International Engineering Journal For Research & Development
Vol.4
Issue 5

E-ISSN NO:-2349-0721

Impact factor : 6.03

SURVEY OF RECENT TRENDS IN BLOCKCHAIN TECHNOLOGY

Nilima V. Pardakhe
dept. of CSE ,PRMIT&R,Badnera
Amrvati, India
nvpardakhe@mitra.ac.in

Dr. Vaishali M. Deshmukh
dept. of CSE ,PRMIT&R,Badnera
Amrvati, India
vmdeshmukh@mitra.ac.in

Abstract-

The technology has reached such level that the modern Internet deals with assets of real life. People want everything in a smart way. Nowadays, there is no longer any doubt about a digital world. This will be a world of AI, robots will replace human completely in the work force. A world of smart houses, smart cities, smart countries, where everything has the ability to connect to the internet (IoT), bringing the real and digital world closer together. Along with other advanced technologies (AI, AR/VR, IoT), Blockchain technology has established a way to digitize all of our activities through cloud based development. Blockchain is a shared public ledger, and it includes all transactions which are confirmed. It is almost impossible to crack the hidden information in the blocks of the Blockchain. However, there are certain security and technical challenges like scalability, privacy leakage, selfish mining, etc. which hampers the wide application of Blockchain. Blockchain is rapidly evolving to be the next disruptive innovation for secured connectivity, promising major changes to how we work and live in the coming century. This paper will highlight the important role of blockchain technology in the development of our future world and survey of recent trends in blockchain technology.

Keywords— Blockchain, Decentralization, Internet of things, Smart contracts, security

I. INTRODUCTION

In this era of computerization of business, organizations focus is mainly on future predication by considering the historical data. The unceasing growth of the Internet of Things (IoT), Cloud and Edge Computing and Big Data are rapidly necessitating novel solutions to manage distributed and decentralized systems. Additionally, in the era of those areas, the enforcement of secure, trusted, and verifiable services is paramount, as the volume of network-connected user data and vulnerable devices is unprecedented and increasing. Blockchain is a distributed and immutable ledger of transactions, in which each transaction is inexorably linked to the prior one. As the primary purpose of the blockchain, operation in untrusted decentralized environments can be secured by both the record of transactions, and decentralized consensus on the validity of the transaction record. In addition, transactions implement operational code, enabling software services between untrusted users. Since first used in cryptocurrencies, interest has been increasing as both industry and academics evaluate the applications and operation of the underlying blockchain technologies. Particularly, blockchain has been envisioned as a viable solution to the many needs of emergent applications, including Internet of Things (IoT), Big Data, Cloud and Edge Computing, Identity Management, and many others. Simultaneously, significant work is ongoing in industry to evaluate the efficacy of blockchain for various business applications, and the frameworks themselves are evolving within this atmosphere to realize the potential future needs.

Despite the potential that blockchain raises, it is clearly balanced in favor of securing user privacy, and leaves unresolved many issues regarding platform utilization from the perspective of a service provider, as well as the intrinsic computational overhead of consensus and scalability, which remains a critical challenge for wide adoption. In addition, despite the potential for blockchains to revolutionize distributed and decentralized architectures, in practice there have been some troubling results which need resolution. Just like any software system, vulnerabilities in the encoded implementation or an underlying operating system may create the potential for malicious subversion of users or the entire system. What's more, certain theoretical aspects of the system itself may afford malicious use. From this perspective, it is imperative that a thorough evaluation be conducted to fully consider the implications of the technology.

A. What is blockchain?

Blockchain is a data-sharing infrastructure used to create peer-to-peer digital currency, the most famous of which is Bitcoin, which was launched in 2008 and more recently Ethereum. Blockchain is an accounting ledger operating in the digital domain, similarly to a company's cash accounting book. However, it allows for the recording and sharing of transactional information publicly within the network. Blockchain stores and transmits information through linked blocks that expands over time. Each block contains information on initialization time and is connected with the previous block. This transmission system is based on an extremely complex encryption system, consisting of multiple independent nodes capable of authenticating information without requiring a "common sign of trust". This node system is a sequence of independent servers, where all users must approve a transaction before it can be validated and logged into the network.

