

INDEX:

Page:

<u>DECLARATION</u>	2
<u>CERTIFICATE</u>	3
<u>DATE:</u>	4
<u>Abstract:</u>	5
CHAPTER 1: INTRODUCTION	1
1.1. Importance of Relevance and Applicability	2
1.2. Purpose of the study	3
CHAPTER 2: LITERATURE SURVEY	4
2.1. Current E-KYC practice and Objective	9
2.2. Operational Definition	11
CHAPTER 3: METHODOLOGY AND TECHNOLOGY	13
3.1. Hypothesis	14
3.2. Data	15
3.3. Functional Probabilities	19
CHAPTER 4: CONCLUSION AND FUTURE WORK	22
REFERENCE	24
RESEARCH PAPER	27

DECLARATION

We 24-PJ-IT-27(ARNAV CHAUHAN, HARSH TALWAR, PRATYAKSH GOEL) hereby declare that this submission is our own work and that, to the best of our knowledge and belief, it contains no material previously published or written by another person nor material which to a substantial extent has been accepted for the award of any other degree of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature:

Name: ARNAV CHAUHAN

Roll NO: 2000300130027

Signature:

Name: HARSH TALWAR

Roll NO: 2000300130051

Signature:

Name: PRATYAKSH GOEL

Roll NO: 2100300139003

CERTIFICATE

This is to certify that Project Report entitled “**Blockchain-Based KYC Implementation: Enhancing Identity Verification and Compliance**” which is submitted by 24-PJ-IT-27(ARNAV CHAUHAN, HARSH TALWAR, PRATYAKSH GOEL) in partial fulfillment of the requirement for the award of degree B. Tech. in Department of Information technology of Dr. A.P.J. Abdul Kalam Technical University, Lucknow, is a record of the candidate own work carried out by him under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Date:

Supervisor

ACKNOWLEDGEMENT

It gives us a great sense of pleasure to present the report of the B. Tech Project undertaken during B.Tech. (VIII- Semester) Final Year. We owe special debt of gratitude to for his/her constant support and guidance throughout the course of our work. Her sincerity, thoroughness and perseverance have been a constant source of inspiration for us. It is only her cognizant efforts that our endeavors have seen light of the day.

We also take the opportunity to acknowledge the contribution of Ms. TANYA SHARMA for her full support and assistance during the development of the project.

We also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the department for their kind assistance and cooperation during the development of our project. Last but not the least, we acknowledge our friends for their contribution in the completion of the project.

Signature:

Name: ARNAV CHAUHAN
Roll NO: 2000300130027

Signature:

Name: HARSH TALWAR
Roll NO: 2000300130051

Signature:

Name: PRATYAKSH GOEL
Roll NO: 2100300139003
DATE:

Abstract:

Systems that use blockchain technology to improve the know-your-customer (KYC) process have only been proposed at a conceptual level and all share certain attributes that make their adoption by financial institutions (Fis) very difficult. We propose and program a blockchain-based system that reduces and shares out among the financial institutions that work with a customer the costs of the KYC process and also makes it possible for Fis to dynamically update information related to customers and disseminates this information among participating Fis. Additionally, our system addresses some of the attributes that hinder the adoption of previously proposed solutions by Fis. The result is a programmed, stand-alone solution that can be implemented by Fis to reduce the cost of the KYC process without requiring any central instance to store the customer's data, and in which Fis share the initial costs of the KYC process as well as the running costs of keeping the information about customers up to date. Our system increases the levels of security and regulatory compliance in the KYC process and significantly reduces the cost of that process for all parties involved.

The know-your-customer (KYC) due diligence process is outdated and generates costs of up to USD 50 crore per year per bank. We propose a new system, based on distributed ledger technology (DLT), that reduces the costs of the core KYC verification process for financial institutions, collages and improves the customer experience. In the proposed system, the core KYC verification process is only conducted once for each customer, regardless of the number of financial institutions with which that customer intends to work. Thanks to DLT, the result of the core KYC verification can be securely shared by customers with all the financial institutions that they intend to work with.

