A Technical Insight on Blockchain Technology and its Applications

[1] Shivani Sharma, [2] Dr. S. Kaushik, [3] Dr. Kuldeep Tomar

[1]PG Scholar, [2] Professor, [3] Professor

[1]Department of Computer Science & Engineering, NGF College of Engineering &Technology, Palwal (India)
[2]Department of Computer Science & Engineering, NGF College of Engineering &Technology, Palwal (India)
[3]Department of Computer Science & Engineering, NGF College of Engineering &Technology, Palwal (India)

We are living in a rapidly progressing world where technology is developing and progressing every single day. We have shifted from analog world to digital world as digital world leads to automation, efficiencies, speed and opportunities. With the increase in technologies, the need for security and the challenge on level of security of data also increased. So security of the system plays a vital role in development of digital world. A robust framework is desired on the prevention of the security breaches. We need processes which are more transparent, secure and efficient. A new technology came into existence named as "BLOCKCHAIN TECHNOLOGY" which have transformed the digital world into a more efficient and flexible world with high level of security. Blockchain is an open, distributed, decentralized, public ledger technology which enables us to maintain a permanent and tamper-proof record of transactional data where multiple authoritative domains that do not trust each other to cooperate, coordinate and collaborate in decision making process. In this paper we will look at the Blockchain Technology and focused exclusively on aspects of the technological infrastructure such as security, anonymity, scalability or the flexibility of consensus mechanisms. We will provide an overview on recent developments, feasibility and benefits of the Blockchain technology. The objective is to have an insight on the basic concept of Blockchain technology and the types of Blockchain technology we have and its uses in different fields. .

Index Terms - Cyber security, Bitcoin, Hyperledger, Smart Contract, IoT.

I. INTRODUCTION

"The Blockchain is an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value" by Don & Alex Tapscott, authors Blockchain Revolution (2016)

We are living in 21st century which is the era of digitalization, where everything has been transformed from analog to digital. Development in technology made the current system efficient and powerful to use. Enhancement of technologies gives us opportunities to develop but obstacles too. These obstacles are nothing but cyber-attacks which leads to compromise of data. Cyber thieves tries to steal data to fulfill different purposes. With the increase in technologies, the need for security and the challenge on level of security of data also increased. So security of the system plays a vital role in development of digital world. Strong measures must be taken to boost cyber security. A robust framework is desired on the prevention of the security breaches. We need processes which are more transparent, secure and efficient.

So to protect our data from intruders we tried to formalize some strategies from early 19th century. In 19th century, "cryptograph" was given by Edgar Allan Poe as a practice and study of techniques for secure communication in the presence of third parties called adversaries . In 1991, Stuart Haber and W. Scott Stornetta introduced "Cryptographically Secured Chain of Blocks" to timestamp documents. In 1992 Bayer, Haber and Stornetta designed "Merkle Tree" to improve the efficiency of "Cryptographically Secured Chain of Blocks" by allowing several document certificates to be collected into one block. Then in year 2008 a new technology named as "BLOCKCHAIN" was conceptualized by a person (or group of people) known as Satoshi Nakamoto [1].

A Blockchain is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way" by lansiti, Lakhani in 2017. It leads to creation of chain of blocks which is termed as Blockchain. Once the data has been stored in Blockchain it is impossible to modify or tamper with that data making Blockchain extremely secure and efficient to use.

In Blockchain we are moving from a centralized system to a distributed and decentralized system because centralization leads to single point of failure and there is complete reliance on a single machine which is not safe. With Decentralization we get multiple points of coordination and the problem of single point of failure get resolved. In Distributed environment everyone collectively executes the job. That is there is no reliance on single machine which makes the system safer.

