International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Blockchain Technology in Cloud Computing

R.M.Aravind [1], Dr.P.Sivaprakasam [2]

Department of Computer Science, Sri Vasavi College, Erode, Tamilnadu, India[1]

Associate Professor, Sri Vasavi College, Erode, Tamilnadu, India[2]

ABSTRACT*:* Cloud computing is a platform for expanding capabilities and developing potentialities enthusiastically short of employing new infrastructure for personnel user, or software systems. In Addition, cloud computing originated from a commercial enterprise concept, the reason for using cloud computing is storing the data and developed into a flourishing IT invention and also for the user who does not having a storage capacity. Cloud computing technology is an Internet Oriented computing model which provides several resources through Cloud Service Vendors and also called Cloud service Provider (CSP) to Cloud Users (CU) on demand basis without buying the underlying infrastructure the user follows pay-per-user basis. The architecture of cloud computing models threatens the security in the existing technology. When deployed in a cloud environment, in this paper different cryptography methods and features also implementing the blockchain technology has been executed that pose a threat to cloud computing are reviewed. This paper is a analysis of specific security issues brought by the user and use of cryptography in a cloud computing system. We will analyze about the general performance, security measures, challenges facing in improvements and future directions.

KEYWORDS*:* Cloud computing, Blockchain Technology Cryptography, Security Disputes.

I. INTRODUCTION

Cloud computing epitomizes the basis of digital Environment. Internet has underway driving all these new technologies. Internet was designed firstly to be durable, but not completely safe. Distributed applications like these are much prone to attacks. Cloud Computing has all the weakness associated with these internet operation and the extra threats arise from the combined, Virtualized and redistributed resources. There are many data confidentiality concerns in cloud computing. Incorrect expose of a data used in businesses in cloud to third parties is one of the major issues that have been found. [2] Commonly, cloud users use the resource allocation and scheduling that is offered by the cloud service provider. Therefore, authenticity in cloud computing platforms is necessary to provide a authenticated transmitting channels through the internet in order to protect transferred data and files [4], [5]. In another way cloud Computing can manipulate any files transferred through these cloud communication and transferred data or files can easily be corrupted or damaged as a result of the misappropriation of the intruders or hackers

II. RELATED WORK

a. In this paper [1] we deal with the problem of security of data during data transmission. The main thing to anxiety about this paper. In cloud computing the encryption of data doesn't have that much of authentication, confidentiality and privacy can be easily achieved.

b. In a protocol or set of procedures that uses the services of a third party auditor or checker not only to verify and authenticate the integrity of data stored at remote servers but also in recovering and getting the data back as soon as possible in intact form. so we using a Block chain Technology for securing the data in a distributed and decentralized ledger of transaction

c. Block chain technology is an immutable distributed ledger with a decentralized network that is cryptographically secured. The blockchain architecture is adept of sharing a ledger via the Peer to Peer repetition of data transmission. Which gets updated each time a block of the transaction(s) is approved to be committed. Blockchain technology or distributed ledgers has surge onto the scene in the past few years as an important future technology. Blockchain is a single nor internationally agreed upon definition of distributed ledgers. We classified the existing blockchain definition into three sections as follow:

Business view:

Blockchain for business is very essential for entities executing with one another. With distributed ledger technology, permissioned applicants can access the same information at the same time to improve effectiveness, build trust and remove friction.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Legal view:

Blockchain ledger transactions are authentic, undeniable transactions, which do not require intermediaries or trusted third party legal entities.

Technical view:

Blockchain analyst in technical view of aspects the ICO Rating is often get tasks to evaluates blockchains, ICO projects, visualize lot of data and more other responsibilities connected with Blockchain and crypto currencies.To understand the crypto currency market we need to analyses it in-depth. There are many popular tools like Coin Market Cap, rating agencies social media. But how they get this data and how they use for analysing market and Blockchain

III. STRUCTURE OF THE BLOCKCHAIN ARCHITECTURE

The blockchain technology is a cryptographically protected transactional singleton set of package machine. The structure of blockchain system is shown in Fig. 1, with details [5] as follows.

