Secured University Result System Using Cryptographic Techniques

Sagar Dhanake[1], Anuja Nakhate[2], Priyanka Kalbhor[3], Medhavi Magar[4], Yogini Jadhav[5]
[1, 2, 3, 4, 5] Dept of Computer Engineering
[1, 2, 3, 4, 5] Dr. DY Patil Institute Of Engineering and Technology,Ambi, Pune

Abstract- *Corruption and fraud in higher education is a global scourge that hinders human capital formation, especially in developing countries. It ranges from political capture of universities to favouritism in admissions, diversion of funds, academic dishonesty and sextortion. Higher education regulatory frameworks should promote accountability and anti-corruption measures as part of accreditation and assessment standards. Donors can use their assistance to bolster anti-corruption compliance in the universities they partner with, strengthen accreditation agencies, and support information technology solutions. Here in this paper we are focusing on the problem of corruption in university result system which occurs due to normal database, centralized authority , etc. So our proposed system will contain the database which will be updated in the encrypted format, database will be stored at multiple servers and for login user have to go through visual cryptography. Using all this techniques it will make sure that there will not be any corruption in the university result system.*

Keywords- Data security, University results, AES, Visual cryptography, Java, Web, JSP, etc.

I. INTRODUCTION

In October of 2017, universities around the world participated in the second annual "international day of action against contract cheating" sponsored by the "International Center for Academic Integrity." The event reflected growing concern about an upsurge in educational fraud, which threatens to devalue higher education and undermine academic integrity, as well as harm students and institutional reputations alike. Fraud and corruption in education exist in various forms beyond contract-cheating. Its global manifestations include diploma mills and the counterfeiting of academic documents, as well as bribery to ensure the licensing of academic institutions, the hiring of academic staff, the passing of examinations, admission into education programs and the award of degrees. The problem is an urgent one. From an institutional perspective, the ramifications of failure to address fraud and corrupt practices are sometimes severe. The most prominent example may be the University of Wales, which was abolished in 2011 because it ran degree validation programs with dubious or downright illegal overseas partner institutions. Dickinson State University in North Dakota was placed on notice by its accreditor, the Higher Learning Commission after it came out that the university had been graduating international students from to-up programs with Chinese and Russian partner institutions without authenticated documents or appropriate academic prerequisites. Reputational damage is another risk of insufficient controls for vetting students' qualifications. Western Kentucky University, for instance, was in 2016 forced to suspend almost half of its international graduate students recruited by an India-based agent – an episode documented by the New York Times. After admission offers were made, it turned out that the students did not meet admission standards and were academically unfit, despite remedial assistance. The institution accrued both real and opportunity costs, and loss of tuition revenues, and risked a deterioration of educational quality. Just as devastating was the impact on the students who were in danger of losing their visas and investments into education abroad. For private companies and the government, the employment of individuals with bogus credentials can be a public relations fiasco. And yet, accounts of persons being employed in critical positions based on fake degrees surface regularly in the news, be it at the U.S. Department of Homeland Security or the National Nuclear Security Administration. So it is very important to make a educational system to be transparent.

II. RELATED WORK

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 multiple parties have verified it. 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 [1].

The achievement degree evaluation of each course is generated in the teaching space, and the automated collection of relevant data such as the ability that students obtained can get from the automated evaluation software. After completing, the data collection of the course fulfillment evaluation, for each student who does not need to be repaired again, based on the quantitative and qualitative combination of grades, process and evidence to make out each learning outcome achievement value of the curriculum standardization support. Then, the achievement value together with the course name, learning outcome name (graduation requirement indicator), the weight of the course and other information will be shaped as a record. And it will be uploaded into a block (note that only qualified records can be packed into the block). Finally, the Meckler tree, hash function, digital signature, timestamp and other technologies will be used to add the record to the blockchain [2].

