JES Journal of Engineering Sciences

Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

ELIMINATING LAUNDERING OF VIRTUAL CURRENCY USING BLOCKCHAIN FROM ONLINE TRANSACTIONS

[1]Mohammed Taha Moin, [2] Dr. Md Ateeq Ur Rahman

[1]*PG Scholar, M.Tech, Dept of CSE, Shadan College of Engineering and Technology HYD, T.S, INDIA*

mohammedtahamoin@gmail.com

[2]*Professor, Dept of CSE, Shadan College of Engineering and Technology HYD, T.S, INDIA*

mail_to_ateeq@yahoo.com

***Abstract*—** Virtual currency is termed as digital cash, virtual cash or any item recognized by private issuers which represents value and can be used for trade or exchange. Virtual currency in E-commerce and social networks has been a vital element in accomplishing various financial activities like paid games, money exchange and internet shopping. E-commerce and social network platforms facilities the utilization of virtual currency and real cash to introduce different financial capabilities and provides a platform for giveaways, promotional quizzes and events where users can participate to get rewarded by virtual currency. Users typically purchase virtual currency by means of real cash. This fact prompts attacker to adopt various illegal and unethical way of acquiring virtual currency with no or very low cost. Then they launder the acquired currency with different techniques for enormous profit. Various businesses are concerned about these attacks which make business activities effective and results in financial losses. It has become significantly important to terminate laundering of virtual currency. So we propose two system designs based on Blockchain transaction model with distributed ledger based KYC solution and centralized based KYC solution. These designs are capable enough to achieve anti-money laundering ecosystem in E-commerce and Social Networks

***Keywords*—** Blockchain, Electronic Commerce, KYC, Social Networks, Virtual Currency

1. INTRODUCTION

E-commerce and social networks have introduced virtual currency to ramp-up financial activities. Virtual currency are used to effectively conduct financial activities in unified way across different platform such as paid online games, internet shopping and paid online e-books. Few of the virtual currencies used in E-commerce and social network are Flipkart Coins, Aliexpress Coins, Amazon Coins and Tencent Q Coins. E-commerce and social network companies provide virtual currency as reward to customer or customer can purchase virtual currency. These companies make products available at special discounts if purchased with virtual currency. This business strategy helps companies to retain loyalty of customers as virtual currency owned by customer can be specifically used only on the issuer's platform. Users typically purchase virtual currency by means of real cash. But users can also acquire virtual currency by participating in various promotional events hosted by these platforms. Promotional events such as quizzes, fantasy games or giveaways in turn users get rewarded with virtual currency. Virtual currency owned by users can also be transferred to any other user by means of various methods like recharging their account or sending gifts [1]. This fact prompts attacker to adopt various illegal, fraudulent and unethical way of acquiring virtual currency with no or very low cost. Then they launder the acquired virtual currency with different techniques for enormous profit. The techniques they use are illegally accessing someone's account (hacking accounts) or they create large number of dummy accounts to participate in various promotional events to receive rewards. They can also use these dummy accounts which are under their control for transferring acquired virtual currency into other accounts. Fig 1 shows process of virtual currency laundering. These attackers do this to earn real money by releasing virtual currency at very low rates which are much lower than rate of return. Attackers usually post advertisements in popular E-commerce and social media

websites [2] to establish a market for selling virtual currency illegally. We can call these attackers as Money launderers which are responsible for massive financial losses to the organization as well as to victim users. They have also diminished the effectiveness of business activities carried out on these platforms and interfered in currency exchange regulation.

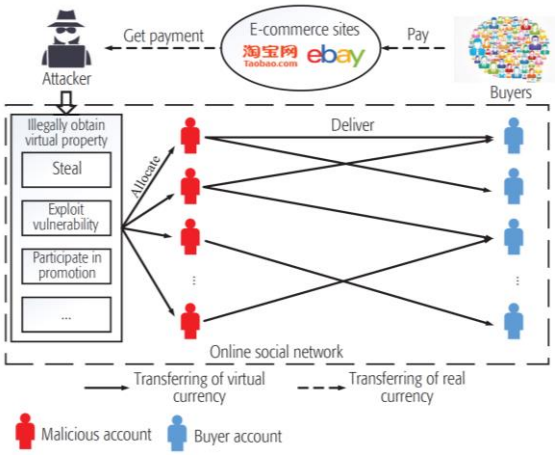

Fig 1. Process of Virtual currency laundering

Virtual currencies can be categorized into three main categories. They are closed-flow virtual currency, open-flow virtual currency and hybrid-flow virtual currency shown in Fig 2. Open-flow virtual currency can be cross exchange with real currency and vice versa, with this currency we can purchase real products as well as we can use virtual services offered by companies. Hybrid-flow virtual currency can be used to purchase real products as well as we can use virtual services offered by companies. Hybrid-flow virtual currency can be used to purchase virtual currency using real currency but once it is purchased we can't convert it back to real currency. Closed-flowed virtual currency can only be used for virtual services offered by companies and this doesn't allow using virtual currency for real products or for cross exchange with real money.