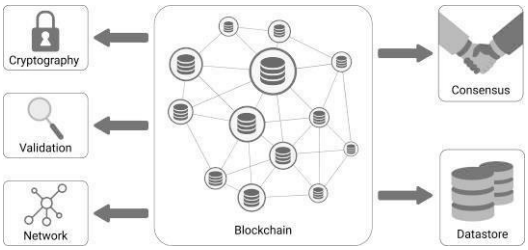

Fig. 1. Blockchain Architecture

Logically, a blockchain is a chain of blocks which contain specific info (database), but in a secure and genuine way that is clustered together in a network (peer-to-peer). In added information, blockchain is a combination of already existing technologies that together can generate networks that secure trust between people or parties who otherwise have no reason to trust.

Fig.2. Client server and p2p network

The configuration of blockchain technology is represented by a list of blocks with transactions in a specific order. The collection of listed data can be stored as a flat file are in the form of a simple database. Two dynamic data structures used in blockchain include:

Pointers

A variables that keep information about the location of another variable. Specifically, this is indicating to the position of another variable.

Linked lists

A sequence of blocks where each block has precise data and links to the following block with the help of a pointer.

Data store

The actual nature of decentralization and distribution stores the data through a network of nodes. Using decentralized data storage capacity offers high scalability, security, affordability, and efficiency. It can really support any kind of digitized facts. In blockchain technology, the data store is a kind of sequential data structure followed by the replication of state machine supporting the fault-tolerant service and complete blockchain data duplicated on each node across the network [5]. Hence, a state represents the status of current blockchain due to the data stored in a changeable data structure. It is used to authenticate the transactions and blocks [6]

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

In the blockchain system, transaction details are stored in the form of blocks and each block relates to each other referring the hash value. The blocks are forward accessible and violates the integrity of blockchain due to a modification in a block's hash value affects all the subsequent blocks. The hash function provides an identification number of a previous block as well as verifies its integrity

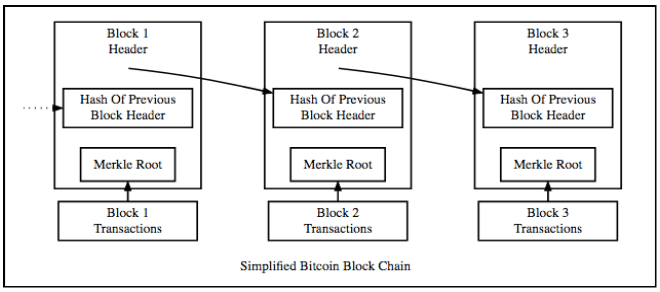

Fig.3 Hash function

Implicit Consensus: Blockchain with Unbounded Through- put [13]

An implied consensus model is suggested to each Node possesses its individual blockchain. Primary advantage gained with this is an absolute throughput. Termination property of BFT is replaced with a property of self-interest. Consensus is not assured for every transaction. This makes this structure scalable with linear message complexity. Instead of consensus of transaction blocks, a special type of blocks are considered, known as check point blocks. The performance and other aspects are analyzed theoretically.

a) Proof-of-Stake Consensus Algorithm for Blockchain [7]
b) PPCoin: Peer-to-Peer Crypto-Currency with Proof-ofStake [8]
c) A Proof-of-Trust Consensus algorithm for Enhancing Accountability in Crowdsourcing Services [9]
d) Consensus Algorithm [10]

Key Characteristics of Blockchain Architecture

Blockchain architecture holds a lot of benefits for businesses. Here are several embedded characteristics:

Cryptography blockchain transactions are authorized and reliable due to the complex computations and cryptographic proof among involved parties

Immutability for every records made in a blockchain cannot be altered or removed.

Provenance refers to the fact that it is possible to track the source of every transaction inside the blockchain data in a ledger.

Decentralization each participant of the blockchain structure has access to the whole distributed database. In place of conflicting to the central-based system, consensus algorithm permits to control the network.

Anonymity each blockchain link the applicant has a generated address, not user identity. This keeps users' anonymity, especially in a public blockchain structure architecture.

Transparency the blockchain system cannot be corrupted but the data is immutable. This is very improbable to happen, as it requires huge computing power to overwrite the blockchain network completely

IV. FUNCTIONAL CHARACTERISTICS

Despite being initially linked to blockchain technology can be used independently in a variety of various use-cases and marketplaces, extending from insurance to the health industry. A blockchain can be useful in virtually any industry in which assets are managed and transactions occur. It can deliver a secure chain of custody for both digital and physical assets complete its functional characteristics that enable the transactions through trust, consensus, security, and smart contracts. These aspects of block chains are explored in the following sections.