Keywords: Blockchain, KYC, AML, Distributed Ledger Technology

CHAPTER-3 Research design and methodology

Sampling techniques are crucial in research to select a subset of participants or data points from a larger population. When studying the implementation of KYC (Know Your Customer) using blockchain, various sampling methods can be applied to gather relevant data. Here are some sampling techniques and their application in this context:

1. **Random Sampling:** Description: Random sampling involves selecting participants or data points entirely by chance from the population. It ensures each element has an equal chance of being chosen.
 - Application: In the context of KYC implementation using blockchain, random sampling can be used to select a random subset of customers or transactions to assess the effectiveness of the blockchain-based KYC system. This method helps avoid bias in the selection process.
2. **Stratified Sampling:** Description: Stratified sampling divides the population into subgroups or strata based on certain characteristics, and then random samples are taken from each stratum.
 - Application: When studying KYC implementation, you may want to ensure representation from various segments of customers, such as new customers, longterm clients, and high-value clients. Stratified sampling allows you to select participants proportionally from each group for a more comprehensive analysis.
3. **Cluster Sampling:** Description: Cluster sampling divides the population into clusters or groups, and then random clusters are chosen for data collection. All individuals within the selected clusters are included in the sample.
 - Application: In a KYC implementation study, you may want to focus on specific geographic regions or specific branches of a financial institution. Cluster sampling helps in selecting entire clusters of customers, ensuring geographical diversity.
4. **Convenience Sampling:** Description: Convenience sampling involves selecting participants who are readily available or easily accessible.
 - Application: While less rigorous, convenience sampling can be used in preliminary

phases to quickly gather data for initial observations. However, it should be supplemented with more robust sampling methods to ensure representativeness and minimize selection bias.

5. **Purposeful Sampling:** Description: Purposeful sampling involves selecting participants deliberately based on specific criteria, expertise, or knowledge.

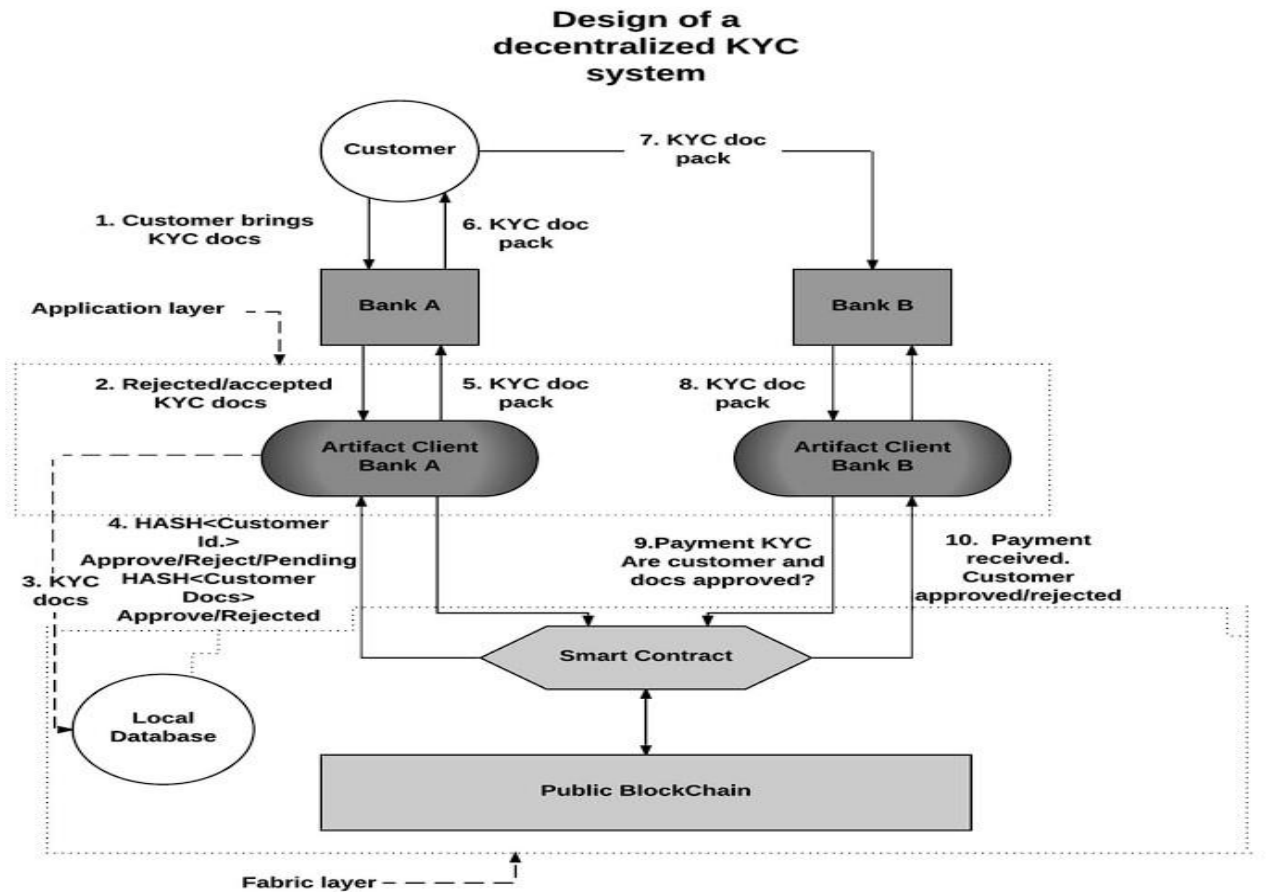
- Application: When conducting in-depth interviews or surveys with experts in the field of blockchain and KYC, purposeful sampling is suitable. It ensures you obtain valuable insights from knowledgeable sources.

