Cost-efficient Blockchain-based e-KYC Platform using Biometric verification

Sahil Bhatia
Computer Science & Engineering Dept.
Indian Institute of Technology
Jodhpur, Rajasthan
m22cs002@iitj.ac.in

Lokendra Vishwakarma
Computer Science & Engineering Dept.
Indian Institute of Technology
Jodhpur, Rajasthan
vishwakarma.3@iitj.ac.in

Dr. Debasis Das
Computer Science & Engineering Dept.
Indian Institute of Technology
Jodhpur, Rajasthan
debasis@iitj.ac.in

***Abstract*—Know Your Customer (KYC) is the authentication and verification process of the user carried out in the financial sector by institutions such as banks, insurance companies, fintech companies, etc., and other sectors such as smart healthcare, real estate, telecommunication, online gaming and gambling companies before engaging in any financial activities. The KYC process is made mandatory for Financial Institutions (FIs) by governments worldwide to keep a check on terror financing and money laundering activities. However, the traditional physical KYC process has limitations such as high operational costs, large time consumption, privacy and security issues, repetitive processes across multiple institutions and user inconvenience. Hence, the FIs are looking for alternatives to the physical KYC. The digitization of the KYC process, known as e-KYC, was explored but had problems such as a single point of failure, repetition of KYC process across multiple FIs and lack of security. Blockchain-based e-KYC has become popular these days and caught the eye of FIs due to inherent properties of the blockchain such as decentralization, transparency, and immutable ledger. Moreover, blockchain-based solution is highly secure and cost-efficient. This paper proposes a blockchain-based e-KYC platform where users can register themselves and get their video KYC done after ether payment. Once successfully verified, the user will receive a KYC key. The user will submit this key to the banks or other FIs in which he wants to register. The FIs can verify whether the user has undergone the KYC process by looking in the blockchain using the KYC key. Our solution requires the user to submit his documents only at the e-KYC platform and not at different FIs for registration, thus preserving his privacy and, at the same time, ensuring the user's authenticity.**

***Index Terms*—Blockchain, KYC, Ethereum, Smart Contract**

I. Introduction

Know Your Customer (KYC) is the process of authentication and verification of the identity of the customers by the Financial Institutions (FI) before performing any financial transactions with them. All FIs are bound to follow the KYC regulations laid out by the government authorities to mitigate the risk of them being utilized by individuals or entities with nefarious intentions to engage in money laundering and terror financing [1]. Based on the findings of Fenergo's global research report titled "KYC in 2022", it is revealed that a significant proportion of corporate and institutional banks allocate substantial financial resources towards the completion of individual clients KYC reviews [2]. Specifically, over half (54%) of these banks incur expenses ranging from $1,500 to $3,000 for the completion of a single client's KYC review, while approximately one in five (21%) banks spend over $3,000 per client review. According to Fenergo's research, it has been observed that significant FIs allocate a substantial amount of up to $30 million per year on KYC processes during the client onboarding phase. A majority of them (52%) take 61 to 150 days to conduct client KYC reviews, wherein a significant portion of this duration is dedicated to collecting and inputting data across various systems. The process of KYC requires clients to visit the organisation's branch office to provide their identity documents and proof of address. The process is highly time-consuming and cumbersome, particularly for consumers living in areas where the organization lacks a physical branch office. The procedure of conducting initial verification and continuous monitoring of activities requires repetition for each customer. Furthermore, every customer must repeat this process when initiating an account with a different FI, as shown in Fig. 1. Hence, the KYC procedure proves to be a laborious and unpleasant process for customers as well as FIs, leading to subpar client satisfaction and decreased number of accounts being opened. According to a poll by Thomson Reuters in 2016, 89% of customers expressed dissatisfaction with the KYC procedure [3]. The customers questioned the onboarding process due to its time-consuming nature and the requirement of submitting multiple documents.

