IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12698

A REVIEW OF BLOCKCHAIN SECURITY IN THE CLOUD COMPUTING ENVIRONMENT

Abhishek Kajal

Asst Professor, Department of CSE, GJUS&T, Hisar, Haryana (India)

Abstract: Nowadays, Most of IT industry preferred Cloud Computing technology to deliver data services at a nominal cost with little efforts and good level of scalability. During this exponential growth of cloud computing technology, security arisen as the major challenge. Researchers have made tremendous progress in comprehending the potential of blockchain technology for the cloud, finding risks, and suggesting mitigations. Even if blockchain has better security characteristics, its integration with cloud computing platforms must take into account its drawbacks, scalability issues, and privacy concerns. To further improve the security and usefulness of blockchain technology in the cloud, research and innovation must continue. Blockchain ensures security in all aspects as confidentiality and authenticity. The current review study looks at the function that block chains play in cloud-based security systems. However, there are a number of studies that make use of block chains, despite the fact that it has been noticed that block chains have significant limitations. On the other side, research that has been done on the cloud, has inadequate security features. It's possible that using blockchain technology with cloud computing can make cloud contents more secure.

Keywords: Blockchain, Security, Cloud computing, Nodes

I. INTRODUCTION

1.1 BLOCKCHAIN

Cloud Computing has turned one of the biggest research topics of current times with exponentially hike in resource sharing to provide user better experience. Though, cloud computing systems are facing severe threats and security issues. During the times of recent pandemic, we witnessed lots of online platform security breaches as Zoom App, Microsoft Azure, Cloudflare, Amazon Web series etc resulting leakage of privacy data affecting millions of users. Few years ago, a survey done by Fujitsu revealed that about 88% of cloud users are worried about security of their private data on cloud storage. However, cloud storage service providers assure their services are reliable and secured. Yet, most cloud users remain doubtful about their data security.

In the times of security concerns, Blockchain emerged major technology that pulls the attention after success of its application in digital cryptocurrencies. Users of the cloud have a great danger of having their data lost, stolen, or attacked, and they lack any way to remedy this poor situation. Users of the cloud aren't even aware of the people they are exchanging information with. Transparency is also a major problem; cloud customers have no idea who is accessing their data or how it is moving through the cloud. Blockchain is a cutting-edge technology that cloud customers can utilize to increase trust and offer security of data when outsourcing and acquiring cloud services. Compared to centralized database security, blockchain can offer more advanced security. Blockchain is usually controlled by a peer-to-peer network and is built to prevent unauthorized tampering. Blockchain can offer security on par with central database storage. Furthermore, when used in a field where data disclosure is necessary, the Blockchain's openness attribute can enable transparency in data. Blockchain continuously examines the list of linked and related records. Because anybody may use it, Bitcoin is an example of an open blockchain, which does not need any special permission to utilize.

There are now a great many variations of the blockchain technology. Access to the network may be limited for some block chains since they were developed to cater to the requirements of a limited number of participants in the network. These are some instances of a private blockchain or one that requires authorization. The technology behind blockchain allows for the secure transfer of value, as well as the creation of a permanent forensic record of transactions. The decentralized digital currency Bitcoin also relies heavily on the same blockchain technology. A distributed database that contains records of all transactions or the events executed in between the participating parties is called a blockchain. Each transaction is audited by the system's users, the vast majority of whom are participants. It includes each and every record of each transaction in its entirety.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12698

The most widely used example of a blockchain technology is the cryptocurrency known as Bitcoin. Blockchain Technology originally came to light when a person or Group of persons called 'Satoshi Nakamoto' issued a white paper on "Bitcoin: A peer to peer electronic payment system" in 2008. Because of this, the ledger cannot be altered in any way. A transaction may be recorded on the blockchain for anything of value, including real estate assets, automobiles, and so on.

A blockchain is a decentralized ledger that may be used to record transactions. In addition to its use in the recording of transactions involving crypto currencies like Bitcoin and other crypto-currencies, blockchains have a wide range of additional uses. Each transaction uploaded to a blockchain is verified by numerous computers on the Internet. A peer-to-peer network is formed by these systems, each of which is designed to keep an eye on a certain category of blockchain transactions. Because these computers are distributed over the network, it is impossible for a single machine to add faulty blocks to the chain. When a new block is added to a blockchain, that block is connected to the one before it via the use of a cryptographic hash that is formed based on the information contained in the block that came before it. Because of this, the chain cannot be broken, and the information contained in each block is preserved in perpetuity. It is also purposefully difficult to edit prior transactions in blockchain as all the succeeding blocks must be adjusted first.

