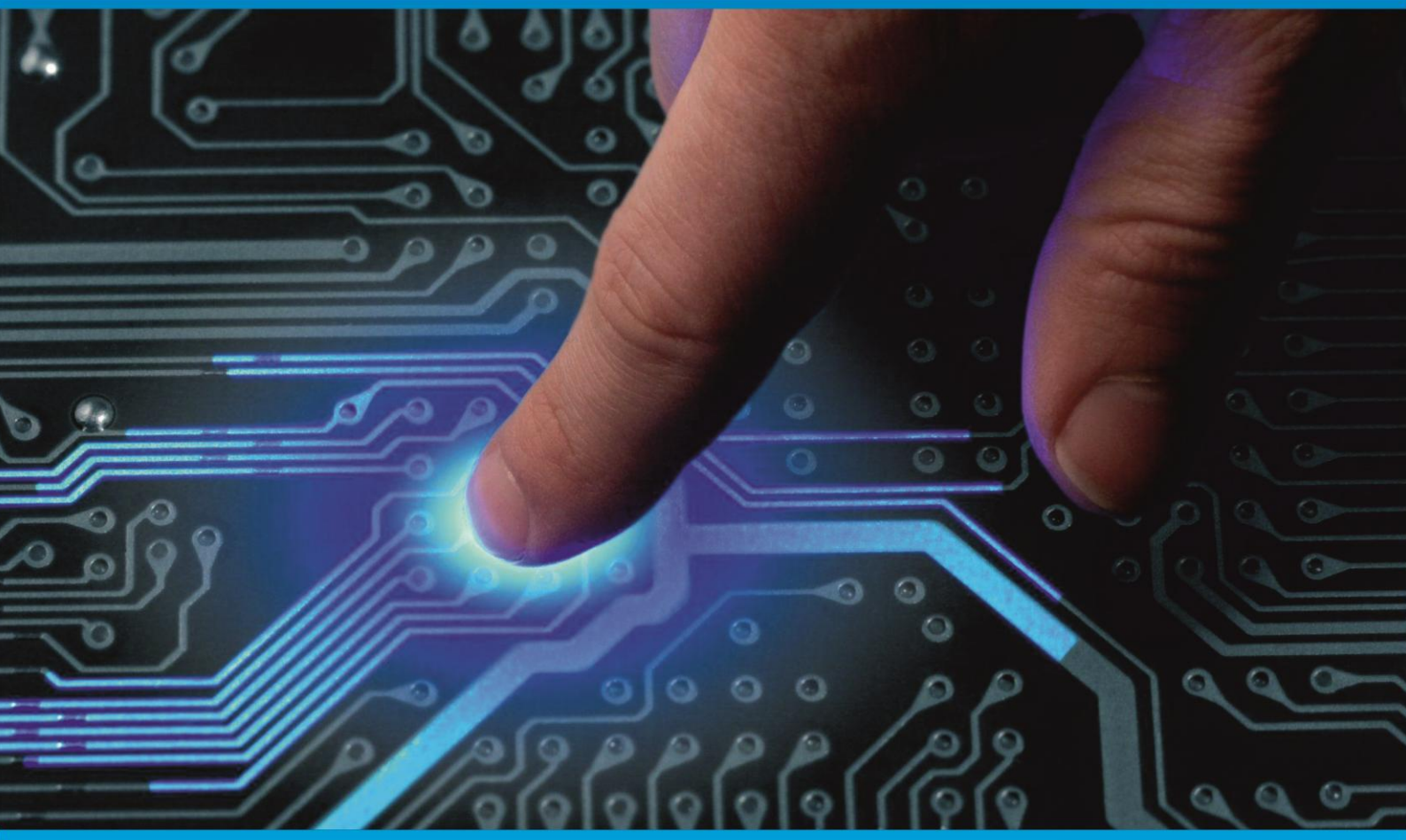
IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 8, Issue 10, October 2020

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.488

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

Smart Contract for Educational Digital Certificate Using Blockchain

Akshada Tuplondhe,Yashashree Pawar, Nitika Jangra, Supriya Bobade, Prof. Hitendra Khairnar

UG Students, UMKSSS's Cummins College of Engineering for Women, Karvenagar, Maharashtra Pune, India

Assistant Professor, UMKSSS's Cummins College of Engineering for Women, Karvenagar, Maharashtra Pune, India

ABSTRACT: In India, according to Ministry of Education statistics, about one million students graduateeach year, some of them will go to countries, high schools or tertiary institutions to continue their studies, and some will be ready to enter the workplace employment. During the study course, the students' all kinds of excellent performance certificates, score transcripts, etc., will become an important reference for admitting to new schools or new works.

