Blockchain Technology

Dr. Reshma Banu[1], Gnaneshwari.D.S[2], Ayesha Taranum[3], Harini.C.B[4], Chinmayi S[5], Spandana.M[6]
Department of ISE, GSSSIETW, Mysuru.

Abstract - Block-chain is the technology behind the bitcoin crypto-currency system. Bitcoin is the decentralized peer-to-peer digital currency is the most popular example that uses a block-chain technology. Block-chain is considered to be both critical and fascinating for ensuring enhanced security and privacy for different application in many other domains including in the internet of thing. Intensive research is currently being conducted in both academia and industry applying the block-chain technology in multifarious application like proof-of-work, a cryptographic puzzle, plays a vital role in ensuring block chain security by maintaining a digital ledger of transactions which is considered to be incorruptible. Block-chain is having wide range of application in both financial and nonfinancial world. The main theory is that the block-chain demonstrates a system of creating a distributed agreement in the digital online world. This allows participating something to know for certain that a digital event happened by creating a certain record in public ledger. There are massive opportunities in this disruptive technology and revolution in this space has just begun.

I. HISTORY AND INTRODUCTION

The core ideas behind block-chain technology emerged in .it was first applied to digital cash in 2008 in the initial paper describing the Bit-coin electronic cash solution, Bitcoin: A peer to peer electronic cash system, which was published by Satoshi Nakamoto. The actual author and owner of the first Bitcoin remain a mystery. Since, then block-chain technology has become tightly linked to Bitcoin and is often assumed to be used for monetary transaction. Many electronic cash schemes existed prior to Bitcoin, but adopting Block-chain technology, Bitcoin achieved compelling capabilities that promoted its use. Its primary benefit was to enable direct electronic financial transactions between users without the need for a third party. By using distributed block-chain and consensus based maintenance, a self-policing mechanism was created, that ensured that only valid transactions were added to block-chain. Finally, the distributed maintenance of the block-chain created a system with complete transparency, which promoted trust in its use. Since all transactions are transparent within the system, and must be verified before being included. it greatly reduces the ability for users to double spend their digital assets. One of the most valuable aspects of applications built on block-chains is that they can enable business to be conducted with untrusted and unknown users.

II. INTRODUCTION

The goal of this paper is to brief the literature on implementation of the Block-chain and similar digital ledger technique in various other domains beyond its applications sample of research is presented. Spanning over last ten years, starting from the early work in the field. Different types of usage of Block-chain and other digital ledger technique, their challenges, applications, security and privacy issues were investigated. Block-chain (BC), the technology behind Bitcoin crypto-currency system, is considered to be essential for forming the backbone for ensuring enhanced security and privacy for various applications in many other domains including the Internet of Things eco-system. International research is currently being conducted in both academia and industry applying Block-chain in varied domains. The proof-of-work (POW) mathematical challenge ensures BC security by maintaining a digital ledger of transactions that is considered to be unalterable. Furthermore, BC uses changeable Public Key (PK) to record the users identify that provides an extra layer of privacy. The successful adoption of BC has been implemented in diverse non-monetary systems such as in online voting. Decentralized messaging, distributed cloud storage systems, proof-of-location, healthcare and so on. Recent research articles and projects/applications were surveyed to ascertain the implementation of BC for enhanced security and to identify its associated the challenges and hence propose solutions for the BC enabled enhanced security systems. The knowledge domain of the research is in the realm of the digital ledger, specifically, in Block-chain and Crypto-currency

III. TECHNOLOGY FUNDAMENTALS OF BLOCK CHAIN

A Block-chain is comprises of two different components, as follows:

1. Transaction - A transaction, in a Block-chain, represents the action trigged by the participant.

2. Block - A block in a Block-chain, is a collection of data recording the transaction and other associated details such as the correct sequence, timestamp of creation, etc. The Block-chain can either be public or private, depending on the scope of its uses. A public Block-chain enables all the users with read and write permissions such as in Bitcoin, access to it. However, there are some public Block-chains that limit the access to only a/either to read or write. On the contrary, a private Block-chain limits the access to selected trusted participants only, with the aim to keep the users details concealed. This is particularly pertinent amongst governmental institutions and allied sister concerns or their subsidies thereof. One of the major benefits of the Block-chain is that it and its implementation technology is public. Each participating entities possesses an updated complete record of the transactions and the associated blocks. Thus the data remains unaltered, as any changes will be publicly verifiable. However, the data in the blocks are encrypted by

a private key and hence cannot be interpreted by everyone. For a new transaction to be added to the existing chain, it has to be validated by all the participants of the relevant Block-chain eco-system. For such a validation and verification process, the participants must apply a specific algorithm. The relevant Block-chain system defines what is perceived as "valid", which may vary from one eco-system to another. A number of transactions thus approved participating nodes to be appended to the existing chain of blocks. Each succeeding block comprises a hash, a unique digital fingerprint, of the preceding one. Figure 1 demonstrates how Block-chain transactions take place, using a step-by-step example. Bob is a going to transfer some money to Alice. Once the monetary transaction is initiated and hence triggered by bob, it is represented as a "transaction" and broadcast to all the involved parties in the networks. The transaction now has to get "approval" as being indeed "valid" by the Block-chain eco-system. Transaction once approved as valid along with the hash of the succeeding block are then fed into a new "block" and communicated to all the participating nodes to be subsequently appended to the existing chain of the blocks in the Block-chain digital ledger.

