Online Transaction Management Using Blockchain Technology

Sreerag Premanathan [1], Ashwin Rana [2], Vishnu A [3], Anondita Guha [4], Dr. Balika J Chelliah [5]
[1]Undergrad Student, Computer Science Department, SRM institute of science and technology, Ramapuram Campus
[2],[3],[4],[5]Undergrad Student, Computer Science Department, SRM institute of science and technology, Ramapuram Campus

Abstract*-In current age of market digitalization, crypto-currencies, online financial houses & transactions and virtual reality, we have reached a point where it is more important than ever to safeguard our finances and financial instructs in this very intangible world of online marketplace and trading where millions of transaction take place online every second of every day in every corner of the world. Using a Blockchain technology based app or as it is called a D-App (Decentralised Application) for tracking, safeguarding and using it as backbone storage for our transactions does the very same function of safeguarding our finances and financial interests. This Blockchain based online transaction manager promises a new approach, a better and safest way of protecting your transactions via online.*

Keywords- Blockchain, Security, Online, Transaction management, Decentrailised Application

I. INTRODUCTION

The idea of this project came from our brief introduction to field of Blockchain technology and the value that it holds, especially more than anything in the field of virtual/online finance. Once we saw the potential of the technology and the benefits of this new and upcoming storage model we were convinced to apply it in a new app or as such apps are called a D-APP or Decentralised Application to present users with the safest online transaction manager possible. Blockchain technology uses a model of distributed identity management.

Blockchain technology would share a piece of transaction occurring online among a field of users/miners all of whom would note the transactions, arrange them according to highest transaction rates mostly, preparing a list of transactions in process and finally compete with one another to crack a hash code to submit their list and win the reward if the list is without a fault accepted by all sections. Now this same functionality can be placed in private organization structure thanks to efforts made by IBM Hyper ledger and co and Etherum bringing almost same functionality in private sector of things without having to go public.

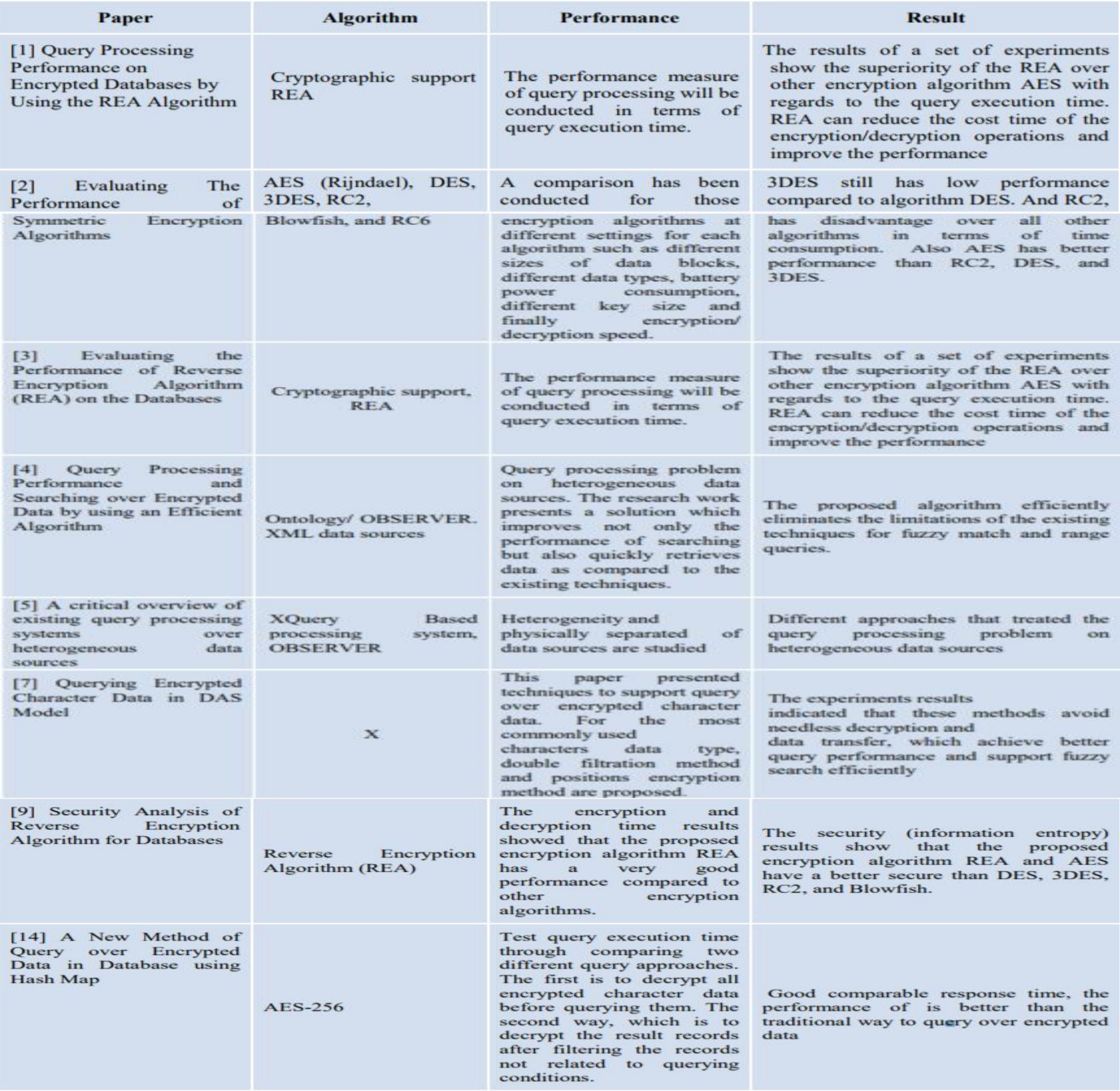
With Blockchain technology we guarantee the users their safety and put them in seat of power and empower them to manage their on identities and safeguard their transactions without even having to know or trust the party at the opposite site of the transactions as their transaction would be forever etched into a block and nothing and no one can corrupt or change it.

