IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain Technology and IPFS based Secure and Transparent KYC for Banking System

Gyanendra Kumar Hansh[1], *Sambhav Agarwal* [2]

[1]*M. Tech Scholar, Dept. of Computer Science & Engineering, S R Institute of Management & Technology (AKTU), Lucknow, India*

[2] *Assistant Professor, Dept. of CSE,* S R Institute *of* Management & *Technology, Lucknow, India*

***Abstract*— Know Your Customer (KYC) is a critical process in the banking sector aimed at verifying the identity of clients to prevent fraud, money laundering, and other financial crimes. However, traditional KYC systems are often centralized, prone to data breaches, and involve repetitive procedures across multiple institutions. This paper proposes a secure and transparent KYC framework by integrating Blockchain Technology and InterPlanetary File System (IPFS). The decentralized nature of blockchain ensures immutability, auditability, and trustless verification, while IPFS provides a distributed file storage system to securely handle large KYC documents off-chain. By leveraging smart contracts, the system enables seamless access control and data sharing among authorized banks without duplicating the verification process. The proposed model enhances data integrity, reduces operational costs, and empowers users with control over their personal information, thus revolutionizing KYC in the banking ecosystem.**

Keywords: Blockchain, IPFS, Know Your Customer (KYC), Banking Security, Decentralized Identity, Data Privacy, Smart Contracts, Financial Technology, Distributed Ledger, Secure Data Sharing.

1. INTRODUCTION

The Know Your Customer (KYC) process is a fundamental component of the banking system, designed to verify the identity of customers and assess potential risks of illegal intentions such as money laundering or terrorist financing. While necessary, traditional KYC procedures are plagued by inefficiencies, duplication of efforts, high costs, and vulnerability to data breaches due to their centralized nature [1], [2].

In recent years, Blockchain Technology has emerged as a transformative solution for improving transparency, trust, and security in various sectors, including finance [3]. With its decentralized ledger structure, blockchain enables tamper-proof record-keeping and auditability, making it well-suited for handling sensitive identity data in KYC procedures [4]. Smart contracts, an integral feature of blockchain platforms, facilitate automatic enforcement of rules and permissions without the need for intermediaries, enhancing both efficiency and trustworthiness [5].

Complementing blockchain, the InterPlanetary File System (IPFS) serves as a distributed storage network that ensures secure, scalable, and persistent access to large volumes of off-chain data such as scanned documents and biometric records [6]. By integrating IPFS with blockchain, sensitive KYC documents can be securely stored off-chain while retaining cryptographic references on-chain, preserving both privacy and integrity [7].

This paper proposes a novel framework that combines blockchain and IPFS to develop a secure, transparent, and user-centric KYC process for the banking industry. The system ensures data privacy, reduces redundant verification efforts, and streamlines onboarding processes across multiple financial institutions. Through this approach, the banking sector can move towards a more collaborative and trustworthy identity verification ecosystem.

Due to the high cost, the uses' KYC documents cannot be uploaded to the Blockchain network. As a result, this paper proposes the use of the International Planetary File System (IPFS) to share KYC documents, which are then shared over the Blockchain network. The IPFS is a distributed shared document framework that aims to link all registering computers to a similar file system. The user can save their hash and transaction history to the IPFS network and then send it to the Blockchain network when needed. The blockchain's data will be much smaller as a result of this procedure.

In this research paper section I contains the introduction, section II contains the literature review details, section III contains the details of problem statement, section IV describe the methodology, section V provide details of results, section VI provide the conclusion of this research paper.

2. RELATED WORK

The traditional Know Your Customer (KYC) process in banking is often centralized, repetitive, and prone to inefficiencies and data security issues. To address these challenges, researchers have investigated the use of decentralized technologies like Blockchain and InterPlanetary File System (IPFS) for creating secure, transparent, and privacy-preserving KYC frameworks.

Parra-Moyano and Ross [1] were among the early proponents of blockchain for KYC, proposing a decentralized system

where users could share their verified identity information with multiple banks, reducing the need for repeated verifications. Their model allowed customers to retain control over their personal data while reducing costs for financial institutions. Similarly, Rannenberg et al. [2] explored blockchain's ability to improve data sovereignty in financial services, emphasizing the advantages of immutable audit trails and distributed trust.

