International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

Blockchain Based User KYC Verification System

Saurabh Yadav[1*], Sambal Singh[1*], Er. Shilpi Khanna[2], Prof. Ajay Kumar Srivastava[3]

[1]*Student, Department of Information Technology and Engineering, Shri Ramswaroop Memorial College of Engineering & Management, Lucknow, India*

2Professor, Department of Information Technology and Engineering, Shri Ramswaroop Memorial College Of Engineering & Management, Lucknow,India

***Abstract*:**

Almost every business is adopting the blockchain technology since it is well-known, dependable, and secure. Transparency, decentralization, immutability, resilience, disintermediation, cooperation, security, and trust are all characteristics of blockchain technology at its core. In this essay, we have concentrated on the potential effects of adopting blockchain to store and track data on the current banking business, particularly the KYC document verification procedure. The KYC procedures used in modern banks are very reliable when done on paper, yet this is an old procedure. A modernized KYC system, integrated with a trustworthy and dependable technology like blockchain, that could survive frauds and address the scalability and security challenges, is absolutely necessary today. The usage of blockchain in the KYC process in the proposed system limits the involvement of middlemen. The client documents are integrated into the bank database with the help of this system, which offers increased efficiency, cost savings, improved customer rendezvous, and end-to-end transparency.

***Keywords*: Blockchain, KYC, Blockchain KYC, Web3 KYC verification system, User identification.**

1. Introduction

With digital currencies, blockchain technology began to gain traction more broadly. The idea of digitalized money was always centralized and governed by layers of security, encryption, firewalls, and anything else that could preserve the anonymity and secret associated with the value of digital money before this disruptive technology came into being. There were inherent problems with this, including managerial overhead, increased ownership costs, compatibility upgrades, additional backups for disaster recovery, and an ongoing risk of data hacking by criminals. This caused sustainability problems and was always accompanied by top managers' and general retail customers' reluctance to adoption. Different intriguing financial strategies also attracted a range of opinions and followers.

In his groundbreaking essay "Bitcoin: A Peer-to-Peer Electronic Cash System," Nakamoto (2008) entirely decentralized the idea of digital currency and overcame the

drawbacks of centralized architecture. By hashing transactions into a continuous chain of hashbased proof-of-work, the network timestamps transactions in this blockchain technology idea, creating a record that cannot be modified without repeating the proof-of-work. In addition to providing evidence of the events actually occurred in the order they were seen; the longest chain also demonstrates that it originated from the largest CPU resource. The nodes that are not working together to attack the network will produce the longest chain and outperform attackers as long as they control the bulk of the CPU power. Many people have recently begun to debate or cast doubt on the blockchain's actual advantages and adoption difficulties. Due to a rapid surge of price stabilization and regulatory tightening across several nations, according to Gartner's hype cycle, blockchain has lost its appeal in the world of cryptocurrencies. Many people have developed a school of thinking that claims investors who want to become extremely wealthy quickly should be disenchanted with blockchain technology. Due to concerns about anti-money laundering (AML) and terrorist financing, initial coin offerings are also operating outside of regulatory oversight.

Is it fair to say that blockchain technology has no future since we have witnessed cycles of cryptocurrency's rise and collapse within the past ten years? Can blockchain technology already be characterised as "just another fad"? Is there no longer a chance to decentralise information? Should we look for another disruptive invention now or wait a little longer? Or, while there are many unanswered concerns regarding the technology, the most important one is whether we require a better management think tank or rather the capacity to produce more proof of ideas for a variety of applications in many industries. The primary theory that the blockchain bubble is likely to collapse has two major flaws, which is why. The most important one is that, before to 2017, there was no other application implemented in real-world use besides cryptocurrency. Only in 2017 did the first beta release, and since that time, the top 100 largest firms have been investing money in it.