B. Why called blockchain?

The blockchain mainly used for Security purpose for securing the data. The data sent to each block on the distributed ledger is based on encrypted Merkle Trees, which is a technical way of saying that no fraudulent transactions can be recorded. If any transaction that does not follow protocol rules is detected by the network nodes, it is expelled immediately. This inherently secure nature of distributed blockchain technology means that it prevents damage to the entire blockchain shared database and can cut off a hacking attempt at one block. Due to this secure nature blockchain mainly used where more protection is needed to database. Also a company, to manage the ledger, it usually requires a competent person to take responsibility for checking all the data and verifying by signing their signature at the bottom of the content. This signature ensures that no one will be able to edit the archived content and is an indication that the data added later will not be accepted. Similarly, in the blockchain system, transaction log information is stored in a file called a block. These records are stored in a cabinet and stacked sequentially, the front block is followed by the next block forming a chain of block called blockchain.

C. How blockchain works?

Anyone has the opportunity to add a new trading block to the accounting ledger, provided that the cryptographic puzzles that the system provides are dealt with. The volunteers involved in solving these puzzles are called Miner, with the tool being a standalone server system. The miners will collect transaction information in the blockchain network every 10 minutes. That information is considered a ticket that allows the miners to enter a contest. Whoever wins will be entitled to create the next new block. After that, the miners will update the blockchain copy and start on another competition. The reward for the winning miner or answer to the current puzzle is 12.5 Bitcoin. This is also the reason that blockchain technology is expected to dominate the world in a few years.

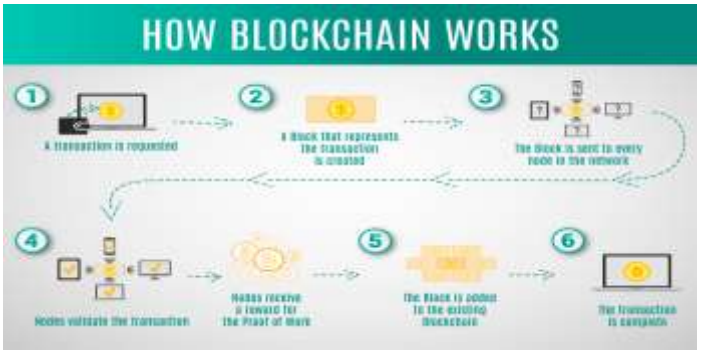

Fig.1: Working of Blockchain

A. Blockchain Taxonomy

The Blockchain system is categorized into three categories, namely, public, private and consortium Blockchain [1].

Public Blockchain

As the name implies, anyone can join the consensus process means each node can participate in the consensus process in a public Blockchain. Anyone can send transactions to and check whether the transactions are valid or not. It is also called decentralized and permission-less networks. In public networks, consensus is

costly and an economic incentive to the miners is usually needed. It is nearly impossible to tamper the public Blockchain, since transactions are stored in different nodes in the distributed network. For this reason, public Blockchain is less efficient too. It takes a significant amount of time to propagate transactions and blocks, because there are a large number of nodes in the network. Transaction throughput is limited and the latency is high.

Private Blockchain

Private Blockchain is fully centralized. It is because the Write permissions are kept centralized to one organization. However, the Read permission is kept public. Private Blockchain is operated in a controlled and a regulated environment. In this type of Blockchain, all participants in this network are not be allowed to transact or participate in the mining process based on the permission imposed. The organization has the full control to determine the final consensus. However, if the majority of the consortium or the dominant organization wants to interfere the Blockchain, the consortium private Blockchain could be reversed or tampered. The fewer the validators, the more efficient is the private Blockchain. Private Blockchain issue a certificated to join the consensus process. The key strengths are efficiency and auditability.