A comprehensive review by Hannan et al. [3] categorized blockchain-based e-KYC solutions into architecture-focused and privacy-focused models. Their analysis of over 30 research papers concluded that most solutions aim to balance security, user control, and scalability, though practical deployment challenges persist, including legal and regulatory concerns.

To complement blockchain's transactional integrity, researchers have integrated IPFS to manage and store large KYC documents off-chain. Mamun et al. [4] proposed a hybrid model using Ethereum blockchain for storing document hashes and IPFS for storing the actual documents. Their system provided end-to-end data security, reduced storage overhead on the blockchain, and improved interoperability among financial institutions.

Singhal et al. [5] introduced the Smart KYC framework using Blockchain and IPFS, which includes modules for customer onboarding, document notarization, and third-party verification. Their model demonstrated increased system efficiency, as verified documents could be reused securely across different banks, eliminating redundancy.

Moreover, Kumar et al. [6] addressed data sharing challenges by proposing a smart contract-driven access control mechanism. Only authorized parties can access the KYC data stored via IPFS, enhancing both data privacy and regulatory compliance. However, they noted challenges around key management, latency in IPFS retrieval, and ensuring cross-jurisdictional data protection standards.

Despite the advantages, scalability and regulatory acceptance remain key barriers. Several researchers, including Ferdous et al. [7], emphasized the need for standardized KYC frameworks and regulatory sandboxes for testing blockchain-IPFS-based implementations under real-world constraints.

Table 1. Literature Review Table: Blockchain and IPFS-Based Secure KYC Systems

Author(s) & Year	Contribution / Key Findings
Parra-Moyano & Ross (2017)	Proposed a blockchain-based decentralized KYC system enabling data sharing and reducing redundancy.
Hannan et al. (2023)	Systematic review of blockchain-based e-KYC models; discussed architecture and privacy concerns.
Mamun et al. (2020)	Integrated Ethereum and IPFS to securely store KYC data; emphasized transparency and decentralization.
Singhal et al. (2020)	Developed 'Smart KYC' system using smart contracts and IPFS; introduced modular verification.
Kumar et al. (2021)	Proposed access control mechanism using IPFS for encrypted KYC document storage.
Ferdous et al. (2021)	Designed a blockchain-based secure KYC framework; stressed compliance with banking regulations.
Zyskind et al. (2015)	Early proposal for decentralized personal data management system using blockchain.
Ali et al. (2021)	Reviewed blockchain-IPFS systems for digital identity and KYC applications.
Tithal et al. (2020)	Developed a prototype for blockchain-based KYC using Hyperledger and IPFS.
Upadhyay et al. (2021)	Proposed multi-bank shared KYC model using smart contracts and IPFS.
Narayanan et al. (2016)	Provided foundational knowledge on blockchain relevant to secure data systems.
Jain & Mehta (2019)	Identified inefficiencies in traditional KYC and discussed blockchain as a potential remedy.
Maesa & Mori (2020)	Investigated privacy-preserving techniques in blockchain-based identity management.
Bhargava et al. (2020)	Proposed lightweight blockchain model for faster KYC verification.
Sharma & Kaul (2021)	Discussed benefits and limitations of decentralized identity systems in banking.
Benet (2014)	Introduced IPFS as a peer-to-peer distributed file system; foundational for off-chain storage.
Christidis & Devetsikiotis (2016)	Highlighted the role of smart contracts in automating trust and verification.
Patil et al. (2020)	Designed a blockchain-IPFS model that ensures auditability and traceability of KYC.
Sayeed & Marco-Gisbert (2020)	Evaluated security and scalability trade-offs in blockchain-based KYC.
Rannenberg et al. (2019)	Emphasized data sovereignty and legal challenges in decentralized identity systems.

