

SECURE BANKING SYSTEM USING BLOCK CHAIN TECHNOLOGY

S.M. Suneetha¹, R. Swarnamuki², G. Varalakshmi³, K. Sangeethakalyaniraman⁴

^{1,2,3}Student, Dept. of Computer Science Engineering, Panimalar Engineering College, Tamilnadu, India

⁴Asst. Professor, Dept. of Computer Science Engineering, Panimalar Engineering College, Tamilnadu, India

Abstract - Block chains are appropriated records that empower parties who don't completely confide in one another to keep up a lot of worldwide states. As the technology landscape is increasing quickly, it's each vital and difficult to own a firm grasp of what the core technologies got to supply, especially with respect to their data processing capabilities. We first survey the state of the art, focusing on private block chains (in which parties are authenticated). We dissect both underway and inquire about frameworks in four measurements: appropriated record, cryptography, consensus protocol, and smart contract. We then present BLOCKBENCH, a benchmarking framework for understanding the performance of private block chains against data processing workloads. We conduct a comprehensive evaluation of three major block chain systems based on BLOCKBENCH, namely Ethereum, Parity, and Hyper ledger Fabric. The results demonstrate many trade-offs within the style house, as well as big performance gaps between block chain and database systems. Drawing from style principles of information systems, we tend to discuss many analysis directions for delivery Block chain performance nearer to the realm of databases to alleviate such hazard, we propose another hybrid block chain development plot that utilizes the blend of verification of-work and the stake, which is the quantity of coins delivered.

Key Words: Block chain, hash values, MD5, Transaction, Security.

1. INTRODUCTION

By securing cash related information over an arrangement of PCs, the errand of exchanging off data ends up being considerably increasingly troublesome for software engineers. As opposed to rupturing just a single server, distorting or making a beguiling trade on a block chain must be practiced if the vast majority of the framework is exchanged off. Hacking a single server can be to an incredible degree troublesome, despite for the most master cybercriminals. Having the ability to deal enough servers to corrupt records on the block chain is in every practical sense unimaginable, especially as developers would need to break each centre point at the same time. Keen Contracts Since block chains can store any kind of automated information, including PC code that can be executed once something like two social events enters their keys; block chains enable us to have smart contracts. This code could be adjusted to make contracts or execute cash related trades once a particular course of action of criteria has been cultivated—the movement of things could hail a receipt to be paid for example. The Block chain is an encoded, appropriated data

base that records information, or as such, it is an advanced record of any exchanges, contracts - that should be autonomously recorded. Block chain has just begun disturbing the monetary administrations part, and it is this innovation which supports the advanced cash bit coin exchange. With Block chain innovation in money related area, the members can associate straightforwardly and can make exchanges over the web without the impedance of an outsider. Such exchanges through Block chain won't share any close to home data with respect to the members and it makes an exchange record by scrambling the recognizing data. The most energizing component of Block chain is that it significantly diminishes the potential outcomes of an information rupture. Interestingly with the conventional procedures, in Block chain, there are differently shared duplicates of similar information base which makes it trying to wage an information break assault or digital assault.

2. RELATED WORKS

In spite of the fact that the Internet is an extraordinary device to help each circle of the cutting edge advanced life, it is still exceptionally defective regarding the absence of security and protection, particularly with regards to Fin Tech and Internet business. Block chain, the innovation behind crypto-money, delivered another upheaval by giving a system to Peer-to-Peer (P2P) exchanges without the requirement for any go-between body, for example, the current business banks [1]. In this way, by applying Block chain or comparable cryptographic money methods, the clients neither need to confide in one another nor do they need an intermediate; rather the trust is showed inside the decentralized system framework itself. Block chain along these lines gives off an impression of being the perfect "Trust Machine" [2] worldview. Truth be told, Bit coin is only a model utilization of the Block chain. The block chain is viewed as novel unrest in the space of registering to empower boundless applications, for example, putting away and checking authoritative reports including deeds and different declarations, human services information, IOT, Cloud, etc.

Tap Scott [3] properly demonstrated Block chain to be the "Overall Ledger", empowering some new applications past checking exchanges, for example, in keen deeds, decentralized as well as self-sufficient associations/taxpayer supported organizations and so forth.

The prime case of SMS OTP is the portable Transaction Authorization Number (versatile TAN or m TAN) that is

utilized to approve exchanges for online bank and portable bank administrations [4]. U shield is another verification strategy for TAN for e-saving money exchanges [5]. Biometrics innovation, (for example, unique finger impression, iris, and voice acknowledgment) has quickened at a colossal pace for the verification and recognizable proof of e-managing an account framework [6] [7] [8].