In Blockchain data associated with every any event in our case transactions taking place online is always time-stamped and makes note of all the authorized participates and actions taking place. No-one can corrupt the data once it is in a block of the Blockchain, also if anyone tries to tamper while it is still in their air a detailedcopy of transactions going to take place is passed to every one of the participating entity so, none of them or anyone outside could tamper with document because pull it off successfully they have to know about all the participants whose only coded id’s are available and then tamper each one of their copy of the event within the stipulated time period.

Having such extensive, exhaustive safety measure ensures the transactions a data is always safe and even without knowing or having to trust any parties or participants involved there is always a trust and guarantee of safety of data.

II. Literature Survey

Various models till now their used hashing or cryptography to solidify their systemssecurities and ones that used Blockchain technology had the disadvantage of being called out foroperating in murky waters. The below analysis of list of papers on which the survey was doneafter coming up with idea clearly shows this differences and even more highlightens the uniqueness and usefulness of our application.



Paper	Algorithm	Performance	Result
[1] Query Processing Performance on Encrypted Databases by Using the REA Algorithm	Cryptographic support REA	The performance measure of query processing will be conducted in terms of query execution time.	The results of a set of experiments show the superiority of the REA over other encryption algorithm AES with regards to the query execution time. REA can reduce the cost time of the encryption/decryption operations and improve the performance
[2] Evaluating The Performance of Symmetric Encryption Algorithms	AES (Rijndael), DES, 3DES, RC2, Blowfish, and RC6	A comparison has been conducted for those encryption algorithms at different settings for each algorithm such as different sizes of data blocks, different data types, battery power consumption, different key size and finally encryption/ decryption speed.	3DES still has low performance compared to algorithm DES. And RC2, has disadvantage over all other algorithms in terms of time consumption. Also AES has better performance than RC2, DES, and 3DES.
[3] Evaluating the Performance of Reverse Encryption Algorithm (REA) on the Databases	Cryptographic support, REA	The performance measure of query processing will be conducted in terms of query execution time.	The results of a set of experiments show the superiority of the REA over other encryption algorithm AES with regards to the query execution time. REA can reduce the cost time of the encryption/decryption operations and improve the performance
[4] Query Processing Performance and Searching over Encrypted Data by using an Efficient Algorithm	Ontology/ OBSERVER. XML data sources	Query processing problem on heterogeneous data sources. The research work presents a solution which improves not only the performance of searching but also quickly retrieves data as compared to the existing techniques.	The proposed algorithm efficiently eliminates the limitations of the existing techniques for fuzzy match and range queries.
[5] A critical overview of existing query processing systems over heterogeneous data sources	XQuery Based processing system, OBSERVER	Heterogeneity and physically separated of data sources are studied	Different approaches that treated the query processing problem on heterogeneous data sources
[7] Querying Encrypted Character Data in DAS Model	X	This paper presented techniques to support query over encrypted character data. For the most commonly used characters data type, double filtration method and positions encryption method are proposed.	The experiments results indicated that these methods avoid needless decryption and data transfer, which achieve better query performance and support fuzzy search efficiently
[9] Security Analysis of Reverse Encryption Algorithm for Databases	Reverse Encryption Algorithm (REA)	The encryption and decryption time results showed that the proposed encryption algorithm REA has a very good performance compared to other encryption algorithms.	The security (information entropy) results show that the proposed encryption algorithm REA and AES have a better secure than DES, 3DES, RC2, and Blowfish.
[14] A New Method of Query over Encrypted Data in Database using Hash Map	AES-256	Test query execution time through comparing two different query approaches. The first is to decrypt all encrypted character data before querying them. The second way, which is to decrypt the result records after filtering the records not related to querying conditions.	Good comparable response time, the performance of is better than the traditional way to query over encrypted data

