RESEARCHERID
THOMSON REUTERS
[Tinu, 5(7): July 2018] ISSN 2348 – 8034
DOI- 10.5281/zenodo.1305003 Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

BLOCKCHAIN TECHNOLOGY- AN EXTENSIVE STUDY ON ITS USERS AND APPLICATIONS

Tinu N.S[*1] & SojaRani.S[2]
[*1&2]Assistant professor, Dept of CSE, New Horizon College of Engg., Bangalore, India

ABSTRACT

Blockchain technology has gained more and more exposure in multidisciplinary domains with its incomparable adaptability and versatility. Blockchain network makes every action accountable and verifiable, the features that contributed to its popularity. However not every application could deliberate it as a solution. This paper attempts to provide an outline of how blockchain works and which all application can adopt this technology, so that, the application could enhance its overall potency. Applications could use blockchain either as a stand-alone technology or could be combined with other technologies for further enhancements. This paper also tries to classify blockchain applications.

Keywords*: Blockchain, Distributedledger,Hashing, Digital Signature*.

I. INTRODUCTION

Blockchain technology was introduced to implement the cryptocurrency concept of Bitcoin[1]. In the current scenario blockchain technology is in a stage of its explosion in numerous application areas. The major reason for this mass adoption is because the blockchain technology assures secured asset transfer without any central authority governance, it could reduce fraudulent transactions, it enables transparency of transactions which are immutable and facilitates ease of audit, it reduces possible downtime and cost, it could streamline the technique in multidisciplinary domain areas. The base of blockchain is cryptographically well secured Distributed Ledger Technology(DLT) that runs on distributed consensus model[2]which is continuously expanding. Blockchain network is a peer to peer network that keeps a record of all the transactions that happens across a numerous interconnected systems. The network is continuously expanding with chaining new blocks to it, hence the name blockchain, that starts with the very first block known as the 'genesis block'. Moreover each 'block' is exclusively connected to the just previous block. Blockchain technology makes use of mainly two cryptographic concepts:- hashing and digital signature.

Hashing: In this cryptographic technique, a specific function/algorithm is applied to an arbitrary amount of input data, which will generate a fixed-size output data called the hash. For example 256 bits. The input can be of any number of bits that represents a single character, an mp4 file, an entire word document, bank transaction spreadsheets. Hash algorithms could be selected depending on the requirement, the most famous ones are MD5, SHA family and many are publicly available[3]. The main purpose of hashing is to fingerprint the files. Once the hash is generated using that particular algorithm, the file can be checked any number of times to ensure its integrity. If the hash generated is the same, then it could be assured that the file has not tampered in any way. A modified file generates a different hash value from the original hash value. In blockchain, a hashing technique is used to represent the current state of the blockchain network. To start with, the first hash value is calculated for the 'genesis' block, by providing the sequence of initial transactions in that block. For every subsequent block generated afterward, it uses its own transactions as well as the previous block's hash as input, in order to determine its block hash. Thus each new block hash points to the block hash that came just before it, guarantees that no transaction in the history could be altered. If any solo part of the transaction changes, so does the hash of the block to which it belongs, and any following blocks' hashes as a result. This makes it easily verifiable by just compare the hashes. This is cool because everyone on the blockchain only needs to agree on 256 bits to represent the potentially infinite state of the

blockchain. The Ethereumblockchain is currently hundreds of gigabytes, but the current state of the blockchain, as of now is this hexadecimal hash representing 256 bits.

Digital Signature: Blockchain technology uses asymmetric cryptography which uses a key pair[4]. Every transaction that is executed on the blockchain is digitally signed by the sender using their private key. This signature ensures that only the authorized holder of the account can move money out of the account. This type of design makes the network resilient as it does not have any single point of vulnerability and immutable.

II. METHODOLOGY

This section discusses in detail about how blockchain works. The blockchain is a network of so-called computing "nodes". Blockchain operates by validating transactions through a distributed network so as to create a permanent, verifiable and unalterable ledger of information. The below mentioned are the general steps to be a part of blockchain network.

Blockchain operates by validating transactions through a distributed network so as to create a permanent, verifiable and unalterable ledger of information. The below mentioned are the general steps to be a part of blockchainnetwork[5].

(i)To be a participating node in blockchain: To be a part of a blockchain system, participating entities would install and run the required software that connects their computer or server to other participants in the network. By running this software, the participants act as individual validators, called network nodes.

(ii)Once a node connects to the network for the first time, a full copy of the blockchain database is downloaded onto its computer or server.

