Quest Journals
Journal of Software Engineering and Simulation
Volume 10 ~ Issue 5 (2024) pp: 45-51
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Kyc through Blockchain

Prince Mohobia, Dr. P.M. Chaudhari, Harsh Sakhare,
Najim Sheikh, Ramin Singh, Devanshu Bhajbhuje
Dept. of Computer Science and Engineering, Priyadarshini College of Engineering, Nagpur

Abstract- *Know Your Customer (KYC) process plays a critical role in helping every bank verify the identity of its customers. Banks must conduct KYC checks to prevent criminals using them to commit crimes such as drug trafficking and terrorism. Current manual KYC processes are insecure, slow, and outdated. E-KYC allows users to quickly complete the recruitment process without leaving their homes. Using blockchain-based KYC verification, these limitations can be eliminated as blockchain provides features such as decentralization, transferability, and security. Governments around the world are using electronic KYC systems to make this task easier and more transparent. Governments around the world are rapidly implementing electronic KYC systems to expedite and improve transparency in this critical activity. This document provides access to unique trust based on a self-governing model that enhances customer privacy, has regulatory authority and helps banks improve the reliability and accuracy of customer data. Presents a management system. Reduce customer acquisition costs. This article aims to offer a solution to this problem. Our solution uses blockchain to perform one-time KYC verification and eliminate multiple checks to ensure database security. Financial institutions on the blockchain network can access a user's KYC information only with the user's permission.*

Index Terms- *Blockchain, KYC Verification, Ethereum Chain, Server, Client*

R*eceived 08 May, 2024;* ***R****evised 18 May, 2024;* ***A****ccepted 20 May, 2024 © The author(s) 2024.*
P*ublished with open access at* ***www.questjournals.org***

I. INTRODUCTION

KYC (Know Your Customer) process is a vital component in a bank's arsenal, dedicated to the critical role of certifying the identities of its clients. This procedure is critical in combating criminal activities such as drug trafficking and terrorism, since it ensures that financial institutions remain watchful gatekeepers in the fight against illegal operations. However, traditional manual KYC methods have been plagued by issues of vulnerability, sluggishness, and obsolescence, rendering them inappropriate for modern-day challenges.

KYCs collect and exchange data on a daily basis between different organizations, enterprises and other agencies. Typically, data is transmitted through multiple intermediaries that use different communication protocols, APIs, and management systems. This also applies to people who verify and certify information, as well as give permission for some operations. As a result, this architecture inevitably creates many errors, inconsistencies and critical vulnerabilities for unauthorized access. A system based on a decentralized distribution register eliminates the risk of monopolizing control. The immutability of the data recorded in the blockchain and in the open source code allows you to make sure that the rules of the game for all participants are the same and there are no «black entries» in the program.

Blockchain platform to implement Blockchain based KYC verification system. Ethereum was developed in 2013 by Vitalik Buterin. Ethereum is a first Blockchain which has introduced concept of smart contract with which distributed apps can be created on top of the Blockchain. Ethereum could be used to develop different applications on top of it and is not limited as just payment alternative. Our proposed system not only solves the problem of doing KYC but can also provide assistance to verify attested documents as required by other non-banking organizations.

II. METHODOLOGY

1. User data collection

Personal data will be collected by individual participants (banks, government agencies, companies or users themselves) and stored in a decentralized network. Access to the data will be provided directly by authorized users or third parties.

In this case it will be possible to provide access not to the user's personal data, but to a special identification card, which certifies the successful completion of the procedure. In this way, personal data will be protected and third parties will be able to verify the identity of their client.

2. Automation and standardization

The routing of KYC workflows can be coded into smart contracts and standardized across all industries. In such an ecosystem, data exchange will be as reliable as monetary transactions in bitcoin or ethereum cryptocurrency payment systems.

3. Risk decentralisation

A system based on a decentralized distribution register eliminates the risk of monopolizing control. The immutability of the data recorded in the blockchain and in the open-source code allows you to make sure that the rules of the game for all participants are the same and there are no «black entries» in the program. Automation and standardization of basic processes limits and controls the degree of human involvement (blockchain records who did what and this information cannot be deleted).

4. Centralized repositories

In the current client-server storage system, based on centralized repositories, where all ecosystem participants are forced to continuously share user personal information, there is a strong tendency to obtain poor quality data (errors, inaccuracies, inconsistencies, false data, etc.). And this trend increases with the number of participants.