The consequences of money laundering of virtual currency have lead many big organizations to take strict actions on usage of virtual currency and also to restrict virtual currency from open-flow virtual currency to closed- flow virtual currency. Companies like Apple Inc. has mentioned policies in App Store Review Guidelines states Apps may not use in-app purchase to purchase credit or currency for use in conjunction with real money gaming of any kind, and may not enable people to purchase lottery or raffle tickets or initiate fund transfers in the app [3]. Even Amazon doesn't allow users to transfer amazon coins to other accounts neither users can redeem amazon coins for real cash. But amazon allows sending amazon coins as gift and many other E-commerce and social networks allow transferring and sending virtual currency to another account or as a gift. So this fact lets money launders to post advertisement to get in contact with buyers and get real cash via bank to bank transfer and send virtual currency to buyers using multiple accounts.

Terminating money laundering from the E-commerce and social network has become a necessary concern. However, there are new problems faced by these platforms to eliminate money laundering. To eliminate money laundering account they have to recognize attackers account and suspend those accounts. In the process of money laundering the attackers doesn't require any traditional attacking technique such as phishing, spam e-mail, sending URL's containing malware or any executable file. Even though some attacker may use spamming for advertisement but the technique or accounts used for spamming are not related to money laundering neither could help in recognizing attacker's accounts. Although there are techniques to

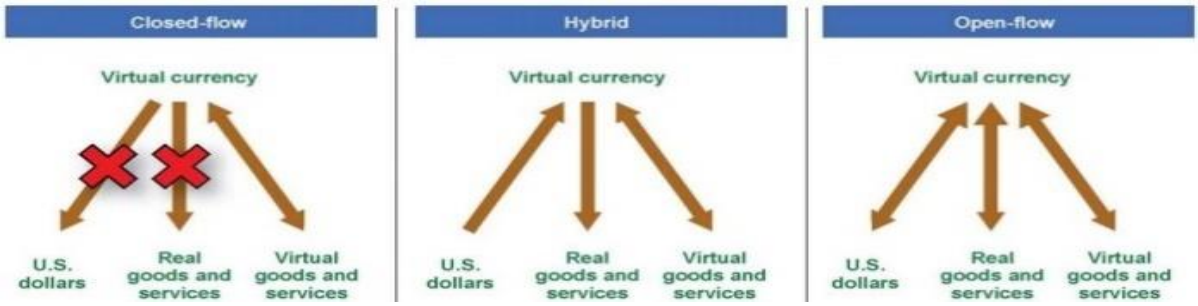

Fig 2. Different Types of virtual currency

recognize malicious accounts which are responsible for money laundering on the network by analyzing the characteristic of accounts on three aspects: account viability, transaction sequences, and spatial correlation among accounts [4] But this method is not capable to recognize some unusual behavioral pattern of accounts. These problems make existing techniques unsuccessful to terminate money laundering from E-commerce and social network.

Contributions: The contribution of this paper is to present a novel system to terminate money laundering from E-commerce and social network. So we have designed two system model based on Blockchain transaction model with distributed ledger based KYC solution and centralized based KYC solution. We used Blockchain to record transaction in a private ledger to store clean and tamper-less transaction information. We use Distributed ledger based KYC solution for the purpose of authentication of user's identity and could also provide KYC service to other organizations to reduce the overall cost incurred in KYC process. We have used Centralized based KYC solution to verify user's identity as user's identity authentication process is carried out by Government agency on which organization can have utmost trust. This design will help companies to link all different account belonging to single user by using KYC ID and record all transactions with transaction details, KYC ID and time stamp. It will also help to stop transferring of virtual currency from compromised account as for transferring virtual currency we need private key of the user. Other contribution of these designs is they can provide access to well-structured and clean data on which data analytics can be performed for effective decision making. We believe that these system designs can achieve anti-money laundering ecosystem in E-commerce and social networks.