Due to the above-mentioned challenges of physical KYC, FIs are shifting towards online methods of conducting KYC, known as e-KYC. The implementation of e-KYC offers consumers the convenience of completing the onboarding procedure efficiently within the confines of their own residences. The use of the technology has resulted in significantly reduced onboarding duration. The e-KYC systems cannot communicate transaction information, hindering traceability in the e-KYC verification process. Utilizing a cloud-based e-KYC system offers enhanced efficiency and flexibility in the authentication process than the host-based e-KYC authentication technique. However, the security and privacy concerns around a cloud-based solution are significant as it stores client data documents that are potentially accessible to public cloud tenants and cloud service providers (CSPs). To mitigate this issue, FIs must upload the e-KYC data on the cloud in encrypted form. However, this implementation brings additional burdens

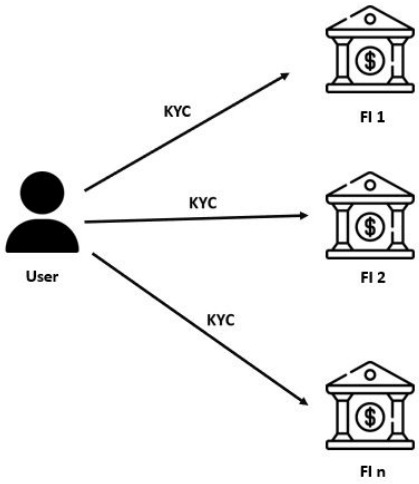

Fig. 1. Traditional KYC system

associated with the verification process, communication, and centralized decryption [4]. Furthermore, there is a lack of universally established criteria for representing e-KYC data, i.e., different nations have distinct formats for representing e-KYC data, and the level of security assurance in transmitting such data will be contingent upon the specific implementation in each country. Also, the user has to repeat the KYC process with different banks due to absence of shared KYC standards among the FIs [5].

There has been an increasing inclination towards utilising blockchain-based e-KYC solutions recently. Blockchain technology facilitates a decentralized system that enhances transparency, trustworthiness, and cost-effectiveness in processing and managing transactions within a multi-user and multi-provider setup [6], [7]. Smart contract is a self-executing software operating on the blockchain platform [8]. Its primary purpose is to facilitate the automated execution of system logic or functions in an efficient manner. This enhances the utilization and programmability of systems operating on the blockchain network. Since it automates the conditions of the agreements, there is no need for the involved parties to trust each other [9]. This research paper proposes a blockchain-based e-KYC platform to curb the drawbacks of existing KYC methods. As per our solution, there is no need to conduct repetitive KYCs by each financial institution. A user only needs to get his e-KYC done using our platform, which can be verified by all the other financial institutions whose services the user wants to avail. Our solution not only meets the government regulations regarding KYC but also is cost-efficient. The outline of this paper is as follows. Section II highlights the related works in this field. Section III presents our proposed model. Section IV presents the implementation setup of the model. Section V gives the performance analysis of the proposed solution and its comparative analysis with some related solutions. Section VI gives a conclusion of the research paper and future scope.

II. Related Works

Recently, blockchain technology and smart contracts have gained prominence in e-KYC. Blockchain is used for storing information, and smart contract is used for the automated execution of KYC-related functions and processes in the blockchain. While some solutions use on-chain storage, others use off-chain storage. On-chain storage means the user data is stored in the blockchain, whereas off-chain storage means the user data is stored in a database. Some solutions also utilise both on-chain and off-chain storage together.