(iii)The network of nodes manages the blockchain database. The nodes act as entry points for new data, as well as the validation and propagation center of new data that have been submitted to the blockchain. Thus every node is an administrator of the blockchain.

(iv) Asblockchain is a distributed ledger working without the need of a centralized third party, there should be some mechanism to come to an agreement among the nodes in order to resolve validation conflicts like whether to add new transaction or accept edited transactions. This mechanism is known as the consensus algorithms. Thus blockchain uses pre-agreed rules for technical and business validity of data that has to be written, and a rule to determine how consensus is achieved.

(v) A block is created by grouping similar transactions together. These blocks are added in chronological order, in a way that resembles a chain, hence the name blockchain. The nodes then store these new blocks on the local blockchain database on their computer or server.

Hurdles to implementation

- Governing uncertainties and legal risks need to be rectified.
- Integration and interoperability with traditional systems.
- Dealing with real time data and updates.
- Privacy and confidentiality
- Scalability,and initial cost.

[Tinu, 5(7): July 2018]
DOI- 10.5281/zenodo.1305003

ISSN 2348 – 8034
Impact Factor- 5.070

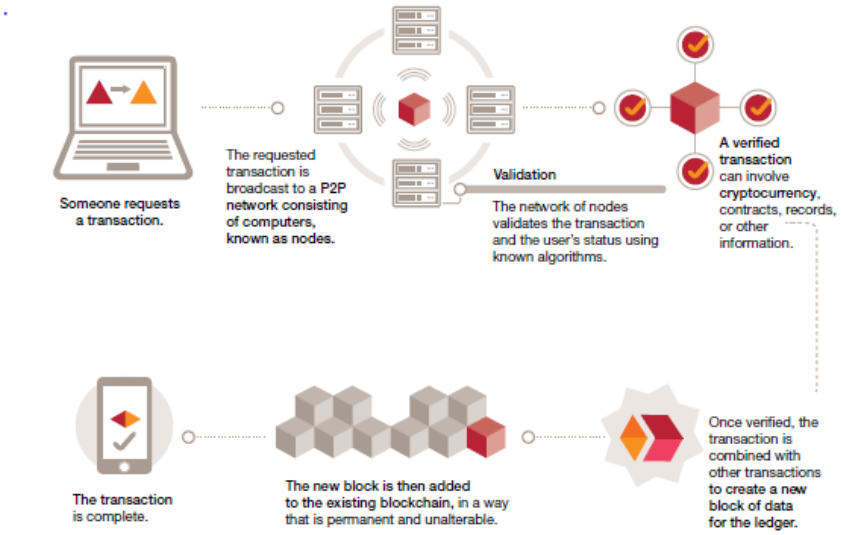

Figure: 1 How Blockchain Works

III. PREREQUISITES TO ADOPT BLOCKCHAIN TECHNOLOGY

Blockchain technology is not a cooked up solution for all use cases of digital transactions with data and assets. In order to adopt blockchain as an ideal solution, one must understand its attributes and identify uses cases where this solution would be feasible and beneficial. This section focus on who can adopt blockchain as a solution. Blockchain technology is appropriate only when multiple parties share their data, which might later undergo change and would need a view of final common information. Nevertheless, multiple parties sharing data is not the only qualifying criteria for blockchain to be a viable solution. To understand better the effectiveness of a blockchain solution, empirically the prerequisites are mentioned below, if three out of the following five is identified, then it is considered success criteria:

1. Multiple parties update data: If the application has to record actions and update data coming from multiple parties.
2. The requirement for verification: When trust amongst parties plays a critical role and they should realize that their actions that are being recorded are valid
3. Intermediaries add complexity: When a transaction is reliant on multiple intermediaries and it increases the cost and complexity of the transaction
4. Interactions are time sensitive: When it is favorable for the business to reduce delay and accelerate a transaction
5. Transactions interact: When transactions created by multiple participants interact and depend on each other.

If at least three out of these five criteria are not valid, then it could be concluded that blockchain is not a satisfactory solution.

The figure mentioned below gives an insight towards how blockchain technology has been adopted widespread around the globe.