III. MODULE DISCRIPTION

The safety and convenience of using Blockchain technology has enabled us to implement this into an online transaction management application. Also the amount of control and confidentiality each and every user has on his transactions only adds to this already wonderful system. When we look it from business aspect of this as it provides a greater and far superior security there is no need to shell out extra cash especially for that. The Blockchain technology with the help of IBM Hyper-ledger and co can be implemented in a private scenario so that the organization running the application has some sort of control over matter but not too much that it will hurt general users trust. And, finally since the key of Blockchain is to satisfy each and every individual participant involved it is always aimed at bettering experience and customizing things accordingly. Various modules involved in this application are:

- Collection of User Details
- Verification
- Authentication
- Identity Management
- Blockchain Management

3.1 <u>Collection of User Detail.</u>

The actual details of users are collected, which involves their name, job, financials and all other details that are important for running a legitimate government rule abiding financial organization this is the front end of the stuff or as commonly called in Blockchain industry an off-chain transaction.

3.2 <u>Verification</u>

The details submitted by the users are verified through a background check and made sure are not falsified so as run a trustworthy relationship of the management application with user.

3.3 <u>Authentication</u>

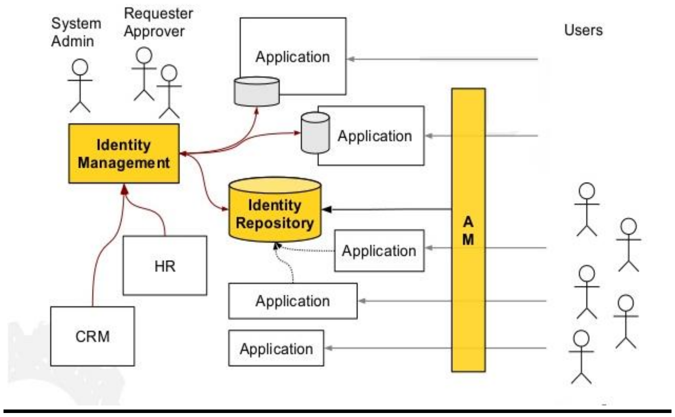
Once the user details are collected and verified they are authenticated and their details are coded into a has file the user is given a hash identity that only they know and code to break that identity with the hash code for identity the hash key is invaluable this key has to be with user all time and he or she should not loose.

3.4 <u>Identity Management</u>

The hashed identity and transactions that it will process are put into a Blockchain every time it does. Also all the personal user data is coded and put into the Blockchain. The management will only posses the hashed identity and name the user in case users forgets it but user needs have a key with him at all time or else he loose access to that particular account.

3.5 <u>Blockchain Management</u>

The private organization would have some member operating in role equivalent to miners while some other public or data signature key authority involvement will also be present so as to level the playing field and making it safe enough so that user can trust the application without trusting anyone. The Blockchain transactions will be monitored and will be broken into blocks accordingly and since it is a private block. It will have more organization power as compared to a public block.