2. RELATED WORKS

Detecting money laundering activities in traditional financial transactions has attracted significant research efforts [5]. In Brazil to detect money laundering in exports industries Paula et al. [6] used the Auto-Encoder. To expose money laundering from bank account transactions and billing Dreewski et al. [7] has proposed a system. Olszewski et al [8] have designed a detection technique to encounter frauds in credit card and telecommunication. To prevent money laundering and to identify group of criminals Colladon et al. [9] has proposed an analysis method.

E-commerce and social network have made a huge impact on internet and business world. Thus there was also increase in spamming and phishing attacks on users through the medium of online social network. So it becomes significantly important to detect attackers on the network. There have been many techniques proposed for detection [10], [11], [12], [13], [14]. Due to the popularity of spamming in social networks these techniques mostly focused on detecting spamming account from which malicious data is send.

Money laundering of virtual currency is different than other traditional spamming activities and spamming detection method are not capable to detect money laundering of virtual currency. In the process of money laundering of virtual currency the attackers doesn't require any traditional attacking technique such as phishing, spam e-mail, sending URL's containing malware or any executable file. Even though some attacker may use spamming for advertisement but the technique or accounts used for spamming are not related to money laundering neither could help in recognizing attacker's accounts.

To detect money laundering of virtual currency in social network Yadong Zhou et al. [4] have proposed a technique to recognize malicious accounts which are responsible for money laundering on the network by analyzing the characteristic of accounts on three aspects: account viability, transaction sequences, and spatial correlation among accounts. But this method is not capable to recognize some unusual behavioral pattern of accounts.

3. EXISTING DRAWBACKS

Money laundering of virtual currency includes banking activities, purchasing activities and account recharging. Methods used to detect spamming and phishing would not work and method of analyzing behavior of account could detect money laundering

accounts. But it fails to detect accounts which pose an unusual behavior. These methods are not capable to track down transactions processed from compromised accounts and get back stolen currency. These problems make existing techniques unsuccessful to terminate money laundering from E-commerce and social network.

4. SYSTEM DESIGN CONCEPTS

4.1 BLOCKCHAIN

Blockchain is a sequence of blocks, which holds a complete list of transaction records like conventional public ledger [15]. Basically, Blockchain can be described as a technique to store transaction/data in the form of blocks. Every block is linked to its previous block. Fig 3 shows an example of a Blockchain.

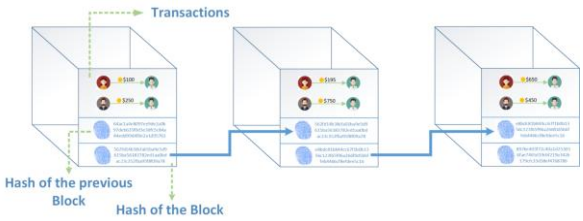

Fig 3. Example of Blockchain

A new block contains hash of its own block, hash of the previous block and data as shown in the Fig 4. Each block in the Blockchain will only have one parent block. The first block in the Blockchain will not have any parent block and it is known as Genesis block. The data section of block usually contains a list of transaction such as Joseph sending ₹ 1000 to Ibrahim would be an example of transaction stored in the block. The block header will contain a hash value and hash of the previous block. A hash is nothing but a mixture of random letters and numbers.

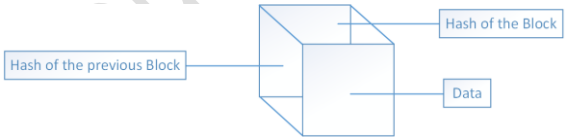

Fig 4. Structure of Block

Every block in the Blockchain will have its unique hash and will also have previous block's hash. Therefore creates a chain of blocks. Even if data of a block is changed by a letter the hash of the block will change and the next block holding the hash of previous block will mismatch. So any changes in Blockchain can easily be found. This attribute makes Blockchain tamper-proof. Blockchain is said to be very secure as Blockchain is stored on all computers connected to peer-to-peer network. A computer which is responsible for maintaining Blockchain on this network is known as node. Whenever a new block is to be added in the Blockchain all nodes/members on the network should check and verify to reach an agreement that all the transactions are valid in the block. If the block stands to be valid then it is added to Blockchain in all computers on the network. This process of adding new block in the Blockchain is called as consensus. If an attacker wants to change the data in the Blockchain then he has to change it on at least 51% of the nodes on the network. These facts make storing data on Blockchain very secure. The software application used on network for Blockchain will generate a public key and private key for the users. A key is similar to hash and it is just like a mixture of random letters and numbers. A public key can be shared to everyone but private key should not be disclosed to anyone. Fig 5 is an Example of private key and public key.