IV. BLOCKCHAIN ARCHITECTURE

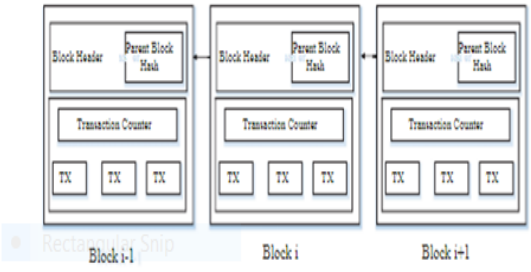

Figure 1: An example of block chain

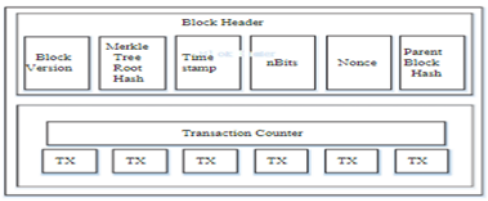

Fig. 2: Block structure

It's a sequence of blocks, which holds a complete list of a transaction records such as Conventional public ledger [14].fig1 illustrates an example of a block chain, with a previous block hash contained in the block header, a block has only one parent block or super block

A. Blocks: It consist of the "block header" & "the block body" as shown in fig 2.

In particular, the block header includes

- **Block Version:** It indicates which set of validation rules to follow.
- **Merkle Tree Root Hash:** The hash has value in all the transaction in the block.
- **Time Stamp:** Current time as seconds in universal time since Jan 1, 1970.

B. Digital Signature: Each user have own pair of private key & public key.

The Private key that shall be kept confidentiality is used to sign the transactions. The digital signed transactions are to sign the transactions

*The digital signed transaction are broadcasted throughout the network. It involves 2 phases

- Signing phase.
- Verifying phase

Key Characteristics of Block Chain: It has following key characters-

- Decentralization
- Persistency
- Anonymity

V. WORKING OF BLOCK-CHAIN

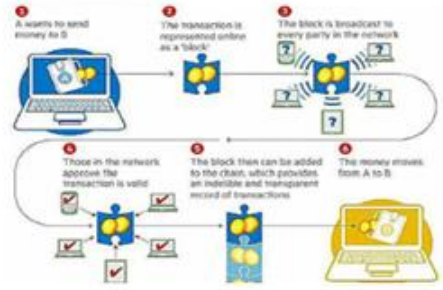

Figure 3

It has both private block chain & public block their workings are as below table

Public Vs Private Blockchains

Private blockchains.	Public blockchains.
1. Conversely, a 'private' blockchain network is where the participants are known and trusted: for example, an industry group, or a group of companies owned by an umbrella company. 2. Many of the mechanisms aren't needed - or rather they are replaced with legal contracts. 3. This changes the technical decisions as to which bricks are used to build the solution.	Ledgers can be 'public' in two senses: 1. Anyone, without permission granted by another authority, can write data 2. Anyone, without permission granted by another authority, can read data Usually, when people talk about public blockchains, they mean anyone-can-write.

VI. CORPORATEFUNDING& INTEREST

*In the year 2015, the bit coin currency has reached high yearly in both prices & volume over Sep-Oct. the digital currency is gaining traction both in the consumer marketplace, as a trade-able security & with regulators

Figure 4

VII. THE FUTURE OF BLOCK-CHAIN

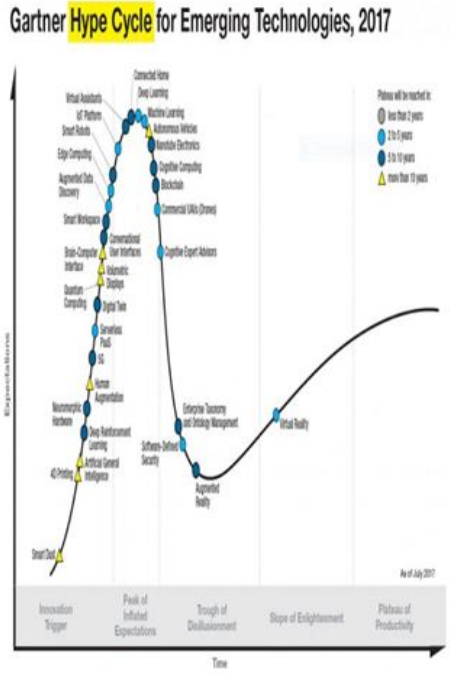

Figure 5

*According the "Gartner Hyper Cycle of Emerging Technologies 2017", shown in above figure, Below, block-chain still remain in the region of "PEAK OF INFLATED EXCEPTION' with forecast to reach plateau in "5-10 years".