Kasturi et al. [10] proposed that the information obtained from customers for the purpose of KYC procedures can be securely maintained on the blockchain. Additionally, clients can be assigned a unique identifier linked to their respective data. The client can utilize the identification (ID) for subsequent KYC procedures. Bhaskaran et al. [11] proposed a solution that utilizes Hyperledger Fabric, a framework offering the necessary membership services for certification and identity management. The client shares their personal information with a service provider, who subsequently transmits it to the blockchain for verification and storage in encrypted form. Other parties can access this data once the user gives consent. However, these methods are not only costly but also unreliable. This is because the amount of data that can be stored on a blockchain is limited by protocol and necessitates a substantial transaction fees. Also, the blockchain's transparency raise privacy-related issues since the data saved on the blockchain is visible to all nodes and its immutability breaches regulations like the General Data Protection Regulation (GDPR), which gives users the right to be forgotten [12]. Storing sensitive data in the blockchain, even in encrypted form, is not advised due to the possibility of breaking the encryption algorithm in future.

Kumar et al. [13] proposed a blockchain-based KYC system as a Proof of Concept (POC). Their solution is based on generating a QR code containing encrypted user KYC data after the user is verified. The user uses the QR code to register with different banks next time. However, there are issues with storing user data in QR codes, such as their storage limit and susceptibility to physical damage or degradation, which can result in the loss or corruption of data. Fugkeaw [4] proposed a solution that combines symmetric encryption and public key encryption to protect e-KYC documents before storing them in the cloud. The solution stores encrypted transactional data in the blockchain. Ostern et al. [14] proposed a blockchain-based KYC system for the conduct of Initial Coin Offerings (ICOs). After verifying the user, the data is stored off-chain, and the KYC token is stored in the blockchain. However, they store the KYC token without encryption or hashing, making it visible to everyone. There is the risk of impersonation in the above solutions as there is no way the verifier can identify whether the user is posing as someone else and submitting others' details and documents. Without video KYC, it might not be possible to have true identification of the user.

Pauwels [15] proposed a solution concept for KYC called

'zkKYC' which leverages self-sovereign identity and zero-knowledge proofs to protect customer privacy while maintaining necessary transparency. Rathee et al. [16] presented an anonymous credential scheme called 'ZEBRA' which leverages zkSNARKs to provide efficient on-chain verification. It ensures privacy for users through unlinkability and supports auditability, revocation, traceability, and theft detection, adding accountability for malicious users.

In our search for related works in the field of blockchain-based KYC systems, we found very few good quality research papers that discussed the gas utilisation of smart contracts and costs incurred by the users and KYC platform in their proposed solutions.

III. Proposed System

Our solution proposes an Ethereum blockchain-based e-KYC platform. In our platform, user data is not stored in the blockchain. Instead, blockchain is used for keeping a record of the e-KYC transactions and verifying subsequent e-KYC requests for a user in other financial institutions. The user data is stored securely in the KYC platform's database and is required only once during user registration. This system ensures that a user can get verified with multiple financial institutions using only a KYC key. He/she does not need to provide any other details. The working of the proposed system is as follows:

A. Registering a new user:

Fig. 2 depicts the process of registering a new user on the KYC Platform. The user needs to carry out this registration process only once. Following is the sequence of steps involved in user registration:

1) A user who wants to get his e-KYC done registers on the platform by submitting the required details and uploading his/her identity documents.
2) The user then needs to verify his email address by entering the correct OTP.
3) After verifying the email, the user will pay the video KYC fee in Ethers using his MetaMask wallet, as shown in Fig. 3. Smart Contract's payment function will be called for the payment.
4) Once the payment is made, the Admin carries out the user's video KYC.
5) After the video KYC:
    a) If the Admin is unsatisfied with the video KYC, the user's KYC process is terminated, and he has to get his video KYC done again.
    b) If the Admin is satisfied with the video KYC, then a unique KYC key and User ID are generated for the user. The KYC key is stored in the platform's database. The user can view the KYC key on his/her profile page.
6) The KYC Hash or KYC Key Hash is created by hashing the KYC key and is stored in the blockchain using the smart contract's hash storage function. The KYC Hash is also stored in the platform's database for subsequent verifications.

