A SURVEY ON BLOCKCHAIN APPLICATIONS

C.Gowri Shankar [1*], T.Bhuvaneswari[2],M.Kanthimathi[3] ,N.Anitha Devi[4] ,S.Manoruthra[5]
[1]*National Engineering College,Kovilpatti,Thoothukudi,Tamilnadu,India.*
[2,3,4,5] *National Engineering College,Kovilpatti,Thoothukudi,Tamilnadu,India.*
[1]*172038@nec.edu.in,*[2]*bhuvaneswari_cse@nec.edu.in,*[3]*kanthimathi_cse@nec.edu.in,*[4]*anitha_cse@nec.edu.in,*[5]*manoruthra-cse@nec.edu.in*

Abstract: In this era of Intelligence, more devices become self-aware by connecting themselves to the internet and moved one step ahead. This will result in a huge amount of data which is needed to be maintained with more care where security comes into the big picture. As the amount of data increases, the platform which transfers data gets more vulnerable. In this meantime, the applications will get expanded and step into the circle of cyber attacks, especially in an online transaction. To overcome these serious issues, blockchain technology can be ideally used and secure the data from being tampered. This paper gives an overview of blockchain technology and its influence in different sectors like health care, business, military, etc.

***Keywords*: Security,Blockchain..**

1. Introduction

For a society to be healthy, it should be far away from unfeasible problems. As it is impossible to avoid, we must become strong and evolve a protective shield against them. In this internet world, security breaches and storage are the commonly faced problems by companies. Blockchain technology came as a boon savior to these issues. In 2009 Blockchain technology [1] architecture platform has been launched and works by storing recorded ledger information in decentralized storage. Besides, [2] this blockchain ledger provides integrity, traceability, and non-repudiation using security mechanisms such as digital signature and hash chains.

2. Blockchain

Bitcoin is the basics construct for blockchain technology, so it is essential to know about the base bitcoin cryptocurrency. In [3] "A blockchain is a chain of hashed timestamps" quoted by Satoshi Nakamoto. Figure 1, indicates each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones behind it. It is later refined and showed blockchain as a sequence of records linked to its former block and each associated with a hash point.

Blockchain achieved its highly secure and immutable nature by combining the following two main characteristics such as data distribution to all nodes on the decentralized network in which it is honest nodes overcome the potential attackers and a cryptographic link among the records that changes progressively.

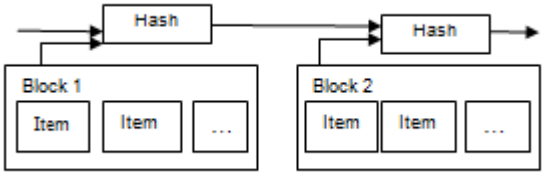

Figure 1. Nakamoto's Proposal on Blockchain

Blockchain Characteristics

As in [4], the core characteristics of blockchain explained as follows:

1.Immutable

As the word indicates, the blockchain will remain as permanent blocks and cannot tamper by others. Hence this would increase the trust among the users.

2.Decentralized Storage

Azaria et al., describes decentralized storage breaks up the stored information from one base server to multiple servers and offers faster access. Through distributed storage, the authentication of a single transaction has verified by redundant data sources

3.Consensus Driven

Trust verification is the most important aspect of security. In a blockchain, each block is verified by consensus models. The best-known method is a proof-of-work(PoW) scheme where a hash function is taken into account in creating conditions for permitting a single participant's conclusion, which inturns verified by others.

4.Transparent

As blockchain is always in open access, the party can audit and track the transaction undergone to date. It is the biggest promise made by the blockchain. Since it is a peer to peer network, the validation is done by miners(regular users) only which makes them more transparent and trustworthy.

Types of Blockchain

Based on different attributes defined, the blockchain is evolved as follows:

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Public blockchain

Public blockchains are open-sourced where anyone is allowed to participate as users, developers, miners, and community members. Here the transaction details are fully transparent and available to everyone for examination. It is also decentralized as a whole and the ownership is not limited to a single entity. Bitcoin and Ethereum are the public blockchains.

Private Blockchain

It is a permissioned blockchain where the participants must need consent to join their network. It is centralized and the transaction details can be accessed only by the system participants. It is much suitable for bigger enterprises where their confidential information should not be leaked to the public. Hyperledger and R3 Corda fall under the private blockchain category.

