Smart Contract for Educational Digital Certificate using Blockchain

Gaikwad Vishal B.[1] Satpute Kartiki V.[2] Jagtap Rajendra V.[3] Prof.Khatal S. S.[4]
[1,2,3,4]Department of Computer Engineering
[1,2,3,4]Sharadchandra Pawer College of Engineering, Dumbarwadi, Otur, Maharashtra, India

Abstract— Blockchain technology has evolved from being an immutable ledger of transactions for crypto currencies to a programmable interactive environment for building distributed reliable applications. Although, blockchain technology has been used to address various challenges, to our knowledge none of the previous work focused on using blockchain to develop a secure and immutable scientific data provenance management framework that automatically verifies the provenance records. In this work, we leverage blockchain as a platform to facilitate trustworthy data provenance collection, verification and management. According to various researches about one million graduates passing out each year, the certificate issuing authorities are seems to be compromised for the security credentials of student data. Due to the lack of effective ant forge mechanism, events that cause the graduation certificate to be forged often get noticed. In order to solve this problem digital certificate systems are introduced even though security issues are still exist. Blockchain is one of the most recent technology that can be adopted for the data security. The immutable property of the block chain helps to overcome the problem of certificate forgery. This paper proposed a custom blockchain for e-certificate generation for academic students. The implementation has done with multiple data nodes on peer to peer network.

Keywords: Blockchain, hyperledger, digital certificate, hashing

I. INTRODUCTION

Graduation certificates and transcripts contain information confidential to the individuals and should not be easily accessible to others. Hence, there is a high need for a mechanism that can guarantee that the information in such a document is original, which means that document has originated from an authorized source and is not fake. In addition, the information in the document should be confidential so that it can only be viewed by authorized persons. Blockchain technology is used to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates would be improved. Technologies exist in related domains, such as digital signatures, which are used in edocuments to provide authentication, integrity, and nonrepudiation. However, for the requirements of an equalification certificate, it has critical security holes and missing functions: for example, it uses the keys to verify the modification of the document, but doesn't start the validation of the public key certificates' status automatically. This may result in a forgery being accepted if the key has been compromised. Furthermore, even the signer's public key certificate has been validated, but the signed document itself hasn't. In our case of an e-qualification certificate, the signed document itself is also a certificate, which may have a valid period (e.g. The problem we are dealing with is a (certificate) issue, therefore, a simple digital signing of the document alone doesn't solve the problem

II. LITERATURE SURVEY

Smart Contracts [1] Also called crypto-contract, it is a computer program used for transferring / controlling the property or digital currents in specific parties. It does not only determine the terms and conditions but may also implement that policy / agreement. These smart contracts are stored on block-chain and BC is an ideal technology to store these contracts due to the ambiguity and security. Whenever a transaction is considered, the smart-contract determines where the transaction should be transferred / returned or since the transaction actually happened.

Currently CSIRRO team has proposed a new approach to integrate BlockOn IOT with [2]. In its initial endeavor, he uses smart-home technology to understand how IOT can be blocked. Blockwheels are especially used to provide access control system for Smart-Devices Transactions located on Smart-Home. Introducing BC technology in IOT, this search again provides some additional security features, however, every mainstream BC technology must have a concept that does not include the concept of comprehensive algorithms. Moreover, this technology cannot provide a general form of block-chain solution in case of IOT usage.

According to IlyaSukhodolski. The Al [3] system presents a prototype of multi-user system for access control over datasets stored in incredible cloud environments. Like other unreliable environments, cloud storage requires the ability to share information securely. Our approach provides access control over data stored in the cloud without the provider's investment. Access Control Mechanism The main tool is the dynamic feature-based feature-based encryption scheme, which has dynamic features. Using BlockChain based decentralized badgers; Our systems provide an irrevocable log for accessibility requests for all meaningful security incidents like large financing, access policy assignment, alteration or cancellation. We offer a set of cryptographic protocols that make the secret or secret key of cryptographic operation confidential. The hash code of the sifter text is only transmitted by the block on laser. Our system has been tested on prototype smart contracts and tested on Iterium Blockchain platforms.

According to Huehuangenet. Al [4] they offer a blockchain and a MedRec-based approach by enabling encryption and attribute based authentication to enable secure sharing of healthcare data. By applying this approach:

1) The fragmented EHR fragment of all patients can be seen as a complete record and can be safely stored against tampering;
2) The authenticity of patients' EHR can be verified;
3) Flexible and finer access control can be provided and
4) it is possible to maintain a cleared audit trail.