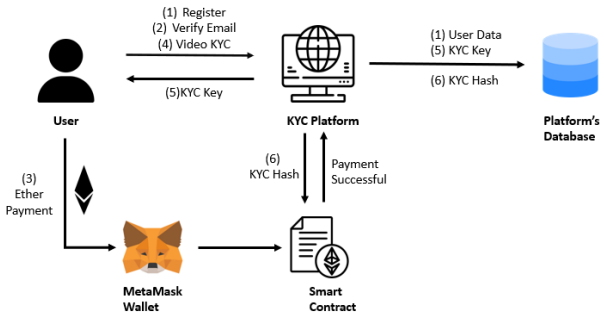

Fig. 2. Registering a new user on the e-KYC platform

B. User Verification by the financial institutions:

Once the user has registered on the e-KYC platform and obtained his KYC key, external platforms such as banks or financial institutions can verify him/her using the KYC key, as shown in Fig. 4. The user does not need to get his KYC again from the financial institution and, hence, does not pay any verification fee. The KYC key proves that the user is already verified and a legitimate customer. Smart contract facilitates efficient and automated processing of verification requests by financial institutions. The steps of the verification by external platforms are as follows:

1) After successful e-KYC, when the user wants to register in a bank or FI, he has to share his KYC key. To maintain confidentiality, the financial institution employs a SHA3 hashing method to hash the KYC key before transmitting

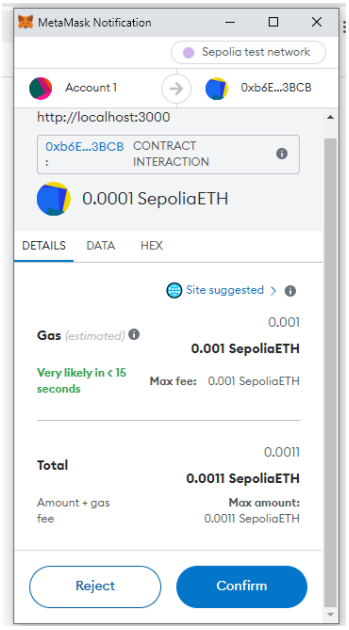

Fig. 3. Making ether payment

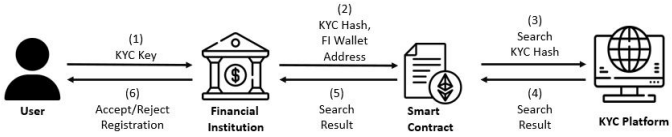

Fig. 4. Verification of the user by FIs

it to the e-KYC platform, as the data transferred through smart contracts is publicly visible.

2) The verification function in the smart contract is called with the FI's Ethereum wallet address and KYC hash. The verifying FI's wallet address is sent to track user's registrations with different FIs. The verifying FI transfers verification fees to the e-KYC platform.
3) The data is then sent to the e-KYC platform. After receiving the data, the KYC platform searches the corresponding KYC hash value in its MySQL DB.
4) The answering function in the smart contract will be invoked, indicating whether the KYC hash was present in the MySQL DB or not.
5) The search result is sent to the verifying FI in form of Boolean value.
6) The FI grants the user access to its services if the result is true.

The working of the solution, as shown in the above 2 subsections, ensures that the user does not need to get his KYC repeatedly with different financial institutions. By performing e-KYC once on our platform, the user can use the obtained KYC key to register with various financial institutions.

