A SURVEY ON DIGITAL NETWORK THROUGH BLOCKCHAIN TECHNOLOGY

RAHUL KUMAR[a1], S.K. PATHAK[b] AND DEEPAK KUMAR SINGH[c]

[abc] Department of Computer Science & Engineering, Dr. K.N. .Modi University, Rajasthan

ABSTRACT

In order to increase the efficiencies, to make the thing faster and accurately we have been switching over digital world from analog world. A wide range of services have been implemented in form of digital technologies that make us efficient in so many means. A wide range of network has been implemented that make possible all of these things. There are two issues that make us insecure while using these technologies. The major issues associated with the present digital world is what happened if nobody are trusted to each other and they have to make a transaction digitally in a secure way without disclosing their identities. Blockchain technology plays a vital role in such scenario. Any kind of collaboration or partnership heavily depends upon trust, but at present world where regulation are increasing or updating day by day, and fraud are taking places rapidly we can't rely only verbal or paper written commitment. In order to solve these issues Blockchain make enable the digital world more promising, safe, and efficient. In this study, authors have shown that how the Blockchain are recorded any kind of transaction that are permanent, well-proved, and temper-proof. This paper also explored the features of transaction recording, fault-provenance, identity management in a decentralized environment without a trusted authority.

KEYWORDS: Decentralized; Distributed; Ledger; Consensus

In each next hour, our means of living and therefore the way to experiencing the globe turning into additional addicted to digital world. within the gift era, wherever most of the factor have taken the place in digital suggests that, wherever rate of fraud and cyber-crime are accumulated day by day, wherever the economic process are largely dependent upon the digital technologies, wherever nobody is prepared to trust one another whereas creating any quite dealings, there are a powerful demand of platform on digital ground which will addresses of these problems. Within the contemporary world, we tend to create largely any kind dealings that passes through the intermediaries. as an example, once a celebration desires to transfer some cash to different parties then these transactions ensue beneath some intermediaries, sort of a monetary establishments, bank that additionally impose the fees for the service. In such a case, each the parties should have the trust over the intermediaries. But, what's going to happen if anyone of the party don't have a trust over the intermediaries. What's going to be if parties concerned in dealings wish to create a secure and well-proof transaction while not together with any varieties of intermediaries? subsequent problems with this system is, if a collection of parties wish to create some dealings among themselves then UN agency are answerable for the valid, consistent, and fraud-free dealings. So, a sturdy framework is extremely demanded on the interference of the protection breaches. We'd like processes that are additional clear, secure and economical. Blockchain have the key feature that addresses all of those problems. "The Blockchain is an incorrupt digital ledger of economic transactions that may be programmed to record not simply money transactions however just about everything of value" by Don & Alex Tapscott, authors Blockchain Revolution (2016). A Blockchain is "an open, distributed ledger which will record transactions between 2 parties expeditiously and during a verifiable and permanent way" by lansiti, Lakhani in 2017. It results in creation of chain of blocks that is termed as Blockchain. Once the info has been keep in Blockchain it's not possible to change or tamper thereupon data creating Blockchain extraordinarily secure and economical to use. Blockchain as a "network of computers, all of that should approve a group action has taken place before it's recorded, during a 'chain' of coding system. the main points of the transfer are recorded on a public ledger that anyone on the network will see." As a promising technique to attain decentralized accord, blockchain has been with success applied into digital currency - bitcoin for serving as a public ledger for transactions. Its secure style for supporting a distributed system with high Byzantine fault tolerance is attracting wide attention everywhere the globe.

The Blockchain technology usually has key characteristics of decentralization, tenaciousness, obscurity and auditability. With these traits, Blockchain will greatly save the value and improve the efficiency [Satoshi Nakamoto, 2008]. Info security and privacy are increased

[1]**Corresponding author**

by Blockchain technology during which knowledge are encrypted and distributed across the complete network [Chatterjee Rishav et al 2017]. It can change good devices to act like an freelance agent which might autonomously perform many transactions [Singh Sachchidanand et al 2016]. Blockchain may be a accord bound secured distributed public/private ledger that keep knowledge over a peer to see network in associate changeless, irreversible and resilient manner [Zheng Zibin et al 2017]. Permanent record-keeping which will be consecutive updated however not erased creates visible footprints of all activities conducted on the chain. This reduces the uncertainty of different facts or truths, therefore making the "trust machine" [Beck Roman 2018].