Due to the lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology is proposed. By the modifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability is made.

The procedure of issuing the digital certificate in this system is as follows. First, generate the electronic file of a paper certificate accompanying other related data into the database, meanwhile calculate the electronic file for its hash value. Finally, store the hash value into the block in the chain system. The system will create a related QR-code and inquiry string code to affix to the paper certificate. It will provide the demand unit to verify the authenticity of the paper certificate through mobile phone scanning or website inquiries.

Through the modifiable properties of the blockchain, the system not only enhances the credibility of various paper-based certificates, but also electronically reduces the loss risks of various types of certificates.

KEYWORDS: Blockchain, SQL Injection, Decentralized, Distributed, Mining, Transaction, QR Code, Node, Consensus.

I. INTRODUCTION

E-certificate generation system which manually creates the certificates based on current student's data. Various centralized methods follow the similar approach for verification but centralized approaches can't defend the various network attacks like SQL injection, collusion, brute force etc. Thus, in order to prevent these attacks, decentralized approach should be implemented.Blockchain is a distributed, decentralized and oftentimes it is public, digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks. In this approach private blockchain is developed using smart contract. A private blockchain always restricts the users from having the authority to validate block transactions and create smart contracts. This is appropriate for the traditional businesses and governance models.

II. PROBLEM DEFINITION AND OBJECTIVES

Problem Definition -

To design and develop a system for dynamic and secure e-certificate generation system using smart contract in blockchain environment. In this work, we also illustrate own blockchain in open source environment with custom

We are profoundly grateful to our project guide for their expert guidance and continuous encouragement throughout to see that this project achieves its target. We would like to express deepest appreciation towards our project manager for supporting us in completing this project. At last we would like to express our sincere gratitude to our professors who helped us directly or indirectly during this course of work.

There are 4 members in the project. The names are:-AkshadaTuplondhe, NitikaJangra, SupriyaBobade, YashashreePawar.

AkshadaTuplondhe is the final year student from Cummins College Of Engineering For Women, Computer Engineering Department.

NitikaJangra is the final year student from Cummins College Of Engineering For Women, Computer Engineering Department.

SupriyaBobade is the final year student from Cummins College Of Engineering For Women, Computer Engineering Department.

YashashreePawar is the final year student from Cummins College Of Engineering For Women, Computer Engineering Department.

mining strategy as well as smart contract also validate and explore system performance using consensus algorithm for proof of validation.

Objectives -

1) To Plan and Build a system for dynamic and secure e-certificate generation system using smart contract in blockchain environment.

2) To design own blockchain in open source environment with custom mining strategy as well as smart contract.

3) To validate and explore system performance using consensus algorithm for proof of validation.

Literature Survey

A.G. Said et. al. [1] proposed a system E-Certificate Authentication System Using BlockchainIn short, the program's purpose is: a valid registry with electronic certificates, i.e. an electronic credential is generated at the applicant's request. At the same time, that student's record is preserved by using hash values in blockchain blocks. The customer is also presented with a particular QR code or serial number, in accordance with the E-certificate. And instead the demand unit (e.g. company to which the applicant has applied for a job) must verify the authenticity of the electronic file using the QR code or the relevant serial number based on the reported details in the blockchain
Jiin-Chiou Cheng et. al. [2] proposed a system Blockchain and smart contract for digital certificate, Then build an electronic paper document file that follows those related details into the database and thus decides the hash value of the electronic file. Finally, the hash value within the ring is stored in the chain process. To be affixed to the paper credential, the software will produce a related QR code and question string data. It will involve the demand device for paper certificate validity verification via mobile phone scanning or web site inquiries. Since of the blockchain's unchangeable property, the network not only increases the credibility of unique paper-based certificates but also the authentication risks of various types of certificates electronically types of certificates
Marco Baldiet. al. [3] Certificate Validation The program solves the problem through Shared Ledgers and Blockchains by introducing a mechanism in which several CAs share a transparent, shared and stable database where CRLs are received. To this end, we find the concept of blockchain-based shared ledgers implemented for use of cryptocurrencies, which is becoming a common solution for many web applications of high protection and reliability requirements.
Oliver et. al. [4] illustrates Using blockchain as a Government degree tracking and assessment tool: a business analysis based on two financial factors comparing the service price as the main players between the customer and the employer. Students need a low-cost and easy-to-check evidence of competence, and employers also need swift and accurate documentation of their degree before recruiting. All models are built for growing regional markets and shares to discover ways of extending this sector in the European Union.