While some businesses are still analyzing the use, others have banded together to crowd-fund any creative blockchain implementations. Some applications, including as smart contracts, video games, distributed ledgers in financial institutions, supply chain logistics, decentralized voting, and many more, have generated a lot of enthusiasm. The second drawback is that organizations, management think tanks, technological nerds, or policymakers have not yet relinquished control in order for blockchain technology to become an enhancing technology. As a result of their growing emphasis on cost-cutting and lack of commitment to disruptive innovation, they are forced to accept the status quo and deal with the drawbacks of centralized infrastructure. This essay is broken up into five sections. The first section covers the relevant academic literature on blockchain technology. The second section focuses on the main obstacles that organizations must overcome in order to carry out routine KYC. The final

section examines the situations in which blockchain technology is an appropriate solution. The final observations are made in the fourth section of this essay. The fifth and final section of this essay discusses the key ideas of policy and decision-making by international banking organizations.

2. Literature Review

The suggested system will operate similarly to the current KYC system. In order to build a more safe and complete system, this paper proposes addressing some of the current system's flaws and incorporating cutting-edge features. Customers and corporate institutions will be able to check and record client KYC papers in the DLT using the suggested system. The suggested solution will make use of IPFS, which will greatly improve the efficiency of DLT storage.

By leveraging blockchain technology, the proposed activity enhanced the current KYC system. The removal of third-party involvement is a well-known DLT feature, and smart contracts are used to create our logic for data mobility. Blockchain technology uses a variety of cryptographic security measures to create a more secure environment for transactions over an unsafe channel. By utilizing DLT, cryptography, and the blockchain consensus mechanism, the suggested KYC process can optimize data storing, updating, sharing, and accessing processes while also enhancing security, transparency, and privacy. Additionally, it boosts customer ownership and the customer experience. IPFS is utilized in this suggested KYC document system. through the Blockchain Technology and the Inter Planetary File System (IPFS). With the use of these technologies, we provide a platform for KYC document verification in the financial system that is affordable, quick, private, secure, and transparent. The user cannot upload KYC documents to the Blockchain network since it is expensive.

KYC documents can instead be delivered on the Blockchain Network after being shared using IPFS. The transaction history and hashes of users can be saved to the IPFS network and shared with the Blockchain network as required. The size of the blockchain data will be greatly reduced by this process. We suggest a Blockchain-based fix to the traditional KYC verification process' high cost. The primary distinction is that, regardless of how many institutions a user registers, the entire verification process is only carried out once for each user, boosting transparency by safely communicating the results via DLT. This strategy makes use of Ethereum for proof of concept (POC). Costs are decreased, the customer experience is enhanced, and transparency is increased by this process. In this paper, a novel trust management platform is presented that is self-sovereign and decentralizes the KnowYour-Customer (DKYC) model. It does this by improving customer security and privacy through consent-based access, incorporating regulator governance, and assisting banks in using reliable and accurate customer data while reducing customer acquisition cost.

3. RELATED WORK

Online transactions and digital information are currently gaining popularity day by day. The idea of digitized information has been made possible by this digital transition, which has evolved the idea of information conveyance in a very time- and cost-efficient manner.

Another timestamping technique involves stamping every digital document with TS (time of creation) before sending it over a network so that the recipient cannot further claim that they did not obtain the transaction record. When the idea of using Bitcoin as a blockchain application was first put forth, it had a number of drawbacks, including the fact that it was only intended to increase digital currency transactions and do away with the need for a third party to act as a go-between between nations in order to alter the value of the local currency. Later, when the blockchain began to extend its reach into other software development industries, it gained additional notoriety globally.

A system is referred to as a consortium blockchain when one or more organizations get together to work on a specific objective without any trust issues. This system implements the PBFT consensus protocol with state machine replication. As the KYC process preferred paper over any digital platform because it is conducted based on the consumer's outward appearance, there were still a number of issues that persisted even after the notion of digital information.

Due to security concerns, it also favors the offline method, but Perry Mayo has given some hints about how to change the KYC process by adopting distributed ledger technology (DLT) for effective system performance and to lower various costs associated with it. He has suggested a blockchain-based KYC solution that will improve process efficiency and lower the cost of onboarding new KYC customers.

Rutter uses the self-sovereign model and the "bank sharing model" to demonstrate the benefit of decentralizing the KYC process while also providing an applied description and evaluation of two different, decentralized circumstances based on Corda. A blockchain-based proof-ofconcept system for managing private blockchain environments was proposed by Norvell et lathe KYC procedure can be made simpler by Moya no et al.'s system, which permits automation and permission document sharing.