BLOCKCHAIN: TECHNICAL PERSPECTIVES

"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). "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 who do not trust each other to cooperate, coordinate and collaborate in decision making process." A brief description of keywords used is shown in Table 1.

Table 1: Representation of keywords

Keywords	Description
Open	Accessible to all
Distributed	Everyone collectively execute the job
Decentralized	No single party control
Efficient	Very fast and reliable
Verifiable	Everyone can check validity of information
Permanent	Information is persistent

With Decentralization we get multiple points of coordination and the problems 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 works on the principle of public ledger. Blockchain is a new revolutionizing technology with distributed ledger system or public ledger system. A public ledger provides a database of historical information available to everyone which could be used to validate future transaction. Distributed ledger or shared ledger or public ledger is a ledger that is replicated, synchronized and spread across multiple nodes.

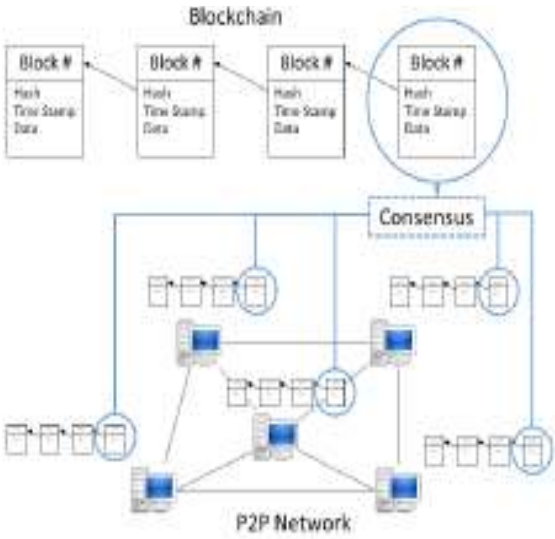

Figure 1: Key element of Blockchain

DIFFERENT TYPES OF BLOCKS IN A BLOCKCHAIN

Genesis Block

A genesis block is that the 1st block of a Block chain. Initial parameters of the Blockchain like level of issue, accord rule etc. are outlined in genesis block to mine blocks. . Genesis Block is that the solely block within the Blockchain that doesn't discuss with previous block as a result of it doesn't have any previous block.

New Block

Blocks are organized into a linear sequence over time. New Blocks are always additional to the end of the chain and a brand new Block is often added to the end of the longest chain.

Orphan Block

Orphan blocks are termed as Detached Blocks. They're valid blocks that aren't a part of the main chain. They're valid and verified blocks, however are rejected ones. Orphan block are happens once over one miner generate a brand new block at same time.

Fork

Once Blockchain is splatted into 2 elements it's termed as Fork. Forks is categorized as Accidental or Intentional:

a) Accidental fork: It happens once 2 or more new blocks are find at nearly a similar time and additional to the Blockchain. The fork is resolved once consequent block or blocks are additional and one amongst the chains becomes longer than the opposite. The network abandons the blocks that aren't within the longest chain and therefore the blocks are referred to as orphan blocks.

b) Intentional forks: they're results of modification in rules of Blockchain. They will be additional classified as arduous Forks and Soft Forks.

i. arduous Forks: we'd like changes in software system and up gradation time to time. Therefore 2 totally different versions of the Blockchain software system are created sharing identical origin that is usually results in arduous forks. It's necessary to figure in accordance with latest rules by enhancing the software system.

ii. Soft Forks: A soft fork might be a backward compatible technique of upgrading a Blockchain. In numerous words, a soft fork is code upgrade that's backward compatible with previous versions of the code. Soft forks don't would like nodes on the network to upgrade to stay up accord, as a results of all blocks on the soft-forked Blockchain follow the recent set of accord rules additionally the new rules.

MAJOR ASPECT OF BLOCKCHAIN

It includes protocol for commitment, consensus mechanism, security, privacy and authenticity. These characteristic are very crucial for Blockchain technology to hold. These features/ aspects of Blockchain technology have been shown in table 4.1 with description of their roles.