Because of the The arbitrary existence of hashing is never a guarantee of producing an appropriate object. Thus, Bitcoin mining is a competitive enterprise where miners are effectively hashed and admitted into the blockchain by awarding new Bitcoin for each block[5].

Miners, a collaborative consumer network, verify and check transactions and set up specialized computation equipment called "hashes." They vote with their CPU strength, demonstrating their approval of legitimate blocks by working to expand them and by declining to operate on invalid blocks[6]. These record strings (hashes) that keep track of any Bitcoin transaction and are repeated on any device in the Bitcoin network.

Blockchain is a decentralized LEDGER used for safe trading of digital currencies, deals and transactions[7], and peer-to-peer network management. All nodes adopt the same internode contact protocol, and verify new objects. If the data is validated in every block no block will change it. To modify individual block data, all corresponding block data will be modified, resulting in network cooperation and denial of the transaction by all nodes.

The The power used to "farm" the cryptocurrency is a key aspect since its costs are rising. According to the Bitcoin statistics site Digiconomist, citizens worldwide use more than 30 terawatts-hours of electricity are mining the crypto-currency. This is greater than, at least, the human energy use 159 countries like Hungary, Oman, Ireland, and Lebanon [8].

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

Bitcoin mining is a Creation of new Bitcoin process by verifying Bitcoin Network transactions. That transaction is stored in a shared ledger, and all of the machines involved in the Bitcoin network check and manage the ledger. This "net" of transactions is known as the ledger, and. transaction is basically a timestamp for the database that may involve data [9].
Narayanan et al. [10] Describe a block string as a data structure composed of a related array of hash pointers. Every entity in the list is a block containing some previous block data and hash. This renders it a tamper-evident file, implying the data can only be applied to the list and the prior data can not be changed without detection.
HyperledgerSawtooth employs a flexible design, which distinguishes different sections of the device. This means the degree of blockchain is decoupled from stage of implementation. The flexible architecture often ensures that it is possible to modify various elements of the network, based on the project requirement. Examples of the modules that can be modified involve transaction laws, making and consensus algorithm. [11]

Lamport et al. [12] present algorithms Under different circumstances, that let the generals reach consensus. In a structure where the generals can send recorded, unforgeable letters, the writers illustrate that the dilemma can be solved with any number of generals and traitors. Nonetheless, because of the huge number of communications this approach would be very costly necessary.

Proof of elapsed time (PoET) is a Built consensus approach to be more effective than PoW. PoET can be seen as a function which makes a node wait randomly. In a "trusted execution setting" the feature to determine the amount of time a node should wait This helps the system to identify any users who try to function until their random time elapses. [13]

A distributed ledger, or a website, they have a global environment. The global state is all the material that is contained in the ledger, including the present status. The knowledge used in the global state differs considerably depending on the context of blockchain. [14]

In Hyperledger Sawtooth, and For other blockchain applications, the transactions are put in batches. Batches are used where transaction order is important. The transactions should be done in the right order by placing certain transactions in the same set. If a transaction does not rely on every other transaction than those that have already been authenticated and deposited in the blockchain, the sender may build a new batch only for that transaction. [15].

