Optimizing the KYC Process using a Blockchain based approach

Niraj Ratnawat[1*], *Saujanya* Pandey[1], *Rudresh* Paradkar[1] and *Soumi* Banerjee[1]

[1]Ramrao Adik Institute of Technology, Department of Information Technology, Navi Mumbai, India

Abstract—The Know Your Client (KYC) process is an essential part of the financial ecosystem. The KYC process requires banks to validate and verify primary documents. The market these days, though, is flooded with KYC utilities that facilitate this process and share these documents with multiple entities, however they provide very little value addition. Blockchain technology, with its concept of immutable timestamped ledgers and distributed systems, can effectively facilitate banks to improve their KYC methods by allowing near real-time data exchange among various entities for quicker and effective validation ensuring data integrity alongside bringing down the time and costs significantly.

1 Introduction

Know Your Customer (KYC) is a process by which financial institutions validate the identity of customers or businesses with whom they conduct business. The KYC procedure is carried out to prevent institutions from being used/exploited for unethical and illegal activities such as money laundering, whether intentionally or unintentionally. In India, all financial institutions except for regional rural banks are bound to follow the RBI KYC directions, 2016 and update the KYC data once in two years to once in ten years according to the risk associated with the customers. Besides being a legal requirement, KYC is an essential instrument to prevent financial scams and unlawful activities. With the rise of organized criminal activities, terror financing, and money laundering, KYC guidelines are now a crucial tool to tackle illegal transactions in the field of international finance. According to a recent survey by Thomson Reuters[1], major financial institutions spend up to $500 million per year on KYC and customer due diligence. In addition to the processing and underlying expenses, financial institutions around the world must pay substantial fines for non-compliance due to uncertainty, ambiguity, and complexity of the process. This calls for the urgent need to remodel the KYC and due-diligence processes as well as the record-keeping system. It affects the overall transactional-experience for the institutions as well as customers.

Typically KYC and due diligence processes are labor-intensive, recurrent, and sluggish, resulting in higher overhead expenses and irregularities. Below are several points that highlight the issues in the current KYC process.

- KYC verification leads to the expenditure of enormous unnecessary costs, human effort, and time by financial institutions.
- Typically the KYC process is very redundant and repetitive as each financial institution has to perform its own KYC process.
- Clients need to submit the same documents for KYC repeatedly at different financial institutions separately, which leads to an unpleasant experience.
- Sometimes the old systems that store sensitive KYC data fail to provide adequate security assurance.

It is, therefore, a pressing priority to call for a solution that solves the problem of repetition of the process, duplication of records that are stored, and the upsettingly lengthy span of the process. It is crucial to keep into one's view that topics such as this require dealing with sensitive data. The regulations concerning data privacy must not be disregarded.

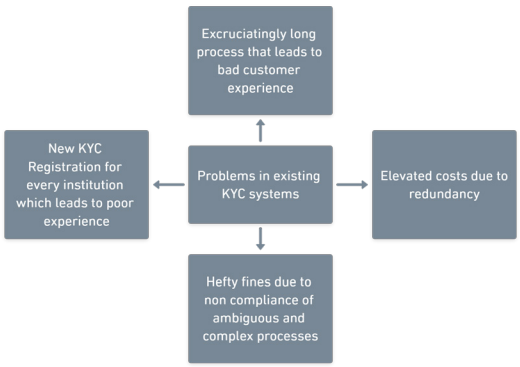

Fig. 1. Problems in current KYC process

2 Literature survey

As a distributed way of storing data, blockchains are currently gaining a lot of consideration. However, because of their irreversibility and openness, blockchains are unlikely to be ideal for personal data. In terms of data privacy, data stored on blockchains can't be altered, which means that personal information in them cannot be deleted, making it crucial to develop blockchain systems with this in mind.

One of the strategies may be to use blockchains solely to provide a timestamp pointing towards data stored elsewhere.

Even if a piece of public information is deleted, it'll still keep a record of the information that once existed. Using blockchains solely as a timestamping system rather than a data store has the added advantage of being more scalable when dealing with massive volumes of data.