Hybrid Blockchain

It is a combination of both private and public blockchains. The hybrid nature includes the privacy benefits from private and transparency characteristics of the public blockchain. This multi-chain networks helps the organization and satisfy their needs in security issues. Dragonchain is a hybrid blockchain available now.

3. Blockchain Applications in Different Sector

Blockchain in Health care

Healthcare in this smart world [5] leads to the integration of the internet into the medical practices of an individual. This collaboration improved the health and the residents quality life by reporting their medical status on their hands through technology. However, this drastic step also made the health sector to face more security challenges like the privacy of medical data.

Over viewing mobile healthcare security, many people are not aware of risk in storing and transferring confidential medical information on their smart phones. Unaware of the threats caused by open Wi-Fi networks, it is very much important to concentrate on security. Besides, most of the institutions have purchased private cloud-based data centers to enhance their research on EHR(Electronic Health Record) data to reach the best conclusion. Under strict laws such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) [5], the patients' records are generally stored in a centralized database, which would result in important issues such as security and interoperability.

At this point, blockchain technology comes into action with a decentralized nature promoting the transparency of data. The robust encryption will secure sensitive medical information, treatment money transactions from cyber attack criminals. Additionally, the blockchain also eradicates the smartphone threats, by permitting only authorized users to access the data stored in the system. Building the security at the top level, the organizational operations can also be preserved which could enhance the drug discovery with high protection.

Block chain in Electronical Health Records

In [7], the Gem health network used an Ethereum Blockchain technology to evolve a Distributed network infrastructure passing the centralized storage. This permits authorized users to access the recent treatment information.

MIT Media Lab has developed the MedRec prototype [6], which applies to Electronical Health Records(EHRs) in 2016. The main aim of MedRec is to use Blockchain architecture as a public ledger to note down any updates related to the medical data by preserving the data integrity, without affecting the patients' access control over it. After successful verification, strangers can access data of patients stored in different medical facilities through MedRec .MedRec was designed to overcome the following issues:

- Slow access and Slow response in a database
- System interoperability
- A detailed explanation of patients history
- Data quality and quantity for advanced research

In, the author developed a health information system (HIS) along with the BiiMED, Blockchain framework. BiiMED is developed using the Ethereum platform with 10 nodes and Smart contracts. It presents a Trusted Third Party Auditor to validate ID and Hash.

Block chain in IoT

IoT plays an important role in our daily life and it has a great effect on our everyday activities. From the early beginning of cryptocurrency, blockchain technology has raised as an effective technology. It is being explored in many fields such as Internet of Things (IoT) security, banking smart energy systems, robotics field, the transport sector, industries, etc. Nowadays most of the businesses are working online and hence this blockchain technology plays a major role everywhere. Data digitization can be carried through the centralization and decentralization process with high level of protection.

Every data is allowed to be stored in blocks together with the transaction history as a blockchain. This category of transaction can be made easier using a no sharing network [9] that negotiates the involvement of any out party. Nowadays, the world is moving ahead towards the automated future and smart devices with the help of Internet of Things (IoT) everywhere.

The Sensor is used to obtain the data values from all environments, which in turn taken by the microcontroller for making decisions over the received data. The data obtained from the sensor will be projected in the LCD from the micro-controller, whereas the collected data can be sent to the Base Station with the help of wi-fi. The data received at the base station server will be automatically stored in the database. After that the users can login and continue with their access through the application service.

Another Approach using IoT

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

The application server will send the login credentials which will be used as a blockchain password to the server, thus requesting a new member to the blockchain. Now a new user account will be requested by a server on the blockchain with the received credentials. Server will save the user Id, device id, and transferred address on the database [10].

When the sensor model executes, the File Transfer Protocol will load and store the information on the blockchain. After creating the block, the application will send an id to the server for accepting the stored information and it will check for the perfect match to display it on the user application. The most significant advantage of using blockchain in IoT is that the data will not be modified and the data cannot be erased.

IoT Security in Blockchain

Security is the major key difficulty in the internet of Things (IoT), due to it's high scalability, environmental conditions and distributive nature. The most fundamental goals that need to be achieved while considering IoT with Blockchain are confidentiality, availability, and integrity. Mostly various Cryptographic algorithms are used in the block chain[11], which will result in a high range of privacy in consumer data.

IoT Devices produce a larger volume of data which is vulnerable to privacy, becoming a major aim of cyber attacks [12]. Various traditional methods [13] of security were very expensive and many security frameworks were highly centralized which leads to difficulty in scalability.