A. Abbreviations and Acronyms

SQL - Structured Query Language
QR - Code Quick Response Code
IOT - Internet Of Things
CSIRO - Commonwealth Scientific and Industrial Research Organization
AI - Artificial Intelligence
HER - Electronic Health Record
KPABE - Key-Policy Attribute-Based Encryption
ABE - Attribute1-Based Encryption
IBE - Identity Based Encryption
IBS - Identity Based Signature
IB-ES - Identity Based Encryption and Signature
DAO - Decentralized Autonomous Organization
DAC - Decentralized Autonomous Corporation
JSP - Java Server Pages
HTTP - Hyper Text Transfer Protocol
RDBMS - Relational Data Base Management System
DML - Data Manipulation Language
DDL - Data Definition Language
DCL - Data Control Language
J2EE - Java 2 Platform Enterprise Edition
JVM - Java Virtual Machine
JDK - Java Development Kit
SDLC - Software Development Life Cycle
DOS - Disk Operating System
MIM - Mobile Information Management
UML - Unified Modelling Language
IDE - Integrated Development Environment ix

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

JRE - Java Runtime Enterprise

B. Functional Requirements

System must validate the previous block before commit block.User can access the data over the internet 24*7.If any block has changed by third party attacker or unauthorized user, it must show during transaction that current blockchain is invalid.It can recover the invalid blockchain using other data nodes, with the help of majority of trustiness.

The node or user wishing to initiate a transaction must register and send the data to the network.The node or user receiving the data shall check the validity of the data received on the network. It then stores the checked data to a block.All nodes or network users validate the transaction by either executing proof of work or proof of stake algorithm to validate the block specifications.

The network's Consensus Algorithm would store the data in the block added to the blockchain. And all network nodes admit the respective block and stretch the block chain base.

Decentralization, Consensus model(s):Applied consensus protocol and focused on features; A). Security, B) Consciousness, Fault tolerance, Transparent, Open-source, Identity and Access, Autonomy, Immutability, Anonymity are the requirements.

III. MATHEMATICAL MODEL

A System represents 5 different phases,

System S = (S1, S2,S3, S4, S5)

where –

S1 is a finite set of states.

S2is a finite set of symbols called as the alphabet.

S3 is the transition function where $\delta : Q \times \sum \rightarrow Q$

S4is the initial state from where any input is processed ($q_0 \in Q$).

S5is a set of final state/states of Q ($F \subseteq Q$).

All (n) data nodes will return 1 when each have the same blockchain

S1 = initial transactional data with genesis block

S2 = {SHA-256, Consensus_Val, Mining**}**

S3 **=** Validate all server(S1 ⊆ S2⊆ S3⊆ S4) all server validation process

S4= Initial transaction T[0]

S5 = {Commit Trans, GetHostoryRecord}

State =>1 :if all chains are validate or same

0 :if any t(n) server consist the invalid chain

Set dependency

Sys= {Phash, Tdata, Chash}

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

GET BLCOKCHAIN FROM EACH NODE AND VALIDATE WITH EACH OTHER.

IV. PROJECT IMPLEMENTATION

System proposed a new dynamic certificate generation approach using own custom blockchain.First students apply for e-certificate on web portal and upload all educational documents.

Web portal is authenticating trusted third party which validate all documents from university, school, colleges, etc.Once successfully verification has done from university, school, colleges it will store data into blockchain and at the same time it generates the unique QR code and returns to student.Student can submit the received QR code to organization instead of physical hard copy of documents.

Organization can submit QR code to portal and pool the e-certificate of respective student and make the validation.The entire process has performed into the blockchain manner with smart contract which is written by us.To execute the system in vulnerable environment and to explore and validate how proposed system eliminate different network attacks like DOS and MiM, etc.

V. TOOLS AND TECHNOLOGY

Eclipse Luna: The IDE provides wizards and templates to let you create Java EE, Java SE, and Java ME applications. A variety of technologies and frameworks are supported out of the box. For example, you can use wizard and templates to create applications that use the OSGi framework or the NetBeans module system as the basis of modular applications. NetBeans IDE is the Standard Java 8 IDE. With its editors, code analyzers and converters, you can update your applications easily and effortlessly, using modern Java 8 language constructs such as lambdas, functional operations, and process references.

JDK: The Java Development Kit (JDK) is a software development environment which is used to develop Java apps and applets. It includes the Java Runtime Environment (JRE), an interpreter / loader (apache), a compiler (javac), an archive (jar), a generator of documentation (javadoc) and other required resources for Apache creation.