4. METHODOLOGY

We have already covered a significant number of current KYC framework difficulties, including centralization, traffic force, adaptability and dependability aspects, among others. According to estimates, using the blockchain system will enable us to cut global costs by about $27 billion annually.

Here, the question of how to improve or what method should be used to make this estimation accurate comes first. We may categories our methods using the list of criteria below. We want a system where a few organizations band together and use established protocols to exchange information among themselves. Every organization is currently going through their KYC procedure.

Any person who wants to use the service made available by that specific organization must go through its KYC procedure. Because they only seek the KYC approval based on their own protocols, rules, and regulations, organizations do not regard the KYC procedure approved by other organizations.

If one organization has already completed the KYC process by any individual, we want to develop a system that will allow other organizations to accept that information. We wish to establish a method in which organizations can address the concerns related the sharing of information (Privacy and Integrity of information) because there may be many issues among the organizations regarding this that occasionally become quite critical.

In the current situation, if a person provides his Aadhar card, pan card, passport, driving license or any other government-issued document to any organization for KYC, that organization verifies these details with the corresponding authority (i.e., Aadhar card to UIDAI, pan card from UTITSL).

Therefore, all that is required to get all the organizations onto a common platform is the use of a technology that can shorten the KYC process by maintaining an immutable public ledger where organizations can readily verify the information. Because we discovered this cuttingedge platform that meets our requirements with nearly impenetrable cryptographic security, KYC optimization was designed using blockchain smart contract technology.

Every organization that represents itself as a peer in a consortium network is only able to check the information under the suggested technique, not to modify them.
It has created the consortium blockchain paradigm depicted in the image above. A collaborative strategy when several organizations get together to carry out necessary activities in accordance with established norms is known as a consortium.

A permissioned model applies to the proposed system, and any organization may obtain the information by providing identification proof for their service. Every organization will be given an identity under the planned system so they can keep track of the records.

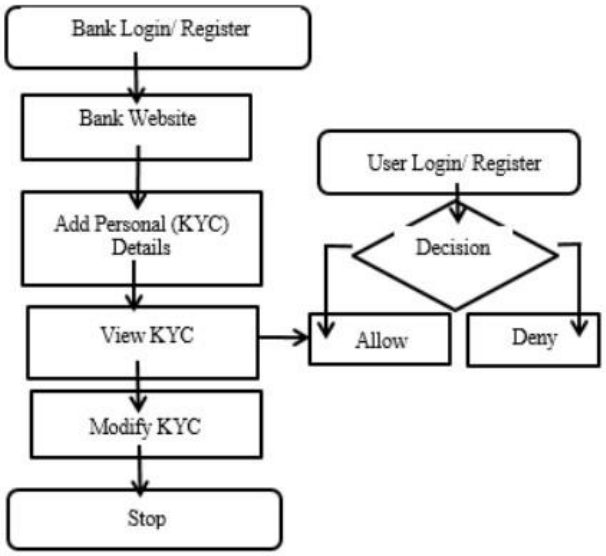
Blockchain's immutability and cryptographic features free this system from data tampering.
Due to data being saved online on the blockchain, maintenance costs associated with duplicate information will also be eliminated, and paperwork will be significantly reduced. Finally, while internal operations inside each organization are spread, they appear to be one cohesive unit from the outside. Such efforts are carried out by blockchain in a very adaptable and dependable manner.

5. IMPLEMENTATION

Although there are many different tools sets available for blockchain, we still need a few particular tools to implement our methodology to improve or optimize the current KYC framework. To construct such a belief system, we chose the Ethereum blockchain development platform, so let's quickly go through the devices and stable elements. The tools listed below have been used by us.
The Remix is a very well-functioning IDE that offers many capabilities with which we may directly connect to our blockchain network by activating Remix's injected web3 provider mode. Smart contracts can be generated in the Remix utilizing the solidity programming language.

It offers the capability to verify whether or not our smart contract is operating as needed. It offers greater GUI elements to help users comprehend what is actually occurring while processing. Access Remix by going to https://remix.ethereum.org/. A programmed called MetaMask that we inject into our web browsers allows us to access the blockchain network from a local browser.