Methodologies like sinkhole assaults, replay assaults, and sticking enemies may result in misusage of IoT segments at the layers corrupting the quality of Services (QoS) [6].

Blockchain in E-Voting System

An online voting system is a protective and interactive voting application in which users can vote from any location with some identity proof. It involves the transmission of votes via the network and will result in a more amount of data which is needed to be maintained with more care where security comes into the picture. Since election security is a national security problem, developing a secure E-Voting becomes a challenge for a long time. While developing the online E-Voting system, we must consider the following design considerations,

- An election system should not be a forced voting.
- It should maintain the confidentiality of votes that is registered by the voters.
- It should allow only the eligible voters with some identity proof.
- An election system should prevent active and passive attacks like modification and monitoring of voting information for some illegal purposes, etc.So it is necessary to provide a secure online voting system with blockchain.

Even though many publications are available, secure E-voting is a relatively unexplored field. Besides designing a secure E-Voting system is an active research area for the past few years to reduce the cost and ensure confidentiality. Gunnlaugur.K et al.[1] used blockchain for providing security to the E-Voting system. They designed G-Ethereum private Proof-of-Authority (POA) blockchain to satisfy the privacy related requirements of e-voting. They have achieved immutability, verifiability, distributed consensus through advanced cryptography. Pawade et al.[2] used a blockchain-based online voting system. They used iris recognition to address the issue of user authentication and considered one Time password for providing additional features. Besides, they have considered blockchain is an important security measure for providing decentralized data storage for user biometric. Pawlak et al[3] used intelligent agents and multi-agents system concept to provide transparency and audit ability in the Blockchain-based e-voting system. Zhang.S et al.[4] proposed novel blockchain-enabled voting(BEV) named chaintegrity, to address three major requirements: robustness ,scalability and verifiability. They used counting Bloom filter and the Merkle hash tree for fast authentication.

Blockchain in Banking

Blockchain banking is one of the most talked topics in the banking sector. It enables banks to process payments more accurately and quickly with minimum processing costs. In addition to this, Blockchain will improve the security related measures of the banking sector. So the banks need to build the infrastructure with blockchain over the global network. Guo et al.[5] Guo et al.[5] surveyed the application of blockchain in the banking sector. They mentioned four challenges for adopting blockchain banking which include Scalability, Security, Cost of a transaction, the time needed to verify the transactions.

Blockchain in Military

Blockchain technology can provide the following advantages to the armies: automated systems management, Prevention against cyberattacks of terrorist groups or other nations, defensive measures of highly efficient weapon systems, information validity on the battlefield or supply chain management and logistics. Kavya et al[6] used consortium blockchain technology for secure messages passing in the military messaging system.

4. Blockchain Issues

Despite the advancement proposed by blockchain, some issues need to be addressed and overcome as in [21].

Units Lack of standardization

Since it's a growing technology, there is no standardization which pulls them down from conquering the top. Though many of the countries have implemented blockchain in different sectors, the varying infrastructure and application make them difficult to progress without a high-level standardization.

Privacy leakage

Though the blockchain offers decentralized storage as a unique advantage, a user has to retrieve the information using

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

a private key for verification. Here the necessary information is decrypted from cipher to plain text which results in privacy leakage.

Key management

Due to the cryptographic process undergone, private and, public keys are required to enable security. The existing key management is not applicable for blockchain ,as a single key cannot manage the entire blocks as its unsafe. Also, one block one key mechanism is the high cost. Hence a good mechanism is needed to be done here.

Scalability and IoT overhead

Since the number of participants, device, and IoT sensors attached to blockchain technology increases day by day, it will be difficult to maintain the stability of computational power. It will also result in a high bandwidth overhead which will lower the data processing.

5. Conclusion

This study provides us an overview of the blockchain concept and its emerging usage in business applications. We showed the blockchain functional characteristics, types, and its issues. This paper also demonstrated the urge to level of interest developed by various business applications in blockchain technology. With the immutable and decentralized nature, blockchain had caught the researchers to explore more in-depth for a secure future.

Acknowledgment

I would like to thank my management to proceed this paper.

References

[1] Zheng, Z., et al.,"An overview of blockchain technology: architecture, consensus, and future trends. In: Big Data (BigData Congress), IEEE International Congress,2017 https://doi.org/10.1109/BigDataCongress.2017.85. IEEE.

