International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 4, June 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

KYC using Blockchain

Sreelakshmi V G[1], Meera P M[1], Senna Mariya Pius[1], Mathews Jose[1], Swapna B Sasi[2]

[1]Student, [2]Assistant Professor,
[1,2]Department of CSE, Jyothi Engineering College, Thrissur, Kerala, India

ABSTRACT

Nowadays everyone uses their personal identification documents on a regular basis, which gets shared with third-parties without their explicit consent and stored at an unknown location. Companies such as government institutions, banks, credit agencies and other financial organizations are considered to be the weakest point in the current identity management system as they are unfortified to theft and hacking of data. Although the financial services sector have been seeking solutions for identity problem for a long time, it is only now that a viable solution has arrived in form of blockchain. KYC (Know Your Customer) using Blockchain eliminates the repeated KYC checks that banks currently perform by maintaining a common secure database in a blockchain. The nature of a blockchain ensures that unauthorized changes to the data are automatically invalidated. The proof of reputation concept makes the verification process more robust and secure. Decentralized computing architecture, blockchain will allow for the accumulation of data from multiple authoritative service provider into a single immutable, cryptographically secured and validated database. Blockchain KYC solution take advantages of a secure, public digital ledger to give almost instantaneous and truly secure verification of identity. Due to the immutable and unalterable nature of the record kept in the blockchain, fraud could become a thing of the past.

KEYWORDS: *Blockchain, KYC, Smart contract, Ethereum*

How to cite this paper: Sreelakshmi V G | Meera P M | Senna Mariya Pius | Mathews Jose | Swapna B Sasi "KYC using Blockchain" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-4, June 2020, pp.1600-1603, URL: www.ijtsrd.com/papers/ijtsrd31542.pdf

IJTSRD31542

1. INTRODUCTION

KYC is an abbreviation for "Know Your Customer" and is a significant term utilized by organizations and alludes to the procedure of check of the character of the customers either previously or during the beginning of working with them. The documents is put together by the client to an association so as to make trust between the two gatherings. At first, there was no real way to confirm the personality of the clients therefore KYC was proposed in the United States in 1990. Around then the reason for KYC was to stop fear monger financing and tax evasion through banks. The fundamental partner of KYC is bank. Banks request that their clients fill KYC record with the goal that they can check their personality. Bank crosschecks the data put together by customers to stop tax evasion, psychological oppressor financing, and budgetary fakes. In this way, at present banks don't permit any record holder without KYC documentation. KYC archive contains client data, ID confirmation, address verification, and photo. At first, the pen-paper approach was utilized for submitting KYC archive however the issue with support of records was noticeable. The errands got furious for the bank to check the personality each time through paper filled by the clients. The odds of the record being lost were more in such case. In this way, computerized KYC framework was proposed, which is called e-KYC. In that approach, the client fills the KYC archive through the web utilization of the association. Information submitted were put away in brought together databases. Anytime, the association can get to the client data through client id. This framework was paperless so by and large expense got decreased however since, information is put away in the brought together database along these lines, escape clauses of the incorporated framework like the single purpose of disappointment, information repetition and outsider inclusion in check despite everything exists. Likewise, information put away in the brought together server can be undermined or assaulted by the programmers in this way, odds of the hole of client private information is more in the current unified framework design. The objective of this paper is to propose a new approach to the KYC verification process. This process is very safer and faster than the other systems. Hence there is no need for further verification for other organisations. The system is Ethereum based decentralized solution. Only hash value and username is stored as data on the blockchain. In most of the KYC systems, there is an option to upload documents such as ID proof, passport, address proof, etc. Therefore the system has all the functionalities of a traditional KYC system including image data is stored in the decentralized database.

2. OVERVIEW OF BASICS

2.1. Blockchain

Blockchain is truly only a chain of blocks, however not in the conventional feeling of those words. At the point when we state the words "blocks" and "chain" right now, are really discussing about digital data stored in an open database. This tech network has been discovered for the innovation with the potential purposes. A blockchain is, in the least complex of terms, a period stepped arrangement of immutable records of information that is overseen by a cluster of computers not possessed by a single element.

Every one of these blocks of information is made sure about and bound to each other using cryptographic standards . The blockchain network has no central authority. Since it is a common and immutable record, the data is open for anyone and everyone to see. Hence, anything that is based on the blockchain is by its very nature straightforward and everybody included is responsible for their activities. The blockchain is a straightforward yet cunning method for passing data from A to B in a completely computerized and safe way. One gathering to an exchange starts the procedure by making a blocks. This blocks are checked by thousands, maybe a great many computers disseminated around the net. The verified blocks are added to a chain, which is put away over the net, making a novel record, however a remarkable record with an exceptional history. [1]

2.2. Smart contract

A smart contract is a computer convention expected to carefully encourage, confirm, or authorize the exchange or execution of an agreement. Smart contract permit the exhibition of credible exchanges without outsiders. Probably the best thing about the blockchain is that, since it is a decentralized framework that exists between completely allowed parties, there's no compelling reason to pay mediators (Middlemen) and it spares you time and struggle. Blockchains have their issues, however they are appraised, verifiably, quicker, less expensive, and more secure than customary frameworks, which is the reason banks and governments are going to them. Smart contracts aid you with trading cash, property, offers, shares, or valuable documents in a straightforward, clash freeway while staying away from the administrations of an agent. The best approach to depict smart contracts is to contrast the innovation with a candy machine. Usually, you would go to a legal advisor or a public accountant, pay them, and pause while you get the report. All the more in this way, smart contracts not just characterize the standards and punishments around an understanding similarly that a customary agreement does, yet additionally consequently uphold those commitments.