By giving the recipient's transaction address, Metamask additionally aids in transferring ether (the digital currency used by Ethereum) to any chosen place. https://metamask.io/ is the URL to use to access and customize Meta Mask. In order to deploy our smart contracts, create our applications, and run them on our local system, we use a tool called Ganache, which offers a personal blockchain environment for Ethereum development.



It can be utilized by obtaining a command-line utility as well as a GUI (graphic user interface). However, Ganache has only been utilized to visualize the local blockchain running system in this proposed paradigm. You may get the Ganache GUI by visiting https://www.trufflesuite.com/ganache. On a local workstation (in a Linux terminal), you may install the Ganache CLI by typing npm. install -g ganache-cli.
Data is now maintained on a central server utilizing a number of consumerprovided characteristics, including an Aadhar ID or another governmentissued ID, a personal phone number, a person's name, mother's name, father's name, gender, date of birth, address, and address pin. In order to implement the KYC protocol's fundamental architecture and preserve its integrity, the proposed system has also recommended adopting some of these parameters. Such parameters have been used in the writing of the Smart Contract (business logic that adheres to a particular paradigm of programming), and this smart contract will accept all of the consumer's input information. However, because Ethereum has gained a range of services, tools, and platforms, it offers a great deal of flexibility in terms of tool setup. However, we decided to use the remix platform to create the smart contracts using the high-level programming language solidity.
Following the configuration of the remix environment, we employed several fundamental data types required to store details, such as unit to store numerical values in accordance with our bit value and uint256 for high bit values of any specific literal used to provide precise information. As needed when developing a protocol, alternative uint1 to uint256 formats can also be utilized, and the string data type is used to store literal string values from user input.

6. USE CASE:

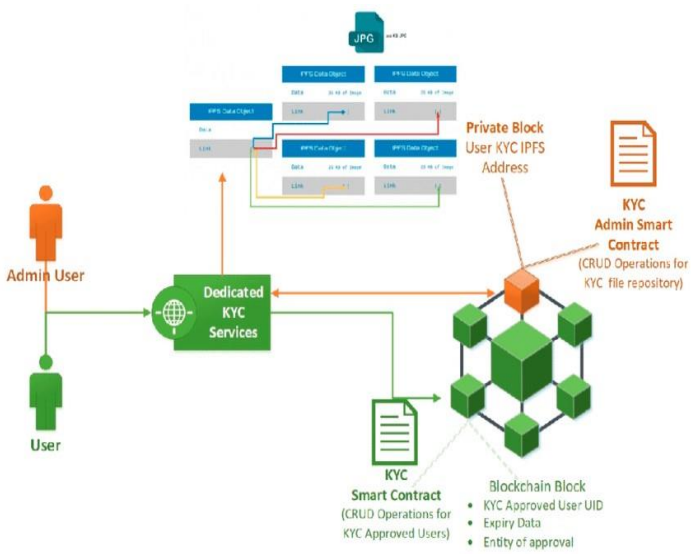
I. BLOCKCHAIN KYC SMART CONTRACT:

In the modern world, there are a ton of banking transactions. For instance, 28.45 million financial transactions were recorded daily by the Society for Worldwide Interbank Financial Telecommunication (SWIFT). Therefore, it is essential to have appropriate methods for confirming the parties' identities and legal

capacities to perform and/or receive a financial transaction in order to prevent transaction fraud.

Financial institutions and other regulated businesses frequently refer to their clients as "Know Your Customer" (KYC) before engaging in financial
transactions with them. The KYC procedure is as follows: if a client needs to make a payment transaction from his or her bank account to another bank account through a payment provider, the payment provider performs the KYC to verify the client's ident ity, for example by the client's name, from the bank where the money was transferred from. The name of the customer is then compared to the name that the client provided. when registering for a payment provider's service.

Additionally, the client's name m ay be cross -checked against external databases like World -Check, which aids businesses in thwarting financial crime.