This paper discusses how Bitcoin uses blockchain. Bitcoin is the first digital currency to see widespread adoption. While payments are conducted between pseudonyms, Bit coin cannot offer strong privacy guarantees: payment transactions are recorded in a public decentralized ledger, from which much information can be deduced. Zero coin (Miers et al., IEEE S&P 2013) tackles some of these privacy issues by unlinking transactions from the payment's origin. Yet, it still reveals payments' destinations and amounts, and is limited in functionality. In this paper, we construct a full-fledged ledger-based digital currency with strong privacy guarantees. Our results leverage recent advances in zero-knowledge Succinct Non-interactive Arguments of Knowledge (zk-SNARKs). First, we formulate and construct decentralized anonymous payment schemes (DAP schemes). A DAP scheme enables users to directly pay each other privately: the corresponding transaction hides the payment's origin, destination, and transferred amount. We provide formal definitions and proofs of the construction's security. Second, we build Zero cash, a practical instantiation of our DAP scheme construction. In Zero cash, transactions are less than 1 KB and take under 6 ms to verify - orders of magnitude more efficient than the less-anonymous Zero coin and competitive with plain Bitcoin[3].

Blockchain is a transaction database which contains information about all the transactions ever executed in the past and works on Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on network to edit the ledger in a secured way which is shared over distributed network of the computers. For making any changes to the existing block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with Block chain history. If majority of the nodes agree in favor of the transaction, then it is approved and a new block gets added to the existing chain. The Blockchain metadata is stored in Googles Level DB by Bitcoin Core client. We can visualize Blockchain as vertical stack having blocks kept on top of each other and the bottommost block acting as foundation of the stack. The individual blocks are linked to each other and refers to previous block in the chain. The individual blocks are identified by a hash which is generated using secure hash algorithm (SHA-256) cryptographic hash algorithm on the header of the block. A block will have one parent but can have multiple child each referring to the same parent block hence contains same hash in the previous block hash field. Every block contains hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called as Genesis block.[4]

Currently, blockchain-based IoT is a hot topic. Previous works have mainly focused on four aspects: authentication (or access control), smart applications, data storage (or the integrity of transferred data) and cloud computing (or edge computing). To the best of our knowledge, previous papers did not include two aspects: (i) They did not realize that servers may perform homomorphic computations on encrypted data without decrypting the data. Moreover, in previous papers, data transferred to servers are typically unencrypted or servers (or computing nodes) can decrypt the transferred data. This leads to a risk of releasing sensitive information since the servers may learn the details of the received data. (ii) They also did not realize that external computing resources can conveniently join in the block chain based IoT system to improve the system performance. In greater detail, servers should perform some authentication from authorities before joining the system.[5]

In order to solve the problem of counterfeiting certificates, the digital certificate system based on blockchain technology would be proposed. By the unmodifiable property of blockchain, the digital certificate with anti-counterfeit and verifiability could be 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 in query 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 unmodifiable 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.[6]

III. PROPOSED SYSTEM

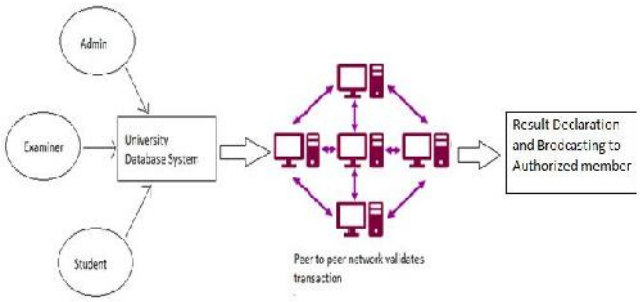

Figure 1 Proposed System

System architecture is the design of the whole system architecture. The database system using block chain is made up of peer to peer network. Student is the person who is the user who access the system for viewing his result. Administrator has control of the system. In the modified system, multiple copies of same database are maintained. So whenever admin or student or examiner makes changes or add any information, it gets reflected into all the databases. These databases are located in different places. So if someone tries to hack into database, it is easily detected, as changes should be made in all the databases for it to be a valid change instead of just one. The data is stored in encrypted form in databases so even if database gets hacked it can't be read. Visual cryptography technique is used to authenticate examiner to ensure that only authorized examiners can login into system.

IV. ALGORITHM

AES:

AES is used to encrypt the database. The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data, the data to be encrypted. This array we call the state array.

Steps:

- Derive the set of round keys from the cipher key.
- Initialize the state array with the block data (plaintext).
- Add the initial round key to the starting state array.
- Perform nine rounds of state manipulation.
- Perform the tenth and final round of state manipulation
- Copy the final state array out as the encrypted data (cipher text).