3.1 Transactions & Smart Contracts

A transaction is an interchange of assets that is managed under the entity service's rules. Such rules are usually operationalized done by the scripting languages and are used for progressive transactions to be performed. These rules

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

also form the source for smart contracts. A smart contract is a fixed a logic rules in the form of a coded script. It can be fixed into the blockchain to govern a transaction. The contract is executed autonomously and is used to govern the transaction (Buterin, 2016). In this way, contracts act as smart software agents (Stark, 2016). Once a smart contract is embedded in the blockchain, it becomes an autonomous agent that is always tamperproof. An application then reads the code when performing a transaction implements and processes the results.

3.2. Consensus & Trust

It is trusted by consensus as all parties must have identical copies of the blockchain but each participant is accountable for verifying it. Blockchain decentralization is core strength, as a copy of the database file is owned by all performers. In order to ensure the reliability of each copy, a consensus algorithm is required.

The consensus algorithm allows to ensure that each added block is legitimate. It also avoids attackers from conceding and forking the chain (Coindesk, 2017). Nakamoto suggested using a proof-of-work approach, in which a hard cryptographic puzzle must be solved by miners (Nakamoto, 2008).Other consensus models such as proof-of-stake, proof-of-burn, proof-of-elapsed-time, and proof-of-capacity have been projected in the literature to overcome some of the weaknesses of the original proof-of-work model by make an attempt to balance fairness and resource expenditure (Kiayias et al., 2017; Zamfir, 2015).

3.3 Public and Private Blockchains

Blockchains can be classified as public, private or hybrid variants, depending on their application (Buterin, 2015; Mougayar, 2016).Public blockchains have no single owner the content are visible by anyone and their consensus process is open to all to participate and they are full decentralized.

Private is also known authorized and access available person. Private blockchains use rights to control who can read form and write the blockchain.

Hybrid also known as association, these blockchains are public only to a privileged group. The consensus process is controlled by recognized, privileged servers using a set of procedures agreed to by all parties. Copies of the blockchain are only distributed among permitted participants; the network is therefore only partly decentralized.we can formalize the afore-noted features of the blockchain into a list of four core characteristics:

Immutable also known as permanent in blockchain the permanent record of transactions. Once a block is added in a ledger, it cannot be altered or changed. This creates trust in the transaction record. In a blockchain the data stored in a file that can be accessed and copied by any node on the network.

Consensus Driven (trust verification) each block on the blockchain is proved autonomously via a Consensus models which provide rules for validating a block, and often use a scarce resource to show proof that adequate effort was made. This mechanism works without the use of a central authority or an obvious trust-granting agent. **Transparent** we can view the full transaction since the blockchain is an open file, any party can access it and audit transactions.This creates provenance under which asset lifetimes can be followed.

V. BLOCK CHAIN IN CLOUD COMPUTING

Authentication- Insight on cloud computing*:*

An encouragement and attractive computing services distributed by the cloud computing via resource pooling and virtualization techniques. Security as a service is a new anxiety in cloud computing paradigms. An organization can offer many application services to the end-users like E-mail and the web. The company may possess certain limitations on their services, all services should accept by the authorized clients. The client should have security context for each application server and log in before it can consume any service [17]. Similar condition can be seen when a user accesses resources in various security domains. It is not measured as an actual solution in terms of security, system coordination and management standpoint if authentication requires several security credentials. In the cloud migration, organizations encounter comparable issues as well. Different entities are offered to acquire those services, and, thus, a proper security mechanism is required. As a service grow up, the management of access control becomes complex and expensive. Most of the applications attention on functionality of system and the organization value. Thus, a single security policy management ensures better approval systems with flexible and scalable.

