ISSN- 2394-5125 VOL 7, ISSUE 08, 2020

A SURVEY OF CHALLENGES OF BLOCKCHAIN IN EDUCATION

Mrs.P.Sheela Rani[1], S.Baghavathi Priya[2]

[1]Assistant Professor, Department of Information Technology, Panimalar Institute of Technology, Chennai, India
[2]Professor, Department of Information Technology,Rajalakshmi Engineering College, Chennai, India
[1]rpsheelarani.2014@gmail.com, [2]bhavs.divs@gmail.com

ABSTRACT

In the higher education sector the advent of Distributed registry in blockchain is used to prepare a digital certificates. Throughout a literature review, this research scrutinized the higher education using blockchain. It intends to discuss the challenges in higher education Institution, implementing a new application to develop an immutable and trusted lifelong learning records for students including the digital tamper proof certificates and digital copyrights of learning resource. Adopting the challenges such as scalability, integrity, interoperability issues in education by using blockchain. This paper provides a crystal clear exploration on blockchain and the siginificance of blockchain technology to be adopted by higher education as a digital technology.

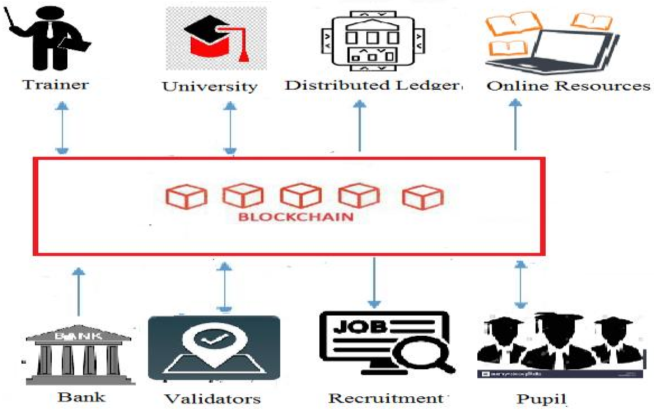
Key words: Blockchain, Digital certifcate ,Smart Contract ,Scalability,Interoperability, Ethereum , Distributed ledger.

INTRODUCTION

Blockchain is an recent Technology**.** The current version of higher education is turning into more and more decentralized, diverse and difficult to confirm and validate, which leads to numerous issues for every emblematic of the commercial enterprise models. That involves the education of experts for his or her introduction addicted to the running world, Still institutes maintains individual Educational records used for all the students which are not connected to all other institutions for verification.

This study traverses a point of view of blockchain security concerns and current latest trends. Now a days most of the institutions and Organizations using Digital Register. This ledger can be stored on any type either public or private network. The nodes which are available in the network use a protocol to verify whether the data is authenticated or not. Modern Technologies are applied to protect data from uncertified changes on the ledger.

Challenges in blockchain such as distributed ledger, online multimedia resources , non tamperable digital certificates provided by universities , data verification by accreditors or validators are described in fig(1).



Fig(1) Blockchain Framework in Education

2 Literature Review

Blockchain and its numerous realistic implementations and a few core principles from current studies in the education field is offered by this section. Secondary research can be made by using this assessment.

[1] In this survey Blockchain has been evaluated by the efficiency in phrases of writing and investigating achievement. Ministry of Education and Training in Vietnam took obligation for every educational institutions at the public level. No one can assured the genuineness of certificates provided along the educational institutions except themselves. Although numerous of them bring up to date graduates lists on their reliable websites on the whole institutions never produce certificates and students details. ECefblock DApp had executed on Hyperledger Fabric tool and the NodeJS has been used to write its interface. By using smart contract protocol ,ECefblock's data was written to a blockchain network. The overall achievement was measured by transaction such as reading and writing from or to the register. In the future, blockchain would be extend the challenges along as privacy, cryptography, 51%attack.