1.2 Working of Blockchain

Bitcoin is perhaps the most well-known use of Blockchain technology. Bitcoin is a kind of cryptocurrency that may be used for the purchase and sale of digital assets over the internet. For successfully carrying out transaction, via internet, Bitcoin relies on cryptographical evidence rather than the confidence of a third party. Digital signatures are used to ensure the security of each transaction.

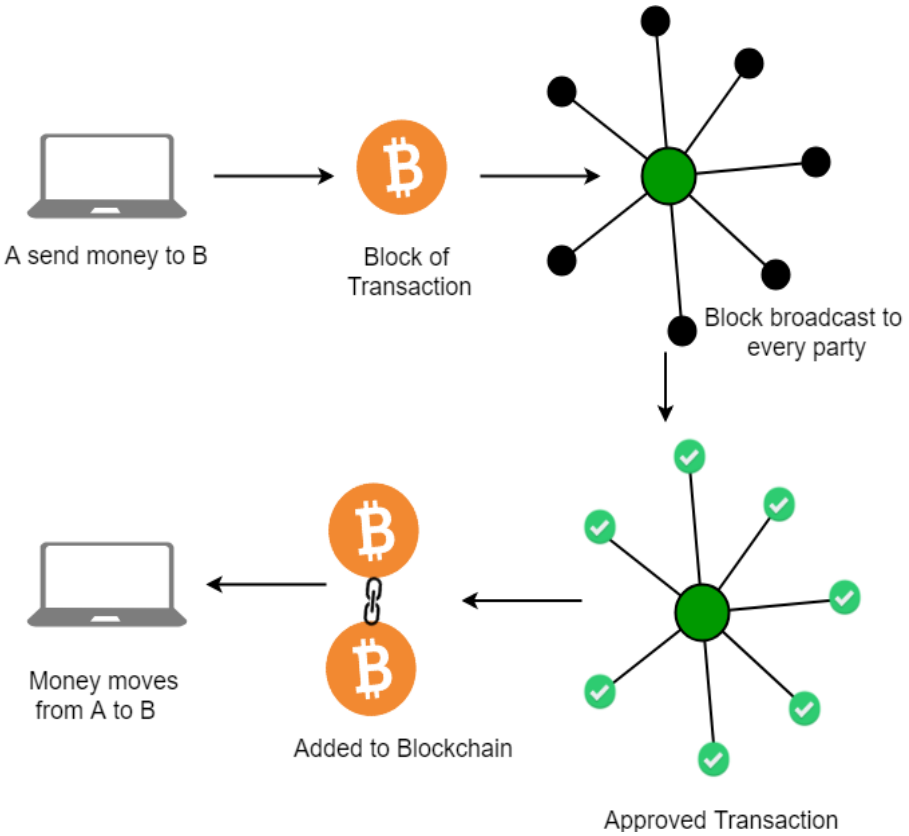

Fig 1 Working of Blockchain

Distributed Database:

There is not a single server or system that is responsible for keeping all of the data for Blockchain. The information is dispersed among the millions of computers located in different parts of the globe and linked together via the blockchain. This approach makes it possible to notarize data since it's present in each node and can easily be verified independently by the people.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023