3. PROBLEM STATEMENTS

we planned to reduce the progressive cost of KYC process by tackling the cost problem of KYC from financial institution perspective by using blockchain. currently, several third-party data providers and external validation agencies offer data and interfaces to extract the required customer information. However, banks struggle to integrate this data to obtain a consolidated view of the customers. This has led to increasing instances of banks' failure to comply with regulatory requirements, resulting in huge penalties and

reputational damage. : post due diligence, banks need to digitize data in the documents to feed it into the repositories. This is an expensive exercise, as it uses advanced technology platforms. The KYC landscape is constantly facing new regulation across different jurisdictions. Therefore, KYC utilities need to keep updating their guidelines. This increases the need for banks to improve their data collection mechanisms for effective risk management and timely compliance. banks do not have a single, unified KYC system for its various lines of business like wealth management, asset management, and brokerage. Maintaining these multiple systems and integrating different interfaces puts banks under immense pressure and adds costs. This paper solves the problem in current KYC process based on three assumptions: : First, a group of financial institutions, working in the same country and therefore obliged to respect the same KYC regulations, agrees on the standards for granting core KYC verification to a customer. Second, all the financial institutions that collaborate in the system agree on the average costs of conducting a core KYC verification process. This cost might of course depend on the complexity of each individual customer, based on predetermined parameters (e.g., client size, volume of documents exchanged, etc.). Third, the national regulator maintains the system and approves financial institutions to work with the system in order to conduct a more efficient and transparent KYC verification process. These three assumptions are necessary to ensure a correct incentive structure across the participating financial institutions.

4. METHODOLOGY

4.1 Blockchain

Blockchain is a purely peer-to-peer version online transaction, where a customer directly sends money to others without the help of a financial organization. All transactions will be hashed to an ongoing proof-of-work chain. Each of this called a block; the running block contains the hash of previous all blocks. Therefore, the whole process is tempered proof, as a single peer cannot add a new block without the proof-of-work . Bitcoin was the first fully decentralized cryptocurrency. While the central purpose of DLT was to create digital money and sending and receiving via the Internet, the technology can also be used to authenticate online document sharing using smart contracts. The smart-contract aims to involve them in properties, which are expensive and controlled in a digital manner.

4.2 IPFS

The InterPlanetary File System (IPFS) is a peer-to- peer(P2P) file-sharing protocol connecting computing devices for sharing/storing files/data. The content is uniquely recognized in the global namespace using the hash code of the file. If the hash code is altered, the data can not be verified which will be identified by IPFS. Besides, IPFS identifies duplication if files with the same content are stored.

4.3 KYC Verification

We considered a scenario in which, in the first phase, a customer went to Bank A to open an account. The customer submitted the account information along with KYC docs to the Bank. The bank then observed the whole information, which, if found correct, will be encrypted using the system's application (a popular encryption tool, gpg4win, and IPFS in our case) which will be available to all banks to share documents with other bank and store a copy to a local database. Afterward, the encrypted file will be stored in the private IPFS network by bank A. Later, the bank will upload the hash value from IPFS, a very small in-memory size, to the Blockchain network. Bank A also keeps a copy of the customer's KYC docs to the local database of it. Finally, Bank A will share the hash value of Blockchain and IPFS to the customer. Later on, the customer can give access to the KYC doc package by just sharing the hash value to any other institution he intended to work with. However, now the customer can go to another bank to open another account. The customer will share his hash value from IPFS, and Blockchain to Bank B. Since Bank B will be granted access to the hash value of the document package by the customer, the Bank will get access to the Blockchain network for the required hash value. Subsequently, the bank will download the encrypted KYC docs from the IPFS network using the hash value retrieved from Blockchain. Lastly, with the help of the private key of the customer, the Bank will retrieve the KYC docs and keeps a copy of KYC docs to the bank's local database. The regulatory bank defined in the proposed solution in the central bank.