As the propelled token would go about as a validation of realness, the chance to design securities ends up being significantly harder than while overseeing paper chronicles. That would give securities trading another dimension of certain accept that has not been open as of not long ago. Instalments Security e-keeping money neglect to protect the honesty of their exchanges [9] [10]. Endeavours toward the portable application in Fin Tech [11] begin a scene; show assailants could take

The clients' cash as a result of a wide assortment of somewhat serious security issues [12].

It's critical for the banks to assemble a compelling danger checking and the board framework for e-managing an account. The utilization of metaphysics makes the standard based master framework increasingly effective for suspicious exchanges discovery of e-managing an account [13] [14]. Bolster vector machine was acquainted with a battle against Master card extortion, illegal tax avoidance and home loan misrepresentation [15] [16]. GANs [17] was exhibited to manage the issue of class unevenness in the utilization of directed arrangement to the location of charge card misrepresentation [18]. Enormous information and a parallel figuring procedure were acquainted with recognizing budgetary extortion [19] [20] [21].

At the point when a false exchange occurs, clients would associate the security with the e-managing an accounting framework after they lose the cash. In any case, banks would scrutinize the personality of the client, which is a diversion among lance and shield. Re-looks for the extortion hazard checking is primarily centred around the personality and security of e-managing an accounting terminal on the client side. While score rule master framework and information-driven model machine learning framework centre on the bank side. The scoring rule depends on mastery, which is helpless against new examples of cheats. The information-driven model depends on machine learning classifiers, and as a rule, needs to deal with the lop-sidedness issue [18] and manage a major volume of information.

To address this issue, we propose an extortion chance observing framework for e-managing account exchanges. The framework is made out of two sections, the web-based scoring subsystem dependent on skill and disconnected machine learning subsystem dependent on enormous information. The online subsystem will create the RAIB (Risk of Activity, Identity, and Behaviour of exchange) score of the exchange and give a hazard level. In the disconnected

subsystem, the huge information system for machine learning is acquainted with handle historical exchanges. Parallel arbitrary woods calculation is proposed for the learning of fake exchanges, which have been shown to be especially viable in misrepresentation discovery [22].

3. PROPOSED SYSTEM

The proposed system in banking sector uses the block chaining technique to improve security and to combine multiple existing data storage platforms into one. The details such as transactions that are made among users, withdrawal of money are stored in every block which is then encrypted. Block contains data, hash values, and hash values of previous blocks which are linked to each other. This prevents hacking of data in banks where hackers find it difficult to change hash values of all the blocks that are linked. The blocks are created using doubly Linked List. A linked list is a data structure consisting group of nodes which together represent the sequence. MD5 (message digest) algorithm is used because it's a perfect solution for security, so it does not support block break.