DOI: 10.17148/IJARCCE.2023.12698

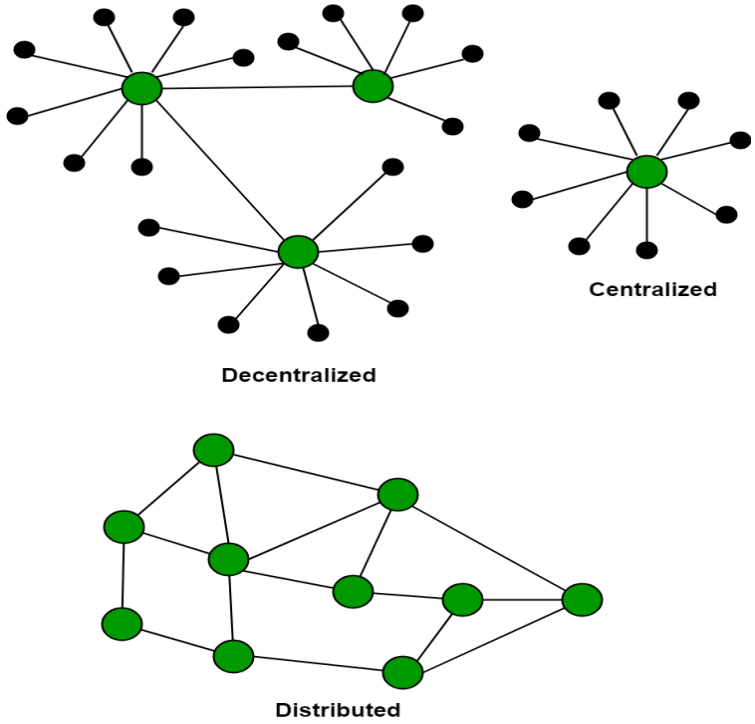

Fig 2 Distributed Block chain

Network of nodes:

A machine that is part of the Blockchain Network is referred to as a node. The client is what establishes the connection between the node and the blockchain. The client contributes to the process of verifying transactions and propagates them into the blockchain. When any computer unit connected to a blockchain, a copy of data on the blockchain gets downloaded in to the system, and that node quickly becomes synchronized with most recent block of data. The term "Miners" refers to any node that is linked to the Blockchain and contributes to the successful completion of a transaction in exchange for a reward.

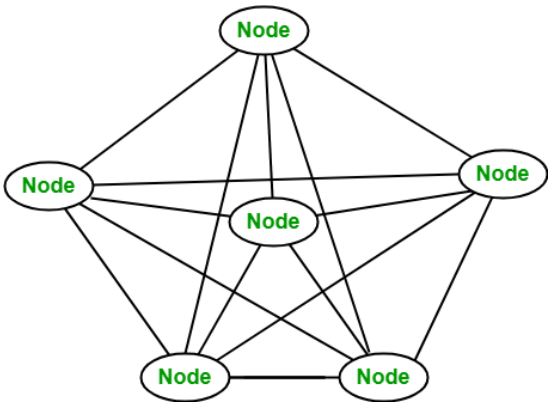

Fig 3 Interconnectivity of nodes

1.3 Nodes

Blockchain nodes are network participants, and as such, their equipment is authorized so as to manage the distributed ledger, and to act as a central point of contact for different types of network operations. To validate the legitimacy of every new block of network transaction is the major responsibility of blockchain node. Nodes are crucial parts of the decentralized network of blockchain technology. Each node in the network is a participant who contributes to the validation and spread of new transactions and blocks. These participants could be computers or other devices that keep a copy of the blockchain's entire transaction history. It's crucial to remember that the precise types and functions of nodes can change depending on how the blockchain is implemented and the network's objectives.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12698

Nodes are given a variety of functions and responsibilities, but they all play a part in the operation and security of the blockchain ecosystem. Nodes are the collective noun for these several computers. The nodes, each of which verifies the legitimacy of the transaction, need to provide their approval before a transaction may go place. After each node in the network has examined a transaction, there is a kind of electronic vote to determine whether or not the transaction is authentic. Some nodes may believe the transaction is legitimate, while other nodes may believe it is fraudulent.

Every node in the network maintains its own independent copy of the distributed digital ledger, also known as the Blockchain. Every node in the network validates the correctness of every transaction. If the consensus of the majority of nodes is that a transaction is legitimate, then it will be included in the next block. Now, even if any item get modified, the original hash will be stored on all of the other machines. They would not agree to the alteration under any circumstances.

1.4 Block

This individual spreadsheet is referred to as a block. The term "blockchain" refers to the whole genus of blocks. Each node in the network has its own copy of the blockchain. A new block is created whenever an existing block meets a certain threshold for the number of transactions that have been validated and accepted. Every 10 minutes, the Blockchain will automatically update itself. It operates in an automated fashion. There is no master computer or centralized computer that tells the computers to carry out this activity. After the spreadsheet, ledger, or register has been brought up to date, the data in it can no longer be altered. As a result, it cannot be forged in any way. Only new entries may be added to it at this time. The registry is updated simultaneously on each and every machine that is connected to the network.