"Bitcoin white paper" - Satoshi Nakamoto. Since it was first suggested to account for the Bitcoin cryptocurrency, the fundamental technologies and concepts behind blockchain have extensively developed[9].

"BlockChain Technology (DLT Technique) for KYC in FinTech Domain: A Survey" - R. Kasturi. According to R. Kasturi et al. [4], the data collected from the clients for KYC can be stored on the blockchain and the client can be given an ID to which their data is mapped. The client can then use the ID for future KYC processes. However, this practice is not just expensive, yet often unreliable, since the volume of data that can be processed on a blockchain is either restricted by protocol or requires a large transaction charge. On ethereum, storing a kilobyte of data costs $22.87, which is incredibly costly and unsustainable.

"Double-Blind Consent-Driven Data Sharing on Blockchain" - K. Bhaskaran According to an approach by K. Bhaskaran and others [6], exchanging KYC data via blockchain could help solve duplicacy problems. Hyperledger Fabric is being used in their approach. The customer must provide the personal information required for due diligence to a vendor, which is then sent to the blockchain for validation and storage by the vendor in an encrypted format. Other organizations for which the consumer wishes to conduct KYC may access this information only with the user's permission. The drawback of this approach is that, contrary to the rule, confidential data such as this cannot be kept in an immutable ledger and if the encryption breaks in the future, all of the customers' personal data could be compromised.

"KYC as a Service (KASE)—A Blockchain Approach." - Dhiren Patel Patel et al [8] proposed a method that combines machine learning and blockchain technologies to partially simplify the due diligence phase. According to their method, the customer's data is checked using machine learning techniques, and if approved, the data is encrypted and the transaction is recorded on the blockchain. They plan to use the Ethereum blockchain in conjunction with the proof-of-work consensus method. However, one of the key flaws in this technique is that, because KYC is such a sensitive process, even a small margin of error is costly. And machine learning algorithms are not yet advanced enough to guarantee 100 percent accuracy. As a result, the practical application of this method is still some time away.

3 Proposed system

This section enumerates the steps of the above proposed KYC process utilizing blockchain technology. But before that, a few concepts pertaining to the thorough understanding of the above proposed system are explained below.

3.1 Digital Signature:

A digital signature is a mathematical technique for verifying the authenticity of digital messages or documents. If the prerequisites are satisfied, a valid digital signature gives the recipient a very strong reason to believe that the message was generated by a recognised sender (authenticity) and that it was not altered en route. It employs asymmetric key cryptography as well as a hashing mechanism.