JRE stands for "Java Runtime Environment," and "Java RTE" can also be written. The Java Runtime Environment sets the minimum specifications for running a Java application; it includes Java Virtual Machine (JVM), core classes, and file support.

Specified to operate Java Virtual Machine (JVM) but the implementation provider is independent in choosing the algorithm. Sun and other companies provided for its implementation. Implementation is a computer program that meets JVM specification requirements. Runtime instances JVM instances are created when you type a Java command at a command prompt to run a Java class.

Apache Tomcat: Java Servlet, Java Server Files, Java Expression Language and Java Web Socket technologies are an open source implementation of the Apache Tomcat framework. The specifications for the Java Servlet, Java Server Sites, JavaExpression Language, and Java Web Socket are developed under the Java Community Process. The Apache Tomcat software is developed and released under the Apache License in an open and participatory environment version 2. Apache Tomcat Project is a partnership of world's best breed developers. Apache Tomcat software allows for a wide range of massive, mission-critical web applications across a number of industries and organizations.

MySQL: MySQL is an open-source framework for the management of relational databases (RDBMS). The MySQLTM software delivers a very fast, multi-threaded, multi-user, and robustSQL database server (StructuredQuery Language). MySQL Server is designed for mission-critical, heavy-load production systems as well as for mass-deployed software embedding. MySQL is under two separate editions: the MySQL Community Server open source, and the Business Version proprietary. MySQL Enterprise Server differentiates itself by a set of proprietary extensions that install as application plugins, but otherwise follow the numbering scheme of versions and are designed from the same code base.

HeidiSQL: HeidiSQL is free software, and aims at making learning fast. "Heidi" allows you to access and edit data and structures from computers that run one of MariaDB, MySQL, Microsoft SQL or PostgreSQL database systems. Invented by Anger in 2002, HeidiSQL is one of the most common tools for MariaDB and MySQL worldwide, with a growth peak between 2009 and 2013.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

VI. ALGORITHM

Algorithm 1: Hash Generation

Input: Genesis block, Previous hash, data d,

Output: Generated hash H according to given data

Step 1: Input data as d

Step 2: Apply SHA 256 from SHA family

Step 3: CurrentHash= SHA256(d)

Step 4: RetrunCurrentHash

Algorithm 2: Protocol for Peer(P to P) Verification

Input: Student Operation query, Current-Node Chain CNode[chain], Other Remaining Nodes blockchain NodesChain[Nodeid] [chain],

Output: Recover if any series is valid and invalid or if the current query is executed

Step 1: Studentgenerate the any OperationqueryDDL, DML or DCL query

Step 2: Get current server blockchain

Cchain←Cnode[Chain]

Step 3: Foreach loop

$$NodesChain\ [Nodeid, Chain] \sum_{i=1}^{n} (GetChain)$$

End for loop

Step 4: Foreach loop (read I into NodeChain) If (!.equalsNodeChain[i] with (Cchain))

Flag 1

Else Continue Commit query

Step 5: if (Flag == 1)

Count = SimilaryNodesBlockchian ()

Step 6: Calculated the majority of system

Recover invalid blockchain from specific node

Step 7: End if

End for

End for

5.3.3 Algorithm 3: Mining Algorithm for valid hash creation

Input: Hash Validation Policy P[], Current Hash Values hash_Val

Output: Valid hash-values

Step 1: System generate the hash_Val for ith transaction using Algorithm 1

Step 2: if (hash_Val.valid with P[])

Valid hash

Flag =1

Else

Flag=0

Mine again randomly

Step 3: Return valid hash when flag=1

VII. SYSTEM ARCHITECTURE

Educational documents verification is very tedious and time-consuming process in real time environment. Certificate generation for entire educational history is easy process to eliminate such consuming tasks.

Dynamic QR-code and unique certificate generation for each students document in proposed system. Data e-certificate stored into the blockchain in secure manner which enhance the security. According to the smart contract system also allow the updates in entire blockchain. This research proposed a custom blockchain generation on open source platform.

Assumptions and Dependencies:

1) New nodes follow block transactions submitted by old nodes.
2) The new node does not match the block transaction sent by the old node.
3) Older nodes are associated with block transactions sent by newer nodes.
4) Older nodes do not follow the block transaction that sends new nodes.