II. LITERATURE REVIEW

The study article "Challenges and Opportunities in Blockchain and Crypto-currencies" [1] was published in 2019 and examined the state of the field. The blockchain is the technology that underpins the digital currency known as Bitcoin, and it has generated a great deal of enthusiasm in the scientific and technological sectors. A blockchain is a distributed ledger that is maintained collaboratively by members in a peer-to-peer network. These individuals are known as miners in the Bitcoin ecosystem.

A comprehensive literature assessment of blockchain-based applications, including their present status, categorization, and outstanding problems was published by Casino et al. [2] in 2019. The purpose of this study is to give a comprehensive literature assessment of blockchain-based applications across a variety of industries. The purpose of this project is to explore the present status of blockchain technology and its applications, as well as to emphasize how certain aspects of this disruptive technology might revolutionize behaviors that are now considered "business as usual." In 2019, Nakamoto et al. [3] in the article titled "Bitcoin: A Peer-to-Peer Electronic Cash System" concluded that if there could any digital currency system completely rely on the concept of peer to peer transaction, then feasibility of individuals to get execute payments in online mode to each another without any interference of any financial institution. The author suggested that a peer-to-peer network may be used as a way to solve the issue of double spending.

In 2018, Burnie, et al. [4] announced examining the interconnection of crypto currencies utilizing correlation networks as their research methodology. The use of correlation networks allowed for the identification of factors that, although being constant over time, still have a significant impact on the development of prices through time. Using the websites and whitepapers of crypto currencies that have the greatest user populations, we were able to identify aspects that may be considered potentially essential.

Jani et al. [5] published their findings in 2018 on an Overview of Ethereum and Its Comparison with Bitcoin. A Brief Introduction to Ethereum, Along with Some Comparisons to Bitcoin The creation of Bitcoin by Satoshi Nakamoto in 2009 has been heralded as a revolutionary step forward in the world of money and currency. Bitcoin is the first example of a digital asset that simultaneously lacks any backing or "intrinsic value" and no centralized issuer or controller. This has led to Bitcoin being hailed as a revolutionary step forward in the world of money and currency.

The future of processing of transactions and smart contracts on the internet of money is a topic that was covered in a study that was published in 2015 by Gareth W. Petersz et al. [6]. They provide an overview of the idea of blockchain technology and its potential to disrupt the world of banking by allowing worldwide money transfer, smart contracts, automated banking ledgers, and digital assets. In addition, they discuss the possible benefits of blockchain technology.

Jesse Yli-Huumo1, et al. [7] presented the most recent findings from their study on blockchain technology in 2016. In

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12698

the course of their investigation, they have carried out a methodical mapping analysis with the intention of collecting all of the pertinent research on Block chain technology. From a purely technical standpoint, they want to get an understanding of the current research issues, problems, and potential future paths using Blockchain technology.

Igor Zikratov, et al. [8] conducted research in 2017 to examine the use of block chain technology to guarantee the integrity of data. The blockchain is a relatively young technology that has already shown a great deal of potential. The first version of this public record of all Bitcoin transactions was released in 2009. They examine the behavior of blockchains in terms of how to store, retrieve, and distribute data in a network that is decentralized.

Edoardo Gaetani et al. [9] published their findings on the Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments in 2017. Because manipulating data might inadvertently have a negative impact on critical business choices, the existence of potential threats to the data's integrity is of the utmost importance. This problem is particularly prevalent in contexts that make use of cloud computing since owners of data cannot exercise control over essential parts of their data, such as the physical storage of data and the control over who may access it.

Block chain based data recording and integrity management system for cloud forensics was the topic of an article that Jun Hak Park, et al. [10] published in 2017. In this study, a blockchain-based data recording and integrity management system for cloud forensics has been offered as a solution to the difficulties that have been identified. In addition, evaluate how well the proposed system performs in comparison to the performance of competing blockchain-based crypto-currencies.

An overview of blockchain technology, including its design, consensus, and potential future developments, was presented and debated in 2017 by Zibin Zheng et al. [11]. First, they provide an explanation of the architecture of blockchains, and then they examine various common consensus techniques that are employed across different blockchains. In addition, a summary of current technological advancements and difficulties is provided. They also outline potential developments for the blockchain in the future.