Blockchain is a consensus oriented secured distributed public/private ledger which stored data over a peer to peer network in an immutable, irreversible and resilient way [2]. It can enable smart devices to act like an independent agent which can autonomously perform several transactions [3]. The Blockchain technology generally has key characteristics of decentralization, persistency, anonymity and auditability. With these traits, Blockchain can greatly save the cost and improve the efficiency [4]. Permanent record-keeping that can be sequentially updated but not erased creates visible footprints of all activities conducted on the chain. This reduces the uncertainty of alternative facts or truths, thus creating the "trust machine" [5]. Information security and privacy are enhanced by Blockchain technology in which data are encrypted and distributed across the entire network [6].

II. STRUCTURE OF BLOCKCHAIN

Blockchain is a growing list of record called blocks where each block points to its previous block. Block contains group of transactions and each new block is added to the longest chain. Initial block is referred as Genesis block which doesn't points to its previous block as shown in figure 1.

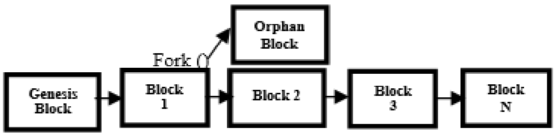

Figure 1: Blockchain Terminology

Genesis block contains a text message "The Times 03/Jan/2009 Chancellor on brink of second bailout for banks" .The message was embedded in the first block by Bitcoin's creator Satoshi Nakamoto. [3]

Fork happens when Blockchain splits into branches. We have accidental forks and intentional forks. When two or more blocks are created at same time it results in creation of accidental fork which splits the Blockchain into two branches. It leads to inconsistent state of the network. The fork is resolved when subsequent block or blocks are added and one of the chains becomes longer than the other. The network abandons the blocks that are not in the longest chain and the blocks are called orphaned blocks. Detached or Orphaned blocks are valid blocks but not part of the main chain. Intentional forks are result of modification in rules of Blockchain.

So to deal with it new blocks are added to the longest chain which is then considered as main chain. Blocks are connected to each other using cryptographically secured hash function forming a chain and this chain acts as a database of historic information available to every peer participating in the network and termed as Public Ledger as shown in figure 2. A ledger often consist of two data structure which includes Blockchain and world state. Blockchain is an immutable linked list of record where blocks cannot be tampered with. World state stores most recent state of transactions where data elements can be modified, added, deleted as transactions on Blockchain.

Once anything is stored over Blockchain it is impossible to tamper with that data as blocks are connected to each other using cryptographically secured hash function. Being a one way function makes Blockchain impossible to tamper with.

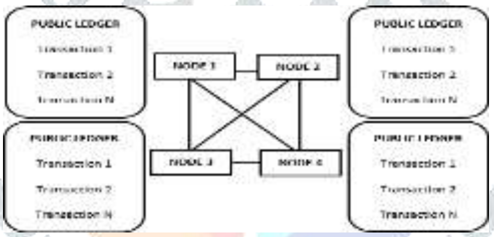

Figure 2: Public Ledger

The public ledger is replicated, synchronized and spread across multiple nodes helping the nodes in the network to validate future transactions. Transactions are added to Blockchain only after majority of nodes agrees upon particular transaction. Consensus mechanism is used to reach on necessary agreement on single state of the network among distributed processes. In this way public ledger acts as a local copy of global information available to every peer which gives Blockchain the power to record transactions between two parties efficiently and in a verifiable and permanent way. The Blockchain technology is attracting a varied audience with its incredible scope in the financial and non-financial field. Blockchain needs to ensure different aspects which include Protocol for commitment, consensus, security, privacy and authenticity as shown in Table1.

Aspects	**Description**
Protocol for commitment	Guarantee that every valid transaction from client must be committed and included into Blockchain within a limited measure of time.
Consensus	Ensure that the local copies are always consistent and updated.
Security	The data needs to be tamper proof. Note that the clients may act maliciously or can be compromised.
Privacy and authenticity	As the data belong to various clients. So protection and genuineness should be guaranteed.

Table 1: Important aspects of Blockchain

III. TECHNICAL ASPECTS OF BLOCKCHAIN

A wide range of technical consideration has been implemented in Blockchain technology which includes cryptography, digital signature, cryptographic hash functions, time stamping document and consensus mechanisms.