This is a direct consequence of the lack of uniform industry standards, as well as the fact that banks, companies, emerging companies, government agencies and KYC service providers use different approaches to data storage and transmission, different communication protocols, API, platform and data management systems.

What's going on with the blockchain. The CMC solution based on a decentralized distribution register will create a system in which data will be stored on a single medium accessible to all platforms. This will automatically standardize the industry and make most interactions between participants unnecessary – there is no point in sharing information if it is all written on the blockchain that everyone has access to.

5. Elimination of secondary verification or cross-checking.

The ordinary person (user) does not control anything. This does not affect what documents he must submit to the KYC procedures, and he does not really know anything about how his personal data will be processed. In addition, banks, companies, and CACs also lose control of the process once the data is shared with other participants. The current system was opaque and beyond any control.

Combining an open source platform, which is itself the source of truth, with smart contracts allows you to build a relationship where all participants know the rules of the game and all participants are confident that no one can break or circumvent those rules.

6. Warning of suspicious activity

With distributed ledgers and smart contracts, the KYC process is easily regulated and controlled by all parties. Any change or update to client data will be tracked by the system, and if anyone breaks the rules, it will be known to all parties.

7. Regulatory Compliance Assessment

Understand the legal and regulatory requirements related to KYC in your jurisdiction or industry. Ensure that your blockchain-based KYC solution complies with these regulations.

8. Technology Stack Selection

Choose the appropriate blockchain platform (e.g., Ethereum, Hyperledger, Corda) and associated technologies for your KYC system. Consider factors like security, scalability, and smart contract capabilities.

9. Reduced Fraud and Identity Theft

Using blockchain for KYC verification improves identity verification while decreasing the risk of fraudulent activities like identity theft and document forgery.

10. Compliance with Regulations
Blockchain-based KYC systems can be designed to automatically check for AML (Anti-Money Laundering) and CTF (Counter-Terrorism Financing) compliance, lowering the risk of regulatory violations.

11. Transparency and auditability
Because blockchain is decentralized and transparent, it allows for real-time monitoring and auditing of KYC activities. This can help organizations demonstrate compliance to regulators and improve accountability.

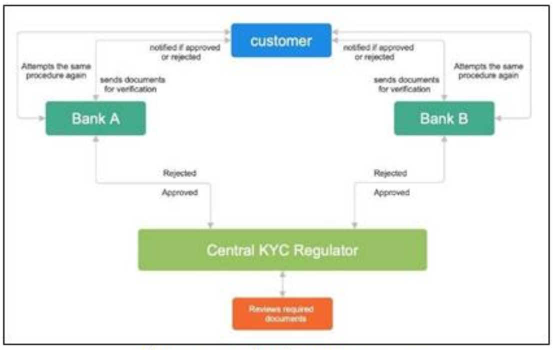

customer
notified if approved or rejected
notified if approved or rejected
Attempts the same procedure again
sends documents for verification
sends documents for verification
Attempts the same procedure again
Bank A
Bank B
Rejected
Approved
Rejected
Approved
Central KYC Regulator
Reviews required documents

Fig.2.1 Standard KYC Process

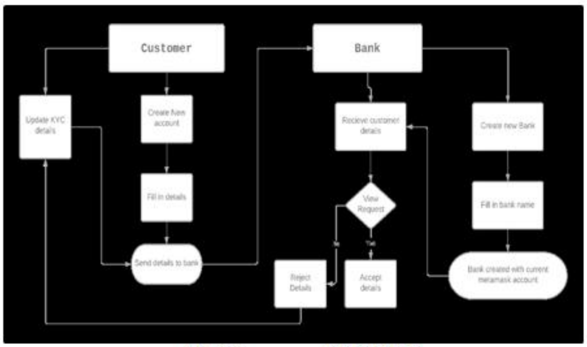


Fig.2.2 Simplified

12. Customer Empowerment
Customers gain more control over their personal data and can choose who has access to it. This gives them the ability to participate in the KYC process and increases trust in the system.

13. Interoperability
Blockchain-based KYC systems can facilitate data sharing and interoperability between different organizations, such as banks and government agencies, streamlining the verification process. While initial implementations may begin on private or local blockchain networks, the architecture can be designed to allow for an easy transition to public blockchains such as Ethereum, allowing for increased scalability and broader adoption.

