ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

A Survey on Block chain and Smart Contract for Digital Certificate

Rohit Choudhary[1], Mayuresh Kasar[2], Mayur Parma[3]

U.G. Student, Department of Information & Technology, D Y Patil Institute of Engineering, Ambi, Pune, Maharashtra, India[1]

U.G. Student, Department of Information & Technology, D Y Patil Institute of Engineering, Ambi, Pune, Maharashtra, India[2]

Assistant Professor, Department of Information & Technology, D Y Patil Institute of Engineering, Ambi, Pune, Maharashtra, India[3]

ABSTRACT:According to the Taiwan Ministry of Education statistics, about one million graduates each year, some of them will go to countries, high schools or tertiary institutions to continue to attend, and some will be ready to enter the workplace employment. During the course of study, the students' all kinds of excellent performance certificates, score transcripts, diplomas, etc., will become an important reference for admitting new schools or new works. As schools make various awards or diplomas, only the names of the schools and the students are input. 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 block chain technology would be proposed. By the unmodifiable property of block chain, 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 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 block chain, 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:block chain, hyper ledger, digital certificate, Hashing.

I. INTRODUCTION

Advances in information technology, the wide availability of the Internet, and common usage of mobile devices have changed the lifestyle of human beings. Virtual currency, digital coins originally designed for use online, has begun to be extensively adopted in real life. Because of the convenience of the Internet, various virtual currencies arethriving, including the most popular—Bit coin, Ether, and Ripple the value of which has surged recently. People are beginning to pay attention to block chain, the backbone technology of these revolutionary currencies. Block chain features a decentralized and incorruptible database that has high potential for a diverse range of uses. Block chain 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 ablock chain .Data are distributed among various nodes (the distributed data storage) and are thus decentralized. Consequently, the nodes maintain the database together. Under block chain, a block becomes validated only once it has been verified by

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

multiple parties. Furthermore, the data in blocks cannot be modified arbitrarily. A block chain-based smartcontract, for example, creates a reliable system because it dispels doubts about information's veracity.

II. EXISTING SYSTEM

During the course of study, the students' all kinds of excellent performance certificates, score transcripts, diplomas, etc., will become an important reference for admitting new schools or new works. As schools make various awards or diplomas, only the names of the schools and the students are input. Students should had to bring the hardcopy of certificates every time with themselves which is not so bearable.

Disadvantages of Existing System:

1. The lack of effective anti-forge mechanism, events that cause the graduation certificate to be forged often get noticed.
2. Risk of documents to be get stolen.

III.PROPOSE SYSTEM

To solve the problem of counterfeiting certificates, the digital certificate system based on block chain technology would be proposed. By the unmodifiable property of block chain, the digital certificate with anti-counterfeit and verifiability could be made. Companies or organizations can thus inquire for information on any certificate from the system. In proposed system, simply the document's details get transfer into electronic format& the QR code is get generated. So at the time of admissions or interviews only QR get scanned by the system & all the accolades are visible to that respective person in digital format.

Advantages of Existing System:

1. The system assures information accuracy and security.
2. No risk of documents to be get stolen.
3. Time consuming process.

IV.LITERATURE SURVEY

Project Name: **Predicting student performance: an application of data mining methods with an educational web-based system**
Author: BehrouzMinaei-Bidgoli, Deborah A. Kashy, GerdKortemeyer, William F. Punch

Newly developed Web-based educational technologies offer researchers unique opportunities to study how students learn and what approaches to learning lead to success. Web-based systems routinely collect vast quantities of data on user patterns, and data mining methods can be applied to these databases. This paper presents an approach to classifying students in order to predict their final grade based on features extracted from logged data in an education Web-based system. We design, implement, and evaluate a series of pattern classifiers and compare their performance on an online course dataset. A combination of multiple classifiers leads to a significant improvement in classification performance. Furthermore, by learning an appropriate weighting of the features used via a genetic algorithm (GA), we further improve prediction accuracy. The GA is demonstrated to successfully improve the accuracy of combined classifier performance, about 10 to 12% when comparing to non-GA classifier. This method may be of considerable usefulness in identifying students at risk early, especially in very large classes, and allow the instructor to provide appropriate advising in a timely manner.

Project Name: **Educational Data Mining: A Review of the State of the Art**
Author: Cristobal Romero, Sebastian Ventura.

Educational data mining (EDM) is an emerging interdisciplinary research area that deals with the development of methods to explore data originating in an educational context. EDM uses computational approaches to analyze

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

educational data in order to study educational questions. This paper surveys the most relevant studies carried out in this field to date. First, it introduces EDM and describes the different groups of user, types of educational environments, and the data they provide. It then goes on to list the most typical/common tasks in the educational environment that have been resolved through data-mining techniques, and finally, some of the most promising future lines of research are discussed.