[2] In this study Blockchain has been contributed a scheme of blockchain-permitted digital privileges administration. In e-learning education, multimedia devices were implemented and controlled successfully. Moreover they specified three smart contract plans in favour of the perception of multimedia digital privileges , protected warehouse and consequently the immediated authentication of digital testimonials correspondingly. And there were furthermore a numeral of transitory links in favour of utilization of their storage produced constant with the learning customers' invites to employers or other parties, which were used in favour of the digital certificates affirmation into career enrolment with alertness. Smart contract Tool has been implemented for the management of digital education certificates. Blockchain has been designed the network structure, together with three sorts of networks and two kinds of blockchains. It includes absolutely decentralized P2P networks (getting to know person group with education testimonial system) and nearby system targeted round every training validate system (Multimedia instructional useful devices nearby groups). This system provided the features of blockchain such as encapsulated as its distribution, decentralization, and trusted encryption and moreover it was used in e learning system. This system also used to build different public networks for multimedia transactions and digital rights administrations. The tediousness specified here was that the proposed system should similarly expanded to apply different specified applications of multimedia information security or digital rights administrations,

[3]In this review blockchain has been presented the renovating firmware platform for developing the progression of firmware renovation. Batch authentication had been helped by this system in support of IOT to reinforce scalability and safeguard. Smart contract combined with Virus Total were entrenched to verify any malware was implanted in the firmware. Batch authentication for signs were projected instead of several sign validation to enhance the scalability. To present elevated accessibility of their renovate platform, P2P file contribution technique has been applied. Ethereum and smart contract tools were used in their prototype. Blockchain had been conducted simulation for IOT resources of firmware to enhance the functional efficiency in respect of cost and communication transparency. Execution of this system is slightly sub normal when compared among the normal system.

[4] In this review Blockchain has been explored an innovative blockchain association with the aim of merging a number of blockchains to assist multiplex distributed application. There were two application structures were used in this system. One was for video distribution and copyright protection and the other was air pollutants tracking and quota replacement. The blockchain has been consolidated together to satisfy the necessity of composite distribution packages. The hardware X86 based UP board 19 and the software UBUNTU were used to make cheap rate AQM station. HyperLedger Fabric tool was used for records depository . Open source video platform Kaltura18 and NKN for content division has been arrogated. This system was used to defend intellectual belongings, and it improves performance , tamper resistant , scalability and accuracy with lower charges. Blockchain has been provided extra flexible statistics storage.In the succeeding future, the construction of blockchain had to be amalgamated into a new particular blockchain, Federation blockchain, to hold the quality of the recent blockchain and inter blockchain transactions.

[5]Blockchain scrupulously examined the significant elements on the whole of the blockchain scheme , starting from the relations entrenched level and the information communication level etc. Depending upon

the total key founding they have classified into 3 main parts. They were Node Clustering , Topology Construction and Broadcast Optimization. Blockchain has been designed, implemented, an integrated and specified Blockchain Network Simulator named as BlockSim to analyze the achievements regarding delay. To reduce the entanglement level a Geographical Proximity Sensing Clustering(GPSC) method that was based on K Means Algorithm. Blockchain has been used SHNT(Structured hierarchical-Network Topology) and PSTB(Parallel Spanning-Tree Broadcast). SHNT was specifically indicated to create the topology of system link among a big network. Coming to the PSTB , it was mainly used to transmit process in together Intra Cluster and Inter Cluster Systems. Blockchain has been implemented by Etherum , Operating System Cent OS7.0 and Gossip Algorithm. Advantages of this system was that it has provided network scalability as well as stability due to BlockP2P. BlockP2P could be issued lower network latency for data broadcast, and maintain network scalability and stability. Comparison between Bitcoin with Ethereum were shown by the investigational results. Ethereum was still at its near the beginning stages of enhancement and as a result that work would be put in by way of the application of the latest version of blockchain.

.

[6] In this article blockchain had analyzed on its main resources, methods, and applications. The application has been resolved which had attributes of decentralization, automatic execution, and non damageable data management. This protoype embodies user confirmation, data affirmation, data register, information sharing, and some other processes. Such data could further be splitted into distinct levels of outstanding, superior, trained, etc., and every level correlate to dissimilar reward regulations. To the restraint of culpabilities and malignant codes in blockchain, smart contracts were made to run in confined sandbox environments rather than straightly on blockchain systems. The consensus algorithm has been used to filter the specific nodes. Blockchaint would be controlled the data worthness from the origin and preventing low grade information from inflowing into this protype. Safeguard, Worthness, Sharing were few complications faced by data management.