ISSN 2348 – 8034
Impact Factor- 5.070

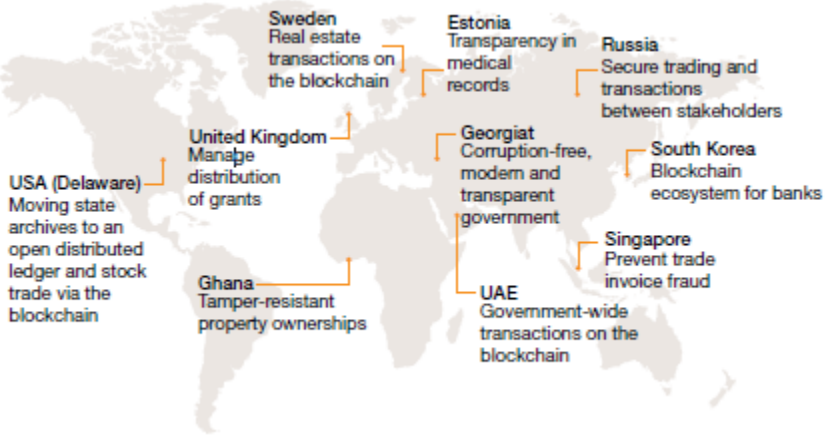

Figure: 2 Global Adoption of Blockchain Technology in Multidisciplinary Areas

IV. CLASSIFICATION OF BLOCKCHAIN APPLICATIONS

Blockchain has been undertaken by many governments around the world as discusses in the previous session. Blockchain concept could be an effective solution in multidisciplinary domain areas. According to Mougayar (2016), blockchain has been identified to support one or more of six elements represented by the mnemonic ATOMIC (Assets, Trust, Ownership, Money, Identity, and Contracts)[6]. Using a blockchain platform signifies that each of these six elements is programmable, and based on this note, blockchains enables new services to release into the market with low-priced transaction fees and faster execution, thus disrupts many traditional business models which rely on often expensive intermediaries. Blockchain applications could be classified as covering four aspects: blockchain as a development platform; blockchain as a smart contract utility; blockchain as a marketplace, and finally, blockchain as a trusted service application (Rosic, 2017)[7].

4.1Blockchain as a Development Platform

The introduction of Blockchain as a Service (BaaS) platforms like Microsoft (Azure) and IBM (Cloud) provide an inexpensive environment for developers to rapidly built on test blockchains before deploying to live ones. Being distributed ledger technology it enables secure sharing of data across industrial networks (e.g. Xage3), and technologies that offer blockchain enabled verification of data transactions (e.g. Guardtime4). These BaaS solutions form the basis for programmable trust, ownership, and identity, and also facilitate the operation and governance of enterprise blockchain applications and services. An example in healthcare, blockchain can be implemented to facilitate a secure and flexible environment for exchanging electronic health records (EHRs). Also helps in sharing information related to the availability of critical drugs, blood, organs. By publishing all medical licenses, fraudulent practice in the medical field can be reduced. Similarly in the education sector, if the certificates of students and faculties are stored in a distributed environment, it could simplify certificate attestation and verification. Another application is in the agricultural field, where it enables to record and manage agricultural land archives as well as agriculture insurance.

4.2 Blockchain as a Smart Contract Utility

Smart contracts provides a programmatic interface to blockchains by providing a collection of code and data. A smart contract is executed appropriate method with the user provided data to deliver a service. The smart contract, when triggered, transacts value based on digital assets. The utility is apprehended in code and stored on the blockchain. This code would be executed when a predetermined condition occurs. Examples include escrow, multi-party transactions, digital notarization, and time stamping. A specific example of this functionality could be perceived in the example of Visa and DocuSign who have partnered to operate a proof-of-concept blockchain project to streamline vehicle leasing experience for customers by simplifying transaction management between multiple parties including sellers, buyers and insurance companies (Hirson, 2015)[8]. Insurance companies can

automate their policies by embedding them into a smart contract. Tracking products with the aid of IOT, in supply chain business and verification of product ownership for royalty payments in the entertainment industry are other good implementation of the blockchain.

4.3Blockchain as a Marketplace

Any robust system necessitates a market for generating value. In the crypto economics marketplace, blockchain offers a payment infrastructure (via cryptocurrencies) and a proof-of-ownership structure (via digital asset tracking), by removing the middleman. This has enabled peer-to-peer marketplaces with no governing authority, such as OpenBazaar6 and Soma7.In these marketplaces, blockchain platforms could be used to directly match buyers and sellers allowing them to transact through smart contracts. Blockchain technology has also being hyped as a provider for the next generation online workforce marketplaces in the context of the gig economy that relies on independent contract workers and freelancers for short-term engagements, and the shared economy where consumers increasingly turn out to be prosumers. In such instances, blockchain platforms liberate service providers from the constraints of any central authority – hence, letting them extend flexible offerings, and payment interactions and service transactions could function in a transparent environment.