Parameters in blockchain technology*:*

The parameters involved in success of blockchain technology, E-Cash and its security E-Cash is the new concept that makes a revolution in e- commerce world. It's just switches the paper and coin of the old systems. Credit card is one of

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

the finest e-cash systems. This system requires a confidential environment with merchants and agents. Bank or issuer stores the E-cash and during the making of a payment, consumer needs to request for it [18]. Different from online, off-line e-cash is kept by customer in a device like smart card or other type of token. Each of this implementation can be classified as recognized or anonymous (untraceable).It means each transaction needs verification and validation from third party such as bank. This application recommends improved security because it uses encryption and digital signature to protects and validate the E-cash message respectively. The fig. 4.1 presents the workflow of e-cash methods, in which entities like bank, consumer and the merchant should be mutual reliable environment.

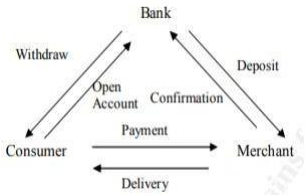

Fig 4.1 Workflow of e-cash

Access control:
It's a kind of structures that facilitate security to the data stored. The resources are valuable in terms of numbers, services and the computational systems. In order to create confidential environment, the entity should create and hold different access rights. Some setups require that access rights can be transferred from a subject to another for some reasons. For instance, a user could sell its contact right to another user [19]. In the same way, an employee of an organization needs to implement a required computation of process in a Virtual Machine assigns the task to another employee also needs to access the same machine.

Integration of Blockchain in cloud computing and its security:
Cloud computing composes huge networks of virtualized services, namely, hardware resources and the software resources. Any sort of services belongs to data centers and known as data farms [9]. The fig. 4.2 demonstrates the P2Pbased cloud architecture.

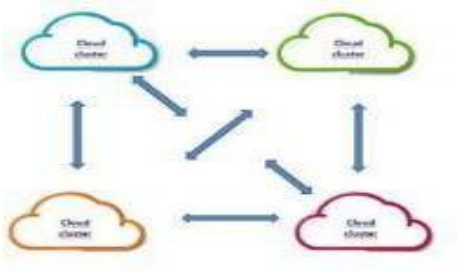

Fig 4.2 P2P based cloud architecture

There are two methods available for incorporating the blockchain in cloud systems:

a) Integrating blockchain with cloud for simplifying enterprise networks like storage, replication and access to transactional database.
b) Integrate with security concepts between task, user, and data management in clouds.

VI. BLOCKCHAIN PLATFORMS

Blockchain is evolving technology and reaching to maturity as acceptance is growing. The first Bitcoin was Blockchain powered platform launched in 2009 and was designed to exchange digital crypto currency without any need of central authority. Bitcoin revolutionizes exchange of money by using peer-to-peer distributed technology and hard to counterfeit due to strong cryptographic protocol and hash function.

Blockchain Runtime Environment:
To be able to process Blockchain transactions and smart contracts Blockchain needed a protected hosting environment. Generally safe operating system, programming language, runtime libraries and supporting libraries reside in this layer.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Blockchain Secondary Storage:
Blockchain platform process high amount of transactions and needs highly protected, reliable and scalable storage to store block data in Blockchain and distributed ledger. This layer offers eternal storage capabilities to platform.

Blockchain Memory Store:
This layer stores latest transactions in memory to support faster data access and also speed up the execution of transactions. Merkle Tree architecture is implemeented in the beginning stage of the Blockchain itself, some of the data structures are used as a memory storage in various Blockchain platforms.

Consensus Protocol Module:
This module contains mechanism to achieve agreement between nodes about transaction validity and authenticity. Once majority of nodes are agree and consensus level is achieved then the given transaction is treated as valid and recorded in the distributed ledger. Some of the famous Blockchain

Consensus Protocol are Proof of Service (PoW), Proof of Stake (PoS), Proof of Importance (PoI), Raft, Byzantine Fault Tolerance (BFT), etc. (Siva, Sindhu, & Sethumadhavan, 2017).

Blockchain Services Layer:
Using this layer Blockchain platforms can be leverage with extra capabilities such as membership management, authorization and access management, event distribution and notification services, exposing platform services using Application Programing Interface (API), etc. However, some of the services like authorization, membership management, access management, etc. are only meaningful for Permissioned Blockchain and optional to Permissionless Blockchain.

Communication Protocol:
Blockchain Protocol implements standard rules that facilitates distributed peer-to-peer communication between participating nodes in Blockchain network. Bitcoin uses broadcasting over TCP connection (Bitcoin Community, 2018) and Hyperledger Fabric is powered by a gossip data dissemination protocol (Hyperledger, 2018) while Ethereum uses devp2p protocol(Ethereum Community, 2018). In case of Bitcoin and Ethereum the node is successfully verified the transaction is rewarded and this process is called mining.