Fig 5. Sample of Private key and Public key

Let's consider an example, Joseph want to send ₹ 1000 to Ibrahim. Now Joseph will create a message and signs it by using his private key to create a digital signature. Then software application that Joseph uses will broadcast the transaction to all nodes on the network. Everyone on the network will verify transaction's signature and check if Joseph is the one who signed that message. They do so by using Joseph's public key. If the network reaches consensus, the transaction will be added to Blockchain. The use of private key, public key and digital signature is known as Cryptography.

4.1.1 Classification of Blockchain Systems

Present Blockchain systems are categorized into three types: Private Blockchain, Consortium Blockchain and Public Blockchain [16].

Public Blockchain: It is a decentralized Blockchain. Every node on the network can see all transaction on Blockchain. All nodes can participate in consensus process. As every

node on the network maintains a copy of Blockchain the attacker has to tamper 51% of nodes on the network. This makes tampering almost impossible on Blockchain. To add a block on public Blockchain the new block is needed to be verified by all nodes on the network as there are many nodes in a network adding new block takes lot of time.

Private Blockchain: It is a centralized Blockchain. Private Blockchain is managed by a single company. There nodes will decide which block is a valid one. There consensus process will be very efficient as their will be only one or few verifiers. When it comes to visibility of Blockchain transaction it depends on their permission. It could be restricted to public and only visible to organization or it could be visible to everyone or it could be that few transactions are visible to public and rest of transactions is restricted. As Blockchain is stored on limited nodes it is possible to tamper the data.

Consortium Blockchain: It is partially decentralized Blockchain. Consortium Blockchain is managed by several companies. Consensus is performed by only few selected nodes. There consensus process will be very efficient as their will be only few verifiers. When it comes to visibility of Blockchain transaction it depends on their permission. It could be restricted to public and only visible to managing organizations or it could be visible to everyone or it could be that few transactions are visible to public and rest of transactions is restricted. As Blockchain is stored on limited nodes it is possible to tamper the data.

4.1.2 Consensus Algorithms

Consensus is a mechanism used in the Blockchain to maintain a real time updated ledger. As in Public Blockchain all nodes will have a copy of ledger. To keep ledgers synchronized in distributed ecosystem there are several different consensus approaches. Few of them are listed below.

Proof of Work: PoW is a consensus strategy used in the Bitcoin network [17]. In PoW node will calculate a hash value for new block. A nonce value is present in the block header the miners keeps on changing the nonce value to generate a different hash value. The calculated value should be lower than or equal to a certain provided value. Once the node generates a target value it sends it to all other node. Then other nodes will check the correctness of new hash value. If it finds to be valid then this block is added to their own copy of Blockchain ledger. The nodes which calculate hash value are known as miners and this process in Bitcoin is called as mining.

Proof of Stack: PoS is more energy efficient when compared to PoW. In PoS miner have to prove that they have more amount of currency. The one who has more stack are unlikely to attack the network and are given the highest chance to create new blocks. In PoS the persons with most stacks will be responsible for maintaining the network.

Delegated Proof of Stake: The difference between DPoS and PoS is that PoS is direct democratic while DPoS is representative democratic [18]. In DPoS stakeholders will choose their delegate who will validate and create new block. As there are less nodes confirmation process is carried out quickly resulting in quick transactions.

Ripple: In ripple consensus there will be server node participating in the consensus. The server will maintain a list of unique nodes it is known as UNL (Unique Node List). When a new block is to be added in the Blockchain the server will query the nodes present in UNL. If these nodes pose agreement of 80% the block is added to Blockchain.

4.2. KYC (KNOW YOUR CUSTOMER)

KYC is abbreviation of Know Your Customer or Know Your Client. KYC is a process in which organizations are authenticating customer's identity. This process is usually done by government bodies or banks for anti-money laundering or for anti-corruption purposes. Presently KYC is also adopted by various companies to ensure customer's illegal intention should not cause potential risk to their business. Nowadays banks have made KYC mandatory. KYC procedure helps banks to know their customer better and all their financial activities. It also helps them to track down or prevent fraudulent transactions. Banks will also keep an eye to make sure if their customers are processing transaction according to the law. These days' online businesses have started adopting KYC for ease of business. But high cost incurred in conducting KYC procedure is one of the challenges faced by organization. To overcome this Jose Parra-Moyano and Omri Ross have proposed Distributed ledger based KYC solution and a centralized based KYC solution [19].