V. EXPERIMENTAL RESULTS

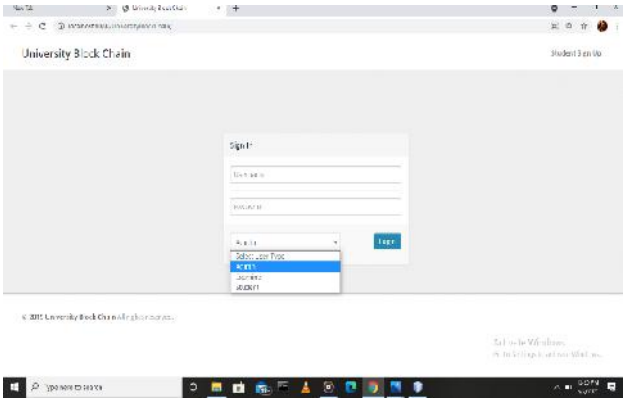

Figure 2 Login Page

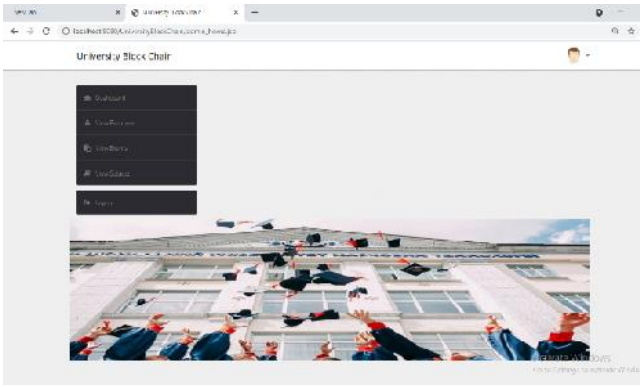

Figure 3 Admin home dashboard

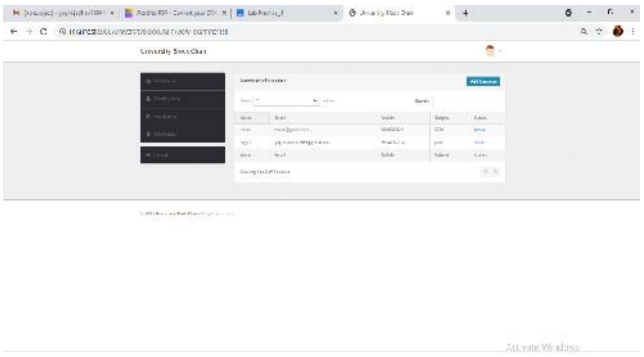

Figure 4 View Examiner

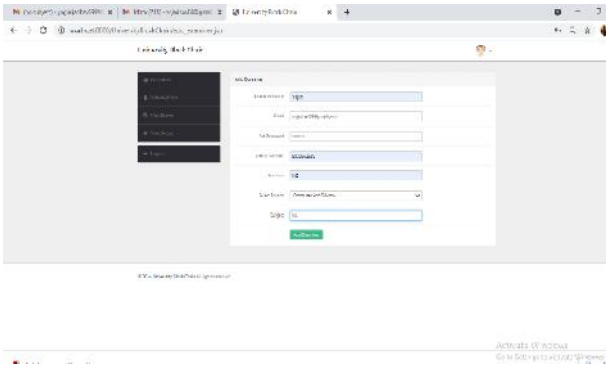

Figure 5 Add Examiner

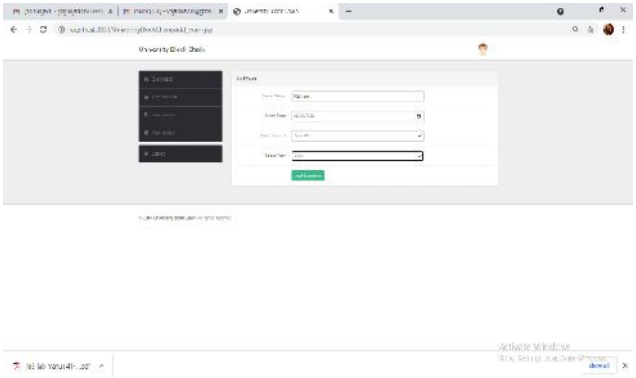

Figure 6 Add Exam

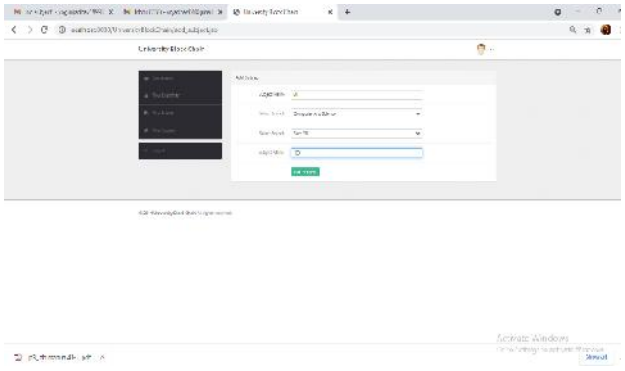

Figure 7Add Subject

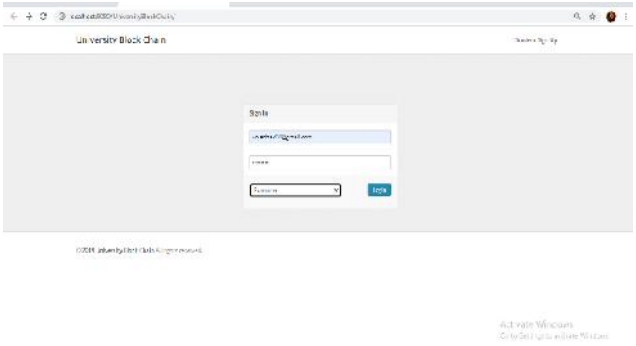

Figure 8 Examiner Login

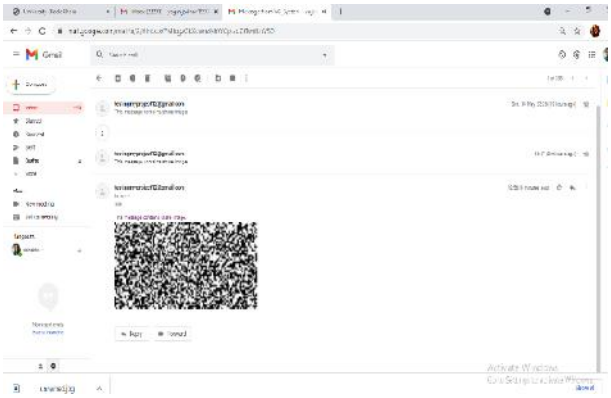

Figure 9 Share 1 image to from Visual Cryptography to examiner mail

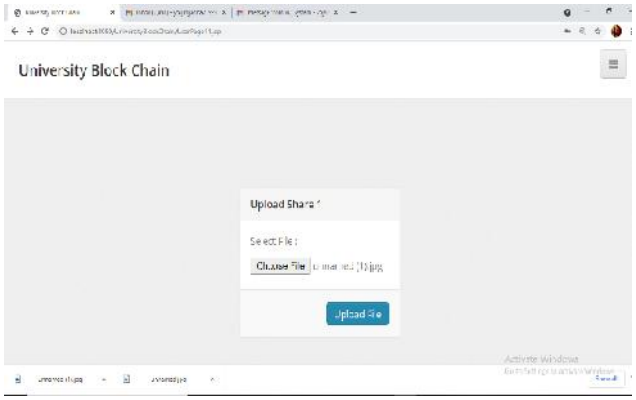

Figure 10 Examiner to upload share1 image

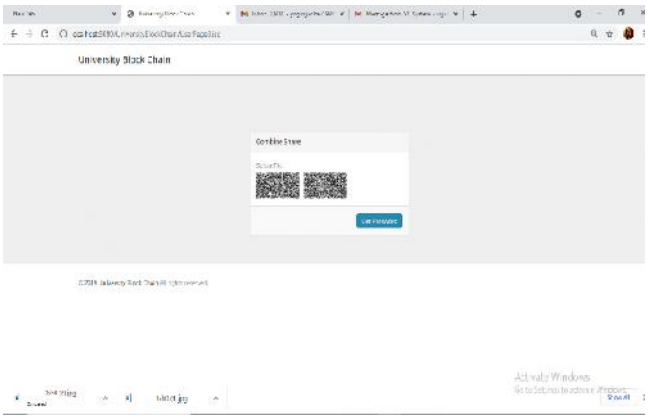

Figure 11 Combine share1 and share2 to go password

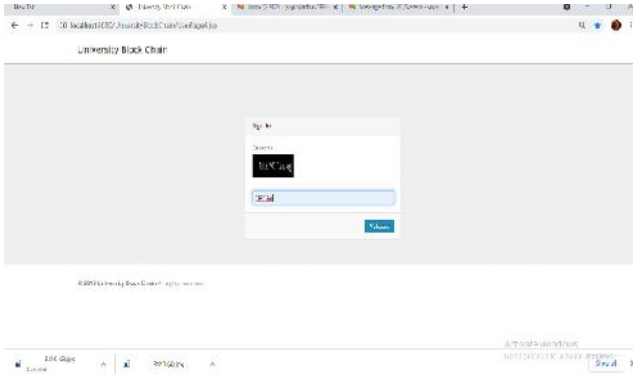

Figure 12Captcha password to examiner validation

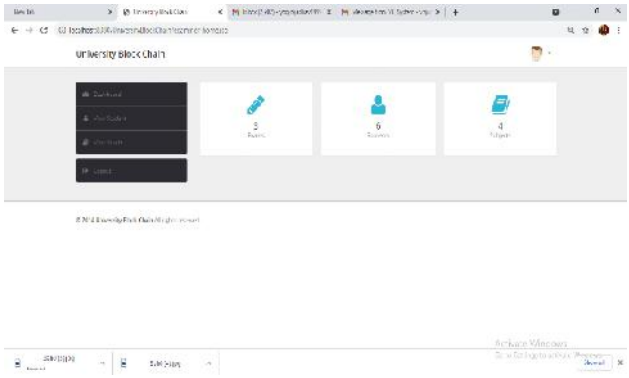

Figure 13Examiner home page after successful login and validation

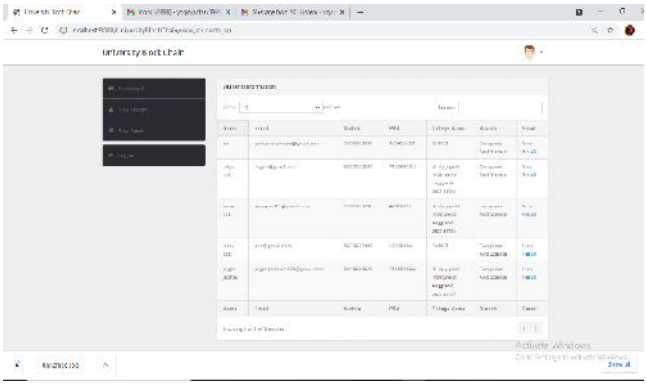

Figure 14 View Student

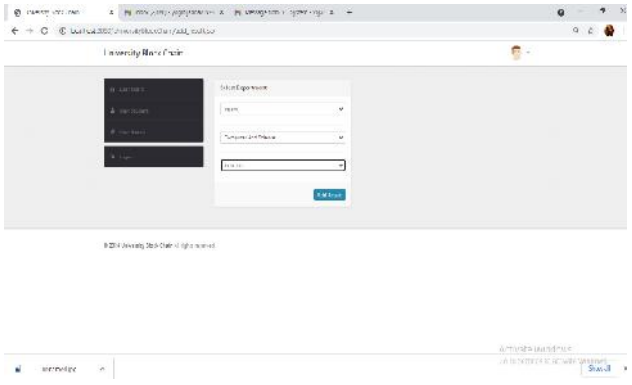

Figure 15 Add new result page