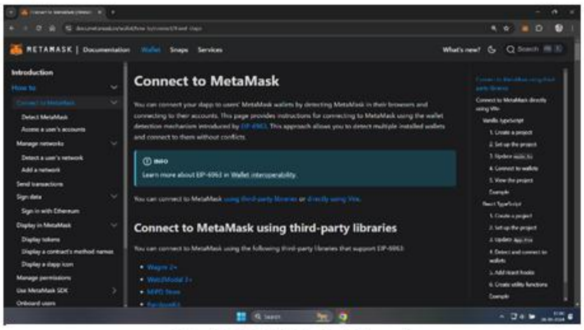
14. Global Accessibility
Blockchain-based KYC solutions can be accessed from anywhere in the world via an internet connection, making the process accessible to users across borders. Reduced Paperwork: By reducing paperwork and manual data entry, the KYC process becomes eco-friendlier and more efficient.

III. RESULT

The benefits of the proposed system include Better governance of data as Data alterations can be tracked and monitored, direct access to the KYC data saving huge amount of time and lastly storage space is effectively utilized as inspite of saving the complete file on Blockchain, only hash is stored over it. Two types of tokens can be sold:

1. Protocol tokens (i.e. useful tokens). The platforms generate them as «digital coupons», the acquisition of which allows investors to access project functions in the future. Such tokens have no property attribute and are free to trade on the market for profit
2. Security Tokens (Tokens) Unlike protocol tokens, these tokens are registered digital securities.

Many ICOs today do not offer such coins because transactions with them require compliance with a number of laws. But other developers see a great future in working with tokenized assets. This means that the initial generation of tokens will already imply some form of investment income.



Connect to MetaMask

You can connect your dapp to users' MetaMask wallets by detecting MetaMask in their browsers and connecting to their accounts. This page provides instructions for connecting to MetaMask using the wallet detection mechanism introduced by EIP-6963. This approach allows you to detect multiple installed wallets and connect to them without conflicts.

ⓘ INFO
Learn more about EIP-6963 in Wallet interoperability.

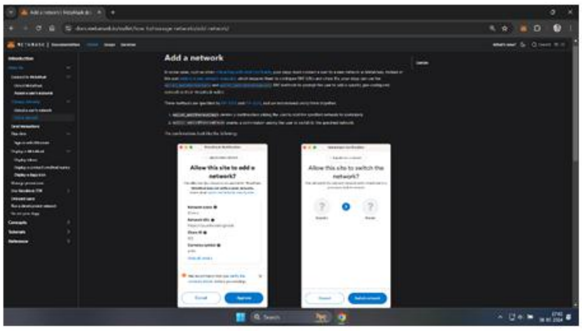
You can connect to MetaMask using third-party libraries or directly using Vite.

Connect to MetaMask using third-party libraries

You can connect to MetaMask using the following third-party libraries that support EIP-6963:

- Wagmi 2+
- Web3Modal 3+
- MIPD Store
- RainbowKit

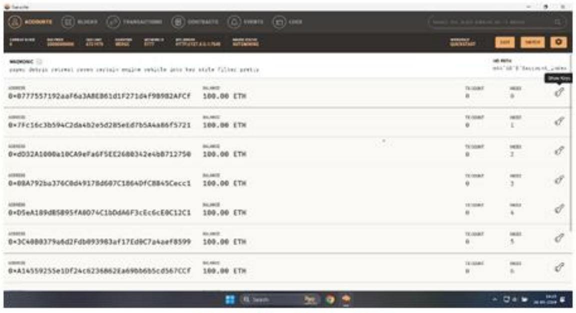
Fig.3.1 MetaMask Manual



Add a network

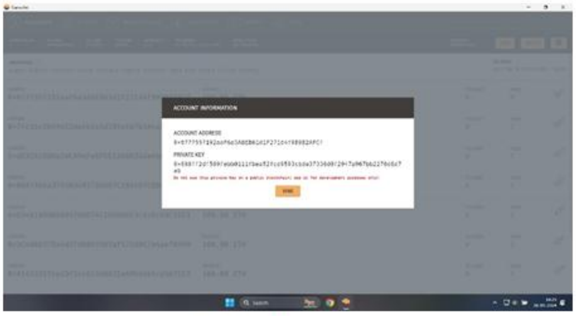
Allow this site to add a network?
Allow this site to switch the network?
Cancel
Approve
Switch network