IV. Implementation Setup

The proposed solution presents a platform for the users to complete their e-KYC. The platform is a web application developed using Node.js consisting of various JavaScript libraries on the client and server side. Ethereum blockchain is used for storing the user's KYC key hash, and a smart contract written in Solidity language automates the blockchain-related processes and functions. Video chat feature developed using socket.io and simple-peer libraries allows real-time user verification. MySql database facilitates user data storage. Following is a detailed description of the implementation setup of our solution:

A. E-KYC Platform

The proposed e-KYC platform was created using Node.js. It is an open-source, cross-platform JavaScript runtime environment designed to build scalable network applications. Following are some of the JS libraries used in this platform:

1) **On Server Side:**
   - **Express:** Express is a flexible Node.js web application framework that provides a robust set of features for web applications. It enhances the application's functionality by providing various middleware such as body-parser, CORS (Cross Origin Resource Sharing) and cookie-parser, etc. It is also used in application routing using HTTP methods and URLs.
   - **Socket.io:** Socket.IO is an open-source library that enables low-latency, bidirectional and event-based communication between a client and a server.
   - **JSON Web Token (JWT):** JWT is a JSON object used for secure information exchange between two parties over the web. Such a token has 3 components: header, payload and signature separated by dots.
   - **Nodemailer:** Nodemailer is a module for sending emails from Node.js applications.
2) **On Client Side:**
   - **React:** The front-end UI of the portal was created using the React library. It is an open-source library developed by Facebook to design the application's view layer.
   - **Axios:** It is a promise-based HTTP client for browser and Node.js. Since it is promise-based, it helps in sending asynchronous HTTP requests.
   - **web3.js:** web3.js is a collection of libraries that allows interaction with a local or remote Ethereum node using HTTP, IPC or WebSocket. It can be used for retrieval of user accounts, interaction with smart contracts, and performing transactions.
   - **Simple-peer:** It is a library that establishes peer-to-peer connections in web browsers. The connection between two browsers is created using WebRTC (Web Real-Time Communication), which allows audio and video communication.

B. Blockchain Technology Used

The blockchain technology used was Ethereum. Smart contract was used to integrate the e-KYC platform into the Ethereum network. It was developed in the Solidity programming language. It will automatically handle all the verification requests made by the financial institutions.

Smart Contract Compilation: The smart contract is compiled in javascript using solc compiler. Solc compiler converts the High-level Solidity language code into the Ethereum Virtual Machine (EVM) bytecode. Bytecode is executed on the Ethereum blockchain by EVM.

Smart Contract Deployment: The smart contract is deployed on the Sepolia Testnet for development purposes. Testnets are blockchain networks specifically created to replicate the operational conditions of a "Mainnet", but they function on a distinct ledger. Developers utilize testnets to conduct risk-free testing of their applications and smart contracts prior to releasing them to Ethereum's Mainnet environment. However, the e-KYC platform can work on Ethereum's Mainnet once used in a practical environment.

MetaMask: Both users and financial institutions use the metamask extension in browsers. It is a cryptocurrency wallet used to interact with decentralized applications and lets users

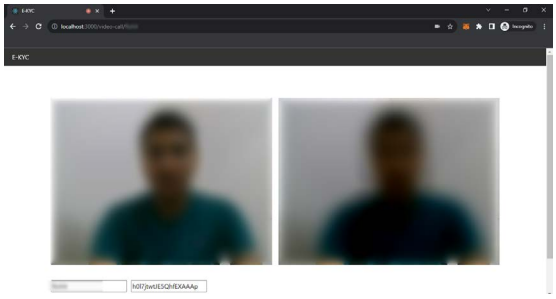

Fig. 5. User verification via Video Chat

store the Ethers. It allows the concerned parties to interact with the Ethereum network through their web browsers.

C. Video KYC

The video call functionality is implemented using Socket.io and simple-peer libraries. Express server allows the different clients to connect to the server. As mentioned earlier, Socket.io facilitates bi-directional communication between the client and server in real time. It uses WebSocket, which is a stateful and full duplex protocol. WebSocket connection will be persistent unless terminated by either the client or the server.
A direct peer-to-peer connection is established between different clients using the Simple-peer library. It uses WebRTC, which allows audio and video communication in the web pages without the intermediate servers. getUserMedia() method prompts the user to access his microphone and camera. Socket.io-client library helps the client establish a socket connection with the server. The steps during the Video Call are as follows:

1) The admin enters the video call page and sends an email to the user facilitated by the Nodemailer module. The email contains the video call link and the admin's unique Socket ID.
2) The user joins the video call page using the received link.
3) The user enters the admin's Socket ID and initiates the video call with the admin.
4) The admin verifies the user and ends the call.