[7] In this study, Blockchain has been consented BOLL (Blockchain of Learning Logs). BOLL was preeminent that supports how learning logs were associated through foundations and expand constant learning logs for trainees. It was a program that excites the trainees to drive their learning records consecutively within universities in a reliable and validatable format. Smart contract has been enacted to govern consent, learning records and action verb for a fastidious learner. Learning tools such as an open-source Learning Management Systems (LMS), Moodle, Digital book reader, and BookRoll were used. GO programming language has been used in Ethereum. Dell EMC PowerEdge R530 hardware (16GB RAM, 512 SSD) has been inserted in Ubuntu 16.04 Server. Smart contract to detain, and was used to construct explicit privacy and safeguarding of lifelong learning records through the execution of the BOLL gadget. This system was used in evaluate an individual's educational attainment, appropriateness for employment, and scholarly assessment. The authenticity of the magazine also can be demonstrated without difficulty. The scalability could be conserved in this system..

.

[8] In this article, an online education was wielded to estimate students' SRL capabilities to perceive the course via EPM strategies. The aim of EPM was to glean perception from the event record that were logged by an academic system, through extensively used Learning Management Systems (LMSs). To create this, a log file with 21,629 occasions from an e-learning course medium for Spanish undergraduate college students was graded. The prototypes have a fixed level of granularity which could be depicted in educational terms and would be the significant fulfillment in prototype detection. The technique Mining models such as Inductive Miner algorithm (IM) allowed them to found prototype in respect of capability for both passing and failing students in this dataset. Good suitability models with values were contributed which means that it captures and proliferates the students' conversations on the Moodle platform. These formats were ever-present in higher education. They would be tested the timestamp variables also.

[9] In this paper blockchain has been proposed a blockchain-primarily based a realistic and relaxed e-vote casting scheme, which met the vital requirements of e-vote casting method. A synchronized model of voting information primarily based on distributed ledger generation (DLT) has been intended to avoid forgery of votes. That model permitted in citizens to differ their vote before the allotted period of time. Customers could vote by using ECDSA signature, which could be considered as an authenticity of the vote . The system has been performed on Linux platform Ubuntu and algorithm elliptic curve cryptography (ECC) and

the programming language Python. The database of votes used by a distributed server of timestamp on a P2P network controlled independently. Drawback of this study was that , using ECC public key cryptography, which was not safe to quantum laptop attacks.

.

[10] In this survey blockchain has been challenged the prototype of model of reliable in an open Higher Educations based on Blockchain Technology which attests the achievements of proficiency by learners coached in distinct Educational Institutions. This system could be evaluated in every institutions. It could be implemented in any training institution to adopt its training to the open requirements of expert biography's demonstrated by workers in the zone. The system had used for those institutions to have an enormous and effective methods for Self Assessing their Training and also used to create the process of hiring ,and evaluating easily and would eradicated the duplicates immediately. Blockchain had been examined by Ethereum platform in order to solve the standard problems. A P2P had developed based on Java Script, MYSQL and HTML5. The main advantage specified was that, the students friendly environment wherein the students could learn completely and in an aesthetic manner. The main disadvantage was that it was failed to validate in certain place and it was not that much feasible in general competencies.

[11] In this review blockchain has been envisioned an architecture for log auditing the use of a permissioned blockchain to lay up veracity proofs. Even exclusive of a intermediary service provider, the solution achieves immutability through collaboration and data sharing among detached nodes. Acquiescence has been granted for dispensation of verification for security analytics purposes while ensuring auditability of the unique log document. Overall performance benchmarks confirmed that the blockchain performance become capable to deal with very high log event frequencies of 3000 to 3500 transactions reliable, depending on the quantity of nodes. Storage necessities were extensive nevertheless due to complete duplication and withholding of all historical facts. For assessment, they build the prototype within the DING fest infrastructure and described their results regarding security and performance. The Exonum framework, SIEM reference architecture and log auditing provider has been carried out. It additionally supplied built in offerings for dispensed timestamps and Bitcoin anchoring. Droplet instances with 4 dedicated digital CPU cores and 8GB of RAM were used. Blockchain has furnished a secure logging device changed into maintained availability, non repudation and integrity of log documents. An stronger prototype will be applied for log rotation to lessen storage costs and other frameworks to look if scalability also can be further progressed.