An introduction to blockchain was written by A. Shanti Bruyn et al.[12] in the year 2017. The purpose of this article is to give a broad examination of blockchain technology. Following the completion of the study, it became abundantly evident that it is very difficult to explain blockchain in a succinct way to those who are not already familiar with the concept. It's possible that the Glossary that comes along with this document will provide you a decent overall concept of this new system. The concept of blockchain security in cloud computing: use cases, problems, and solutions were first introduced in 2017 by Jin Ho Park and colleagues [13]. In this article, they explain the idea of blockchain technology as well as the current research trends associated with it. In addition to this, they will look at the specifics of how to incorporate blockchain security into cloud computing and its many safe solutions.

Blockchains for Governmental Services: Design Principles, Applications, and Case Studies was a proposal that was made in 2017 by Ivan Martinovic, et al. [14]. There are significant opportunities to improve both efficiency and security via the use of blockchain technology in public life and the provision of services by governments. From a purely technical standpoint, it makes it possible to retain records in ways that are both straightforward and effective, while also being resistant to the effects of powerful adversarial models.

2017 saw the publication of Sonke Bartling et al [15] Blockchain for science and the development of new knowledge. The blockchain technology has the potential to render digital commodities irreversible, transparent, decentralized, externally verifiable, and distributed. The first portion of the research cycle, the experiment itself or the data collection, might take place outside of a blockchain environment, but the rest of the cycle could be conducted there.

III. PROBLEM STATEMENT

Research is looking at a variety of problems associated with conventional blockchain technology, such as scalability concerns pertaining to the blockchain. These problems have the potential to result in centralization, which casts a shadow over the future of most prominent blockchain technology application as crypto currency. The ecosystems of the internet of things are quite varied. In contrast to generic computer networks are made of the devices with good processing capabilities, but not each one would be capable of performing at the same appropriate pace. Storage will also be a challenge to overcome. Blockchain does away with the need of a centralized server to record transaction data and device ID; nevertheless, the ledger still has to be kept on each of the nodes individually. In addition, the size of the ledger will expand as more time passes. This is beyond the capability of a broad variety of intelligent equipment like sensors, which only have a relatively little amount of storage space available. Lack of skills: few people understand

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12698

how blockchain technology truly works and when you add IoT to the mix that number will reduce considerably. On the other hand, research into cloud computing took into account firewalls and encryption as potential means of protecting cloud data. However, the use of block chains might potentially improve the safety of cloud applications.

IV. NEED OF RESEARCH

Blockchain technology seems very fruitful to enhance the security of cloud computing systems. By going through literature review, we can conclude that it improves cloud security by enhancing data integrity, improved identity and access management, an immutable audit trail and better encryption. These features provide more secure cloud environment, decreasing the risks associated with private data breaches, reducing malicious activities and unauthorized access. Research in the fields of cloud computing by using block chain technology can cope up to the difficulties surrounding performance, security, accuracy, and flexibility of cloud systems.

V. CHALLENGES TO BLOCKCHAIN SECURITY

Blockchain technology provides many security advantages. It has drawn a lot of interest recently because it has the potential to completely transform many industries, including cloud computing. Extensive research has been done to examine the capabilities, vulnerabilities, and potential mitigations of blockchain technology for cloud security. However, there are still various issues and challenges with blockchain security as listed below:

1. Transaction Security
2. Private Key Security
3. Blockchain contract vulnerabilities
4. Wallet Security

About half of the attacks take place on a blockchain network when a single entity or collection of entities holds more than 50% of the network's computational power. They can alter the consensus mechanism in this circumstance, perhaps allowing double spending or excluding legitimate transactions. Blockchain networks frequently need a lot of computational power to prevent this security threat, making it economically unfeasible to conduct such an assault. Another key concern is the software used in bitcoin because a bug in it might have serious consequences.

Another most challenging concern is that bitcoin address uses the hash value of a public key and is encrypted using a combination of personal and public keys. Therefore, without an unlocking script that contains the value produced from the union of a public key and a personal key, the Bitcoin transaction locking script address cannot be unlocked. The Bitcoin wallet contains information such as the address's personal key, which is utilized to create the unlocking script. As we are aware, in order to utilize Bitcoin, information is necessary and crucial, thus it follows that if we lose information inside the wallet, we also lose Bitcoin. As a result, the Bitcoin wallet ends up becoming the main target of a hacker attack. Private keys should be kept most secured, as they manage access and control to digital assets of users.