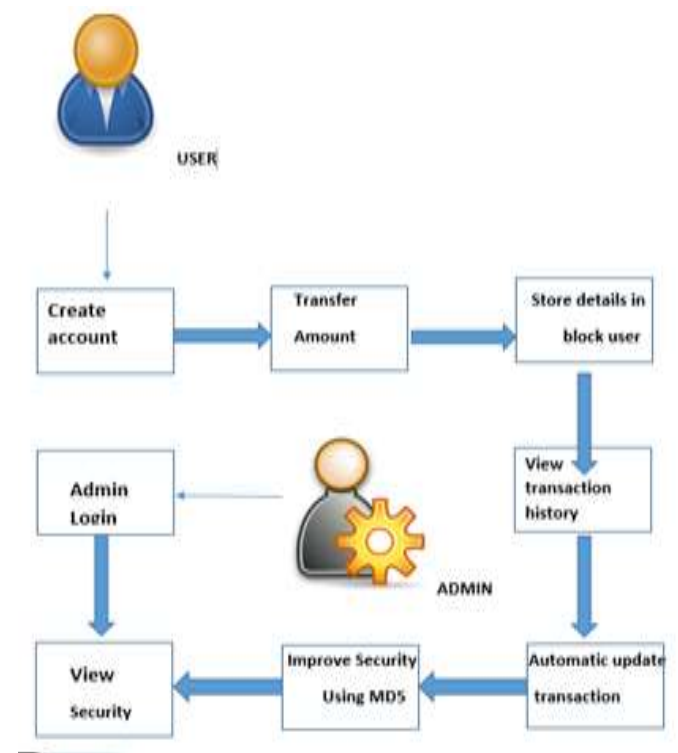


Figure 1. System Architecture

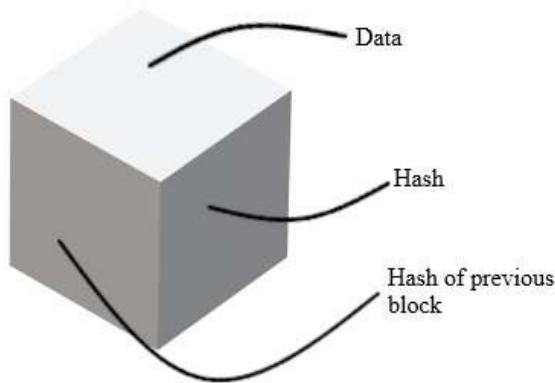


Figure 2. Single Block

3.1. SYSTEM MODULES:

A. BLOCK CHAIN:

The block chain is an ethical advanced record of monetary exchanges that can be modified to record money related exchanges as well as essentially everything of esteem. Information hung on a block chain exists as a common — and persistently accommodated — database. The block chain database isn't put away in any single area, which means the records it keeps are really open and effectively evident. No incorporated form of this data exists for a programmer to degenerate. Facilitated by a great many PCs all the while, its information is open to anybody on the web.

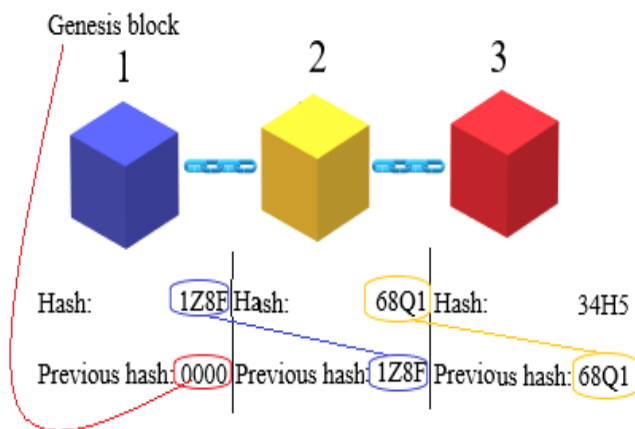


Figure 3. Connection of Block chain

B. IDENTITY MANAGEMENT:

Identity management (ID management) is a wide authoritative region that bargains with distinguishing people in a framework and controlling their entrance to assets inside that framework. Such data incorporates data that validates the identity of a client, and data that depicts data and activities they are approved to get to and additionally perform. It additionally incorporates the administration of clear data about the client and how and by whom that data can be gotten to and adjusted

C. BANK MANAGEMENT:

This programming will perform and satisfy every one of the undertakings that any client would want. The motto is to build up a product program for dealing with the whole bank process identified with client accounts, worker accounts and to keep each track about their property and their different exchange forms productively. Hereby, our primary target is the consumer loyalty's thinking about the present quicker world. In the ongoing years, PCs are incorporated into practically all sort of maintains and sources of income everybody goes over in the daily practice. The accessibility of the product's for pretty much every procedure or each framework has taken the world in its best apparatus and affixes the everyday life. So, we have attempted our best to build up the product program for the Bank Management System where every one of the undertakings to deal with the bank framework is performed effectively and proficiently. It deals with every one of the exchanges like new record passage, store just as pull back section, and exchange of cash for different procedures, advance passage, overseeing charges money or check, and so on.

D. CRYPTOGRAPHY:

Using MD5 algorithm for password security. The MD5 Message-Digest Algorithm is a generally utilized cryptographic hash work that creates a 128-bit (16-byte) hash value. Although MD5 is a broadly spread hashing calculation, is a long way from being secure, MD5 produces genuinely feeble hashes.

E. TRANSPARENCY:

The implication of transparency is that the majority of an association's activities ought to be sufficiently trustworthy to tolerate open investigation. Progressively, the nature of internet-based life and different interchanges implies that even activities proposed to be mystery might be brought into the general population's mindfulness, regardless of an association's earnest attempts to keep them covered up. In general, transparency is the nature of being effectively observed. The significance of transparency is somewhat extraordinary in a software engineering setting, coming nearer to importance imperceptible or imperceptible. Optional importance alludes to finish consistency, as, in a straightforward PC framework or program, the yield is completely unsurprising from knowing the information.

4. EXPERIMENTAL RESULTS

The system that block chain offers alludes to finish correspondence of fundamental data among all members inside the framework. All exchanges and going with subtleties discover their place inside the record accounts, accessible for all gatherings included. Every exchange is irreversible, implying that treating with information is unimaginable. The exchange framework offers a stage where all assets can be assessed by a solitary unit of estimation,

autonomous everything being equal. Coins that would turn out because of block chain innovation can be a commendable substitute of a few fiats without a moment's delay.

