]. This can be attained by arraying Blockchain technology to track billions of devices connected to the IoT eco-systems and used to enable and/or synchronize transaction processing. Applying Blockchain in the IoT ecosystem will also increase reliability by axing the Single Point of Failure (SPF). The cryptographic algorithms used for encryption of the block data as well as the hashing techniques may offer better security.

5. Authentication

The need for blockchain based identity authentication is particularly salient in the internet age. While there exists somewhat defective systems for founding personal identity in the physical world, in the form of Social Security numbers, state liquor identification cards, drivers' licenses and even passports or national identity cards, there is no equivalent system for securing either online authentication of our personal identities or the identity of digital entities. Facebook accounts, now often used as login for different digital applications, and media access control (MAC) addresses, may come close, yet both can hardly function as trustworthy forms of identification when they can be changed at will.

Client Privacy : The blockchain is a public ledger, therefore all the transactions stored in the blocks can be read by anyone. A client can protect its privacy by generating new addresses for each transaction. Doing so allows the client to isolate each of its transactions in such a way that it is harder for an attacker to associate them all together.

There are several techniques we can use to prevent *Denial of-Service (DoS)* attacks on the blockchain infrastructure. The main issue is that because of the halting problem, we cannot redirect if a smart contract deployed on the blockchain will terminate.

Secure Communications the personal keys are exchanged over *DTLS channels* between the key server, the resource servers, and the clients. Authentication between the resource servers and the key server is achieved on the basis of certificates, and between the clients and the key server, through a challenge-response.

Data Security : Conventional models of data security rely on creating harder and harder "walls" – adding multiple factors to authentication for access and stronger encryption. They typically rely on the same fundamental concept: once you enter the system, you can access the data. Compartmentalization is typically minimal. Edward Snowden used a combination of social engineering and a low-tech "spider" to crawl over 1.7 million documents.8 With blockchain, there exists the potential to "scatter the stack", rendering the cost of any one breach or combination of breaches much lower.

Decentralized Security : Underlying all of the above applications of blockchain technology is the importance of the data being securely held – in the sense that it cannot be tampered with. Data protection and privacy is another aspect of data security. The decentralized nature of blockchain may initially appear to be at odds with privacy; this is indeed a valid concern however there are some developments to reunite the two.

6. Conclusion

This paper has taken care of the blockchain first discussion of the blockchain which given basicness and characteristics of the blockchain technology whatever the application maybe. Secondly the classification of the model which has been divided based on some criteria. Third focus is all about applications where this technology majority blooming and trending so for. Finally consideration is on authentication of the same where all entities and entries has secured via basic security methodologies.

REFERENCES

1. Applications karim sultan1 , umar ruhi1 and rubina lakhani conceptualizing blockchains: characteristics & applications 11th iadis international conference information systems 2018. Https://arxiv.org/pdf/1806.03693
2. Data Insertion in Bitcoin's Blockchain Andrew Sward, Ivy Vecna, Forrest Stonedahl,,ISSN 2379-5980 (online) DOI 10.5915/LEDGER.2018.101 https://www.fool.com/investing/2018/04/11/20-real-world-uses-for-blockchain-technology.aspx

3. Applications of Blockchain Technology beyond Cryptocurrency Mahdi H. Miraz , Maaruf Ali-Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.
4. Don Tapscott and Alex Tapscott, Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World, 1st ed. New York, USA: Penguin Publishing Group, 2016.
5. Maaruf Ali and Mahdi H. Miraz, "Recent Advances in Cloud Computing Applications and Services," International Journal on Cloud Computing (IJCC), vol. 1, no. 1, pp. 1-12, February 2014, Available: http://asdfjournals.com/ijcc/ijcc-issues/ijcc-v1i1y2014/ijcc-001html-v1i1y2014/
6. Xueping Liang et al., "ProvChain: A Blockchain-based Data Provenance Architecture in Cloud Environment with Enhanced Privacy and Availability," in Proceedings of the 17th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing (CCGrid '17), Madrid, Spain, May 14 - 17, 2017, pp. 468-477, Available: https://dl.acm.org/citation.cfm?id=3101176&CFID=994896989&CFTOKEN=44228545
7. Mahdi H. Miraz, Maaruf Ali, Peter Excell, and Picking Rich, "A Review on Internet of Things (IoT), Internet of Everything (IoE) and Internet of Nano Things (IoNT)," in the Proceedings of the Fifth International IEEE Conference on Internet Technologies and Applications (ITA 15), Wrexham, UK, 2015, pp. 219 – 224, Available: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7317398
8. IoTChain: A Blockchain Security Architecture forthe Internet of ThingsOlivier Alphand, , Michele Amoretti, Timothy Claeys, Simone Dall'Asta,Gianluigi Ferrari,Franck Rousseau, Bernard Tourancheau, Luca Veltri, Andrzej DudaDepartment of Engineering and Architecture, University of Parma, ItalyUniv. Grenoble Alpes, CNRS, Grenoble INP, LIG, F-38000 Grenoble, France

AUTHOR PROFILE

Dr. S. Thavamani is an Associate Professor in Department of Computer Applications, Sri Ramakrishna College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India. She has a teaching experience of 22 years in the field of Computer science. She has authored 4 Books in the field of Computer Science. She has Published a Patent. She has received various awards like the "***Best Faculty Award"*** *from ARUNAI International Research Foundation (AIRF Awards – 2017),* **"** ***Incessant Service Award"*** for recognizes "***Being A Truly Inspirational Teacher****",* and *"****Best Team Award - MOOC – "Spoken Tutorial",*** from Sri Ramakrishna College of Arts and Science (Autonomous), ***"The Best Paper Award***" from Tiruppur Kumaran College for Women, Tiruppur, Appreciation Award for the " **Using ICT based Teaching and Learning methodology"** for students of Tamil Nadu from **Spoken Tutorial IIT Bombay.** Her area of Specialization is Distributed Computing and P2P Networks. She has presented more than 25 Papers in various International and National Conferences and she has published 26 international Journals. She is currently a supervisor for M.Phil. and Ph.D research works of various Universities. She acted as a coordinator of Various Workshops and Seminars.