VI. CONCLUSION

In this review paper, an overview of blockchain technology with cloud security is discussed. It is concluded that the scope of blockchain technology in cloud security is extremely significant and encompasses various areas as distributed ledger technology used by blockchain offers an unchangeable and impenetrable record of transactions and data to enable cloud providers to guarantee the integrity of data stored in the cloud by using blockchain, prohibiting unwanted additions or deletions. Further, blockchain technology can enable secure and decentralized identity management systems to eliminate reliance on centralized authorities.

Users can manage their identities and access rights, boosting cloud service security by lowering the possibility of identity theft and unauthorized access. In short, the purpose of this research was to investigate the role that block chains play in cloud-based security systems. However, there are a variety of studies that use block chain, and it has been shown that such block chains have specific constraints. The flip side of the coin is that cloud-based research has poor security characteristics. It's possible that integrating blockchain technology with cloud storage would make cloud contents even more secure. The suggested review would be fruitful for research works in the data security of cloud content that makes use of block chains.

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified ⁜ Impact Factor 8.102 ⁜ Peer-reviewed / Refereed journal ⁜ Vol. 12, Issue 6, June 2023
DOI: 10.17148/IJARCCE.2023.12698

REFERENCES

[1] Mahmoud, Qusay & Lescisin, Michael & AlTaei, May. (2019). Research Challenges and Opportunities in Blockchain and Cryptocurrencies. Internet Technology Letters. 2. e93. 10.1002/itl2.93.
[2] Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. Telematics and informatics, 36, 55-81.
[3] Nakamoto, S. (2019). Bitcoin: A peer-to-peer electronic cash system. Manubot.
[4] Burnie, A. (2018). Exploring the interconnectedness of cryptocurrencies using correlation networks. arXiv preprint arXiv:1806.06632.
[5] Jani, Shailak. (2018). An Overview of Ethereum & Its Comparison with Bitcoin.
[6] Gareth W. Petersz ,Efstathios Panayiy (2015)" Understanding Modern Banking Ledgers through Blockchain Technologies: Future of Transaction Processing & Smart Contracts on Internet of Money"
[7] Jesse Yli-Huumo1, Deokyoon Ko (2016) "Where Is Current Research on Blockchain Technology?—A Systematic Review",
[8] Igor Zikratov, Alexander Kuzmin, Vladislav Akimenko, Viktor Niculichev, LucaYalansky (2017)"Ensuring Data Integrity Using Block chain Technology" Proceeding Of 20th Conference Of Fruct Association
[9] Edoardo Gaetani, Leonardo Aniello, Roberto Baldoni, Federico Lombardi (2017)"Blockchain-based Database to Ensure Data Integrity in Cloud Computing Environments"
[10] Jun Hak Park, Jun Young Park, Eui Nam Huh(2017) "Block Chain Based data logging and integrity Management Systemfor Cloud Forensics"
[11] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang , "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends" 2017 IEEE
[12] A. Shanti Bruyn , "Blockchain an introduction" VU,August 26, 2017
[13] Jin Ho Park & Jong Hyuk Park (2017) "Blockchain Security in Cloud Computing: Use Cases, Challenges, & Solutions", Symmetry 2017.
[14] Ivan Martinovic (2017) "Blockchains for Governmental Services: Design Principles, Applic
[15] ations, & Case Studies", Centre for Technology & Global Affairs | University of Oxford
[16] Sönke Bartling (2017) "Blockcha in for science & knowledge creation",
[17] An Binh Tran, Xiwei Xu Ingo Weber, (2017) "Regerator: a Registry Generator for Blockchain",
[18] Harry Halpin, Marta Piekarska (2017) "Introduction to Security & Privacy on Blockchain",
[19] Mahdi H. Miraz, Maaruf Ali , "Applications of Blockchain Technology beyond Cryptocurrency" Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.
[20] Mohamed Amine Ferrag, Makhlouf Derdour, Mithun Mukherjee, Abdelouahid Derhab, Leandros Maglaras, Helge Janicke, "Blockchain Technologies for the Internet of Things: Research Issues and Challenges" 2018.
[21] Carmen Holotesc, "Understanding Blockchain Technology and how to get involved" Researchgate, 2018.
[22] Dylan Yaga ,"Blockchain Technology Overview" National Institute of Standards and Technology Internal Report 8202, 2018.