Consortium Blockchain

Consortium Blockchains is not decentralized but "partially decentralized". The consensus process involves validating the blocks with only a few selected sets of responsible nodes exist. The visibility of a transaction of a Blockchain persists depending on the Read permission granted on a consortium Blockchain, even though transactions in a public Blockchain are visible to the public. The organization is soul responsible whether the stored information is public or not. Same as the private Blockchain, consortium Blockchain is more efficient with lesser validators. In this type of Blockchain, only the certified nodes can join the consensus process. Many public Blockchains are emerging and attract many users. Many business applications use consortium Blockchain example Hyperledger (Hyperledger, 2015). Ethereum also is a tool for building consortium Blockchains. There are still many companies implementing consortium Blockchain for efficiency and auditability.

II. BACKGROUND

Each block in a blockchain contains transaction data, a hash function and hash of the previous block. Blockchain is managed by a peer-to-peer (P2P) network. On the network, no central authority exists and all blocks are distributed among all the users in the network. Everyone in the network is responsible for verifying the data that is shared, and ensuring that no existing blocks are being altered and no false data is being added. Blockchain technology enables direct transaction between two individuals, without the involvement of a third party and hence provides transparency. When a transaction happens, the transaction information is shared amongst everyone in the blockchain network. These transactions are individually time stamped. When these transactions are put together in a block, they are time stamped again as a whole block. Blockchain can be used to prevent cyber-attacks in three ways – by being a trusted system, by being immutable and by network consensus.

A blockchain based system runs on the concept of human trust. A blockchain network is built in such a way that it presumes any individual node could attack it at any time. The consensus protocol, like proof of work, ensures that even if this happens, the network completes its work as intended, regardless of human cheating or intervention. The blockchain allows one to secure stored data using various cryptographic properties such as digital signatures and hashing. As soon as the data enters a block in the blockchain, it cannot be tampered with and this property is called immutability. If anyone tries to tamper with the blockchain database, then the network consensus will recognize the fact and shut down the attempt.

Blockchains are made up of nodes; these can be within one institution like a hospital, or can be all over the world on the computer of any citizen who wants to participate in the blockchain. For any decision to be made, the majority of the nodes need to come to a consensus. The blockchain has a democratic system instead of a central authoritarian figure. So if any one node is compromised due to malicious action, the rest of the nodes recognize the problem and do not execute the unacceptable activity. Though blockchain has a pretty incredible security feature, it is not used by everyone to store data.

III. METHODOLOGY

Blockchain is a peer to peer security system that is substituted conventional centralized signature based security by distributed consensus algorithm or protocols. Amazingly, there is no trusted third party. Besides, the parties do not have any trust among themselves. Hence, it is mandatory to have a consensus algorithm for this type of distributed ledger technology. It is the vital part of this core technology. The nodes

of a Blockchain run a fault-tolerant consensus protocol. This protocol ensures that all the nodes agree on a order in which entries are appended to the Blockchain [12]. For the Blockchain applications to run on smoothly, There are two known problems in Blockchain application, namely, double spending problem and Byzantine Generals Problem [13]. The solution should be achieved not only for function but also to avoid the increasing risk of malicious activities over the Internet or the Internet of things (IoT). The double spending problem is spending the currency at the same time in two transactions. Blockchain solves this problem by verifying the transactions by many distributed nodes together. Byzantine Generals Problem occurs in the distributed system. Different nodes can receive data through peer to peer communication. However, malicious attack on some nodes leads to the changes of communication contents. Normal nodes need to obtain the consistent results and be able to distinguish the information that has been tampered.

A. Proof of work(PoW)

PoW [9] is a mechanism, where each existing node of the network calculates a hash value of the constantly changing block header. The key idea is to allocate Bitcoins through the hashing power competition among the nodes. In a decentralized network, someone has to be selected randomly to record the transaction. It is done through a random selection. The consensus requires the calculated hash value and it is to be equal to or smaller than a certain given value. When a node reaches its target value, it would broadcast the block to other nodes and confirm the correctness of the hash value, all other nodes must mutually confirm. If the block is validated with other miners, then append this new block to their own Blockchains. The PoW procedure is known as mining in Bitcoin and nodes that find out the hash values are called miners.