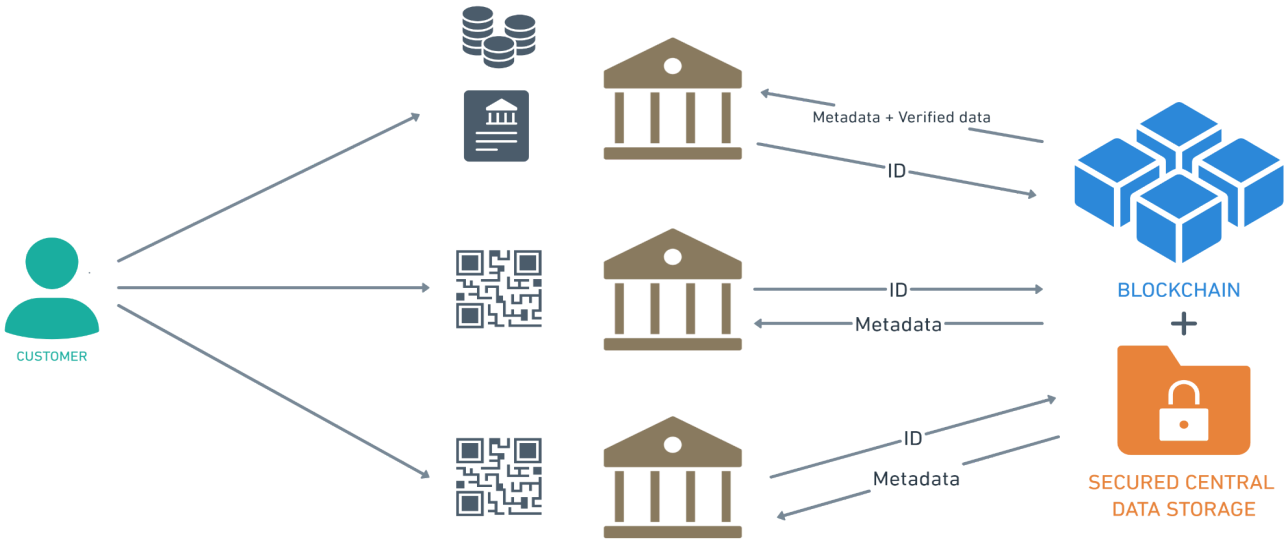

Fig. 2. Proposed KYC System

The sender generates a hash of the document, signs it with their private key, and then sends the signature and hash over. The sender's public key may then be retrieved and compared to validate the signature using the message hash and signature. This method ensures both data integrity and validity.

3.2 Smart Contract:

Simply said, a smart contract is a piece of software that runs on Ethereum's blockchain. It's a single address on the Ethereum blockchain that contains a collection of code (its functions) and data (its state). Ethereum accounts come in the form of Smart Contracts. This means they have some balance in their account and can perform transactions through the network. They are not, however, user-controlled. Instead, they are deployed to a network and run according to a set of instructions. User accounts can then engage with a smart contract by sending transactions that cause the smart contract to perform a function. Smart contracts, like conventional contracts, may set rules and have them enforced automatically through programming. Smart contracts can't be erased by default, and their interactions are permanent.

4 Working

The working of the proposed KYC system involves a two-step process - the *addition* and the *verification* process.

4.1 Addition Process (new users):

All the steps listed below for the addition process can be referred to from fig. 3 below.

1. A new client registers on the KYC portal using an existing cryptocurrency wallet such as metamask wallet.

2. The client searches for the desired organization on the portal to perform KYC with, via the search organization functionality.

3. The client visits the organization profile page, selects 'Perform KYC' option and uploads their documents which are then encrypted before being sent to the organization. A new unique request ID is generated during this step.

4. The organization official then downloads the decrypted documents via the portal and performs due diligence to establish the identity of the client.

If the documents are:

a) rejected, the client is notified and asked to initiate a new KYC request with the suggested changes.

b) approved, hash of the documents & hash of the request ID are signed by the organization and sent to the client's account.

The encrypted documents are uploaded to a secure server by the portal once the request is approved.

The client now selects the option to finalize the request, signs the request ID and pays the transaction fees for uploading the digital signatures, public keys and timestamp to the smart contract. The smart contract performs various validations using the digital signatures to check the authenticity of the sender and the data and approves, if all the data is found to be correct.

A new QR code containing the request ID is now generated and the KYC addition is now complete. This QR code can now be used to lookup the details of the KYC request universally.