[12] In this study, Blockchain has been demonstrated a innovative PKI skeleton with transparent testimonials transparency primarily based on blockchain, which they dentoed as CertLedger, to cast off the divide-world assaults in addition to offer testimonials removal transparancy. Every TLS testimonials verification, data safeguard , with whole removal method had controlled in CertLedger and also depended on CA certificates organization. For the duration of a TLS link , TLS customers got a proficient testimony of lifestyles in the testimonial at once provided by its domain proprietor. Therefore, solitude become absolutely conserved with the aid of getting rid of the traceability problem through OCSP servers. This prototype provided completely specific, proficient, and straightforward certificates verification procedure disposing of a traditional insufficient and incompatible certificates validation strategies carried out by using unique software program providers. No need to validate the certificates and protect the CA certificate any longer by TLS clients. An experimental results has been exposed by a prototype of CertLedger on a private Ethereum and smart contract. To get evidence in support of the TLS testimonials they applied Eth proof NodeJS API. This scheme resolved the consequences like divide world assault, testimonial cancellation and verification problems with reliable testimonials , key depository administration.

[13]In this Work, Blockchain has been showed a innovative company level solitude security methods for blockchain based transaction scheme. This scheme has performed a stability among privacy safeguard and safety measures management. There were 3 significant features of protocol safegaurd, transaction solitude in addition to that recognition tractability has been executed by this system and also it adequate for several trading framework, more than ever for public to public transactions. Three zero knowledge three zero knowledge non intervention evidence protocols established depend on discrete log. Their execution has been adapted by Bitcoin Trading scheme, integrated among Zerocoin Trading scheme along with Cross Chain Technology . They used Go language for implementation. This system enchanted powerful user

privacy safeguard and moreover the organizations be turned up user details when an prohibited transactions takes place. Scalability could be preserved in this system.

[14]In this survey, blockchain has been envisioned a protected huge scale immediate disbursement (SLIP) scheme for enhancing the capability of blockchain scheme which realized an collective sign system for connecting a number of Off Chain passages like tokens disabled in those passages could pass information from one passage to the other passages. A sum of dispersed Tokens in those passages was the aggregate of all Locked in tokens rather than the small amount of Locked in Tokens. As well, as payers could be aggregated the sign increases, Payees had to evaluate a sequence of transactions once in all transaction, whereas miners which maintained that blockchain systems had to affirm every communications to every one, which creates SLIP scheme well-organized. In order to prevent in opposite to Double Spending ,Over Spending, and venomous decision attacks. The SLIP has been recognized and executed. The flexibility of Tokens in several Off Chain passages has improved by SLIP scheme. The SLIP device has to be executed the offchain negotiability, security, immediate payments, offline bills. The investigation failed to detect a few techniques to enhance the scalability.

[15] In this paper, Blockchain has been settled for the photo forensics scheme to infer photo fraud problems, photo tracking problems, and copyright disagreement problems. Blockchain to infer photo faking problems, photo tracing problems, and copyright dispute problems. Blockchain technology has been incorporated with image authentication technologies to present a new mining protocol to stimulate miners to verify photos for users. This accords users to their access and on-chain photo proofs through which one can uphold and go over the copyright photos and the operating records of them. Ethereum platform had applied to examine the safety of the scheme. It was a self-executing program by way of digital agreement imposed in a protected environment. It had the capability of photo forensics with verification, copyright security, and trackability and also acceded authenticable transformations not including any extra depository. The drawback specified here was to enhance the throughput and also to reduce relevant gas cost.