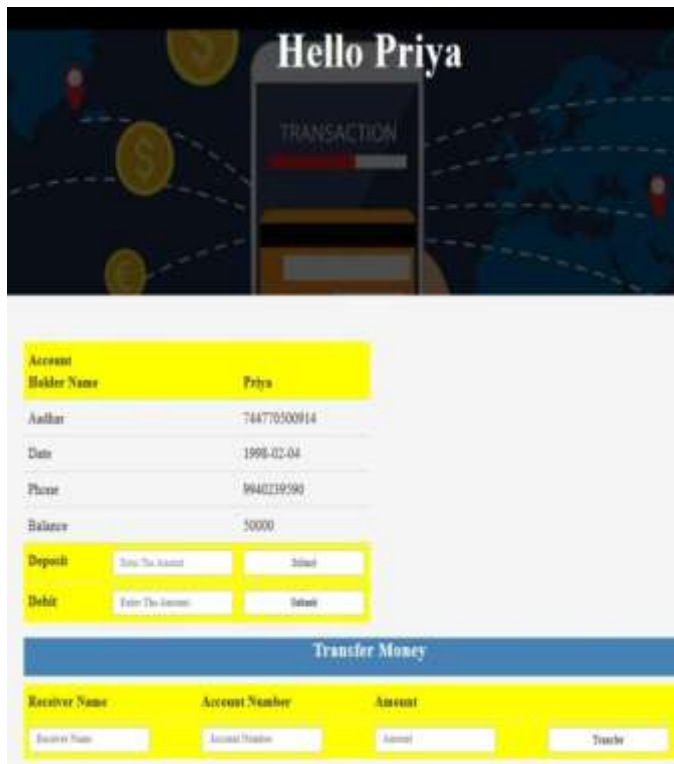


Figure 4. Block user details



Figure 5. Hashed Transaction view for third parties



Account Holder Name	Details	Status
John	Used	<input type="button" value="Delete"/>
Mary	Deleted	<input type="button" value="Delete"/>
July	Used	<input type="button" value="Delete"/>

Figure 6. Admin page

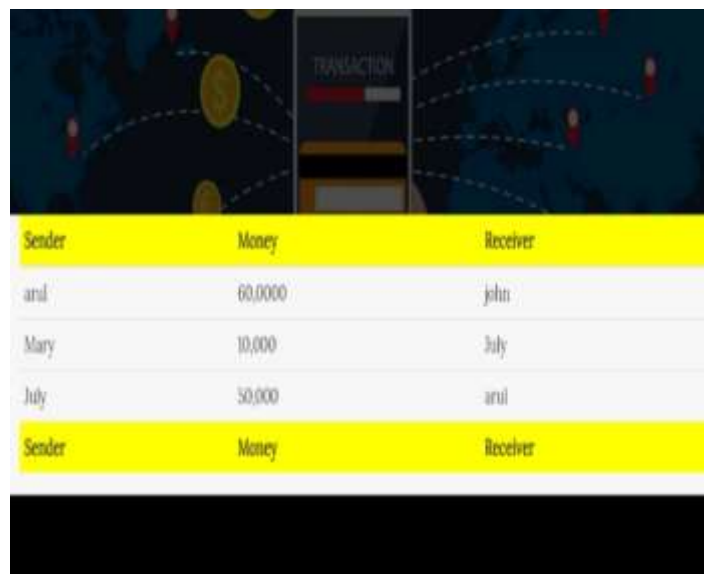


Figure 7. Block users transaction page

5. CONCLUSION

Block chain Technology is a standout amongst the most predictable advances when it requires monitoring money related properties. Block chain innovation has pulled in numerous organizations that need to include the particular highlights of it to their security structures. Numerous investigations have been done for computerized monetary forms and block chain innovation, which speaks to that both of these advances will be proceeding to upset the world.

Subsequent to perceiving the advantages of Block chain Technology, a few money-related establishments have begun spending extensively in this specific field. Block chain can likewise help in shortening the stream of dark cash and managing the broad cash cleaning in the economy in light of the fact that each location utilized for exchanges is put away perpetually on the databases, making every one of the exchanges provable and dependable. The legislature is watching Block chain as an approach to investigate a scope of alternatives which may apply a fitter control on the country's economy.