Fig.3.2 MetaMask Manual



```
ADDRESS                                      BALANCE
0x0777557192aaF6a3A8E861d1F271d4f98982AFCf   100.00 ETH
0x7Fc16c3b594C2da4b2e5d285eEd7b5A4a86f5721   100.00 ETH
0xdD32A1000a10CA9eFa6F5EE2680342e4b0712750   100.00 ETH
0x08A792ba376C0d49178d607C1864DfC8845Cecc1   100.00 ETH
0xD5eA189d85895fA8074C1bDdA6F3cEc6cE0C12C1   100.00 ETH
0x3C4080379a6d2Fdb093983af17Ed0C7a4aef8599   100.00 ETH
0xA14559255e1Df24c6236862Ea69bb6b5cd567CCf   100.00 ETH
```

Fig.3.3 Ethereum Network

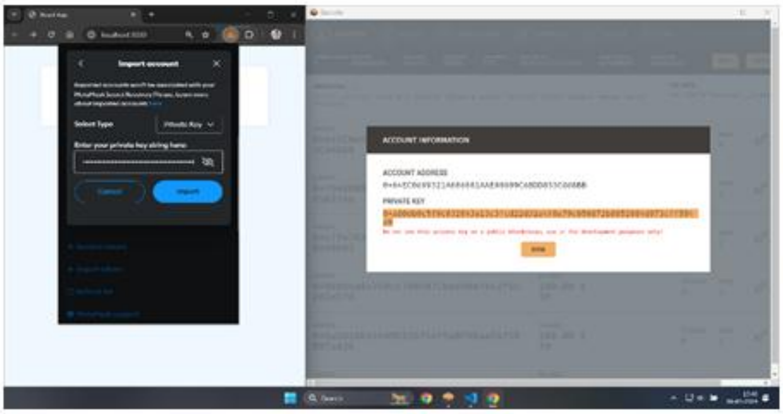


ACCOUNT INFORMATION

ACCOUNT ADDRESS
0x0777557192aaF6a3A8E861d1F271d4f98982AFCf

PRIVATE KEY
[illegible]

Fig.3.4 Unique Id



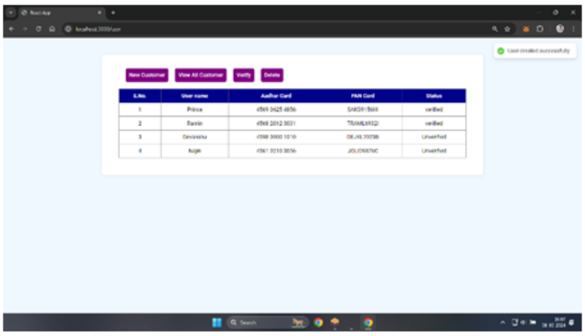
Import account

ACCOUNT INFORMATION

ACCOUNT ADDRESS
[illegible]

PRIVATE KEY
[illegible]

Fig.3.7 Importing Private key



S.No.	User name	Aadhar Card	PAN Card	Status
1	Prince	4569 3425 4856	SAKD91/5688	verified
2	Ramin	4566 2012 9031	TRAMLM92I	verified
3	Devanshu	4588 3000 1010	DEJKL7073B	Unverified
4	Nujje	4561 3210 3056	JOLJD6876C	Unverified