Challenges and Future Directions

The following are the challenges and requirements involved in support of cloud based blockchain transactions [10]. The transactions involved in blockchain networks are enormous in nature.Elasticity and scalability are the main function of the cloud systems in dynamic environment.

a) In view of security: From the user view, the data are hidden and stored in data centres. Thus, the transactional activities should be assigned with tuning purposes. It means that the cloud service allows their customers to have control over the locations in which their data is stored and processed.

b) System resilience and fault tolerance: The system should be able to finding the alternate node, if any one node fails in network, the data centers and use of multiple software applications there will be an immediate backup.

c) Security towards blockchain improvements: Software should centrally assign in distributed cloud environment and the use of multiple software applications.

d) Lack of skills: Need to upgrade the skills of employees with blockchain to build decentralized applications or the organisations should be ready to pay high salary for the blockchain experts.

e) Energy consumption: Proof of Work is the mostly used consensus mechanism solves the complicated puzzles with more amount of energy.

f) Lack of standards: Immutability is one of the pillars in blockchain. On the off chance that awful information is offered effectively, they will wind up on a blockchain; in like manner, if an archive contains bogus data however is offered right, it will wind up on a blockchain. Shared ledger and smart contracts increase the efficiency but with the reduction in cost but acquiring worldwide industry gauges for new IT is troublesome, and it could take some time for associations to have a mutual worldwide blockchain standard.

g) Ecosystem: Encompassing blockchain and supporting distributed services required in a decentralized system includes cloud storage, archiving, domain name servers and communication.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

VII. CONCLUSION

In recent trends blockchain is a popular financial technology which supports variety of Information Processing Units (IPU) on virtual financial transactions. The customers of blockchain store their data in their P2P networks for effective utilization of the computing resources. The two main algorithms like proof-of- work and proof- of -stake are mostly used for declaring security to the blockchain transactions.

This paper evaluate the applications of blockchain in cloud computing. Briefly discussed the integration of blockchain network with cloud systems Blockchain gives rise to many complications even now, such as the security of transactions, wallet, and software and different review have been conducted to solve these issues.

Blockchain is addressing. Data is stored and collected in distributed ledger, secured using cryptographic functions and almost temper resistance. Blockchain endorse trust and transparency between participating parties and ignores the need of third parties. Smart contracts are the digital contracts between parties and a new way of doing business. While Code is the law in Blockchain and records in ledger are the proofs of a result.

The future directions can be focused with,

- The secrecy of user evidence should be ensured when using blockchain.
- Cloud computing environment and the user information should be completely removed.
- Therefore, this study discussed the method of providing security by presenting a method of secure blockchain on data transfer in cloud computing.
- Digital Advertising now faces a lot of challenges such as domain fraud, bot traffic, lack of transparency and long payment models, due to the issue like incentives are not affiliated
- In Cyber Security blockchain prepared a public ledger, in that data is verified and encrypted using advanced cryptography technology. In this method, the information or data is less likely to be attacked or altered without authorization.
- Blockchain is the world of computing the world had seen the endless collection of options in the use of blockchain technology. Currently, most of the countries are developing their blockchain approaches to hold the future.
- In cloud storage the data on a federal server is unprotected to hacking, loss of data, or human error.
- With the help of blockchain technology, it is possible to build the cloud storage more secure, authenticated and robust against hacking.

Assessment of cloud service providers:

Cloud Service Providers	Benefits	Drawbacks
Amazon Web Services (AWS)	Computing capacity is five times more than other cloud service providers .There are various datacenters is available in various places like U.S., Ireland, Japan, Singapore, Brazil and Australia called as “regions”. Provides ability to configure their security firewall according to requirement either private or public.	AWS does not offer hardware level change, by means that if applications need some hardware changes to improve its performance, then it is not thinkable by AWS. • Major disadvantages of AWS are that it does not provide Multicast Network. • It has higher operating cost.
Microsoft Azure	Speed of Microsoft Azure is fast in the key areas thus giving an edge in competitive business. Microsoft Azure can work under challenging environment. It provides greater disaster retrieval system	One of the drawbacks of Microsoft Azure is that it requires management and maintenance. Microsoft cares only the applications that are based upon windows for technical support.