[2] Zhao, H., et al.,." Lightweight backup and efficient recovery scheme for health blockchain keys. In: Autonomous Decentralized System (ISADS)", IEEE 13th International Symposium, 2017 https://doi.org/10.1109/ISADS.2017.22.

[3] Nakamoto S" Bitcoin: A Peer-to-Peer Electronic Cash System". Bitcoin.org: 9. DOI: 10.1007/s10838-008-9062-0.

[4] Karim Sultan, Umar Ruhi and Rubina Lakhani, "Conceptualizing Blockchains: Characteristics & Applications", 11th IADIS International Conference Information Systems 2018.

[5] Jinglin Qiu, Xueping Liang, Sachin Shetty, Daniel Bowden," Towards Secure and Smart Healthcare in Smart Cities Using Blockchain",IEEE,2018.

[6] Azaria A, Ekblaw A, Vieira T, Lippman A, "Medrec: Using blockchain for medical data access and permission management in Open and Big Data (OBD)", IEEE International Conference , 2016 (pp. 25-30).

[7] Mettler, M, "Blockchain technology in healthcare: the revolution starts here. In: e-Health Networking, Applications and Services (Healthcom)", IEEE 18th International Conference, 2016. https://doi.org/10.1109/HealthCom.2016.7749510.

[8] Rateb Jabbar, Noora Fetais, Moez Krichen, Kamel Barkaoui," Blockchain technology for healthcare: Enhancing shared electronic health record interoperability and integrity", IEEE,2020

[9] Melkamu Kerebh Kebede, Dr Santosh Kumar Pani, "Reshaping IOT Through Blockchain" Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019)

[10] Abdi Sultan, Muhammad Sheraz, A. M., and Mushtaq, A. "Internet of things security issues and their solutions with blockchain technology". American Journal of Computer Science and Information Technology .

[11] Misbah Anwer et all, "Security of IoT Using Block chain: A Review" 2020 International Conference on Information Science and Communication Technology.

[12] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini,"Security, privacy and trust in internet of things: The roadahead," Computer Networks, vol. 76, pp. 146–164, 2015.

[13] Dorri, Ali, Salil S. Kanhere, Raja Jurdak, and Praveen Gauravaram. "Blockchain for IoT security and privacy: The case study of a smart home." In 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops), pp. 618-623. IEEE, 2017.

[14] Agrawal, Rahul, Pratik Verma, Rahul Sonanis, Umang Goel, Aloknath De, Sai Anirudh Kondaveeti, and Suman Shekhar. "Continuous security in IoT using Blockchain.", IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP),2018 pp. 6423-6427.

[15] Friorik Hjalmarsson, Gunnlaugur.K, Hreioarsson,Mohammad Hamdaqa,Gisli Hjalmtysson,"Blockchain-Based E-voting System",IEEE 11th International conference on cloud computing,2018.

[16] Pawade D., Sakhapara A., Badgujar A., Adepu D., Andrade M. ,Secure Online Voting System Using Biometric and Blockchain. In: Sharma N., Chakrabarti A., Balas V. (eds) Data Management,

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731

Analytics and Innovation. Advances in Intelligent Systems and Computing, vol 1042. Springer, Singapore,2020.

[17] Michal Pawlak,Aneta Poniszewska-Maranda,Natalia Kryvinska,Towards the intelligent agents for blockchain e-voting system,9 th international conference on Emerging Ubiquitous and Pervasive Networks,Procedia Computer Science 141(2018) 239-246.

[18] Zhang, S., Wang, L. & Xiong, H. Chaintegrity: blockchain-enabled large-scale e-voting system with robustness and universal verifiability. Int. J. Inf. Secur. 19, 323–341(2020). https://doi.org/10.1007/s10207-019-00465-8.

[19] Guo, Y., Liang, C. Blockchain application and outlook in the banking industry. Financ Innov2,24(2016). https://doi.org/10.1186/s40854-016-0034-9.

[20] K. K R and K. M, "Military Message Passing using Consortium Blockchain Technology," 2020 5th International Conference on Communication and Electronics Systems (ICCES), COIMBATORE, India, 2020, pp. 1273-1278, doi: 10.1109/ICCES48766.2020.9138014.

[21] Thomas McGhin , Kim-Kwang Raymond Choo , Charles Zhechao Liu , Debiao He ," Blockchain in healthcare applications: Research challenges and opportunities", Journal of Network and Computer Applications, February 2019.

ISSN (Print): 2204-0595
ISSN (Online): 2203-1731