VIII. CONCLUSION

There are a number of research guidelines for implementing blockchain technology for e-certificate transactions due to the scope of this area and the need for more reliable and efficient information management systems. Interoperable infrastructure certainly plays an important role in the use of cases involving general data exchange and communication problems on most e-certificate transactions.

From a more technical point of view, the most realistic design method to build an interoperable ecosystem using blockchain technology while addressing serious security and privacy concerns in e-certificate transactions is required.

If there is a need to create decentralized applications using existing blockchain, there is also a need to educate software engineers and domain experts about the potential, as well as additional work on secure and efficient software practice to implement blockchain technology in e-certification transactions for education. About the limitations of this new technology.

Similarly, validation and testing approaches to gauge the efficacy of Blockchain-based health care architectures compared to existing systems are also important (e.g., through the performance metrics related to time and computational costs or assessment metrics related to its feasibility).

FUTURE WORK

1) Future research will focus on this overall scalability and speed over time to improve the user experience.
2) We can get the details of the school or college from which the student has graduated.

APPLICATIONS

3) Peer to peer communication transaction applications.
4) Bitcoin transaction applications.
5) Zebpay transaction application

ACKNOWLEDGMENT

We are profoundly grateful to our project guide for their expert guidance and continuous encouragement throughout to see that this project achieves its target. We would like to express deepest appreciation towards our project manager for supporting us in completing this project. At last we would like to express our sincere gratitude to our professors who helped us directly or indirectly during this course of work.

REFERENCES

[1] A.G. Said, R.P. Ashtaputre, B. Bisht, S.S. Bandal, P.N. Dhamale, "E-Certificate Authentication System Using Blockchain," International Journal of Computer Sciences and Engineering, Vol.7, Issue.4, pp.191-195, 2019.
[2] Cheng JC, Lee NY, Chi C, Chen YH. Blockchain and smart contract for digital certificate.In2018 IEEE international conference on applied system invention (ICASI) 2018 Apr 13 (pp. 1046-1051).IEEE.
[3] Baldi M, Chiaraluce F, Frontoni E, Gottardi G, Sciarroni D, Spalazzi L. Certificate Validation Through Public Ledgers and Blockchains. InITASEC 2017 (pp. 156-165).
[4] Oliver M, Moreno J, Prieto G, Benítez D. Using blockchain as a tool for tracking and verification of official degrees: business model.
[5] George F. Hurlburt and Irena Bojanova, "Bitcoin: Benefit or Curse?," in IEEE, 2014
[6] Satoshi Nakamoto, Bitcoin: A Peer-to-Peer Electronic Cash System, 2008, White Paper.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | Impact Factor: 7.488 |

|| Volume 8, Issue 10, October 2020 ||

[7] Nirmala Singh and Sachchidanand Singh, "Blockchain: Future of financial and cyber security," in IEEE, Noida, 2016.
[8] Henrique Rocha ,MarcusDenker and StephaneDucasse Santiago Bragagnolo, "SmartInspect: solidity smart contract inspector," in IEEE, Itly, p. 2018.
[9] GWYN D'MELLO. (2017, Dec.) https://www.indiatimes.com/technology/news. [Online]. https://www.indiatimes.com/technology/news/bitcoin-miners-are-using-more-electricity-than-irelandother-159-countries-no-kidding-335114.html
[10] Narayanan A., Bonneau J., Felten E., Miller A. &Goldfeder S. (2016) BitcoinandCryptocurrency Technologies: A Comprehensive Introduction. Princeton: Princeton University Press
[11] Introduction to HyperledgerSawtooth (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/introduction.html) 49
[12] Lamport, L., Pease, M., &Shostak, R. (1982). The Byzantine generalsproblem.Menlo Park, CA: SRI International.
[13] PoET 1.0 Specification (2018) Retrieved January 4, 2019 fromhttps://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/poet.html
[14] Global State (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/global_state.ht ml
[15] Transaction and Bathces (2018) Retrieved January 4, 2019 from https://sawtooth.hyperledger.org/docs/core/releases/latest/architecture/transactions_and_batches.html

INNO SPACE

SJIF Scientific Journal Impact Factor

Impact Factor:
7.488

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details