According to VipulGoyalet.Al [5] develops new cryptosystems to share encrypted data properly, which we call key-policy attribute-based encryption (KPABE).In our cryptosystem, Cefhettextis labeled with a set of properties and controls that it connects to private key access configurations that a user can decrypt the encryption. We display the utility of our product to share audit log information and broadcast encryption. Our creation supports private key providers, which subscribe to categorized identification-based encryption (HIBE).

Hao Wang et Mate Al [6] They offer a secure electronic health record (EHR) system based on special-based cryptococcurs and blockchain technology. In our system, we use attribute-based encryption (ABE) and identity-based encryption (IBE) to encrypt medical data and to use identity-based signature (IBS) to apply digital signatures. . In order to obtain various functions of ABI, IBE and IBS in crypto, we present a new cryptographic primitive, it is called a joint feature-based / identity-based encryption and signature (C-AB / IB-ES). It simplifies system maintenance and does not require the installation of separate cryptographic system for various security requirements. In addition, we use block connection techniques to ensure the integrity and inspection of medical data. Finally, we offer a demonstration application for medical insurance business.

According to Yan Michalevskyet. Al [7] system introduces the first practical decentralized ABE scheme with proof of policy-hiding.Our creation is based on the basic encryption of decentralized internal product, which is an encryption strategy launched in this paper. This ABB scheme supports results, disputes, and threshold policies, which protect the access policies of those parties that are not authorized to decrypt content. In addition, we handle the receiver's privacy issue.

Using our plan with Vector Commitment, we hide a complete set of attributes presented by the individual with the recipient; Just disclose the feature that regulates the authority. Finally, we propose random-polynomial encoding that immerses this scheme in the presence of corrupt officials. Al [8]they successfully address these issues by offering a clear policy feature-based data sharing plan with direct cancellation and keyword search. In the proposed scheme, the non-terminated users' private key is not required to be updated during the cancellation of direct revocation of features. In addition, a keyword search has been realized in our plan, and the search is stable with the increase in time features. Specifically, the policy is hidden in our plan, and therefore, the privacy of users is preserved. Our security and performance analysis show that the proposed plan can deal with security and efficiency concerns in cloud computing.

According to SarmadullahKhanet.Al [9] embedded power transactions in blockchain are based on their defined characteristics through the signature of many manufacturers. These signatures have been verified and customers are satisfied with the features that do not open any information that meet those features. The public and private key manufacturers have been created for these customers and using this key ensures that the support process is authorized by customers. There is no central authority required in this perspective. To protest against collision attacks, the makers are given secret pseudo-functional work seeds. Comparative analysis shows the efficiency of the proposed approach to existing people.

According to Ruuguet. Al [10] To guarantee the validity of the EHR surrounding the block channel, he has submitted a special-based signature scheme with multiple officials, in which the patient supports the message according to the specifications, but there is no evidence that he does not have any other information. In addition, there are many officers without generating a reliable individual or a central person in order to generate and deliver a public / private key, which avoids the escrow problem and adapt to the mode of data storage distributed in the Block. By sharing the secrecy of the secret pseudo-festive festivals in the authorities, this protocol opposed the attack of N-1 affiliated with officials. Under the computational Billine Diffie-Hellman concept, we also formally demonstrate that, in relation to the specialty-signatory's enforceability and complete privacy, this specialty-based signature scheme is safe in random decorative models. Comparison shows the efficiency and qualities among the proposed methods and methods in other studies.

III. PROPOSED APPROACH

In this research 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 illustrates own blockchain in open source environment with custom mining strategy as well as smart contract. Finally validate and explore system performance using consensus algorithm for proof of validation. Educational documents verification is very tedious and time consuming process in real time environment. E-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.
System proposed a new dynamic certificate generation approach using own custom blockchain. First student apply for e-certificate on web portal with upload all educational documents. Web portal is authenticate 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 same time it generates the unique certificate id or QR code and returns to student. Student can submit the received QR code or certificate id to organization instead of physical hard copy of documents.

organization can submit QR code or id to portal and pool the e-certificate of respective student and make the validation.

The entire process has perform 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.

Blockchain -Blockchain is the fundamental technology underlying the emerging cryptocurrencies including Bitcoin [2]. The key advantage of blockchain is widely considered to be decentralization, and it can help establish disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems without

mutual trust and centralized control among individual nodes, based on such techniques as data encryption, time-stamping, distributed consensus algorithms, and economic incentive mechanisms. As such, blockchain can offer a novel solution to the longstanding problems of high operation costs, low efficiency and potential security risks of data storage in traditional centralized systems. Blockchain can be considered as the next generation of cloud computing, and is expected to radically reshape the behavior model of individuals and organizations, and thus realize the transition from the Internet of Information today to the future Internet of Value. Blockchain is a distributed database that is widely used for recording distinct transactions. Once a consensus is reached among different nodes, the transaction is added to a block that already holds records of several transactions. Each block contains the hash value of its last counterpart for connection. All the blocks are connected and together they form a blockchain. Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under blockchain, a block becomes validated only once it has been verified by multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A blockchain-based smart contract, for example, creates a reliable system because it dispels doubts about information's veracity.