*These technologies is shown going down-hill into the region of the "THROUGH OF DISILLUSTRATIONMENT" Because of wide adoption of block chain in wide range

*Block-Chain possesses a great potential in empowering the citizens of the developing countries if widely adopted E-governance application for management process

VIII. BLOCK- CHAIN APPLICATION

A. Block Chain Recommendation for IOT to Exploit -

- Trust Building
- Cost Reduction
- Accelerate Data Exchanges\
- Scaled Security For IOT

B. Financial Application -

- Private Securities
- Insurance

C. Non-Financial Application

- Notary Public
- Applications of Block-Chain in
- Decentralized proof of existence of documents
- Decentralized Storages
- Decentralized IOT
- Block-Chain based Anti-Counterfeit solutions
- Internet Application

IX. CONCLUSION

The application of the block-chain technology and concept has grown beyond its use for bitcoin generation and transactions. The properties of its security privacy and time-stamping have seen its adoption beyond its initial application areas. Block-chain and its variants are used to secure any type of transactions, whether it be human to human communication or machine to machine. Its adoption appears to be secure with the global emergence of the internet of things. The block-chain has been especially identified to be suitable in developing nations where ensuring trust is of a major concern. The invention of blockchain can be seen to be a vital and much needed component of the internet that was lacking in security and trust before. Blockchain are also digitizing assets other than money. Companies that needed to maintain a public record such as holding land title, marriage or birth records should consider how their problems sets might be addressed by blockchain technologies. Blockchain also have strong potential for storing and recording supply chain records. A blockchain can record each step in a product's life from when it is created in a factory, to when it was shipped and subsequently delivered to store and finally to when a consumer purchased it.

There are many potential uses a opportunities for blockchain technologies. Blockchain technologies have the power to disrupt many industries. To avoid missed opportunities and undesirable surprises, organization should start investigating whether or not a blockchain can help them.

X. REFERENCES

[1]. Nirkshetri," can blockchain Strengthen the internet of things?", IT professional,vol.19,no.4,pp.68-72,may 2017,available:http://ieeexplore.ieee.org/document/8012302/

[2]. Mahdi H. Miraz , "Blockchain: Technology Fundamentals of the trust machine", Machine Lawyering ,Chinese university of hongkong, 23rd December

2017,Available:http://dx.doi.org//10.13140/RG.2.2.22541.64480/2
[3]. Don Tapscott and alex Tapscott, Block-chain Revolution: How the technology behind bitcoin is changing money, business ,and the world,1st edition Newyork, USA :penguin publishing group,2016.
[4]. Mareruf Ali and Mahdi h Miraz,"cloud computing Applications ,"in proceedings of the international conference on cloud computing and E-governance -ICCCEG 2013,internet city, Dubai, united Arab Emirates,2013,pp.1-8,Available:http://www.edlib.asdf.res.in/2013/iccceg/paper001.pdf
[5]. S.Nakamoto," bitcoin: A peer-to-peer electronic-cash system,"2008.Available:http://dx.doi.org/10.2139/ssrn.
[6]. G.W.peters, E. panayi, and A.chapelle," Trends in crypto-currencies and blockchain technologies: A monetary theory and regulation perspective",2015.Available:http://dx.doi.org/10.2139/ssrn.
[7]. "crypto-currency market capatilizations,"2017.Available:https//coinmarketcap.com
[8]. G.Foroglou and A.-L.Tsilidou," further applications of the blockchain,"2015.
[9]. C.miguel and L. Barbara ,"practical byzantine fault tolerance ,"in proceeding of the third Symposium on operating Systems Design and implementation,vol.99,new orleans,USA,1999,pp.173-186
[10]. D.maziers," the stellar consensus protocol :A federated model for internet-level consensus ,"Stellar Development Foundation,2015.
[11]. Balani, Naveen. How blockchain can help to solve the problem of trust in IoT.19 06 2016.
[12]. Nakamoto, s.,"Bitcoin: A peer-to-peer Electronics cash System,"2008.http://bitcoin.org/10.6028/NIST.FIPS.186-4
[13]. Clarke,A.c.," Hazards of prophecy :The Failure of imagination ,"from profiles of the future :An inquiry into the limits of the possible,1962.
[14]. Narayan, A., Bonneau,J., Felten,E., Miller,A., and Goldfede,s., Bitcoin and Cryptocurrency technologies :A comprehensive Introduction, Princeton University press4,2017.
[15]. https://www.multichain.com/blog/2017/05/blockchainimmutability-myth/
[16]."Bitcoin blockchain size reaches 100GB,"coinfox,December 19,2016. https://www.coinfox.info/news/6700-bitcoin-blockchain-size-reaches100gb
[17]. National institute of Standards and technology(NIST),secure Hashing website ,https://csrc.nist.gov/projects/hash-functions
[18]."hyperledger Business Blockchain Technologies", The Linux Found. https://www.hyperledger.org/projects
[19]. Cachin,c.," Architecture of the Hyperledger blockchain fabric ,"in workshop on distributed Crypto currencies and consensus ledgers july 2016
[20]. Greenspan,g.," The Blockchain Immutability Myth", multi chain ,may 4,2017.https://www.multichain.com/blog/2017/05/blockchainimmutability-myth/