B . Proof of Stake (PoS)

It is an energy-saving alternative principle to PoW. PoS requires people to prove their ownership of the amount of currency. It is less likely to attack in a network by the people 5having more currencies.

C. Delegated Proof of Stake(DPoS)

DPoS is similar to POS. Miners get their priority to generate the blocks according to their stake. Miners validate newtransactions and record them on global ledger [14]. In DPOS is representative, the delegates are elected by stakeholders to generate and validate a block.

D. Practical Byzantine fault Tolerance (PBFT)

A well known method in distributed systems is Byzantine Fault Tolerance (BFT). It is considered as an excellent method for solving the errors in the transmission. However, the early Byzantine system requires exponential operations. PBFT is a replication algorithm to bear Byzantine faults (Miguel and Barbara, 1999). With the help of PBFT, the algorithmic complexity of BFT is reduced to a polynomial level and greatly improved the efficiency. Hyperledger Fabric (hyperledger, 2015) utilizes the PBFT as its consensus algorithm, since, PBFT could handle up to 1/3 malicious Byzantine replicas.

IV. RECENT ADVANCES

Applications of the Blockchain have multiplied extending well beyond the financial system, and ranging from the sharing economy, through smart contracts and the digital vote, to the management of the logistics chain. The areas of application thus transcend economic sectors, and the Blockchain is already poised to transform all existing industries. This technology is set to radically change the organization of transport, the Supply Chain, advertising, the energy production and distribution sector, the real estate market, insurance etc.

A. Smart Contracts

Smart Contracts [7], [15] is an agreement between two parties that has the potential to be digitalized and automated. It is a digitalized transaction system which performs a contract. It is a self-executing contracts that provides an assurance to the various parties. Once the conditions are fulfilled, then the contract is honored with no possibility of there being any fraud or interference with a third party. This technology is blooming and becoming more popular with the emerging use of Blockchain over the Internet and IoT. At the time of the invention of smart contract, there was no such compatible technology which can be clubbed with it. Today by applying Blockchain techniques, smart contracts can be utilized more easily. Digital cash protocols are fine examples of smart contracts. This innovative approach might replace those contracts that are involved in asset deals based on predefined aspects. Blockchain also ensures that all participants who are involved in t know the contract details in addition to removing the third parties and once conditions are fulfilled contractual terms implement automatically. Smart contracts are used in financial derivatives, insurance premiums, property law,

and crowd funding agreements, among others. A prominent example for Blockchain technology is Ethereum which is an open source combining Smart Contract. It is a decentralized system originally proposed in [3]. Smart contract can be considered as a replacement of conventional hardcopy contract in near future. In other way, we can say dealing with every contract in a smart way. However, even a small bug in the coding of smart contract will bring disastrous damage in the virtual world.

B. Digital Identity and Security

OneName is an American start-up using the Blockchain to generate a digital identity which only the user will be able to use to log on for their various Web services. There will no longer be any need to memorize countless user names and passwords: only a single digital identity will be needed. Estonia, a forerunner in this field, has, for a few years now, been running a digital identity project enabling its citizens to aggregate their personal information in a secure manner: this gives them a digital identity for voting purposes, medical references, a driving license, etc. A more recent project, undertaken in partnership with the Tallinn stock exchange, will enable shareholders to vote at shareholder meetings obviously without having to go to them. For its part, the start-up FollowMyVote is banking on the digitalization of the electoral system. Observing the numerous problems experienced by several countries in terms of electoral fraud, this startup is proposing to apply the Blockchain to ensure that the voting process is audited and traceable.

C. Health and pharmaceuticals

The healthcare sector also abounds with potential applications. In the area of pharmaceutical industries, for example, the legitimacy, authenticity, and traceability of clinical results are paramount. BlockRX uses the Blockchain technology to ensure the traceability of the supply chain. Another use case in the area of healthcare is for medical records. By digitalizing them, information about the patient can be transferred more easily from one healthcare professional to another (with the patient's agreement, of course).