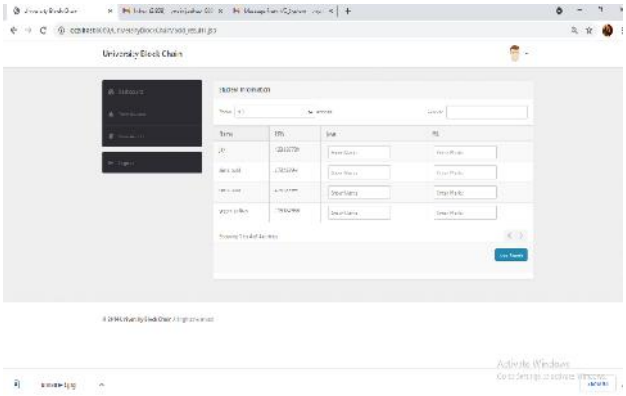

Figure 16 Add result for student

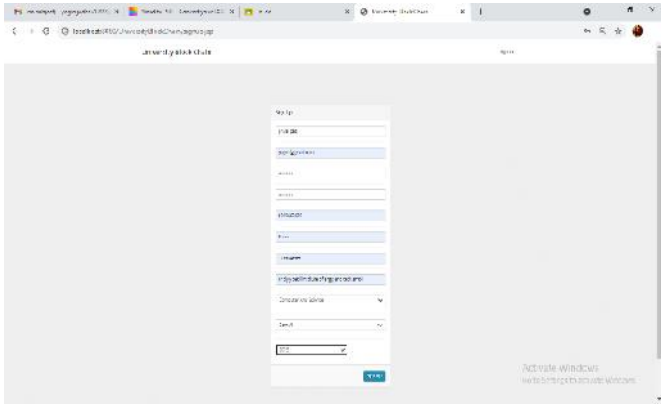

Figure 17 Student Registration page

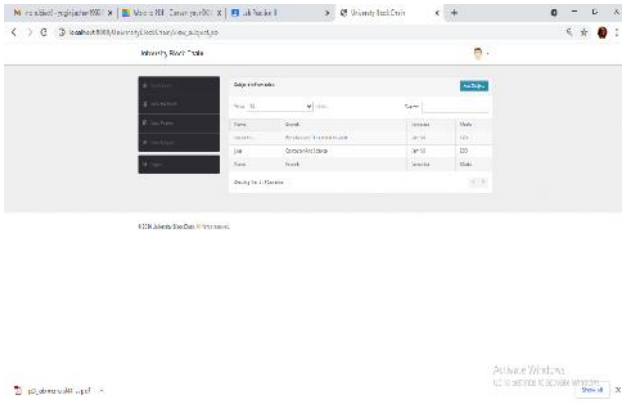

Figure 18 Student view subject

VI. CONCLUSION AND FUTURE WORK

This project aims to implement system for secure and transparent management of results by introducing block chain features. The outlined of the result system has been developed by designing, analyzing & testing the architecture, which helps to overcome the limitation of previous work. We are going to implement a visual cryptography for login of examiner so that there will not be any unauthorized login, the AES will assure data security as it will be in the encrypted

format. Using cryptographic techniques the system will be secure, efficient and transparent.

VII. ACKNOWLEDGEMENT

Our project usually falls short of its expectation unless aided and guided by the right persons at the right time. We avail this opportunity to express our deep sense of gratitude towards all the encouragements and support. At this level of understanding it is difficult to understand the wide spectrum of knowledge without proper guidance andadvice.