EMERGING TYPE OF BLOCKCHAIN

We have broadly classify Blockchain into three categories names as Public Blockchain, Private Blockchain and Consortium Blockchain:

Public Blockchain

Anyone can access the network and participate in reading, writing, and audit the Blockchain, as it is a fully decentralized, permission less, and open-source system.

The creation, validation and visibility of transaction is accessible to everyone. To validate transactions, decision making happens through a consensus algorithm such as Proof of Work (PoW) or Proof of Stake (PoS).The system is open to all which means there is no central authority to authorize anyone. The establishment of trust is among peers is established via consensus mechanism. The system is open source and it is highly secured using cryptography and consensus protocol. There are numerous public Blockchain. Examples: Bitcoin, Ethereum, etc. Bitcoin is the first cryptocurrency generated using Blockchain technology and is based on public Blockchain principle. Then Ethereum was conceptualized based on Blockchain principle allowing us to construct smart contract and decentralized applications.

Table 1: Important aspects of Blockchain

ASPECTS	DESCRIPTION
Protocol for commitment	Ensure that every valid transaction from client must be committed and included in block chain within a finite amount 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 privacy and authenticity needs to be ensured.

Private Blockchain

In Private Blockchain we want permission to participate and closed system is established beneath the management of a private or an organization. Non-public Blockchain is simply opposite to public Blockchain. In

private Blockchain users are documented a cloister and users recognize one another. We permissioned scan and write access to information. Though users recognize one another however they are doing not trust each other. Security and accord mechanism remains needed for consensus vote or multi-party consensus algorithmic rule is employed. Non-public Blockchain networks are sometimes applied to internal systems of one private company, that's we have a tendency to run Blockchain among best-known and identified participants. . Write permissions are unbroken centralized to at least one organization. Scan permissions may even be public or restricted to an absolute extent. It's laborious to tamper with information however easier to validate transactions, creating the system quicker and more cost effective. Examples: MONAX, Multichain, Hyperledger

Consortium / Federated Blockchain

A federate or consortium Blockchain could be a permissioned and cluster-owned system wherever permissions are unconditional in a very group of firms or people. There's over one central authority who can give access to pre-selected nodes to read, write, and audit the Blockchain. The creation, validation and visibility of any dealing is restricted to members of consortium. Agreement is achieved through a selection or multi-party consensus rule whose rules rely on the agreement of the participants it provides the additional advantage of removing the consolidation of power to only 1 company. After we need collaboration of varied organization then this Blockchain network is most ideal. That's federate Blockchain operate below the leadership of a bunch. As against public Blockchain, they don't permit any individual with access to the net to participate within the method of confirmative transactions. Federate Blockchain is quicker and extremely ascendible. It provides a lot of group action privacy. Association Blockchain is usually utilized in the banking sector. Nodes are elite a cloister to manage the agreement method. One will visualize a association of twenty financial institutions, every in operation a node and therefore the condition includes that twelve nodes should validate the block so as to incorporate it in Blockchain. Example: R3 Corda

Table 2: Comparision aming different types of Blockchain

Feature	Public Blockchain	Private Blockchain	Federated/Consortium Blockchain
Access	Anyone	Single organization	Multiple selected organizations
Participants	Permission less and Anonymous	Permissioned and Known identities	Permissioned and known identities
Security	Consensus mechanism(Proof of Work/ Proof of Stake)	Pre-approved participants Voting/Multiparty Consensus	Pre-approved participants Voting/Multiparty Consensus
Transaction Speed	Slow	Lighter and faster	Lighter and faster

CONCLUSION

Blockchain technology can be applied in government, health, science, literacy, publishing, economic development, art, and culture, and possibly even more broadly to enable orders-of-magnitude larger-scale human progress. Most of the technical leader have been invested a lots towards the Blockchain technology. Blockchain technology is the most promising technology to improve transparency without any authority control. There are huge opportunities where Blockchain technology can be implemented effectively by addressing the present challenges.

REFERENCES

Satoshi Nakamoto,"Bitcoin: A Peer-to-Peer Electronic Cash System". October 2008.

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.

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.

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.

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

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

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

https://en.bitcoin.it/wiki/

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

www.nptel.ac.in

https://github.com/corda/corda

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.