D. Insurance

Another area of great interest for the Blockchain is insurance. Here, there are multiple possibilities, and we are still in for some surprises. For example, peer-to-peer insurance (e.g.: Dynamis) is putting an end to the usual, tripartite relationship between payers, insured parties, and insurers. It enables each individual to participate both in the pool of insured parties, and in the investment gains. By way of another example, parametric insurance (e.g.: Rainvow), for its part, enables the insured party to be compensated automatically when a certain event occurs, thanks to Smart Contracts. In this way, thanks to
the interconnectivity of objects (IoT) and the programming of events, it is possible to record automatic insurance contracts. A striking example is the potential for insuring agricultural production against bad weather. Using sensors (of rainfall or temperature, for example), the payment of compensation (to the insured producer) will be triggered automatically, for example, after 2 months of drought (fictitious example).

E. Financial sector and digital assets

Beyond the Bitcoin, there are many potential applications in the financial sector. In 2015 the NASDAQ unveiled Linq: the very first platform for the issuance of private equity managed entirely using the Blockchain. Through this new system, private investors can trade in the stock of private companies. There is thus no need for certificates for the issuance of stock or the holding of shares in the companies: everything is digitalized and immortalized in the Blockchain. We refer to these as digital assets. Openchain2 and Chain are other examples of this. The first digitalizes all assets, whilst the second concentrates on the revolution in the financial system.

F. Processes and information exchange

Ultimately, any exchange between different parties can be managed by the Blockchain technology. Whether it involves digital money, proof of identity, an insurance payment, or a transfer to a supplier or customer, the logic remains the same: the process requires an exchange and the historization of transactions, and it must be traceable, efficient, transparent, and capable of being audited. Considering the incredible disruptive potential of this technology and its applications, one thing seems almost obvious: faced with such potential, it becomes important for one to weigh up all the consequences of
the Blockchain and its applications on one's business models, revenue models, growth models.

G. Blockchain Internet-of-Things (IoT)

The Internet of Things (IoT) is a new technology paradigm that has ramped up recently. It is imagined as a future possibility of global network devices which are capable of interacting with each other. Its a machine to machine interactive infrastructure. The IoT is gaining vast attention from a wide range of industries. It is basically an ecosystem of connected physical objects that are accessible through the Internet. Things that are embedded with electronics, software, sensors and network connectivity, which enables these objects to collect

and exchange data. Blockchain based IoT architecture handles most security and privacy challenges due to some salient features of Blockchain. Blockchain ensures scalability and robustness by using participating nodes resources and decreases delay by eliminating many to one traffic problems. In IoT, it is desirable to realize a network which is secure over untrusted parties. This can be done with the help of Blockchain. With the help of Blockchain, the real identity of the user is not revealed as each user can interact with a generated address.

V. CONCLUSION

Blockchain is an effective technology that can help prevent data breaches in the healthcare industry. It is a secure and reliable method of recording, storing, and sharing sensitive data. Caregivers will definitely benefit from implementing this technology, while remaining HIPAA compliant with this method of trustworthy digital protection by using the blockchain technology it is possible to make accurate estimations or predictions about future results. Also we have discussed how the medical or healthcare related data can be secured. This paper has used various classification techniques and Blockchain technology to a group or individuals who are in the process for accessing the Data. Since using machine learning techniques and blockchain method in classification studies results in accurate outcomes accompanied with significant saving in terms of time, cost and security, it is highly recommended to make use of machine learning techniques and blockchain method in Data Processing and for providing the security to access those data.

REFERENCES

[1] J. Qi, P. Yang, G. Min, O. Amft, F. Dong, and L. Xu, "Advanced Internet of Things for personalised healthcare systems: A survey," Pervasive and Mobile Computing, vol. 41, pp. 132-149, 2017.

[2] T. Pawar, N. Anantakrishnan, S. Chaudhuri, and S. P. Duttagupta, "Impact of ambulation in wearable-ECG," Annals of Biomedical Engineering, vol. 36, no. 9, pp. 1547-1557, 2008.