Hence, we take this opportunity to express our sincere gratitude to our respected Project guide **Prof. Sagar Dhanake** who as guide evolved an interest in us to work and select an entirely new idea for project work. They have been keenly co- operative and helpful to us in sorting out all thedifficulties.

We are also thankful to our subject teachers for their well wishes and inspiration, for their continuous advice and support without which it would have been impossible. Lastly, we would like to express our deep appreciation to our classmates and our indebt ness to our parents for providing moral support and trustingus.

REFERENCES

[1] Yi Liu and Qi Wang An Database management based on Blockchain International Conference on Applied System Innovation 2018.

[2] Bin Duan,Ying Zhong, IEEE Member, Dayu Liu:- Institute of Electrics, Chinese Academy of Sciences Beijing, China Education application of blockchain technology: learning outcome and meta-diploma IEEE 23rd International Conference on Parallel and Distributed SystemsICPADS.2017.001142017.

[3] Eli Ben Sasson ; Alessandro Chiesa ; Christina Garman ; Matthew Green ; Ian Miers ; Eran Tromer ; Madars Virza,Zerocash: Decentralized Anonymous Payments from Bitcoin IEEE Symposium on Security and Privacy,IEEE.SP.2014.362014.

[4] Sachchidanand Singh- IBM Software Lab., Nirmala Singh- Tech Mahindra Blockchain: Future of Financial and Cyber Security 2nd International Conference on Contemporary Computing and Informatics 2016.

[5] LIJING ZHOU , LICHENG WANG , YIRU SUN, AND PIN LV State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing 100876, China Corresponding author: Licheng Wang Bee Keeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation National Key Research and Development Program, ChinaACCESS.2018.2847632, 2018.

[6] Jiin-Chiou Cheng, Narn-Yih Lee2, Chien Chi3, and Yi-Hua Chen4 1,2,3Department of Computer Science and Information Engineering, Southern Taiwan University of Science and Technology, Tainan, Taiwan Blockchain and Smart Contract for Digital Certificate Proceedings of IEEE International Conference on Applied System Innovation IEEE ICASI 2018- Meen, Prior & Lam 2018.