Public (user) and private (admin) Know Your Customer (KYC) smart contracts

II. Traditional KYC System Problems:

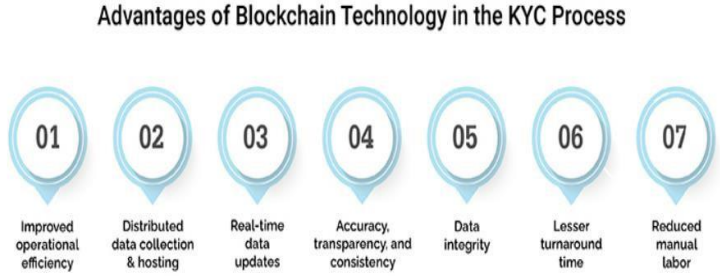
In nations that offer electronic services to verify a person's identification, performing KYC is a simple task. However, it is dangerous for financial institutions to take on clients if such services are unavailable. As a result, the KYC procedure used to onboard a new client takes time, and each financial institution is required to conduct its own KYC.

For example, when a customer wishes to create a bank account, the bank submits the customer's information to the registries, who then enter it in their databases and the customer becomes "KYC Compliant". Every time the customer has to open a new bank account, the same procedure is followed.

BLOCKCHAIN BASED FINANCE	TRADITIONAL BANKING FINANCE
No Intermediary.	Transactions are facilitated by banks.
Supply is determined by an algorithm and is known for years to come.	Supply is determined by central banks of respected currencies and may change depending on the debt issued.
Cross border payments can be done in a few minutes.	Cross border payments may take up to a week.
KYC/AML is not necessary if the transfer is made from person to person.	Have to pass KYC/AML if you want to utilize banking services.
Cross border payment commission may be counted in few cents per transaction in some cases.	SWIFT (~$15-$45) ACH (~$3) SEPA (free, but some banks charge).

III. Blockchain to the Rescue:

Many KYC-related issues, including the on-boarding problem, can be resolved with the help of blockchain technology. Once validated, the client's information can be spread among numerous banks using the blockchain of the public distributed ledger. As a result, after a KYC has been completed, other financial institutions may access it with the client's specific consent.



As a result, the KYC process will be significantly simpler, quicker, less timeconsuming, and more affordable. Furthermore, centralized database-based KYC systems reveal a weakness. Due to the append-only data structure of blockchain, the KYC data is replicated across numerous different nodes, making it indelible and traceable.

IV. Blockchain-Based KYC POC:

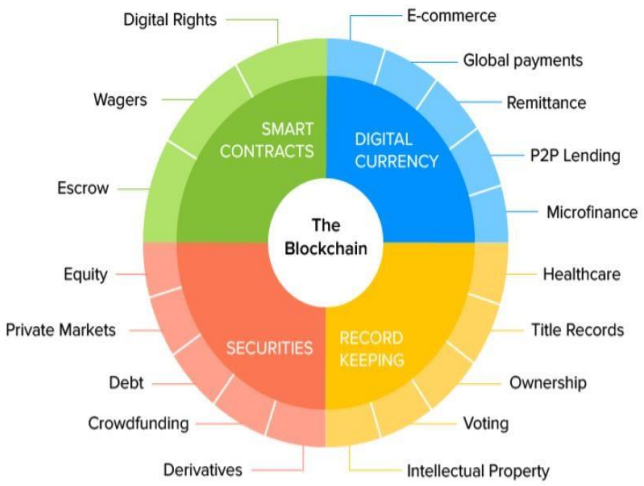
The KYC process can be supported by the blockchain, as this use case indicates.

- A client gives permission for KYC to be performed by a bank by submitting identification cards, financial information, etc.
- The bank will assess and verify customer identity and financial information.
- to verify the client's identity and declare them to be "KYC Compliant."
- The bank updates a blockchain platform with KYC data and status to show that it has been confirmed.
- The customer receives a token from the bank that serves as a record of his or her KYC status.
- The customer may grant permission for a third party to verify his KYC status.
- The targeted bank can examine the KYC data.

V. Blockchain KYC POC Implementation:

We used the Ethereum blockchain platform and the Solidity7 programming language to create the smart contract in order to implement the blockchain KYC. The smart phone's source code contract may be found on Github8. We employ a peer-to-peer file system called the Inter-Planetary File System (IPFS) to store the KYC documents such identity cards and passports because blockchains have a storage capacity constraint.