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

Google Cloud Platform	Google cloud provides full access of information from anywhere through web-based applications that are powered by Google cloud. • This cloud platform provides better pricing than other cloud platforms, so a user has to pay for only the compute time they use. • Based on worthy security system that has been built over past 15 years, and secures services like Gmail, Search, etc.	GCP shortages behind AWS on the basis of features provided. Every year a new feature is added to AWS which is then followed by Google cloud. In Google cloud the network pricing is expensive. It is faraway behind AWS and Azure in terms of invention range.
IBM Cloud	IBM cloud recovers from disaster pretty quickly. This is here IBM cloud has better hand over others. Workload is distributed in a organized way such that the users get good response to their applications.	IBM cloud deficiencies in security when compared to other cloud platforms. This cloud is not permitted for all also for the first month, which might be helpful for students and companies professionally as well as for learning purposes.

Table I . Assessment of cloud service providers

REFERENCES

[1] Sanjoli Singla, Jasmeet Singh"Cloud computing securityusing encryption technique",IJARCET, vol.2, ISSUE 7.
[2] R. Bala Chandar, M. S. Kavitha , K. Seenivasan," A proficient model for high end security in cloud computing", International Journal of Emerging Research in Management &Technology, Vol.5, Issue 10.
[3] C.Cachin, Architecture of the Hyperledger blockchain fabric. In Workshop on Distributed Cryptocurrencies and Consensus Ledgers. 2016.
[4] IDC, "IDC Ranking of issues of Cloud Computing model," ed, 2009, http://blogs.idc.com/ie/?p=210, Accessed on July 2011. [5] Cloud Computing Use Case Discussion Group, "Cloud Computing Use Cases Version 3.0," 2010.
[5] M. Muzammal, Q. Qu, and B. Nasrulin, "Renovating blockchain with distributed databases: An open source system," Future Generation Computer Systems, vol. 90, pp. 105-117, 2019.
[6] H. Chen and Y. Wang, "SSChain: A full sharding protocol for public blockchain without data migration overhead," Pervasive and Mobile Computing, vol. 59, p. 101055, 2019.
[7] E. Garcia Ribera, "Design and implementation of a proof-of-stake consensus algorithm for blockchain," B.S. thesis, Universitat Polite`cnica de Catalunya, 2018.
[8] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof- of-stake," self-published paper, August, vol. 19, 2012.
[9] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-oftrust consensus protocol for enhancing accountability in crowd sourcing services," IEEE Transactions on Services Computing, 2018.
[10] S. Jeon, I. Doh, and K. Chae, "Rmbc: Randomized mesh blockchain using dbft consensus algorithm," in Information Networking (ICOIN), 2018 International Conference on. IEEE, 2018, pp. 712–717.
[11] X.Fu, H. Wang, P. Shi, and H. Mi, "Popf: A consensus algorithm for jcledger," in Service-Oriented System Engineering (SOSE), 2018 IEEE Symposium on. IEEE, 2018, pp. 204–209.
[12] D. Schwartz, N. Youngs, A. Britto et al., "The ripple protocol consensus algorithm," Ripple Labs Inc White Paper, vol. 5, 2014.
[13] Z. Ren, K. Cong, J. Pouwelse, and Z. Erkin, "Implicit con- sensus: Blockchain with unbounded throughput," arXiv preprint arXiv:1705.11046, 2017.
[14] Aitken R (2017) What's The Future Of Online Marketplaces & Blockchain's Technology Impact? Available at: https://www.forbes.com/sites/rogeraitken/2017/10/24/whats-the-future-of-online-market placesblockchains technology-impact/#6b3a6a0863a0 (accessed 6 January 2018).

|| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 7.512| || Volume 9, Special Issue 2, October 2020 ||

3rd International Conference on Emerging Trends in Science, Technology and Mathematics [ICETSTM 2020]

18th September 2020

Organized by

Department of Computer Science, Parvathy's Arts and Science College, Dindigul, Tamilnadu, India