Project Name: **Mining Association Rules Based on Apriori Algorithm and Application**
Author: SHI Lin, BAI Jin-niu

In the data mining research, mining association rules is an important topic. Apriori algorithm submitted by Agrawal and R. Srikant in 1994 is the most effective algorithm. Aimed at two problems of discovering frequent itemsets in a large database and mining association rules from frequent itemsets, the author makes some research on mining frequent itemsets algorithm based on apriori algorithm and mining association rules algorithm based on improved measure system. Mining association rules algorithm based on support, confidence and interestingness is improved, aiming at creating interestingness useless rules and losing useful rules. Useless rules are cancelled, creating more reasonable association rules including negative items. The above method is used to mine association rules to the 2002 student score list of computer specialized field in Inner Mongolia university of science and technology.

Project Name:**Concepts and Techniques**
Author: Jiawei Han, MichelineKamber

Data mining is the task of extracting precious information from masses of raw data. The results of data mining could find many different uses and more and more companies are investing in this technology. Data Mining: Concepts And Techniques (The Morgan Kaufmann Series In Data Management Systems) explains all the fundamental tools and techniques involved in the process and also goes into many advanced techniques.
This book not only introduces the fundamentals of data mining, it also explores new and emerging tools and techniques. It explains basic data mining concepts like OLAP, concept description, data preprocessing, classification and prediction, association rules and cluster analysis. It then presents advanced data mining techniques like extracting information from varied and complex sources other than just relational databases. This includes multimedia databases, object databases, time-series databases and spatial databases. It also looks at harvesting data from varied sources on the world wide web and extracting useful information from it.

Project Name **APRIORI Algorithm**
Author: Anita Wasilewska.

The Apriori algorithm was proposed by Agrawal and Srikant in 1994. Apriori is designed to operate on databases containing transactions (for example, collections of items bought by customers, or details of a website frequentation). Other algorithms are designed for finding association rules in data having no transactions (Winepi and Minepi), or having no timestamps (DNA sequencing). Each transaction is seen as a set of items (an *itemset*). Given a threshold the Apriori algorithm identifies the item sets which are subsets of at least transactions in the database.
Apriori uses a "bottom up" approach, where frequent subsets are extended one item at a time (a step known as *candidate generation*), and groups of candidates are tested against the data. The algorithm terminates when no further successful extensions are found.

V. CONCLUSION

Data security is one of the major features of block chain technology. Block chain is a large and open-access online ledger in which each node saves and verifies the same data. Using the proposed block chain-based system reduces the likelihood of certificate forgery. The process of certificate application and automated certificate granting are open and

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 11, November 2018

transparent in the system. Companies or organizations can thus inquire for information on any certificate from the system. In conclusion, the system assures information accuracy and security.

FUTURE SCOPE:
1) Easy to upload resume on company website.
2) Easy to result upload.
3) Time consuming process for the company as well as student.

REFERENCES

[1] M. Dorigo, V. Maniezzo, A. Colorni, "Ant system:Optimization by a colony of cooperating agents," IEEETransactions on Systems, Man and Cybernetics, vol. 26(1), pp. 29-41, 1996.
[2] M. Dorigo, G.D. Caro, L.M. Gambardella. "Ant algorithms for Discrete Optimization," Artificial Life, vol. 5, pp. 137-172, 1999.
[3] M. Dorigo, L.M. Gambardella, "Ant Colony System: A Cooperative Learning Approach to the Traveling Salesman Problem," IEEE Transactions on Evolutionary Computation, vol. 1 (1), pp. 53-66, 1997.
[4] T. Stützle, H.H. Hoos, "MAX-MIN ant system," Future Generation Computer Systems, vol. 16 (8), pp. 889–914,2000.
[5] S. Fidanova, "ACO Algorithm with Additional Reinforcement," M. Dorigo et al. (Eds.): ANTS 2002, LNCS 2463, pp. 292-293, 2002.
[6] I. Watanabe, S. Matsui, "Improving the Performance of ACO Algorithms by Adaptive Control of Candidate Set," Evolutionary Computation, 2003. CEC '03. The 2003 Congress on 2 (8-12), pp. 1355-1362, 2003.
[7] M.L. Pilat, T. White, "Using Genetic Algorithms to Optimize ACS-TSP," M. Dorigo et al. (Eds.):ANTS 2002, LNCS 2463, pp. 282-287, 2002.
[8] H. Huang, X.W. Yang, Z.F. Hao, R.C. Cai, "A novel ACO algorithm with adaptive parameter," Lecture Notes inBioinformatics, 4115, pp. 12-21 2006.
[9] H. Huang, Z.F. Hao, "An ACO algorithm with bidirectional searching rule," Dynamics of Continuous Discreteand Impulsive Systems-Series B-Applications & Algorithms, 13, pp. 71-75, 2006.
[10] Z.F. Hao, H. Huang, Y. Qin, R.C. Cai, "An ACO Algorithm with Adaptive Volatility Rate of Pheromone Trail," Lecture Notes in Computer Science, 4490, pp. 1167– 1170, 2007.
[11] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou, "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts", Proceedings of IEEE Symposium on Security and Privacy (SP), pp. 839-858, 2016.
[12] M. Sharples, J. Domingue, "The blockchain and kudos: A distributed system for educational record reputation and reward", Proceedings of 11 th European Conference on Technology Enhanced Learning (EC-TEL 2015), pp. 490-496, 2015.