Cryptography is used to achieve secret communication in presence of adversaries by transforming message to make them secure and proof against attacks. Cryptography provides data confidentiality, data integrity, authentication and non-repudiation which makes data more secured.

Digital Signature is used to verify the authenticity of digital message. A Digital code is included in the document which provides authentication, integrity of document and non-repudiation.

Time stamping Documents is used to make the system secure against forgery and time stamping the entries results in lessen of fraud.

Cryptographic hash function is a mathematical algorithm that maps data of arbitrary size to a bit string of a fixed size and is designed to be a one-way function.

Consensus is used to reach on a common agreement on distributed system. A consensus mechanism is a fault-tolerant mechanism that is used in Blockchain systems to achieve the necessary agreement on a single data value or a single state of the network among distributed processes or multi-agent systems. We have various consensus mechanism which includes Proof of work, Proof of Stake and Proof of Burn as shown in table 2.

Proof of work	Proof of Stake	Proof of Burn
Do some work to mine a Block	Acquire sufficient stake to mine a Block	Burn some wealth to mine a block
Consumes physical resources like CPU, power and time	Consume no external resources but only participation in transaction	Consumes virtual or Digital resources like the coin
Power hungry	Power efficient	Power efficient

, Table 2: PoW vs PoS vs PoB

Other consensus mechanisms are Raft algorithm, Parox algorithm and Byzantine Fault Tolerance (BFT) algorithm.

IV. TYPES OF BLOCKCHAIN

Blockchain is a stunning technology which started its journey from bitcoin and is capable of doing much more than a financial transaction. Bitcoin revolution motivated mainstream companies to use the main Blockchain idea in industry, manufacturing, supply chain, finance, governance, IoT etc. . With the evolution of this idea Blockchain has been categorized as Public Blockchain, Private Blockchain and Consortium Blockchain to make it suitable to attain in different areas as different areas have different requirement which needs to be fulfilled to get desired goal. Different types of Blockchain have different functionality which has been described in this paper in detailed manner.

V. PUBLIC BLOCKCHAIN

The Public Blockchain is also known as permissioned Blockchain. Public Blockchain is a fully decentralized, permission less and open source system where anyone can access the network without any authentication and participate in reading, writing and auditing the Blockchain.

The first public Blockchain came in 2008 and named as Bitcoin. Bitcoin is a cryptocurrency which makes it beyond the control of bank or government. Anyone can join the bitcoin network without any authentication and can play any type of role. Software runs on each machine of user and no central authority keeps track of anything. Decision making happens through a consensus algorithm Proof of Work. It is based on challenge response protocol where nodes in the network tries to solve the challenge posed by the network. In bitcoin three cryptographic primitives are used – Cryptographic Hash Function, Digital Signature and Public Key Cryptography. In Each bitcoin user may have one or more digital wallet each having a public key and private key. Seed nodes are responsible for adding new peers/nodes in the network.

Bitcoin Transaction: If a user A wants to send some Bitcoin to user B. User A opens his wallet and then put address of user B with the amount of Bitcoin he wants to send. Then user A digitally signs the transaction with his private key and broadcasts transaction over the network. The nodes in the network validates the transaction (FORTH language is used to validate the transaction) with the help of public ledger available to every node and propagates the transaction to miners. Miners collect all the transactions and try to create a block containing those transaction and aims to connect it with the existing Blockchain using the cryptographically secured hash function. The miner who solves the cryptographic computation in the least time adds his block to the existing Blockchain and that updated Blockchain is propagated to the network.

In bitcoin, a block consists of two parts which includes Block Header and List of Transactions as shown in figure 3. Block header contains metadata about a block such as previous block hash, mining statistics which includes version, nonce, difficulty and timestamp and Merkle tree root. List of transactions are organized as a Merkle tree. A Merkle tree is constructed by recursively hashing pair of transactions using double SHA-256 until there is only one hash called Merkle root. The Merkle tree root is used to construct the block hash. In bitcoin a block may contain 500 transactions and the explicit size of block is around 1 MB as introduced by Satoshi Nakamoto in 2010.