Journal of Engineering Sciences
Vol 10, Issue 9, Sept /2019
ISSN NO:0377-9254

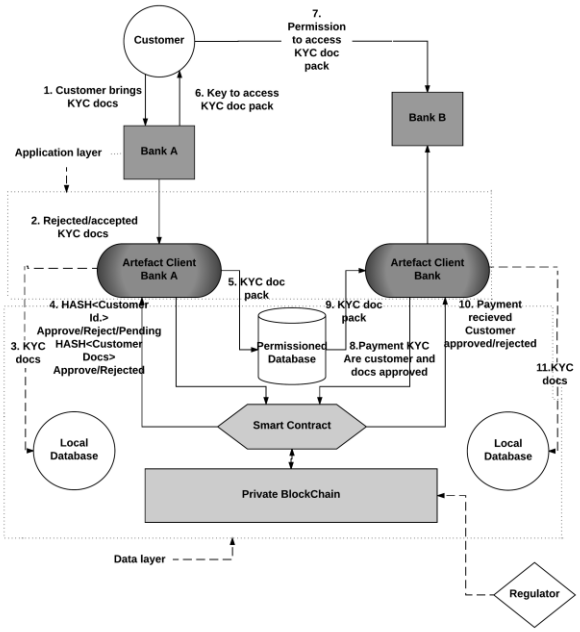

Fig 6. Design of Distributed based ledger KYC system

Fig 6 shows the design of Distributed ledger based KYC solution. In this design customer's home bank will collect all KYC documents and verify it. After validating the documents they will hash it and create a document package. They will digitally sign the document and store it on distributed ledger. Later on customer could also provide the KYC document package access to other bank or business. Other banks or business organization can communicate with smart contract to get the status.

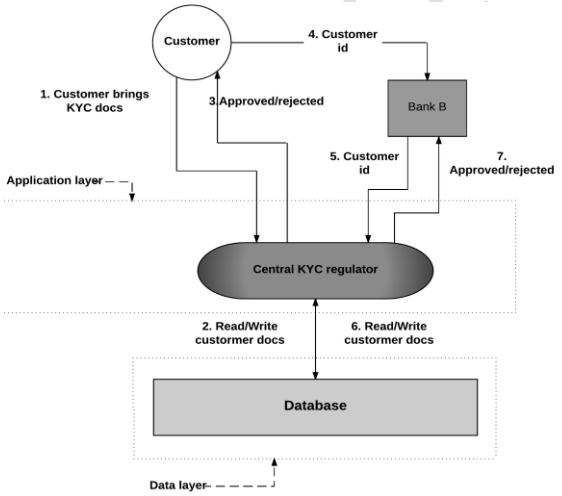

Fig 7. Design of Centralized based KYC System

Fig 7 shows the design of centralized based KYC solution. In this design KYC process is carried out by one central entity. They will take up all KYC responsibilities and will provide KYC status of customer when needed by other institutions. Usually this entity will be government regulated entity which will maintain the privacy and stability of KYC process such as Aadhar authentication system in India.

5. PROPOSED MODELS

Our purpose is to design a system which can help to create an anti-money laundering ecosystem in Ecommerce and social network platforms. So we propose two system designs based on Blockchain transaction model with different KYC solution.

First system design is with Distributed ledger based KYC solution. Second system design is with Centralized based KYC solution. In our system design we have implemented Blockchain technology to record transaction in a private ledger and KYC ID of users is also been recorded along with transaction details. This facilitates an organization to recognize all accounts owned by a single person and they can group transaction processed from different account by a single person. Blockchain technology uses cryptography which helps to stop transactions from compromised accounts as an attacker needs private key of the user to process transaction.

Blockchain based system design with Distributed ledger based KYC solution is shown in Fig 8. In this system model when a new user wants access of virtual currency or other transaction options in his account. He has to get KYC done for his account. He has to provide his identity proof like passport, national card etc., to the organization. After authenticating user's identity organization stores user's KYC details with unique KYC ID in a private ledger which is managed and maintained by the organization. Now user account gets its KYC ID. Whenever user performs any activity like recharging virtual currency from bank, transferring virtual currency or sending gift using virtual currency to another account or purchasing products through virtual currency for every activity user's KYC ID is shared with transaction details to organization's server. In organization's servers a consensus is carried out. If consensus is satisfied transaction is added to private ledger of transactions. This facilitates organization by providing information of all transaction processed by different accounts owned by single person. This design helps organization to create anti-money laundering system where attackers

can't create dummy account to participate in promotional activities for acquiring virtual currency and transfer that virtual currency to buyer's account using these dummy accounts. have to conduct authentication process entirely from start and also benefits the Distributed ledger managing organization for providing such service.