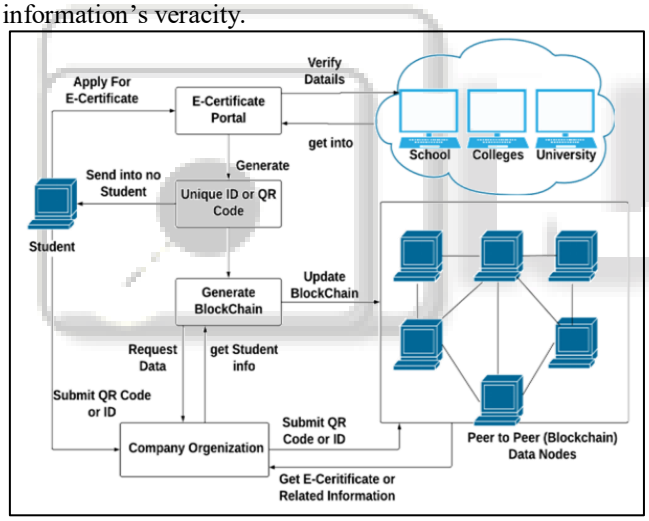

Fig. 1: Proposed Architecture

IV. Conclusion

In this overview we have described the first dataflow clustering algorithm that clearly records the density of regions shared by micro clusters and uses this information for recovery. We have combined the shared density graph with the algorithm required to maintain graphs in the online component of data flow mining algorithms. Even if we shared that the worst-case memory requirement of the Shared Density graph increases with data dimension, complexity analysis and experiments, it appears that the process can be applied effectively to mediumsized data sets. This study shows that shared densityreclustering works well when clustering elements in online data streams create slightly larger MCs. Other popular recycling policies can improve slightly on the effect of share density rewriting and significant MCs are needed to achieve comparative results. This is an important advantage because it means that we can tune the online element to create lesser-clusters for shared-density reclustering. This improves performance and, in most cases, shared memory graphs have more memory stored than shared offsets for shared density graphs.

Data stream clustering algorithm that records the density of the area shared by the micro-cluster and uses this information for recovery. We have combined the shared density graph with the algorithm required to maintain graphs in the online component of data flow mining algorithms.

Digital Certificate-Digital certificate which adopts digital signature technology, presents to the user by the authority to confirm the user himself in the digital fields used to confirm a user's identity and access authorization to the network resources [1]. Digital certificates can be applied to e-commerce activities on the internet and e-government activities, whose scope get involved in application of identity authentication and data security, including traditional commercial, manufacturing, retail online transactions, public utilities etc.

Reference

[1] "Smart Contracts," http://searchcompliance.techtarget.com/definition/ smart-contract, 2017, [Online; accessed 4-Dec- 2017]
[2] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchainin internet of things: Challenges and Solutions,"arXiv:1608.05187 [cs], 2016. [Online]. Available:http://arxiv.org/abs/1608.05187%5Cnhttp://www.arxiv.org/pdf/1608.05187.pd
[3] Sukhodolskiy, Ilya, and Sergey Zapechnikov. "A blockchain-based access control system for cloud storage." Young Researchers in Electrical and Electronic Engineering (EIConRus), 2018 IEEE Conference of Russian.IEEE, 2018.
[4] Yang, Huihui, and Bian Yang. "A Blockchain-based Approach to the Secure Sharing of Healthcare Data."Proceedings of the Norwegian Information Security Conference. 2017.
[5] Goyal, Vipul, et al. "Attribute-based encryption for fine-grained access control of encrypted data." Proceedings of the 13th ACM conference on Computer and communications security.Acm, 2006.
[6] Wang, Hao, and Yujiao Song. "Secure cloud-based EHR system using attribute-based cryptosystem and blockchain." Journal of medical systems 42.8 (2018): 152.
[7] Michalevsky Y, Joye M. Decentralized Policy-Hiding Attribute-Based Encryption with Receiver Privacy.
[8] Wu, Axin, et al. "Hidden policy attribute-based data sharing with direct revocation and keyword search in cloud computing." Sensors 18.7 (2018): 2158.
[9] Khan S, Khan R. Multiple authorities attribute-based verification mechanism for Blockchain mircogrid transactions. Energies. 2018 May;11(5):1154.
[10] Guo, Rui, et al. "Secure attribute-based signature scheme with multiple authorities for Blockchain in electronic health records systems." IEEE Access 776.99 (2018): 1-12