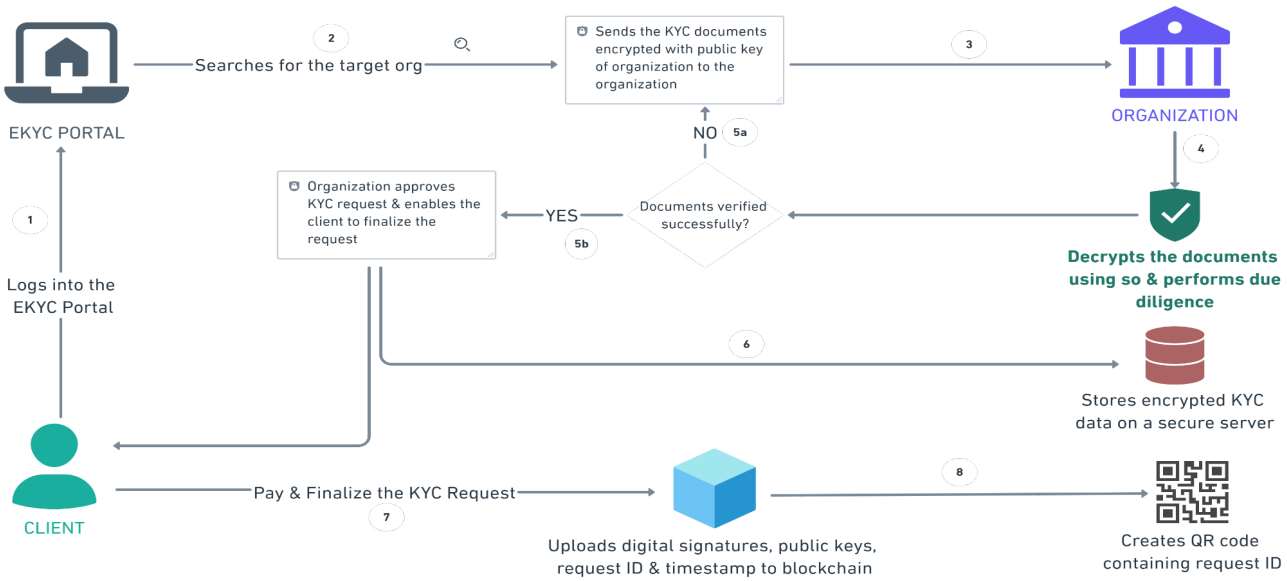

Fig. 3. KYC Addition process for new client

4.2 Verification Process (subsequent KYC verifications):

All the steps listed below for the verification process can be referred to from fig. 4 below.

1. The client who already has a KYC registered with an organization logs into the eKYC portal using their cryptocurrency wallet.

2. The client then searches for the target organization and sends their QR for the registered KYC along with a verification request to the target organization.

3. The organization extracts the *addition* request ID from the QR code, queries blockchain for the details of the registered KYC and validates data to establish the identity of the sender and adding organization.

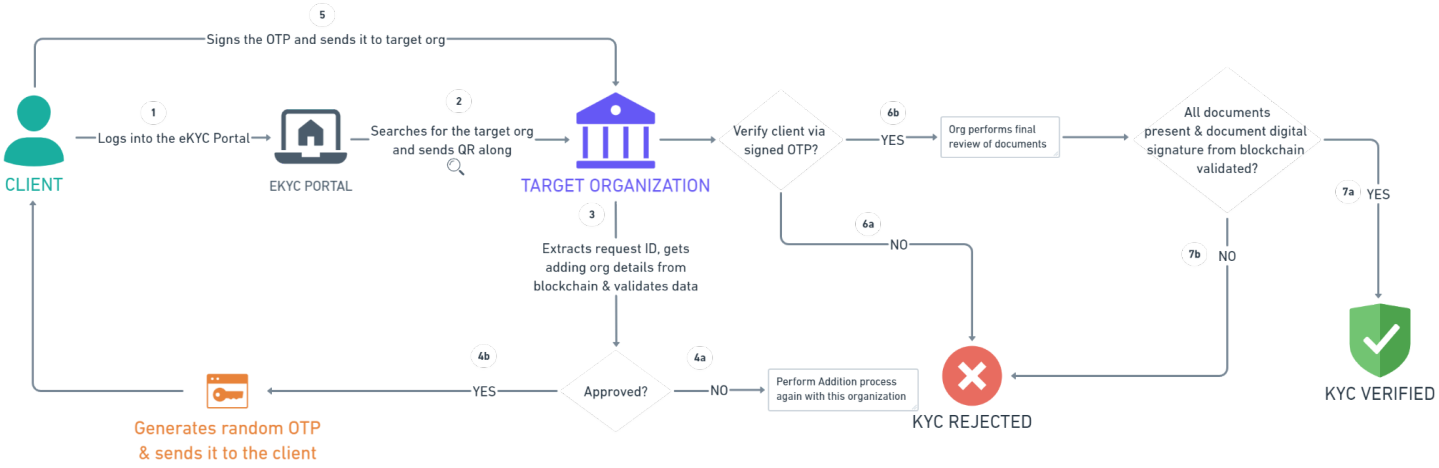

Fig. 4. KYC Verification process for registered client

4. If the target organization:

a) does not approve the previously registered KYC on grounds of not trusting the adding organization or not being able to verify the data, their verification request is rejected with appropriate reasoning.

b) is able to validate the data from blockchain and approves the adding organization, it then sends a randomly generated OTP to the client's registered email-id and phone to re-verify the identity of the client.