5. RESULTS

The proposed system empowers the distribution of encrypted updates to customer KYC data in real-time. It takes up to 7.6 seconds for KYC first-time registration by the customer in the home bank (Bank A) and for Bank B to access the customer KYC data through smart contract takes 8.2 seconds. So, the Hyperledger Fabric KYC system takes (16.8 to 21 second) [25]. While in the traditional KYC system, as per Thomson Reuters survey, it takes 3 to 4 months for a customer to get their onboarding from each bank [2]. Customers have various relationships with several banks and are expected to provide the same data multiple times to different banks. So, duplication of the same activities takes place in the traditional KYC verification process [26]. From the experiment results, it is confirmed that the Hyperledger Fabric KYC system can challenge the inefficiencies arising from duplicated conduct of similar tasks and speed up KYC clearing transfers [27]. The KYC verification process's cost is immense, costing millions of dollars per annum in the traditional KYC process [28]. Corporations are not cautious about reporting KYC changes to the banks regularly in the traditional KYC system [31]. The Hyperledger Fabric KYC system can provide a historical record of all compliance activities and documents pertaining to each customer, and supported by the other studies of [32]. KYC and customer due diligence systems are not normally linked to the traditional KYC system's transaction monitoring systems [33]. The Hyperledger Fabric KYC system can enable customer identifications for fraudulent histories and authorize the reviewing information and documents to detect illegal activities, and supported by the other studies of [34].

Customer approaching two different banks. In the first stage, the customer went to Bank A to provide the Bank with his KYC document for verification. Bank A goes through our proposed system design and provides the customer with a hash value and a personal decryption key. The customer will then go to Bank B and Bank C with these two keys, and both banks will testify the KYC doc in a blink. We used the IPFS network to upload and retrive KYC doc at banks end. Nevertheless, before sharing out KYC docs into the IPFS network, we considered encrypting the file for extra security and reducing file size. Since anyone can access the KYC docs from the IPFS network by just knowing their hash values.

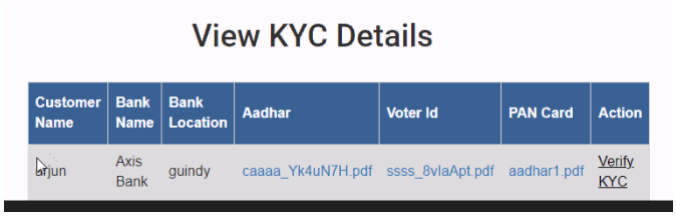

Figure: 1 View KYC details

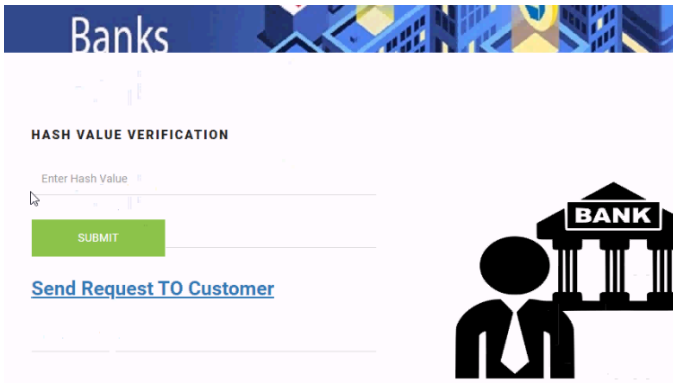

Figure: 2 Hash Value Verification

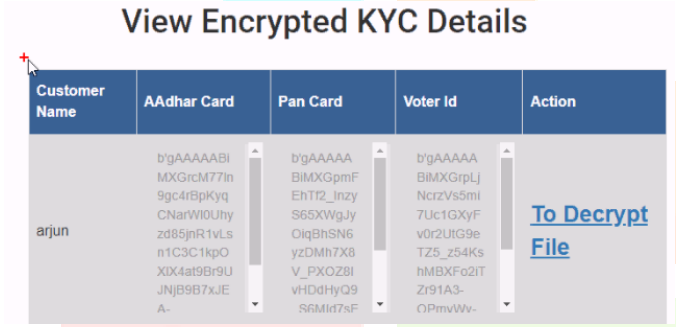

Figure: 3 Encrypted KYC details

6. CONCLUSION

The integration of Blockchain and InterPlanetary File System (IPFS) presents a transformative approach to addressing the inefficiencies and security challenges inherent in traditional Know Your Customer (KYC) processes within the banking sector. By leveraging the immutability, decentralization, and transparency of blockchain along with the distributed, tamper-resistant storage of IPFS, banking institutions can achieve a secure, efficient, and privacy-preserving KYC framework.