4.4 Trusted-Service Application

Finally, blockchain acts as a trusted service application, by facilitating highly specialized applications for any purpose presumable. This more generalized consumption of blockchains that enable all types of applications through a blend of programmable assets, trust, ownership, money, identity, and contracts is sometimes referred to as blockchain 2.0 (Bheemaiah, 2016; Swan, 2015a)[9][10]. On the front-end, trusted service applications constructed on the blockchain using smart contracts can provide disintermediated, secure services to end users. On the backend, many of these applications are vested in public blockchains (e.g. Bitcoin and Ethereum) so that it cannot be shut down or restricted. Moreover, many companies provide APIs (application programming interface) permitting developers to build applications using blockchain protocols and mechanisms (Bheemaiah, 2016).

Based on the discussion of potential blockchain business applications, a 2x2 matrix (Figure 3) for mapping industry sectors against blockchain scope (public vs private vs hybrid), and blockchain access (as a service or as application) is demonstrated[11].

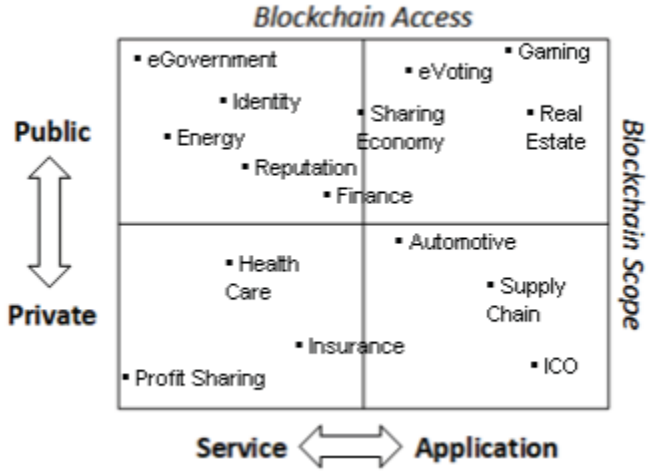

***Figure: 3*2x2 matrix**

V. CONCLUSION

Blockchain technology is in the urge of explosion by being adopted globally in applications. This widespread popularity of the technology enables it to come up with amazing innovations and many government bodies are taking steps towards understanding and adapting to the usability and potentiality of this comparatively new

technology. Though started with cryptocurrency, blockchain is gaining in popularity in other domains like real estate, smart contracts, healthcare, crowdfunding, supplychain management etc. Rather than being used as a standalone technology, blockchain is now combined with many other technologies like IoT to make smart cities possible in another few years. Innovations being done in this area are absolutely fast and unimaginable.

REFERENCES

1. *Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. https://bitcoin.org/bitcoin.pdf*
2. *N.S Tinu, "A Survey on BlockchainTechnology- Taxonomy, Consensus Algorithms andApplications" in International Journal of Computer Sciences andEngineering, Volume-6, Issue-5, May 2018,pp. 691–696.*
3. *National Institute of Standards and Technology (NIST), Federal InformationProcessing Standards (FIPS) Publication 180-4, Secure Hash Standard (SHS),August 2015. https://doi.org/10.6028/NIST.FIPS.180-4*
4. *National Institute of Standards and Technology (NIST), Federal InformationProcessing Standards (FIPS) Publication 186-4, Digital Signature Standard, July2013. https://doi.org/10.6028/NIST.FIPS.186-4*
5. *https://www.pwc.in/assets/pdfs/publications/2018/blockchain-the-next-innovation-to-make-our-cities-smarter.pdf*
6. *Mougayar W (2016) The business blockchain : promise, practice, and application of the next Internet technology. Wiley.*
7. *RosicA (2017) William Mougayar: The Future Of Blockchain? | HuffPost.*
8. *Hirson R (2015) The Future Of Car Leasing Is As Easy As Click, Sign, Drive | DocuSign Blog. Available at: https://www.docusign.com/blog/the-future-of-car-leasing-is-as-easy-as-click-sign-drive/*
9. *Bheemaiah K (2016) Block Chain 2.0: The Renaissance of Money. Available at: http://www.wired.com/2015/01/blockchain-2-0/*
10. *Swan M (2015a) Blockchain. O'Reilly Media, Inc. DOI: 10.1017/CBO9781107415324.004*
11. *Karim Sultan1, Umar Ruhi1 and Rubina Lakhani2Conceptualizing blockchains:Characteristics& applications,11th IADIS International Conference Information Systems 2018*