[16] In this study Blockchain has been examined the product to be reliable of smart contracts , privacy-securing and decentralized, DL-Tags were displayed as a result to maintain its life span. Both the shareholders and the product users could verify the product’s legitimacy without notifying their identity, via consensus on the product’s specificationas and states registered on the blockchain. The information has enhanced as a documentation of the product’s origination and its travel through the supply network as halting tag replicating and exploiting. DL Tags allow preserving the privacy of the product’s interchanging data among the manufacturer, ecommerce supply network and the customer withot revealing that details outer to the supply network. Distributed Ledger Technology (DLT) has been implemented by Ethereum platform and Public Key Infracture. For executing the DL Tags results, It needed the consumption of a public and consentless distributed ledger platform aiding smart contracts. Influencing of subsisting Smart Tags data, Cloning and reusing of subsisting smart tags, great series of responsibility when a product is normally paid for, Usually not initiated and not accepted during shipping or delivery, Encircling of the whole TIS system by the construction of illegitimate smart tags.

[17] In this analysis blockchain has been illustrated as a novel Time Lock Encryption structure, with the recent views of computable reference clocks and determinable. This model has been witnessed that it was of self decisive and removeable safety based one. There were several properties like multi linear maps and its evaluation which of random order . Blockchain has been reached a innovative level called as the computational reference clocks which was an expansion of the Standard computational prototype. Reference clock was based on the bitcoin and evidence encryption by applying SNARKS. The receivers that are uniquely frail computational resources must be decoded after the deadline without any further interaction with the senders and receivers. Future evaluation could be endeavoured to discover a greater realistic scheme based on their construction. It could be used a extra well organized removable evidence encryption structure. Development could made via other methods of figuring out their computational reference clock from different kinds large public computations.

[18] In this study a worldwide blockchain-established higher education credit platform has been carried. That platform took the gain of the blockchain on the method to generate an internationally depend on Higher

Education Credit and Grading System. It conveyed a worldwide combined outlook in favour of learners along with organizations. Higher Educational Institutions(HEI) has to update data of students educational origination and the relevant information of the courses completed. Learners be comfort from crystalline aspect of their courses and the information employers could be validated and verified by the employers. Execution has been applied at the EduCTX platform which was based on the Open Supply ark blockchain. And also they projected a DPOS disbursed consensus version of the blockchain. HEIs activities associated to students and fake detection and prevention were carried by this system. A student could immediately check his/her completed course records.. In that way fraud could be prevented. In future this system will be implemented in smart contracts and the work will be magnified.

[19] In this paper, Blockchain has been overlooked as a foundation and paradigm for solitude protecting E-Government Systems, and thus conceivably approving via every government with an objective of verifying both reliability and solitude, while concurrently raising certainty in the communal zone. The subsisting peers of the matrix evaluates the E-Government appliance, and one among the peers organizes the network node and discourse of the new applicant. A user ID is allocated to any new customer and a blockchain wallet for the stockpile of one's transaction. Ethereum platform and Elliptic Curve Cryptography(ECC) algorithm has been employed by them to enforce assigned proof of stake and Smart Contract for initiating smart contract cooperatively with insurance contracts and tax, land registry and employment contracts. By prepending transactions and bolting the block, low CPU utilization, low memory expending and fast key generation has acquired. Interoperability Issues have also been taken care of. Since Ethereum platform was at its prior phases of progress, a following work with its suitable genre of blockchain technology will be released incase to set the needs of the communal sectors and for one's data in increasing certainty and privacy.

Conclusion

The reviewed literature suggests that there are several advantages to the use of blockchain in higher education. This research is focused solely on students life long learning records in higher education . The main challenges are to present further suitable methods in favour of users by examining the lifetime of records, testimonials , scalability, interoperability, integrity issues are also assessed by this review. The analysis were made by early stage tools like Ethereum and smart contract. In future research the best prototype could be implemented by using the Hyperledger platform to find solutions to their security problems in life long learning records including digital Certificates and digital copyrights of learning resources and issues.