This review highlights how various studies have demonstrated that blockchain-based KYC systems significantly reduce data duplication, enhance user control over personal information, and foster trust between financial entities. Additionally, incorporating IPFS alleviates the burden of storing large documents on-chain while ensuring high availability and security. Smart contracts further automate verification processes, improving efficiency and reducing operational costs.

Despite these advantages, real-world deployment still faces challenges, such as interoperability, regulatory acceptance, key management, and scalability. Therefore, future research should focus on developing standardized protocols, enhancing compliance mechanisms, and conducting large-scale pilot implementations.

Ultimately, blockchain and IPFS-based KYC systems represent a promising leap toward a more transparent, secure, and user-centric digital banking infrastructure, aligning well with the vision of decentralized finance (DeFi) and modern data governance principles.

REFERENCE

[1] J. Parra-Moyano and O. Ross, “KYC Optimization Using Distributed Ledger Technology,” Business & Information Systems Engineering, vol. 59, no. 6, pp. 411–423, 2017.

[2] K. Rannenberg, C. Thum, M. Hansen, and D. Slamanig, “Enhancing Identity and Access Management with Blockchain and Smart Contracts,” in Proceedings of the IEEE Security and Privacy Workshops, San Francisco, CA, USA, 2019.

[3] M. A. Hannan, M. A. Shahriar, M. S. Ferdous, M. J. M. Chowdhury, and M. S. Rahman, “A Systematic Literature Review of Blockchain-Based e-KYC Systems,” Computing, vol. 105, no. 4, pp. 935–959, 2023. [Online]. Available: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10100622/

[4] A. A. Mamun, M. S. Kaiser, and M. A. Yousuf, “Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology,” in IEEE Region 10 Symposium (TENSYMP), Dhaka, Bangladesh, pp. 1–6, 2020.

[5] N. Singhal, M. K. Sharma, S. S. Samant, P. Goswami, and Y. A. Reddy, “Smart KYC Using Blockchain and IPFS,” in Advances in Cybernetics, Cognition, and Machine Learning for Communication Technologies, Springer, 2020, pp. 77–84.

[6] A. Kumar, R. Rajput, and S. Tyagi, “Blockchain-Based Access Control Mechanism for KYC Data Sharing Using IPFS,” Journal of Information Security and Applications, vol. 58, p. 102742, 2021.

[7] M. S. Ferdous, M. A. Hossain, and R. Khokhar, “A Framework for Blockchain-Based Secure KYC in Banking,” Information, vol. 12, no. 8, p. 323, 2021.

[8] W. Shbair, M. Steichen, and J. François, "Blockchain orchestration and experimentation framework: A case study of KYC," in *IEEE/IFIP Man2Block 2018-IEEE/IFIP Network Operations and Management Symposium*, 2018.

[9] N. Sundareswaran, S. Sasirekha, I. J. L. Paul, S. Balakrishnan, and G. Swaminathan, "Optimised KYC Blockchain System," in *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, 2020: IEEE, pp. 1-6.

[10] S. Nakamoto, "Re: Bitcoin P2P e-cash paper," *The Cryptography Mailing List*, 2008.

[11] Y. Lootsma, "Blockchain as the newest regtech application—the opportunity to reduce the burden of kyc for financial institutions," *Banking & Financial Services Policy Report*, vol. 36, no. 8, pp. 16-21, 2017.

[12] K. A. Lacey and B. C. George, "Crackdown on money laundering: a comparative analysis of the feasibility and effectiveness of domestic and multilateral policy reforms," *Nw. J. Int'l L. & Bus.*, vol. 23, p. 263, 2002.

[13] R. J. Herring, "BCCI & Barings: Bank Resolutions Complicated by Fraud and Global Corporate Structure," *Systemic Financial Crises: Resolving Large Bank Insolvencies*, pp. 321-345, 2005.

[14] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain," in *2017 IEEE international conference on systems, man, and cybernetics (SMC)*, 2017: IEEE, pp. 2567-2572.