The client enters the OTP and signs it using their private key and sends it to the target organization.

If the target organization is:

c) not able to validate the signature, the verification request is rejected.

d) able to verify the signature, the verification request proceeds to the next stage.

The target organization now has to quickly view the documents for their completeness and validate the digital signature of documents from the blockchain.

e) If the documents are complete and the signature is validated, the KYC verification request is successful.

f) If not, the KYC verification request is rejected.

5 Result

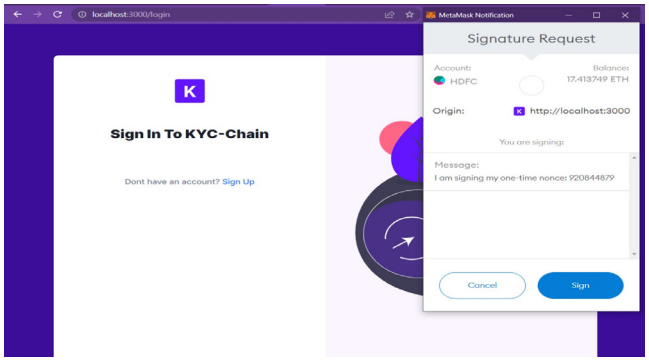

Fig 5. Login screen of the eKYC platform

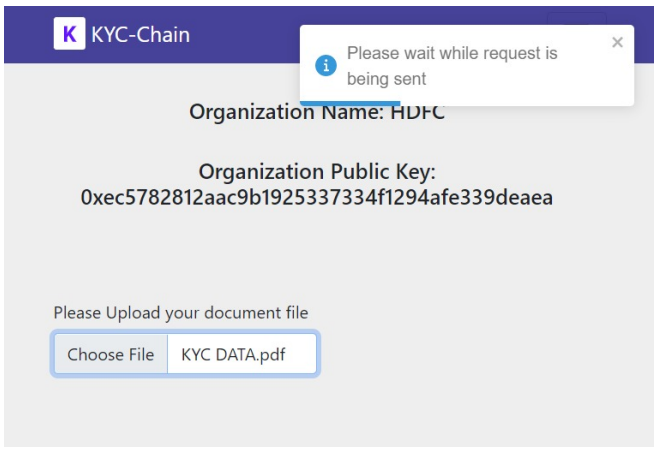

Fig. 6. Addition request initiated by user

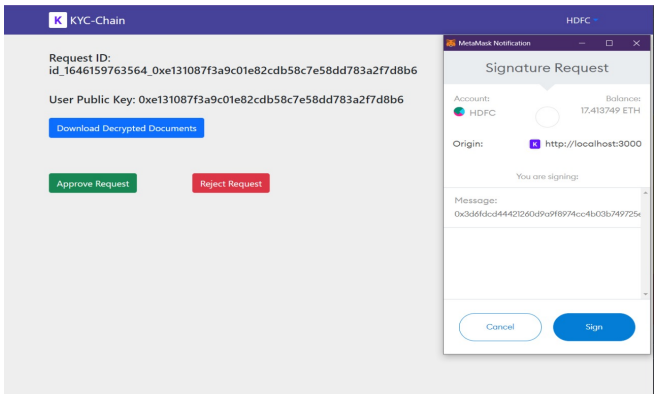

Fig. 7. Organization's view of processing client requests

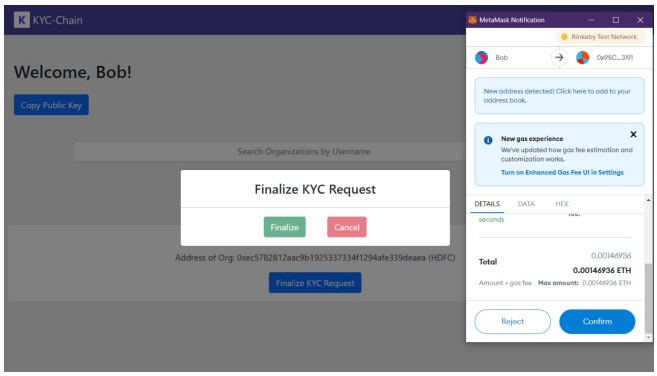

Fig. 8. Organization's view of finalizing client requests

Fig. 9. QR code with relevant information generated after user request approved

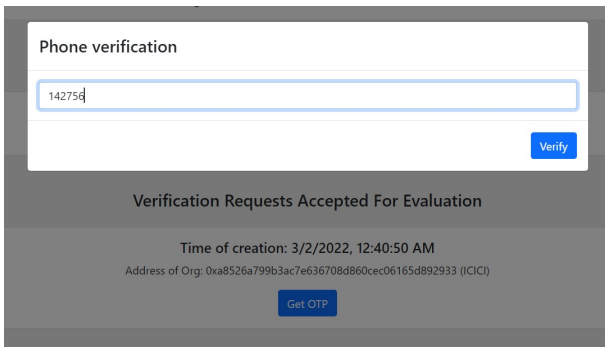

Fig. 10. User identification via OTP verification

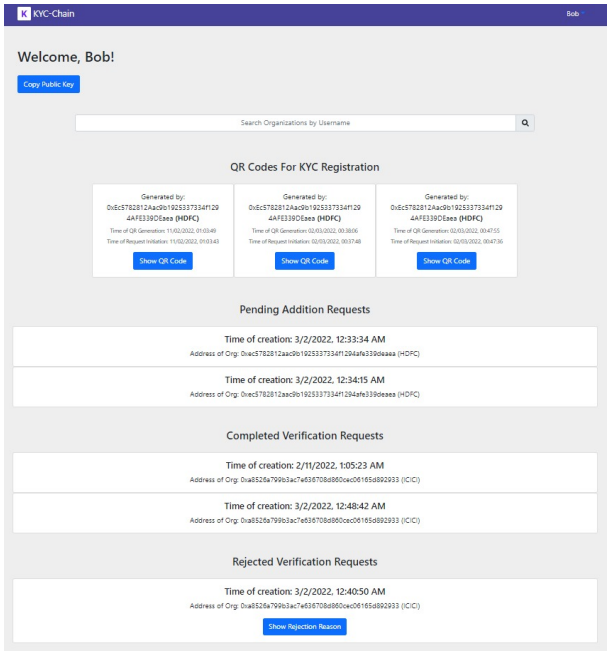

Fig. 11. User's dashboard with all requests data

Fig. 5 shows the login screen of the eKYC portal, which is integrated with Metamask wallet through one-click login functionality, after which the user is redirected to the platform's dashboard.

Fig. 6 shows the interface available to the user after clicking 'Perform KYC' on the organization's profile page.

Users can upload their documents and initiate an addition request.

Fig. 7 shows the interface available to organizations to process the received requests from users.

Once an organization proceeds with processing a user's request, the next step is finalizing the user request as shown in Fig. 8.

A critical step of each user request before finalizing the request is verification of the user's identity to ensure security. This is done by performing an OTP verification from the user's side, as shown in Fig. 10.

A user's KYC request is completed by generating a QR Code for the same, containing all the relevant information, as shown in Fig. 9.

All the ongoing, completed, and rejected requests are available on the user and organization's dashboard as shown in Fig. 11.

6 Comparative Analysis

6.1 BlockChain Technology (DLT Technique) for KYC in FinTech Domain: A Survey [4]

- The proposed system involves leveraging the blockchain for storing users' entire KYC data.
- The KYC data collected from the clients could be stored on the blockchain and referenced with an ID mapped to the data of the respective user.
- In contrast to this solution, our system makes use of a secure centralized server to store sensitive information, which is referenced on the blockchain via unique request IDs.