[15] Aru I (2017) Full Stack Development Tools Lowering Blockchain Entry...|News|Cointelegraph. Availableat:https://cointelegraph.com/news/full-stack-development-tools-lowering- blockchain-entry-barriers (accessed 4February 2018).
[16] Bheemaiah K (2016) Block Chain 2.0: The Renaissance of Money.Availableat:http://www.wired.com/2015/01/blockchain-2-0
[17] Huh, S.; Sangrae, C.; Soohyung, K. Managing IoT devices using blockchain platform. In Proceedings of the 2017 19th International Conference on Advanced Communication Technology (ICACT), Bongpyeong, Korea, 19–22 February 2017
[18] Armknecht, F.; Karame, G.; Mandal, A.; Youssef, F.; Zenner, E. Ripple: Overview and Outlook. In Trust and Trustworthy Computing; Conti, M., Schunter, M., Askoxylakis, I., Eds.; Springer International Publishing: Cham, Switzerland, 2015; pp.163–180.
[19] Vasek, M.; Moore, T. There's No Free Lunch, Even Using Bitcoin: Tracking the Popularity and Profits of Virtual Scams. In Proceedings of the International Conference on Financial Cryptography and Data Security, San Juan, Puerto Rico, 26–30 January 2015; Springer: Berlin/Heidelberg, Gemany, 2015.
[20] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. \
[21] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," IEEE Communications Surveys & Tutorials, 2018.
[22] R. Yuan, Y.-B. Xia, H.-B. Chen, B.-Y. Zang, and J. Xie, "Shadoweth: Private smart contract on public blockchain," Journal of Computer Science and Technology, vol. 33, pp. 542-556, 2018.
[23] T. McConaghy, R. Marques, A. Müller, D. De Jonghe, T. McConaghy, G. McMullen, et al., "BigchainDB: a scalable Blockchain database," white paper, BigChainDB, 2016.
[24] M. S. Sahoo and P. K. Baruah, "HBasechainDB–A Scalable Blockchain Framework on Hadoop Ecosystem," in Asian Conference on Supercomputing Frontiers, 2018, pp. 18-29.
[25] J. Chen and Y. Xue, "Bootstrapping a blockchain based ecosystem for big data exchange," in Big Data (BigData Congress), 2017 IEEE International Congress on, 2017, pp. 460-463.
[26] H. Yu, Z. Yang, and R. O. Sinnott, "Decentralized Big Data Auditing for Smart City Environments Leveraging Blockchain Technology," IEEE Access, vol. 7, pp. 6288-6296, 2018.
[27] Y. Lu, "The blockchain: State-of-the-art and research challenges," Journal of Industrial Information Integration, 2019.
[28] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," IEEE Cloud Computing, vol. 4, pp. 50- 59, 2017.
[29] X. Liang, S. Shetty, D. Tosh, C. Kamhoua, K. Kwiat, and L. Njilla, "Provchain: A blockchain-based data provenance architecture in cloud environment with enhanced privacy and availability," in Proceedings of the 17th IEEE/ACM international symposium on cluster, cloud and grid computing, 2017, pp. 468-477.
[30] S. Sahoo, A. M. Fajge, R. Halder, and A. Cortesi, "A Hierarchical and Abstraction-Based Blockchain Model," Applied Sciences, vol. 9, p. 2343, 2019.
[31] C. Yang, X. Chen, and Y. Xiang, "Blockchain-based publicly verifiable data deletion scheme for cloud storage," Journal of Network and Computer Applications, vol. 103, pp. 185-193, 2018.
[32] C. H. Liu, Q. Lin, and S. Wen, "Blockchain-enabled Data Collection and Sharing for Industrial IoT with Deep Reinforcement Learning," IEEE Transactions on Industrial Informatics, 2018.
[33] V. Suma, "Security and Privacy Mechanism using Blockchain," in 2019 Journal of ubiquitous Computing and Communication Technologies (UCCT) (2019), pp. 45-54.
[34] J. Wang, L. Wu, K.-K. R. Choo, and D. He, "Blockchain Based Anonymous Authentication with Key Management for Smart Grid Edge Computing Infrastructure," IEEE Transactions on Industrial Informatics, 2019.
[35] J. Li, J. Wu, and L. Chen, "Block-secure: Blockchain based scheme for secure P2P cloud storage," Information Sciences, vol.465, pp. 219-231, 2018.
[36] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," Future Generation Computer Systems, vol. 101, pp. 1028-1040, 2019.