2.3. Ethereum

Ethereum is as of now the most generally utilized shrewd agreements improvement stage that can be seen as an exchange based state machine: it starts with a beginning states and gradually executes exchanges to transform it into some last states. It is the last states which we acknowledge as the accepted "rendition" in the realm of Ethereum. Not at all like the UTXO model of Bitcoin, Ethereum presents the idea of accounts. There are two types of records: 1) remotely possessed accounts and 2) contract accounts. The thing that matters is that the previous is constrained by private keys without code related with them, while the last is constrained by their agreement code with related code. Clients can just start an exchange through an EOA. The exchange can incorporate paired information (payload) and Ether. On the off chance that the beneficiary of an exchange is the zero-account ∅, a keen contract is made. Or then again if the beneficiary is an agreement account, the record will be actuated and its related code is executed in the nearby EVM (the payload is given as information). The exchange is then communicated to the blockchain arrange where excavators will check it, as appeared in Fig. 2. So as to keep away from issues of system misuse and to evade the unavoidable issues coming from Turing culmination, every programmable calculation (e.g., making contracts, making message calls, using and getting to account stockpiling, what's more, executing tasks in the virtual machine) in Ethereum is liable to expenses a prize for diggers who contribute their processing assets. The unit used to gauge the expenses required for the calculations is called gas.S.[2]

3. CURRENT KYC PROCESS

Financial organizations are binded by regulators to onboard their customers before conducting any activity with them, in order to avoid working with customers that pursue either of the aforementioned illicit activities. The KYC process consists of an exchange of documents between the clients and the financial institution that intend to work together. The process has the collection of basic identity information from all beneficiaries to check for illegitimate activity and politically exposed persons. The process also includes risk management with regard to onboarding new customers, the monitoring of transactions, and specific customer policies for banks. The process is costly for financial institutions and may expose them to large fines if it is not conducted in accordance with the existing regulations.

The KYC process is initiated when a customer intends to work with a financial institution. Consecutively, the customer and the financial institution agree on the terms of a relationship. Then, the customer sends the required documents to the financial institution in order to enable the institution to conduct the KYC verification process. The financial organizations analyzes the documents and generates an further, internal document that serves as the certification that assures regulators that this customer has been either validated or rejected and that the KYC process has been properly conducted. This process is repeated every time the customer intends to work with a new financial institution. In the current setting, every time a customer initiates a relationship with a financial organization the costs of the KYC verification process reoccur. This example case shows how, for this single client, the exchange of documents and the core KYC validation must be take on three times, such that the total costs that are generated by this clients are three times those of a single KYC process. At this point, it is supreme to differentiate between the “core KYC verification process”, which is the minimum KYC verification that all financial institutions are obliged by law to conduct, and additional, bank specific processes. While further documentation can be asked for by each financial organizations to create an “additional aura of information” for every client, our solution focuses merely on the core KYC verification process, which is that shared by all the financial institutions in a jurisdiction. [3]

4. CHALLENGES IN CURRENT PROCESS

Here are some major KYC compliance challenges that banks and financial institutions are facing:

- Data combining: currently, several third-party data providers and external validation agencies offer data and interfaces to extract the required customer information. However, banks struggle to integrate this data to obtain a consolidated view of the customers. This has led to increasing instances of banks' failure to comply with regulatory requirements, resulting in huge penalties and reputational damage.
- High cost: post due diligence, banks need to digitize data in the documents to feed it into the repositories.

This is an expensive exercise, as it uses advanced technology platforms. [4]

- Disintegrated approach: banks do not have a single, unified KYC system for its various lines of business like wealth management, asset management, and brokerage. Maintaining these multiple systems and integrating different interfaces puts banks under immense pressure and adds costs.