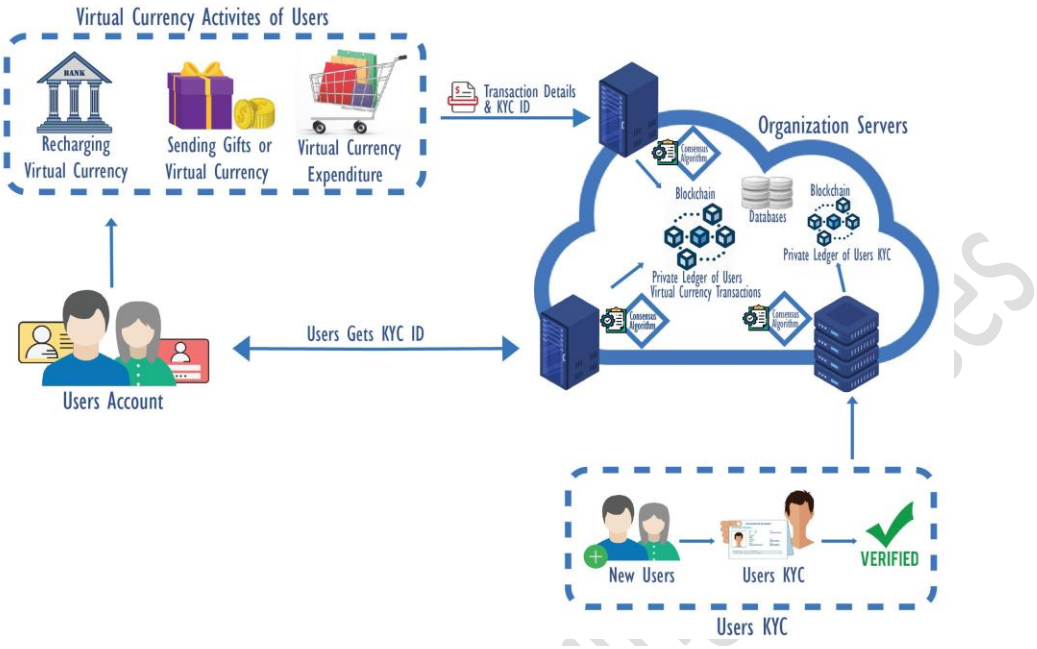

Fig 8. System design based on Blockchain with distributed ledger based KYC solution.

Attackers can't steal virtual currency from compromised account as consensus and cryptography in Blockchain will not let them do so. Additionally organization can make benefits by providing KYC status (verified/rejected) to other organizations by creating a smart contract to which other organization can communicate and pay the service fee to get the status.

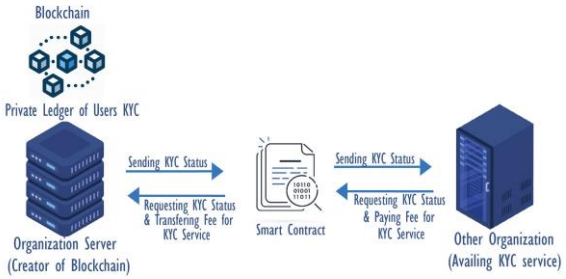

Fig 9. Organization's KYC service to other organization

Fig 9 shows KYC status service provided to other organization. If user wants to work with other organization he can just give his KYC ID to other organization. They will communicate with the smart contract of Distributed ledger managing organization to obtain the status. KYC status service will reduce the verification process time, saves money of other organization as they don't

Blockchain based system design with Centralized based KYC solution is shown in Fig 10. In this system design a new user has to provide e-KYC ID to E-commerce or social network organization. This e-KYC ID can be obtained by getting their KYC done from Government regulated KYC agency. After getting e-KYC ID from user, organization can communicate with Government regulated KYC systems to get KYC status (verified/rejected). Once organization obtains KYC status they can store it in their databases and assigns e-KYC ID with user's account. Now whenever user performs any activity like recharging virtual currency from bank, transferring virtual currency or sending gift using virtual currency to another account or purchasing products through virtual currency for every activity user's KYC ID is actions. This facilitates organization by providing information of all transaction processed by different accounts owned by single person. This design helps organization to create anti-money laundering system where attackers can't create dummy account to participate in promotional activities for acquiring virtual currency and transfer that virtual currency to buyer's account using these dummy accounts. Attackers can't steal virtual currency from