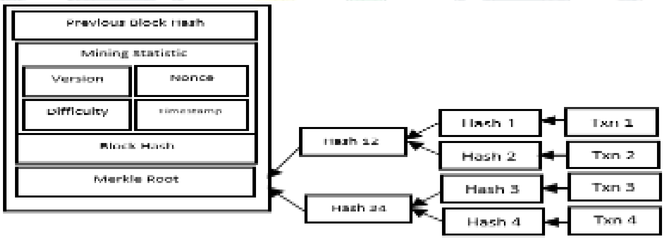

Figure 3: Block in a Bitcoin Blockchain

A node in a bitcoin network can be a normal node which can make or validate the transaction or miner node. Anyone who have GPU's can participate in the mining procedure by just running a piece of software. Miners get rewarded for each block they have mined. According to bitcoin principle the reward for mining Bitcoin block is reduced to half after every 210,000 blocks. Bitcoin solves the problem of double spending as each node in the network have a copy of public ledger to validate the future transaction.

At present BTC price of 1 BTC = $5014 (as of 05th, April 2019 at 07:46 pm). The Bitcoin Blockchain size as of April 2019 is approximately 197.7 GiB [7]. The number of bitcoins generated per block is set to decrease geometrically, with a 50% reduction for every 210,000 blocks, or approximately 4 years [8]. Bitcoin propagation delay latency has a mean time of 12.6 seconds which states that 95% of the nodes can see the block within 40 seconds [9].

The concept of mining pool is used in bitcoin which states that the miners can share the processing power over the network to mine a new block and then split the reward proportionally to the amount of work they contributed. Mining pool methods include pay per share (PPS), Pay per Last N Share (PPLNS) and Propositional.

Other cryptocurrency based on Blockchain principle includes Litecoin, Bytecoin, Peercoin, etc with their own features and principles. At present we have more than 1500 cryptocurrency.

VI. PRIVATE BLOCKCHAIN

Private Blockchain is permissioned and closed system mainly designed to provide effective and efficient enterprise solutions. In private Blockchain users are authenticated priory and they know each other. Consensus mechanism is still required as nodes do not trust each other. Different access permissions are granted to each node participating the network. It is impossible to tamper with data but easier to validate transactions making system highly secure, faster and cost effective.

Hyperledger is an open source project by Linux foundation to match requirements of an enterprise Blockchain framework. Hyperledger holds different Hyperledger platforms and Hyperledger tools. It has five platforms which are Burrow, Iroha, Fabric, Sawtooth and Indy. It has five tools which are Quilt, Cello, Caliper, Explorer, and Composer.

Hyperledger Fabric is an open source, permissioned platform which includes execution of smart contract, configurable consensus and membership services. In Hyperledger fabric nodes are authenticated by special services called membership services. Nodes which are part of the network can see the transactions. Nodes are given special rights priory by membership services. Nodes are divided into three types which include committing peer, endorsing peer and ordering node. Each node have specific responsibility to perform in the network. Firstly the transaction is endorsed, ordered and then validated. The concept of channels is used to provide privacy between ledgers. Smart contracts are used by endorsing nodes are named as chaincode. The Hyperledger fabric v1 architecture is shown in figure 4.

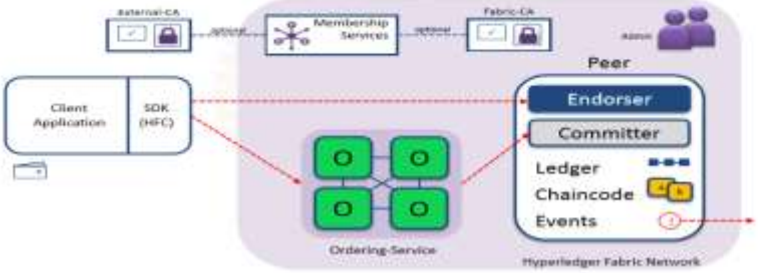

Figure 4: Hyperledger Fabric V1 Architecture

Image courtesy: www.nptel.ac.in [10]

VII. CONSORTIUM BLOCKCHAIN

Online Consortium Blockchain is permissioned and closed system primarily designed to produce effective and efficient solutions to group of companies that come along and work for the benefit of the network. Here multiple selected organizations or group come together and build a consortium. Consortium Blockchain are primarily deployed in banking sector. Suppose we have a consortium of 100 financial institution and each operate a node forming a network. For a block to be valid it must be signed by 90 nodes.