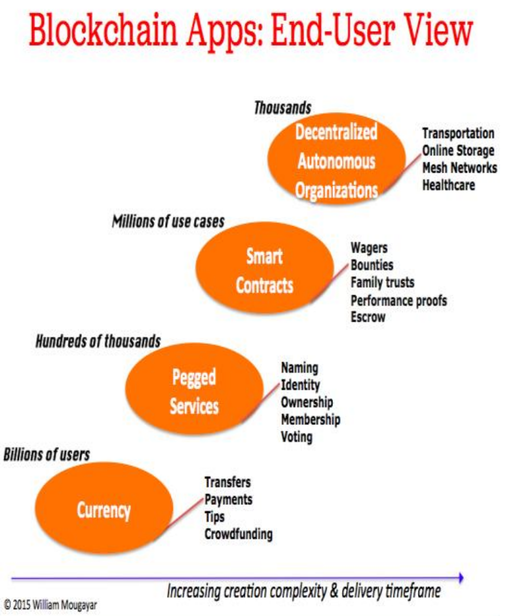


Figure 1 Block Diagram for the applicationFigure 2 End User View

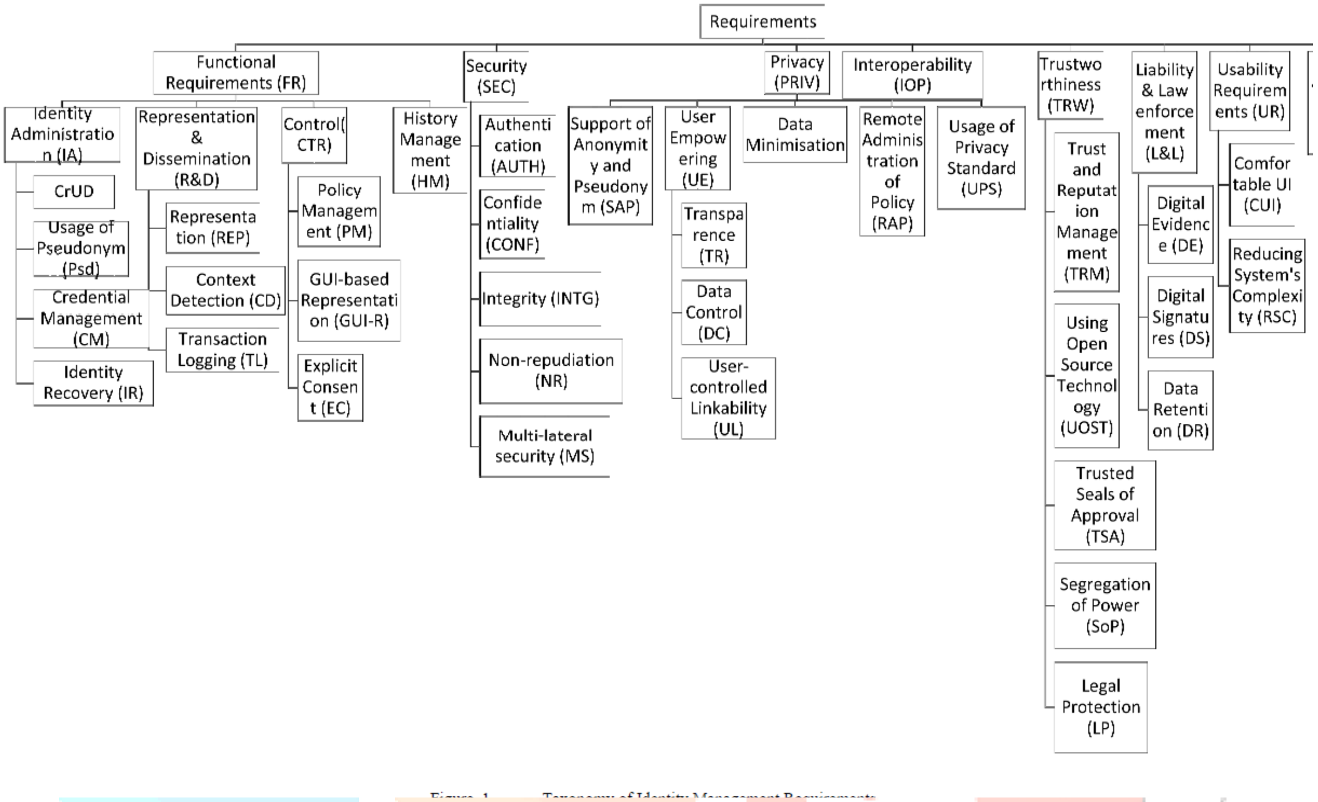

Requirements
Functional Requirements (FR)
Identity Administration (IA)
CrUD
Usage of Pseudonym (Psd)
Credential Management (CM)
Identity Recovery (IR)
Representation & Dissemination (R&D)
Representation (REP)
Context Detection (CD)
Transaction Logging (TL)
Control(CTR)
Policy Management (PM)
GUI-based Representation (GUI-R)
Explicit Consent (EC)
History Management (HM)
Security (SEC)
Authentication (AUTH)
Confidentiality (CONF)
Integrity (INTG)
Non-repudiation (NR)
Multi-lateral security (MS)
Support of Anonymity and Pseudonym (SAP)
Privacy (PRIV)
User Empowering (UE)
Transparence (TR)
Data Control (DC)
User-controlled Linkability (UL)
Data Minimisation
Interoperability (IOP)
Remote Administration of Policy (RAP)
Usage of Privacy Standard (UPS)
Trustworthiness (TRW)
Trust and Reputation Management (TRM)
Using Open Source Technology (UOST)
Trusted Seals of Approval (TSA)
Segregation of Power (SoP)
Legal Protection (LP)
Liability & Law enforcement (L&L)
Digital Evidence (DE)
Digital Signatures (DS)
Data Retention (DR)
Usability Requirements (UR)
Comfortable UI (CUI)
Reducing System's Complexity (RSC)
Figure 1 Taxonomy of Identity Management Requirements

Figure 3 Proposed working model functions

IV.Draw backs and Preventive Measures

The biggest drawback of using a Blockchain technology for online transactions and transaction management is the no. of transactions per second it can handle it is very close to 3.3 to 7 transactions per second which is a very low operating capacity. But by making this application use not just one but multiple private Blockchain and only allowing the registered users use the Blockchain higher efficiency from user side of this could be obtained with a slight trade off in terms of operating costs which could be made up form user annual subscription. Also only other area truly that could be considered a kick back or draw-back is over reliance on the key but having the user make changes of his transactions as it happens reflect upon the connected bank account would help solving the issue in case users loses an account key. He can apply for a new account