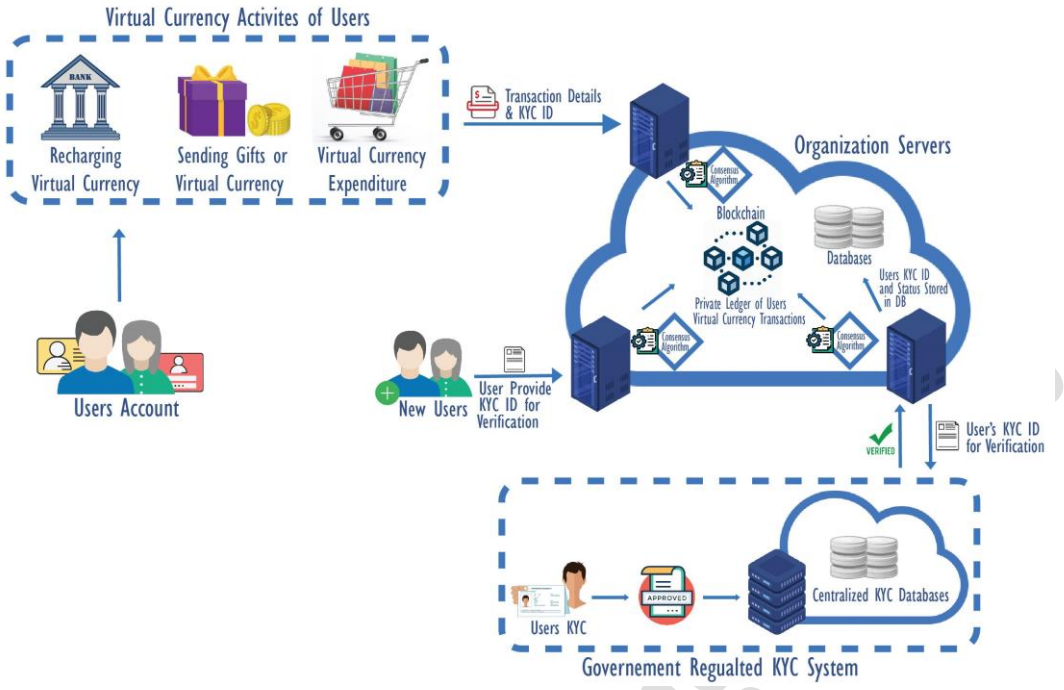

Fig 10. System design based on Blockchain with Centralized based KYC solution.

compromised account as consensus and cryptography in Blockchain will not let them do so. Therefore these system designs provide E-commerce and social network platform an anti-money laundering ecosystem.

6. CONCLUSION

In this article we have presented two system designs based on Blockchain transaction model with two different KYC solutions, they are centralized based KYC solution and Distributed ledger based KYC solution. These designs can terminate money laundering of virtual currency in E-commerce and social network. Blockchain Ledger could provide clean transactions data which can be used for data analytics to make business decision for growth of organization. Huge numbers of researchers are attracted to Blockchain domain as Blockchain is said to be new age internet. Most of the banking sector and other domain are heavily investing on Blockchain. In future E-commerce and social network can run their entire business on block chain. These designs will help them to get started with Blockchain and terminate virtual currency laundering.

REFERENCES

[1] Y. Wang and S. D. Mainwaring, "Human-Currency Interaction: Learning from Virtual Currency use in China," Proc. SIGCHI Conf. Human Factors in Computing Systems, ACM, 2008, pp. 25–28.

[2] Y. Zhou, "*ProGuard*: Detecting Malicious Accounts in Social-Network-Based Online Promotions," in *IEEE Access*, vol. 5, pp. 1990-1999, 2017. doi: 10.1109/ACCESS.2017.2654272

[3] "App Store Review Guidelines - Apple Developer", *Developer.apple.com*, 2019. [Online]. Available: https://developer.apple.com/app-store/review/guidelines/#gaming-gambling-and-lotteries.

[4] Y. Zhou, "Analyzing and Detecting Money-Laundering Accounts in Online Social Networks," in *IEEE Network*, vol. 32, no. 3, pp. 115-121, May 2018. doi: 10.1109/MNET.2017.1700213

[5] Palshikar G.K. "Detecting Frauds and Money Laundering: A Tutorial". In: Srinivasa S., Mehta S. (eds) Big Data Analytics. BDA 2014. Lecture Notes in Computer Science, vol. 8883, chap. 12, pp. 145–160, Springer International Publishing, Cham, 2014. doi: 10.1007/978-3-319-13820-6_12

[6] L. Paula, "Deep Learning Anomaly Detection as Support Fraud Investigation in Brazilian Exports and Anti-Money Laundering," 2016 15th IEEE Int'l. Conf. Machine Learning and Applications (ICMLA), Anaheim, CA, 2016, pp. 954–60.