A snapshot of the Video Call is shown in Fig. 5.

D. Database Server

The e-KYC platform is connected to the local database server. The database server used is MySQL. We can access the database from the Node.js application using MySQL driver. The database stores the user details.

V. Performance Analysis

The performance of the proposed KYC platform is evaluated on parameters such as costs incurred by the customer and the platform for user registration and verification. We also analysed the time elapsed in the KYC process of each user. Finally, we present a comparative analysis of our solution with some of the related solutions.

A. Cost Analysis

The user has to pay a one-time fee to the KYC platform. The fee is needed to be paid in Ethers. We have tried to keep the KYC fee as minimal as possible. The user must pay 0.0001 ETH, approximately 13.45 INR, as of 14 Sept 2023. In addition to the KYC fee, the transaction fee is paid to the miner to mine the transaction in a block in the Ethereum network. The KYC registration process utilises 28,151 units of Gas. The Gas price can be varied to get the transaction mined quickly. We have set the Gas price to 5 Gwei, which results in a total transaction fee (Gas used * Gas price) of 0.00015 ETH, i.e. approximately 20 INR.
The KYC platform incurs costs while storing the KYC Key hash in the smart contract and responding to user verification requests. The costs will be in the form of transaction fees for the above two tasks. The hash storage cost in the smart contract is 49,174 units of Gas. The Gas price can be varied to decide between the cost and time to get the transaction mined. The user verification process also consumes around 34,467 units of Gas. FIs have to pay a minimal amount of verification fee to our platform. The response to the user verification request utilises 22,839 units of Gas.

The user pays registration fees to the platform, and different FIs pay verification fees to verify the user's KYC status. These 2 costs help the platform break even the costs incurred during user onboarding. Thus, our solution provides a cost-efficient method of conducting e-KYC for both users and FIs.

B. Waiting Time Analysis

The user has to register only once on the platform. The only time-consuming processes for the user are Ether payment and Video KYC. Based on the Gas price set, the transaction mining time is around 20-40 seconds based on how busy the Ethereum network is. However, the user has to wait only for the transaction to be processed while making payment. This takes less than 10 seconds. The user also has to undergo video KYC, which is performed after a successful Ether payment by the user. The admin will then schedule a video call with the user. The video call is done to verify whether the user is legitimate and is not impersonating anyone else. This process is also not very time-consuming and can be done within a minute.

C. Comparative Analysis

The comparative analysis of our proposed solution with various related works is shown in Table I. Only our, Kumar et al.'s [13], Fugkeaw's [4] and Ostern et al.'s [14] solutions do not store user data on the blockchain in compliance with government regulations like GDPR. However, these solutions do not have the functionality of video verification, unlike ours, to avoid impersonation of users during registration.
Furthermore, only Ostern et al. [14] have discussed gas utilisation during the KYC process and their solution utilises 141,000 amounts of gas, which is a little more than our solution. Although the gas utilisation might seem almost equal but their solution neither includes any video call payment transaction

TABLE I
COMPARATIVE ANALYSIS WITH RELATED SOLUTIONS

Solution	User Data storage	Data in Blockchain	Biometric Verification	Gas Used per user
Kasturi et al. [10]	On-chain	User data	No	N/A
Bhaskaran et al. [11]	On-chain	Encrypted user data	No	N/A
Kumar et al. [13]	Off-chain	Verifier's Digital sign, public key	No	N/A
Fugkeaw [4]	Off-chain	Encrypted transaction data	No	N/A
Ostern et al. [14]	Off-chain	KYC Token	No	141000
Ours	Off-chain	Hashed KYC key	Video verification	134631

fees nor subsequent user verification fees. Thus, we can say that our solution provides a cost-efficient method of e-KYC.