without having to worry about his previous transaction. The security of the overall system is guaranteed by just implementing Blockchain system into whole functionality of this application. Also it provides a great deal in customer satisfaction and help individual users maintain separate identities and unknown identities while transacting that allows them to operate in trusting environment without necessarily having to trust anyone. Also since managed by private organisation using private Blockchain gives them enough space for additional creativity for customer satisfaction. Plus, it avoids the major concerns that other Blockchain transaction management has been facing, Of national interest and avoidance of taxes that such system is liable to, by reflecting all transaction changes into the users bank with a statement.

V. Conclusion and Future Scope

Thus we can provide all new and great application that is much needed in this era of market digitalization and online transactions. And, all this is achieved at no cost to user’s comfort ability. We can with use of application assure both the safety of user and his transactions also making it operate within the legitimate lines so that it does operate in any dark waters. Future scope of this application would be to come up with a digital identity management application that follows same model but has different functionality than the online transaction management. It will focus on consolidating all the access credentials to all the social media sites that the user is a part of and providing him with a universal identity and key to open all the social media that is secure and safe. It will involve storing all the social media access in a block of Blockchain per user and user has an identity and key to open and access all these.

VI.Acknowledgement

This application is supported by the hyper ledger project, the yo generator. I would like to thank Balika Sir for his kind input and insight to our project.

VII. References

- IBM Hyperledger Project
- Blockchain
- A comparative analysis of identity management systems-Md.Sadek Ferdous, Ron Poet
- Multiple target tracking and identity management with applications to aircraft tracking-Inseok Hwang,Hamsa Balakrishna, Kaushik Roy, Claire Tomlin