REFERENCES

- [1] Nir Kshetri "Can Block chain Strengthen the Internet of Things?," IT Professional, vol. 19, no. 4, pp. 68 - 72, May 2017,
- [2] Dr.Mahdi H. Miraz, "Block chain: Technology Fundamentals of the Trust Machine," Machine Lawyering, Chinese University of Hong Kong, 23rd December 2017.
- [3] Don Tap Scott and Alex Tap Scott, Block chain Revolution: How the Technology behind Bit coin Is Changing Money, Business, and the World, 1st Ed. New York, USA: Penguin Publishing Group, 2016 Mulliner C., Borgaonkar R., Stewin P., Seifert J.P. SMS-Based One- Time Passwords: Attacks and Defense. In: Proceedings of the Conference on Detection of Intrusions and Malware & Vulnerability Assessment (DIMVA), 2013.
- [4] Xu H.Y. China's Internet Financial Risks and Countermeasures. Inter- national Conference on Financial Management, Education and Social Science (FMES 2017), 2017.
- [5] Akinyede R.O., Esese O.A. Development of a Secure Mobile E-Banking System. International Journal of Computer (IJC), Vol 26, No 1, 2017.
- [6] Gatali I.F., Lee K.Y., et.al a qualitative study on adoption of biometrics technologies: Canadian banking industry. In: Proceedings of the 18th Annual International Conference on Electronic Commerce: e-Commerce in Smart connected World, 2016.
- [7] Tray nor P., McDaniel P., La Porta T. Security for Telecommunications Networks. Springer, 2008.
- [8] Reaves B., Scaife N., Bates A., et.al Mo (bile) money, Mo (bile) problems: analysis of branchless banking applications in the developing world. In: Proceedings of the 24th USENIX Security Symposium (USENIX Security 2015), USENIX Association, 2015.
- [9] Hauptert V., Müller T. On App-based Matrix Code Authentication in Online Banking. Technical Report Freidrich-Alexander-Universität Erlangen Nurnberg, 2016.
- [10] Schueffel P. Taming the Beast: A Scientific Definition of Fintech. Journal of Innovation Management, 4(4) 32-54, 2017.
- [11] Hauptert V., Maier D., Müller T. Paying the Price for Disruption: How a FinTech Allowed Account Takeover. In: Proceedings of the 1st Reversing and Offensive-oriented Trends Symposium, 2017.
- [12] Rajput Q., Khan N. S., Larik A., Haider S. Ontology Based Expert- System for Suspicious Transactions Detection, Canadian Center of Science and Education, Computer and Information Science; Vol. 7, No. 1, 2014.
- [13] Leonard, K. J. Detecting Credit Card Fraud Using Expert Systems. Computers and Industrial Engineering 25(1-4), 103-1, 1993.
- [14] Quah J. T. S., Sriganesh M. Real-time credit card fraud detection using computational intelligence, Expert Systems with Applications 35 (4), 1721-1732, 2008.
- [15] Abdel Hamid D., Soltani K., Ouassaf an Automatic Bank Fraud De-tecton Using Support Vector Machines. The International Conference on Computing Technology and Information Management (ICCTIM). Society of Digital Information and Wireless Communication, 2014.
- [16] Good fellow I. J., Pouget-Abadie J., Mirza M., Xu B., Warde-Farley D., Ozair S., Courville A. C., Bengio Y. Generative adversarial nets. In Proceedings of NIPS, pages 2672-2680, 2014.
- [17] Fiore U., Santis A. D., Perla F., Zanetti P., Palmieri F.. Using generative adversarial networks for improving classification effectiveness in credit card fraud detection. Information Sciences, in press.
- [18] Alexandre C., Balsa J. A Multi-Agent System Based Approach to Fight Financial Fraud: An Application to Money Laundering. Preprints 2018, 2018010193.
- [19] Melo-Acosta G. E., Dui tama-Muñoz F., Arias-Londoño J. D Fraud Detection in Big Data using Supervised and Semi-supervised Learning Techniques. IEEE Colombian Conference on Communications and Com- putting (COLCOM), 2017
- [20] Hormozi H., Hormozi E. Credit Cards Fraud Detection by Negative Selection Algorithm on Hadoop. In Proceedings of the 5th Conference on

Information and Knowledge Technology (IKT), pp. 40-43, 2013

- [21] Bhattacharyya S., Jha S., Tharakunnel K., Westland J. C. Data mining for credit card fraud: A comparative study, *Decision Support Systems*, 50 (3), 602–613, 2011.
- [22] Bahnsen A. C., Aouada D., Ottersten Example-dependent cost- sensitive decision trees, *Expert Systems with Applications*, 42 (19), 6609– 6619, 2015.