5. PROPOSED SYSTEM

Blockchain's immutable ledger that is appropriated more than a large number of gadgets over the world is an ideal supplement to the obscure procedure of KYC that is being utilized everywhere throughout the world at this moment. With the expansion of smart contracts, a ton of the scam detection that depends on people right currently can be computerized. Robotizing these procedures makes them less inclined to mistakes as well as recoveries a ton of overheads in time and cash. For KYC document storage, it bodes well for the banks to build up a common private blockchain, like the one being utilized by Civic. In the wake of onboarding a customer once, a similar data can be utilized later on by different foundations without burning through cash on confirming the records indeed. Like Civic, whenever a foundation solicitation to see the information, the client would get a brief on their own gadget asking to either permit or deny the solicitation. This permits clients to deal with their delicate archives and furthermore makes it simpler for banks to acquire the reports they requirement for consistence. [5]

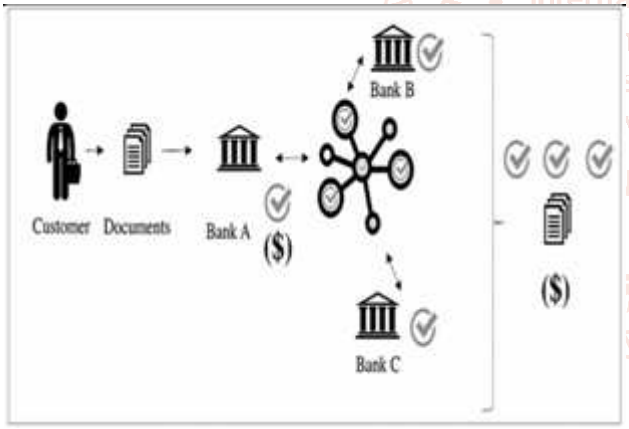

Figure1 KYC using blockchain process

5.1. The Process

At whatever point another client goes into the environment, the 'Trusted Party' that is the bank confirms the reports. When checked for veracity, the bank transfers this information onto the blockchain. At whatever point any new information is should have been annexed, the record could empower encoded updates to the record. These updates can be gotten to by different elements progressively as and when required.

5.2. Advantages

- Unique ID: Each user who enroll on Blockchain identity management system will get a unique identity number. User's unique ID number consists of all personally identifiable information in an encrypted format that is stored on decentralized database. Users can simply share unique ID with any third-party verify themselves directly through the Blockchain Identity Management.
- Consent: A blockchain identity management system will not store any customer information. Moreover, the framework utilizes Smart contracts to empower the controlled information revelation. Consequently, information control is beyond the realm of imagination on the blockchain. Identity management system linked with blockchain is profoundly secure for character holders too. No exchange of client data can happen without the express assent of the client. It makes the client control their actually recognizable data.
- Decentralized: No close to home distinguishing proof reports of the clients will be put away in a centralized server. All the reports that distinguish clients get put away on their gadget sponsored by centralized database, making it safe from mass information ruptures. Utilizing the Blockchain KYC the executives upheld by centralized database doesn't permit any programmer to take the recognizable data. Since the framework will be decentralized, there will be no single purpose of disappointment (SPOF). Single purpose of disappointment speaks to the piece of the framework; in the event that it fizzles, the framework will quit working. Thusly the nonappearance of SPOF guarantees that the framework will never settle.
- **A universal ecosystem:** The blockchain KYC doesn't set to any geographical boundaries. So, users can use the platform across the borders to authenticate their identity.

6. CONCLUSION

Blockchain innovation is an emerging solution for decentralized transactions and data management without the need of a trusted third party. The Proposed system is a proper swap for inheritance KYC system. Also it provides all the necessary features of a legacy KYC system. The decentralized engineering likewise benefits the clients as far as security, ease of use, and trust. Everything from the immutable nature of blockchain to their capacity to help improve transparency in client ID will hugely help improve the procedure and reduce fraud. Government bodies will also benefit as risk officers will have better access to data so the relationship between the financial sectors and regulators will be more transparent. This provides the provision for a massive reduction of financial fraud and crimes in the long term. Effective usage of the Blockchain KYC can improve the degree of security and protection. The immutable and decentralized ledger allows third parties to validate the user's data without wasting time and money.

7. ACKNOWLEDGEMENT

We take this opportunity to express our heartfelt gratitude to all respected personalities who had guided, inspired and helped us in the successful completion of this paper. First and foremost, we express our thanks to The Lord Almighty for guiding us in this endeavour and making it a success. We take immense pleasure in thanking the Management of Jyothi Engineering College and Fr. Dr. Jaison Paul Mulerikkal CMI, Principal, Jyothi Engineering College for having permitted us to carry out this paper. Our sincere thanks to Fr. Dr. A K George, Head of the Department of Computer Science and Engineering for permitting us to make use of the facilities available in the department to carry out the paper successfully.

Last but not least we extend our gratefulness to all teaching and nonteaching staffs who were directly or indirectly involved in the successful completion of this paperwork and to all our friends who have patiently extended all sorts of help for accomplishing this undertaking.

8. References

[1] J.-S. L. Wen-Bin Hsieh, "Design of a time and location based one-time password authentication scheme," in *7th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 4-8 July 2011.

[2] M. S. J. F. R. S. Wazen Shbair, "Blockchain orchestration and experimentation framework: A case study of kyc,", *HAL Blockchain orchestration,* May 2018.

[3] B. K. Shailesh Kumar Shivakumar, "Advanced security design for financial applications,," External Document, 2016.

[4] H. S. Oluwatosin, "Client-Server Model," *IOSR JCE,* vol. 16, no. 2278 8727, February 2016.

[5] A. K. P. Sinha1, "Decentralized KYC System," *I. R. J. of Engineering and T. (IRJET),* 2018.