VI. CONCLUSION AND FUTURE SCOPE

Our proposed solution presents an e-KYC platform for users to register and complete their video KYC. After successful verification and ether payment, they receive a KYC key. This KYC key is the only thing the user must submit to a bank or financial institution to verify and register himself. Per our solution, the user's sensitive details and documents are not sent to the Financial Institutions. Additionally, even the administrators do not know the user's KYC Key, which ensures the user's privacy. Moreover, the FIs can verify whether the user is legitimate by verifying the KYC key using the smart contract. All the KYC key hashes are stored in the platform's database. The video KYC feature helps in avoiding any potential attempt of impersonation.

To make the user experience pleasant, we have tried to minimise the waiting time and video KYC fees. The Ether payment takes very little time to complete, and so does the video KYC process.

As a future task, we may try to deploy our solution on Ethereum Mainnet instead of Testnet. Also, we can look to further reduce the gas utilisation in our solution by writing optimal smart contracts. Exploring other blockchains can also be considered.

REFERENCES

[1] D. Malhotra, P. Saini, and A. K. Singh, "How blockchain can automate kyc: systematic review," *Wireless Personal Communications*, vol. 122, no. 2, pp. 1987–2021, 2022.

[2] "KYC compliance for banks: Addressing the cost," https://resources.fenergo.com/blogs/kyc-compliance-for-banks-addressing-the-cost, 2023.

[3] "Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity," https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html, 2016.

[4] S. Fugkeaw, "Enabling trust and privacy-preserving e-kyc system using blockchain," *IEEE Access*, vol. 10, pp. 49 028–49 039, 2022.

[5] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, no. 7, p. 103553, 2022.

[6] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized business review*, 2008.

[7] H. Huang, W. Kong, S. Zhou, Z. Zheng, and S. Guo, "A survey of state-of-the-art on blockchains: Theories, modelings, and tools," *ACM Computing Surveys (CSUR)*, vol. 54, no. 2, pp. 1–42, 2021.

[8] V. Buterin *et al.*, "A next-generation smart contract and decentralized application platform," *white paper*, vol. 3, no. 37, pp. 2–1, 2014.

[9] J. Kolb, M. AbdelBaky, R. H. Katz, and D. E. Culler, "Core concepts, challenges, and future directions in blockchain: A centralized tutorial," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1–39, 2020.

[10] V. Pachaiyappan and R. Kasturi, "block chain technology (dlt technique) for kyc in fintech domain: a survey," *Int J Pure Appl Math*.

[11] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna *et al.*, "Double-blind consent-driven data sharing on blockchain," in *2018 IEEE international conference on cloud engineering (IC2E)*. IEEE, 2018, pp. 385–391.

[12] "GDPR Article 17: Right to erasure ('right to be forgotten')," https://gdpr.eu/article-17-right-to-be-forgotten/.

[13] M. Kumar, P. A. Nikhil, and P. Anand, "A blockchain based approach for an efficient secure kyc process with data sovereignty," *Int J Sci Technol Res*, vol. 9, pp. 3403–3407, 2020.

[14] N. K. Ostern and J. Riedel, "Know-your-customer (kyc) requirements for initial coin offerings," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 551–567, 2021.

[15] P. Pauwels, "zkkyc: A solution concept for kyc without knowing your customer, leveraging self-sovereign identity and zero-knowledge proofs," *Cryptology ePrint Archive*, 2021.

[16] D. Rathee, G. V. Policharla, T. Xie, R. Cottone, and D. Song, "Zebra: Snark-based anonymous credentials for practical, private and accountable on-chain access control," Cryptology ePrint Archive, Paper 2022/1286, 2022, https://eprint.iacr.org/2022/1286. [Online]. Available: https://eprint.iacr.org/2022/1286