Fig.3.9 User Created Successfully

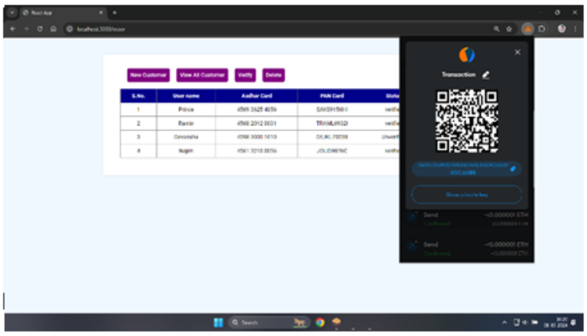


Fig.3.10 Verified User

IV. RELATED WORK

Bharti Pralhad Rankhambe proposed a method based on distributed ledger technology that can significantly reduce the overall KYC (Know Your Customer) expenses for banks while working with a regulatory authority. This system can eliminate redundant tasks performed by different financial institutions, which enhances effectiveness, transparency and reduces costs. By integrating customer records into the bank database, the proposed system removes the need for middlemen, thereby increasing customer satisfaction. Furthermore, this approach optimizes data storing, updating, sharing, and accessing processes, enhances security, transparency, and privacy, and ensures that all customer records are easily accessible. It does this by utilizing the DLT, The proposed approach to blockchain technology involves cryptography and a consensus mechanism. This approach enhances customer ownership and improves the customer experience. In a consortium network, each institution acting as a peer can only verify the details and not modify them. Furthermore, although internal operations within each business are dispersed, they appear as one cohesive unit from an external perspective.

The consortium blockchain approach proposed by Ashok Kumar Yadav allows any firm to request data by submitting a service proof of identity. Each organization is assigned an identity to maintain record-keeping. By saving the data online on the blockchain, we can eliminate maintenance costs associated with duplicate information and significantly reduce paperwork.

E. Sai Vikas Reddy proposed an approach based on blockchain technology that lowers the expense of the standard KYC verification process. Irrespective of the number of institutions a customer registers with, the verification procedure is conducted only once for each customer, enhancing transparency by securely communicating the outcomes via DLT. In this scenario, the customer solely registers with one financial institution, thereby reducing the need to register with different financial institutions and eliminating the duplication of effort. With this approach, ethereum is used for proof of concept (POC). This approach improves customer satisfaction, boosts transparency, and lowers overhead costs.

Syed Azhar Hussain and other researchers proposed a selfgoverned, distributed approach called Know-Your-Consumer (DKYC). This approach enhances customer privacy by requiring prior permission. It also helps regulators oversee the process and allows banks to use reliable and valid customer details. Additionally, it lowers the cost of customer acquisition. The scoring system is constructed via the Proof of Importance consensus algorithm. This enables current conventional identity establishments, such as Civilian Identities, Regulators, National Security Numbers, and other private sector identity stores, to participate and be member of the network to determine the scoring. Prof. A. L. Maind proposed a blockchain-based approach which eliminates middlemen and enables one-time KYC for users. Users have access to the data at any time, from any location, for a variety of purposes. Blockchain technology is secure because it is decentralized, transparent, and doesn't involve third parties. It also processes transactions faster. In the paper "KYC Verification Using Blockchain" by Sunitha N.V., P. Ashwini, Sandhya, Shriraksha Bhat, and Tushara Sasi, a new e-KYC scheme called e-KYC Trust Block is introduced. This scheme uses blockchain technology and the ciphertext policy attribute-based encryption (CP-ABE) method, along with client consent enforcement, to ensure trust, security, and privacy compliance. We also use attribute-based encryption to protect sensitive transactions stored in the blockchain and allow for fine-grained access. Our experiments show that our system is efficient and scalable in practice.

In this paper, Jose Parra Moyano, Omri Ross, and Ioan Buciu propose a new system to improve the Know Your Customer (KYC) process. The current KYC process is outdated and costs banks up to USD 500 million each year. The authors suggest using Distributed Ledger Technology (DLT) to decrease costs and enhance the customer experience. In the proposed system, the core KYC verification process is only done once, regardless of how many financial institutions the customer plans to work with. Customers can securely share their verification results with any institution through DLT. This system improves efficiency, reduces costs, increases transparency, and enhances the customer experience.

The title of the first paper is "Enabling Trust and PrivacyPreserving e-KYC System using Blockchain" by Somchart Fugkeaw. The paper discusses how banks use electronic know your customer (eKYC) systems on the cloud to verify customer identity data. The security and privacy of e-KYC documents stored in the cloud are important. Existing e-KYC platforms use strong authentication and traditional encryption, but this approach has encryption dependency and communication and key management overheads.

The title of the second paper is "Putting smart contracts into action for Know Your Customer (KYC) in a decentralized architecture that prioritizes privacy" by Nikolaos Kapsoulis. The paper discusses how enterprise blockchain solutions can protect user privacy in the context of Know Your Customer (KYC). The proposed solution involves using a decentralized schema with two types of smart contracts. Users register and upload their KYC information in a public KYC smart contract using exploited IPFS storage. Actions are recorded as blockchain transactions on the permissioned blockchain of Alastria Network. An admin user can approve or reject the validity and expiration date of the user's KYC documents through the public KYC smart contract.