Corda is a distributed ledger platform for permissioned network and inspired by Blockchain technology. Corda is specifically designed for financial services use cases. R3 is a consortium of more than 60 of the world's biggest banks and leads the development of Corda. Corda is mainly designed for data privacy and open sourced on November 2016 [11]. R3 offers Corda enterprise edition which is compatible with open source Corda. Corda does not have any global broadcast. It has a UTXO state-machine model. It has distributed ledger but no Blockchain .Contracts can be written in JVM based language such as Kotlin, Java, Scala and Clojure.

VIII. SMART CONTRACT

In 1996 Nick Szabo presented the concept of smart contract. It is a preprogrammed automatic protocol used for digitally making, performing a legal contract and then validating it on a decentralized platform by avoiding intermediaries (middleman). The purpose of smart contract is to provide protection and reduce transactional cost. Opposed to crowdfunding which is a centralized platform for executing contracts, Blockchain can be used as an astonishing technology to realize smart contact. Using Blockchain technology it would be impossible to make any type of change in the smart contract as it is written on public ledger (Blockchain). At present we have various smart contract platforms which include Hyperledger, Ethereum, ripple etc.

IX. BLOCKCHAIN USE CASE

Blockchain can be used for cross border payment. Steller protocol and network provides a decentralized, hybrid Blockchain platform with open membership used for cross border payments. Ripple protocol and network is a protocol for banks to clear and settle payments in real time through distributed consensus [10]. The ability to create/store/transfer digital assets in a distributed, decentralized and tamper-proof way is of a large practical value for IoT systems. While micro-payments in IoT may be the most obvious use of Blockchain technology, we consider the storage/sharing of data & code the most useful at the current state of IoT deployments. IBM's ADEPT system that is built on Bluemix is an excellent example of early Blockchain use within IoT. ADEPT showcases scalable storage of IoT configuration data and provides a platform for micro-payments. [12] Blockchain provides shared KYC (Know Your Customer) information on Blockchain thus eliminating redundancies, increasing information and standardizing the process. Blockchain can be used in mortgage and syndicated loans making the process effective and fraud less. Blockchain technology can provide effective solution in supply chain by providing traceability across supply chain.

X. CONCLUSION

With the increase in technologies, the need for security and the challenge on level of security of data also increased. Blockchain is an impressive technology consummating major security goals by providing efficient and efficacious solutions to problems. It started its journey from bitcoin and growing rapidly in each and every field. At present Blockchain is at boom and research is still going on this astonishing technology. This paper conclude that there are numerous opportunities of research in this technology.

REFERENCES

[1]. Satoshi Nakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System".

[2]. Chatterjee Rishav , Chatterjee Rajdeep " An Overview of the Emerging Technology: Blockchain", International Conference on Computational Intelligence and Networks, DOI 10.1109/CINE.2017.33, 2017 IEEE

[3]. Singh Sachchidanand, Singh Nirmala,"Blockchain: Future of Financial and Cyber Security ", 2nd International Conference on Contemporary Computing and Informatics (ic3i), 978-1-5090-5256-1/16/ 2016 IEEE

[4]. Zheng Zibin , Xie Shaoan "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends", 6th International Congress on Big Data , 978-1-5386-1996-4/17 , DOI 10.1109/BigDataCongress.2017.85, 2017 IEEE

[5]. Beck Roman " Beyond Bitcoin: The Rise of Blockchain World", IEEE COMPUTER SOCIETY, 0018-9162/18/$33.00 © 2018 IEEE