References:

[1] Thanh Chung Dao, Binh Minh Nguyen, and Ba Lam Do, Springer "Challenges and Strategies for Developing Decentralized Applications Based on Blockchain Technology",pp 952–962, 2020

[2].Junqi Guo[1,2] & Chuyang Li [1,2] & Guangzhi Zhangi[1,2] & Yunchuan Sun [2,3] & Rongfang [Bie 1,2], " Blockchain enabled digital rights management for multimedia Resources of Online Education", Springer 2019.

[3].Jen Wei Hua,c, Lo Yao Yeha,d* ,, Shih Wei Liao b, Chu-Sing Yangc, " Autonomous and malware proof blockchain based firmware update platform with efficient batch verification for Internet of Things devices" , ELSEVIER pp 238-252 , 2019.

[4]Zhitao Wan, Minqiang Cai, Xianghua Lin, and Jinqing Yang, Springer, "Blockchain Federation for Complex Distributed Applications", pp 112-125, 2019.

[5] Weifeng Hao1, Jiajie Zeng1, Xiaohai Dai1, Jiang Xiao1, Qiangsheng Hua1, Hanhua Chen1, Kuan Ching Li2 and Hai Jin1, "BlockP2P: Enabling Fast Blockchain broadcast with Scalable Peer to Peer Network Topology " , Springer, pp 223=237,2019.

[6]Liangming Wen1,2, Lili Zhang1, and Jianhui Li1,"Application of Blockchain Technology in Data Management: Advantages and Solutions", Springer , pp 239-254, 2019.

[7] Patrick Ocheja1*, Brendan Flanagan2, Hiroshi Ueda2 and Hiroaki Ogata2, Enhanced Learning (2019) 14:4 , Springer Open Access "Managing lifelong learning records through blockchain" 2019.

[8]Rebeca Cerzo1, Alejandro Bogarin2 , Maria Esteban 3, Cristobal Romero2, "Process mining for self regulated learning assessment in e-learning", Springer2019.

[9]Haibo Yi," Securing E-Voting based on blockchain in P2P network", Springer 2019.

[10]David Lizeano1, Juan A. Lara 1, Bebo White2, Shadi Aljawaraneh3, “Blockchain based approach to create a model of trust in open and ubiquitous higher education”, Springer 2019.

[11]Benedikt Putz*, Florian Menges, Gunther Pernul, “ A secure and auditable logging infrastructure based on a permissioned blockchain” Elsevier , 2019.

[12]Murat Yasin Kubilay a *, Mehrnet Sabir Kiraz b, Haci Ali Mantar a, “CertLedger: A new PKI model with Certificate Transparency based on Blockchain”,Elsevier , pp 333-352.2019.

[13] Haibin Zhenga,b , Qianhong Wuc,d, Jan Xiee , Zhenyu Guanc,* , Bo Qinf , Zhiqiang Gua,: “An organization-friendly blockchain system” Elsevier, 2019.

[14]. Lin Zhong a,b , Qianhong Wua,c , Jan Xied , Zhenyu Guana,* , Bo Qine “A Secure Larage Scale instant Payment System based on blockchain:, Elsevier , 349-364, 2019.

[15] Lin Renpeng Zoua , Xixiang Lva,* , Baocang Wang b “Blockchain-based photo forensics with permissible transformations” Elsevier ,2019.

[16]Federico Matteo Beneie ,Pavale skoeir and Ivana Podnar Zarko, “DL Tags:DLT and Smart Tags for Decentralized, Privacy Preserving and Verifiable Supply Chain Management” IEEE Access Volume 7 , 2019.

[17] Jia Liu1 · Tibor Jager2 · Saqib A. Kakvi2 · Bogdan Warinschi” How to build time-lock encryption” Springer, pp-2549–2586, 2018.

[18]Mmuhamed Turkanovieid , Marko Holblid, Kristjan Kosic, Marjan Hericko and Aida KAmisalicid, “ EduCTX: A Blockchain based Higher Education Credit Platform”, IEEE Access, Volume 6 , 2018.

[19] Noe Elisa1, Longzhi Yang1, Fei Chao2, Yi Cao3, “ A framework of blockchain based secure and privacy preserving Egovernment System “, Springer ,2018.