David Chaum, a cryptographer, suggested a protocol like blockchain in his 1982 dissertation called "Computer Systems Established, Maintained, and Trusted by Mutually Suspicious
Groups."

In 2008, Satoshi Nakamoto came up with the idea for the first decentralized blockchain. Nakamoto made improvements to the design by using a method like Hash cash to timestamp blocks. This method didn't need a trusted party to sign the blocks. Nakamoto also added a difficulty parameter to keep the rate of adding blocks stable. The design was then put into action by Nakamoto in the following year. It became a key part of the cryptocurrency bitcoin. The blockchain serves as the public ledger for all transactions on the network.

Satoshi Nakamoto created the first decentralized blockchain in 2008. Nakamoto improved the design by using a Hashcash-like method to timestamp blocks without needing a trusted party's signature. Nakamoto also introduced a difficulty parameter to control how quickly blocks are added to the chain. The following year, Nakamoto implemented the design as a core part of the cryptocurrency bitcoin. The blockchain serves as the public ledger for all transactions on the network.Satoshi Nakamoto used the words "block" and "chain" separately in his original paper. However, by 2016, these words were combined into the single word "blockchain" and became popular.

Ethereum is a blockchain that is decentralized and has smart contract functionality. The platform's native cryptocurrency is called Ether. Ether is the second largest cryptocurrency after bitcoin in terms of market capitalization. The software is open source.

V. CONCLUSION

This paper suggests using blockchain for KYC verification as a way to cut costs and streamline the process. The system verifies your identity once, and banks can access it through the blockchain network. By maintaining a secure database on the blockchain, information will be more secure and tamper-proof. From the research data, we found that this program is the best compared to other programs because it solves the problem of removing KYC information.. The blockchain architecture integrates data from various providers into a protected database, removing the need for third-party authentication.. It makes it possible to create a system where users only need to go through the KYC process once to verify themselves. The technology allows financial institutions to use an honest ledger to verify customers' KYC processes, eliminating the need for reverse verification. It makes it possible to create a system where users only need to go through the KYC process once to verify themselves. The technology allows financial institutions to use an honest ledger to verify customers' KYC processes, eliminating the need for reverse verification.

Technology Used

1. Frontend – React JS
2. Backend –

- Ethereum Development Network (Ganache)
- Web3.js
- Truffle

REFERENCES

[1]. What is KYC: how to do KYC online: different types of KYC: Paisabazaar. www.paisabazaar.com/ Aadhar-

[2]. card/what-is-kyc/. retrieved on June 4, 2022

[3]. Electronic know-your-customer (e-KYC) exposure draft— Bank Negara Malaysia

[4]. Jarra-Moyano, T Thoroddsen, and O Ross (2018) KYC system that is optimized and dynamic, based on blockchain technology. 3248913 is available at SSRN.

[5]. Hanbar, H., Shukla, V., Vyjayanthi, C., and Modi, C. (2019)) Smart contracts and distributed ledger technology are being used to optimize Kyc.

[6]. A systematic literature review of blockchain-based e-KYC systems1: This article, published in 2023, provides a comprehensive analysis of the existing researches at the intersection of e-KYC and blockchain. It also identifies the limitations and future directions of this domain.

[7]. How Blockchain Can Automate KYC: Systematic Review2: This article, published in 2021, conducts a PRISMA guided systematic review on the blockchain technology for KYC and its application areas from 2014 onwards. It also presents the blockchain platforms such as Ethereum and Hyperledger along with related case studies.

[8]. What is KYC and How Can KYC on Blockchain Help? This 2022 article explains the concept of KYC and how blockchain can be used to perform KYC with a single click. It also includes a flow diagram that shows how this can be used.

[9]. Blockchain and KYC: This 2018 article introduces the concept of blockchain and KYC and how they can be combined to improve the efficiency, security, and customer experience of the KYC process. It also discusses the key issues and benefits of using blockchain for KYC.

[10]. Bangladesh Financial Intelligence Unit: electronic know your customer (e-KYC) guidelines. https://www.bb.org.bd/mediaroom/circulars/aml/jan082020bfiu25.pdf. Date accessed: October 13, 2021