[6]. Elisa Noe , Yang Longzhi "A framework of blockchain-based secure and privacy-preserving E-government system", Wireless Networks, https://doi.org/10.1007/s11276-018-1883-0(0123456789().,-volV)(0123456789().,-volV) ,Springer

[7]. https://charts.bitcoin.com/btc/chart/blockchain-size

[8]. https://en.bitcoin.it/wiki/

[9]. Decker, Christian, and Roger Wattenhofer. "Information propagation in the bitcoin network." 2013 IEEE Thirteenth International Conference on Peer-toPeer Computing (P2P). IEEE, 2013

[10]. www.nptel.ac.in

[11]. https://github.com/corda/corda

[12]. Samaniego Mayra, Jamsrandorj Uurtsaikh, Deters Ralph, "Blockchain as a Service for IoT Cloud versus Fog ",2016 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), 978-1-5090-5880-8/16 $31.00, DOI 10.1109/iThings-GreenCom-CPSCom-SmartData.2016.102, 2016 IEEE

[13]. Tareq Ahram1, Arman Sargolzaei2, Saman Sargolzaei3,4, Jeff Daniels5, and Ben Amaba6 "Blockchain Technology Innovations ", 2017 IEEE Technology & Engineering Management Conference (TEMSCON)

[14]. Halpin Harry, Piekarska Marta. "Introduction to Security and Privacy on the Blockchain", 2017 IEEE Europeon Symposium on Security and Privacy Workshops (EuroS&PW), DOI 10.1109/EuroSP.2017.26.43, 2017 IEEE

[15]. Vujičić Dejan, Jagodić Dijana, Ranđić Siniša ,"Blockchain Technology, Bitcoin, and Ethereum: A Brief Overview ",17th International Symposium INFOTEH-JAHORINA, 21-23 March 2018 , 978-1-5386-4907-7/18/$31.00 ,2018 IEEE

[16]. Yli-Huumo Jesse, Smolander Karl,"Where Is Current Research on Blockchain Technology?—A Systematic Review", DOI:10.1371/journal.pone.0163477 October 3, 2016

[17]. Mahdi H. Miraz1, Maaruf Ali,"Applications of Blockchain Technology beyond Cryptocurrency ",Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018

[18]. Nofer Michael , Gomber Peter , Hinz Oliver , Schiereck Dirk, “Blockchain”, DOI 10.1007/s12599-017-0467-3, Springer Fachmedien Wiesbaden 2017

Author’s Profile

Dr. Kuldeep Tomar did his Ph.D in the area of Computer Network Security. He is currently working as Professor and Head in Department of Computer Science and Engineering in NGFCET, Palwal, Faridabad, and Haryana. He has guided thesis/Dissertation of post graduate students in the field of Network Security, Artificial Intelligence, Cryptography, etc. He has done certification on “Research Writing” and “Blockchain Architecture and Use Cases” from IIT Kharagpur (NPTEL). He was born in Sonepat, Haryana on 2nd Oct, 1978. He has done M.E/ M.Tech in Computer Science and Engineering from C.I.T.M., Faridabad, India. He has a total experience of 15 years in different organizations. He also has worked as Assistant. Professor in Skyline Institute of Engineering & Technology, Gr. Noida; as Senior Lecturer in B.S.A.I.T.M., Faridabad; as Technical Head/Manager at SSI (Software Solutions Integrated Ltd. and as Sr. Faculty at Hartron Workstation (Haryana Govt. Undertaking). He has published more than 15 papers in International/National Journals and conferences etc. Has is also written a book. He has been a member (Institutional Nomination) of Computer Society of India, Membership No:N1039627.

Shivani Sharma is a research scholar in the department of Computer Science and Engineering , NGFCET, Palwal, 121102, India. She was born in Haryana on 16th April 1994. She did her B.Tech in Computer Science and Engineering from MVNU,Palwal,Haryana, India. She has cleared GATE 2017. She has done certification on “Blockchain Architecture and Use Cases” from IIT- Kharagpur (NPTEL).