The two key benefits of IPFS are that it offers a persistent, decentralized means of storing and exchanging files and that it lacks a single point of failure.In contrast to central data storage systems. Therefore, IPFS is utilized by blockchain businesses, smart contract apps, banks, and legal archives. Each IPFS file is assigned a distinct fingerprint (cryptographic hash) in the KYC case, and this fingerprint is maintained in the KYC smart contract.



7. CONCLUSION:

For developers and researchers, a blockchain experimentation framework is a useful tool for deepening their understanding of the technology. Consequently, there is a highly controllable and customizable environment is essential for conducting lengthy blockchain experiments. The use of the Grid'5000, a sizable distributed platform that is simple to control and modify, was suggested in this study.

The blockchain KYC application has been considered as a direct application of leveraging this technology.

A POC has been put into practice. We presented preliminary and fundamental findings on the use of the framework (the testbed and the orchestration tool) for blockchain research.

Assessment tests carried out in a large-scale real-world setting.

Future research will focus on reassessing the evaluation of blockchain environments from various angles and will pay more attention to the security and privacy concerns of private blockchain applications.

ACKNOWLEDGEMENT:

We appreciate the support of our college Shri Ramswaroop Memorial college of engineering and management, Lucknow for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

REFERENCES:

1. S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” 2008.

2. Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An overview of blockchain technology: Architecture, consensus, and future trends,” in Big Data (BigData Congress), 2017 IEEE International Congress on. IEEE, 2017, pp. 557–564.

3. G. W. Peters and E. Panayi, “Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money,” in Banking Beyond Banks and Money.
Springer, 2016, pp. 239 278.
https://www.ansible.com/

4. Vukolić, Marko. "The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication." In *International workshop on open problems in network security*, pp. 112125. Springer, Cham, 2015.

5. Pilkington, Marc. "Blockchain technology: principles and applications." In *Research handbook on digital transformations*. Edward Elgar Publishing, 2016.

6. Lopez, David, and Bilal Farooq. "A multi-layered blockchain framework for smart mobility data-markets." *Transportation Research Part C: Emerging Technologies* 111 (2020): 588-615.

7. Beck, Roman, et al. "Blockchain technology in business and information systems research." (2017): 381-384.

8. Bhaskaran, Kumar, et al. "Double-blind consent-driven data sharing on blockchain." 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2018.

9. Christidis, Konstantinos, and Michael Devetsikiotis. "Blockchains and smart contracts for the internet of things." Ieee Access 4 (2016): 2292-2303.

10. Fujimura, Shigeru, et al. "BRIGHT: A concept for a decentralized rights management system based on blockchain." 2015 IEEE 5thInternational Conference on Consumer Electronics-Berlin (ICCE-Berlin). IEEE, 2015.

11. Kishigami, Junichi, et al. "The blockchain-based digital content distribution system." 2015 IEEE Fifth International Conference on Big Data and Cloud Computing. IEEE, 2015.

12. Britton, M. (2018) Could Blockchain Solve the KYC/AML Challenge? [online] https://www.bcsconsulting.com/blog/new-technology-canenable-human-bank/(accessed 25 February 2019).

13. Civic (2017) *Secure Identity Authentication* [online] https://www.civic.com/developers (accessed 10 August 2018).

14. Glaser, F. (2017) ‘Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis’, in Proceedings of the 50th Hawaii International Conference on System Sciences [online] https://doi.org/10.24251/HICSS.2017.186.

15. Hevner, A.R., March, S.T., Park, J. and Ram, S. (2004) ‘Design science in information systems research’, *MIS Q*, Vol. 28, No. 1, pp.75–105 [onine] https://dl.acm.org/citation.cfm?id=2017212.2017217.

16. Hong Kong Monetary Authority (2017) *Whitepaper 2.0 on Distributed Ledger Technology* [online]https://www.hkma.gov.hk/media/eng/doc/keyfunctions/finanicalinfrastructure/ infrastructure/20171025e1a1.pdf (accessed 25 February 2019).