[7] R. Drezewski, J. Sepielak and W. Filipkowski, "The Application of Social Network Analysis Algorithms in a System Supporting Money Laundering Detection," Information Sciences, vol. 295, pp. 18–32, Feb 2015. doi: 10.1016/j.ins.2014.10.015

[8] D. Olszewski, "Fraud detection using self-

organizing map visualizing the user profiles," Knowledge-Based Systems, vol. 70, pp. 324 – 334, Nov 2014. doi: 10.1016/j.knosys.2014.07.008

[9] A. Fronzetti Colladon and E. Remondi, "Using Social Network Analysis to Prevent Money Laundering," Expert Systems with Applications, vol. 67, pp. 49–58, Jan 2017. doi: 10.1016/j.eswa.2016.09.029

[10] X. Hu, J. Tang, and H. Liu, "Online social spammer detection, "in Proceedings of the Twenty-Eighth AAAI Conference on Artificial Intelligence. AAAI, 2014, pp. 59–65.

[11] "Leveraging knowledge across media for spammer detection in micro blogging," in Proceedings of the 37th international ACM SIGIR conference on Research & development in information retrieval. ACM, 2014, pp. 547–556.

[12] Z. Chu, S. Gianvecchio, H. Wang, and S. Jajodia, "Detecting automation of twitter accounts: Are you a human, bot, or cyborg?" IEEE Transactions on Dependable and Secure Computing, vol. 9, no. 6, pp. 811–824, Nov 2012. doi: 10.1109/TDSC.2012.75

[13] Z. Miller, B. Dickinson, W. Deitrick, W. Hu, and A. H. Wang, "Twitter spammer detection using data stream clustering," Information Sciences, vol. 260, pp. 64–73, Mar 2014. doi: 10.1016/j.ins.2013.11.016

[14] F. Wu, J. Shu, Y. Huang, and Z. Yuan, "Social spammer and spam message co-detection in micro blogging with social context regularization," in Proceedings of the 24th ACM International on Conference on Information and Knowledge Management. ACM, 2015, pp. 1601–1610.

[15] D. Lee Kuo D. Lee Kuo Chuen, Ed., *Handbook of Digital Currency*, 1st ed. Elsevier, 2015. [Online]. Available: http://EconPapers.repec.org/RePEc:eee:monogr:9780128021170

[16] V. Buterin, "On public and private blockchains," 2015. [Online].Available:https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/

[17] Y. Zhang and J. Wen, "An iot electric business model based on the protocol of bitcoin," in Proceedings of 18th International Conference on Intelligence in Next Generation Networks (ICIN), Paris, France, 2015, pp. 184–191.

[18] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," IEEE, pp. 557-564, Honolulu, HI, Jun 2017. doi: 10.1109/BigDataCongress.2017.85

[19] J. Parra Moyano and O. Ross, "KYC Optimization Using Distributed Ledger Technology", *Business & Information Systems Engineering*, vol. 59, no. 6, pp. 411-423, Dec 2017. doi: 10.1007/s12599-017-0504-2

AUTHOR's PROFILE:

MOHAMMED TAHA MOIN received the B.E degree in computer science and engineering from the Osmania University (OU) in May 2017. Currently he is working toward his masters (by dissertation) degree at the Jawaharlal Nehru Technological University of Hyderabad (JNTUH). He is an IEEE student member. His research interest lies in security domain. Specially, he loves to work with Web Technologies, Blockchain and Human computer Interaction.

Dr. MD ATEEQ UR RAHMAN, received the B.E, M.Tech (CSE) and Ph.D.(SIT) degrees from Gulbarga University, Visvesvaraya Technological University and Jawaharlal Nehru Technological University Hyderabad, INDIA respectively in 2000, 2005 and 2014 respectively. He has vast academic and administration experience and has worked under various capacities as Assistant Professor, Associate Professor and Professor in Different Engineering Colleges from 2005 to till date. Presently he is working as Professor and Research Coordinator in Computer Science & Engineering Dept, Shadan College of Engineering & Technology, Affiliated to J.N.T.U.H University, INDIA. His research areas of interest include Spatial Data Mining, Image Processing, Cloud Computing and Computer Networks etc.