6.2 Double-Blind Consent-Driven Data Sharing on Blockchain [6]

- This solution presents a system that uses blockchain to encrypt user data and store it in a secure manner.
- The customer must submit personal information to a vendor for due diligence requirements, which is then sent to the blockchain to be validated and stored in an encrypted format by the vendor.
- This approach also involves storing encrypted data on the blockchain as opposed to storing on a centralized secure server in our approach.

6.3 KYC as a Service (KASE)—A Blockchain Approach [8]

- This system proposes storing transaction records after the verification process.
- Machine learning techniques could be combined with blockchain techniques to partially simplify the due diligence process.
- This approach involves performing the due diligence process as compared to manual verification in our approach. Reason being, machine learning algorithms are not yet fully dependable enough to handle such sensitive tasks.

7 Conclusion

The proposed KYC implementation can be used in multiple Banking/Financial services use cases like Lending and Borrowing, Portfolio Management, Stock Exchange, Insurance company, Trade Finance, Mutual Funds and offers a unique yet simple and effective solution to tackle the existing challenges. This approach can help in bringing down the costs, redundancy and duration of the process significantly, thereby, optimizing the current KYC process in terms of non redundant storage and decreased amount of time for overall process. This optimization, however, cannot be measured quantitatively given there is no single standard for KYC processes across institutions. But the overall process remains largely similar, and the proposed system clearly is an optimization over the existing process. However, one of the most worrisome aspects of the presently most popular implementation of blockchain technology is the consensus algorithm it uses, known as Proof of Work, which largely relies on electrical energy usage. This has a harmful influence on the environment and needs to be addressed as soon as possible. Newer consensus algorithms, such as Proof of Stake, are being developed that are more eco sustainable and may be readily adopted by current systems.

8 Future Scope

The current system makes use of a public blockchain. Due to the lack of an authorization system in public distributed ledgers, there's nothing preventing anyone from engaging with and participating in the blockchain's consensus mechanism. As a result, scaling challenges arise, and throughput is relatively lower. To overcome these issues, a consortium blockchain can be utilized, which combines elements from both public and private blockchains. Further, the algorithm used in the smart contract can be optimized to reduce transaction charges.

9 References

[1] https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

[2] "'Know Your Customer' (KYC) Guidelines - Anti-Money Laundering Standards". Archived from the original on 2012-08-01.

[3] Master Direction - Know Your Customer (KYC) Direction, 2016 of RBI Circular dated February 25, 2016.

[4] Block Chain Technology (DLT Technique) for KYC in FinTech Domain: A Survey, R. Kasturi and Vimalkumar Pachaiyappan, International Journal of Pure and Applied Mathematics Volume 119 No. 10 2108, 259-265.

[5] Trunomi, E. G. P. P. Gdpr key changes https://www.eugdpr.org/

[6] K. Bhaskaran et al., "Double-Blind Consent-Driven Data Sharing on Blockchain," 2018 IEEE International Conference on Cloud Engineering (IC2E), 2018, pp. 385-391, doi: 10.1109/IC2E.2018.00073.

[7] Buckley, Ross & Arner, Douglas & Barberis, Janos. (2016). The Emergence of Regtech 2.0:From Know Your Customer to Know Your Data. Journal of Financial Transformation. 44. 79-86. DOI=https://dx.doi.org/10.2139/ssrn.3044280.

[8] Patel, Dhiren R. et al. "KYC as a Service (KASE)—A Blockchain Approach." (2020).

[9] Bitcoin white paper. 2008. Satoshi Nakamoto. https://bitcoin.org/bitcoin.pdf

[10] https://www.evry.in/globalassets/india/pdfs---brochures/ekyc-using-blockchain.pdf

[11] https://www.tcs.com/content/dam/tcs/pdf/Industries/Banking%20and%20Financial%20Services/Reimagining%20KYC%20Using%20Blockchain%20Technology.pdf