[3] L.-J. Kau and C.-S. Chen, "A smart phone-based pocket fall accident detection, positioning, and rescue system," IEEE journal of biomedical and health informatics, vol. 19, no. 1, pp. 44-56, 2015.

[4] M. Ermes, J. Pärkkä, J. Mäntyjärvi, and I. Korhonen, "Detection of daily activities and sports with wearable sensors in controlled and uncontrolled conditions," IEEE transactions on information technology in biomedicine, vol. 12, no. 1, pp. 20-26, 2008.

[5] D. Riaño et al., "An ontology-based personalization of healthcare knowledge to support clinical decisions for chronically ill patients," Journal of biomedical informatics, vol. 45, no. 3, pp. 429-446, 2012.

[6] M. S. Organization. (2018, Nov 2). Top 83 AI startups in Healthcare. Available: http://www.medicalstartups.org/top/ai.

[7] Y. Gordienko et al., "Deep learning with lung segmentation and bone shadow exclusion techniques for chest x-ray analysis of lung cancer," in International Conference on Theory and Applications of Fuzzy Systems and Soft Computing, 2018, pp. 638-647: Springer.

[8] M. T. Brown and J. K. Bussell, "Medication adherence: WHO cares?," Mayo Clinic proceedings, vol. 86, no. 4, pp. 304-314, 2011.

[9] K. Teng. (2012, May). What Is Personalized Healthcare? From patients to medications, one size does not fit all. Available: https://health.clevelandclinic.org/what-is-personalizedhealthcare.
[

[10] A. Ara and A. Ara, "Case study: Integrating IoT, streaming analytics and machine learning to improve intelligent diabetes management system," in 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), 2017, pp. 3179-3182.

[11] R. Vargheese and Y. Viniotis, "Influencing data availability in IoT enabled cloud based e-health in a 30 day readmission context," in 10th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2014, pp. 475-480.

[12] M. D. Naylor, L. H. Aiken, E. T. Kurtzman, D. M. Olds, and K. B. Hirschman, "The importance of transitional care in achieving health reform," Health affairs, vol. 30, no. 4, pp. 746-754, 2011.
[13] S. Tilson and G. J. Hoffman, "Addressing Medicare hospital readmissions," Congressional Research Service, 2012.

[14] S. Shahrestani, "Assistive IoT: Deployment Scenarios and Challenges," in Internet of Things and Smart Environments: Springer, 2017, pp. 75-95.

[15] M. A. Hanson et al., "Body Area Sensor Networks: Challenges and Opportunities," Computer, vol. 42, no. 1, pp. 58-65, 2009.

[16] M. J. Rothman, S. I. Rothman, and J. Beals IV, "Development and validation of a continuous measure of patient condition using the Electronic Medical Record," Journal of biomedical informatics, vol. 46, no. 5, pp. 837-848, 2013.

[17] Junfeng Xie, Helen Tang, Tao Huang, F. Richard Yu, "A Survey of Blockchain Technology Applied to
Smart Cities: Research Issues and Challenges," IEEE
Communications Surveys & Tutorials, 1553-877X (c) 2018 IEEE.

[18] Shuai Wang , Liwei Ouyang, Yong Yuan," Blockchain-Enabled Smart Contracts: Architecture,

Applications, and Future Trends," IEEE TRANSACTIONS ON SYSTEMS, MAN, AND CYBERNETICS: SYSTEMS, 2168-2216 _c 2019 IEEE.

[19] Thomas K. Dasaklis, Fran Casino," Blockchain Meets Smart Health: Towards Next Generation Healthcare Services", 978-1-5386-8161-9/18©2018 European Union.

[20] Jingwei Liu_, Xiaolu Li_, Lin Ye*y*, Hongli Zhang*y*, Xiaojiang Duz, and Mohsen Guizani," BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records"978-1-5386-4727-1/18/©2018 IEEE.

E-ISSN NO:2349-0721