[15] J. Sousa, A. Bessani, and M. Vukolic, "A byzantine fault-tolerant ordering service for the hyperledger fabric blockchain platform," in *2018 48th annual IEEE/IFIP international conference on dependable systems and networks (DSN)*, 2018: IEEE, pp. 51-58.

[16] S. A. Baset, L. Desrosiers, N. Gaur, P. Novotny, A. O'Dowd, and V. Ramakrishna, *Hands-on blockchain with Hyperledger: building decentralized applications with Hyperledger Fabric and composer*. Packt Publishing Ltd, 2018.

[17] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Workshop on distributed cryptocurrencies and consensus ledgers*, 2016, vol. 310, no. 4: Chicago, IL.

[18] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2018: IEEE, pp. 264-276.

[19] B. K. Mohanta, S. S. Panda, and D. Jena, "An overview of smart contract and use cases in blockchain technology," in *2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, 2018: IEEE, pp. 1-4.

[20] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (sok)," in *International conference on principles of security and trust*, 2017: Springer, pp. 164-186.

[21] D. Puthal, N. Malik, S. P. Mohanty, E. Kougianos, and C. Yang, "The blockchain as a decentralized security framework [future directions]," *IEEE Consumer Electronics Magazine*, vol. 7, no. 2, pp. 18-21, 2018.

[22] V. Gramoli, "From blockchain consensus back to Byzantine consensus,"*Future Generation Computer Systems*, vol. 107, pp. 760-769, 2020.

[23] L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[24] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, 2017: IEEE, pp. 1-5.

[25] A. R. Rajput, Q. Li, M. T. Ahvanooey, and I. Masood, "EACMS: Emergency access control management system for personal health record based on blockchain," *IEEE Access*, vol. 7, pp. 84304-84317,
2019.

[26] D. Mulligan, "Know your customer regulations and the international banking system: towards a general self-regulatory regime," *Fordham Int'l LJ*, vol. 22, p. 2324, 1998.

[27] R. Beck, M. Avital, M. Rossi, and J. B. Thatcher, "Blockchain technology in business and information systems research," ed: Springer, 2017.

[28] V. Chang, P. Baudier, H. Zhang, Q. Xu, J. Zhang, and M. Arami, "How Blockchain can impact financial services–The overview, challenges and recommendations from expert interviewees," *Technological Forecasting and Social Change*, vol. 158, p. 120166, 2020.

[29] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen, and V. Weerakkody, "Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis," *Journal of Enterprise Information Management*, 2020.

[30] N. Ullah, W. S. Alnumay, W. M. Al-Rahmi, A. I. Alzahrani, and H. Al- Samarraie, "Modeling Cost Saving and Innovativeness for Blockchain Technology Adoption by Energy Management," *Energies*, vol. 13, no. 18, p. 4783, 2020. [Online]. Available: https://www.mdpi.com/1996-1073/13/18/4783.

[31] B. Viritha, V. Mariappan, and V. Venkatachalapathy, "Combating money laundering by the banks in India: compliance and challenges," *Journal of Investment Compliance*, 2015.

[32] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, vol. 2, no. 1, pp. 1-12, 2016.

[33] N. Mugarura, "Customer due diligence (CDD) mandate and the propensity of its application as a global AML paradigm," *Journal of Money Laundering Control*, 2014.

[34] A. Al Mamun, S. R. Hasan, M. S. Bhuiyan, M. S. Kaiser, and M. A. Yousuf, "Secure and Transparent KYC for Banking System Using IPFS and Blockchain Technology," in *2020 IEEE Region 10 Symposium (TENSYMP)*, 2020: IEEE, pp. 348-351.

[35] P. Voigt and A. Von dem Bussche, "The eu general data protection regulation (gdpr)," *A Practical Guide, 1st Ed., Cham: Springer International Publishing*, vol. 10, p. 3152676, 2017.

[36] E. Prasad, "Central banking in a digital age: Stock-taking and preliminary thoughts," *Hutchins Center on Fiscal & Monetary Policy at Brookings*, 2018