6. **Snowball Sampling:** Description: Snowball sampling is used when researching hard-to-reach or niche populations. An initial participant is selected, and they refer the researcher to others, creating a "snowball" effect.

Application: In the context of blockchain-based KYC, snowball sampling can be used to identify and gather insights from individuals or organizations that have successfully implemented such systems, which might be a relatively small and specialized group.

3.1 Hypothesis:

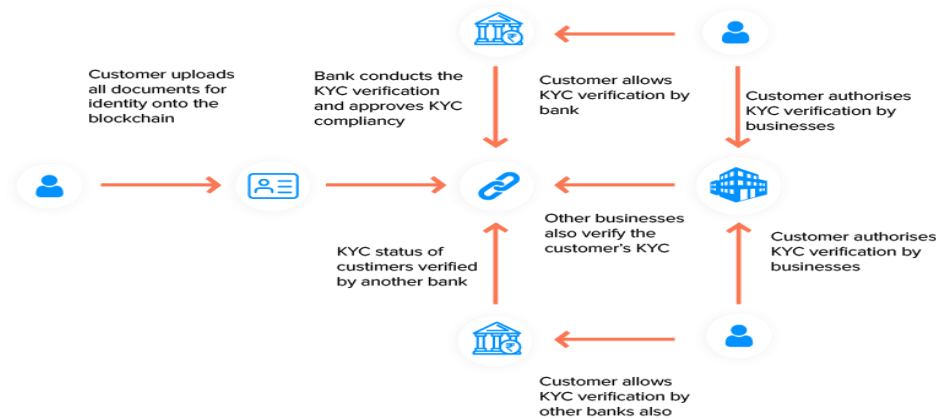
- "Implementing KYC processes using blockchain technology in the financial services sector will result in improved efficiency, enhanced security, and reduced compliance costs, leading to a more streamlined and cost-effective customer onboarding and identity verification process."
- This hypothesis suggests that the use of blockchain in KYC will have positive effects on various aspects of the process, and these effects can be measured and observed through quantitative and qualitative assessments. It forms the basis for your research, which will involve gathering data and evidence to support or refute this statement.



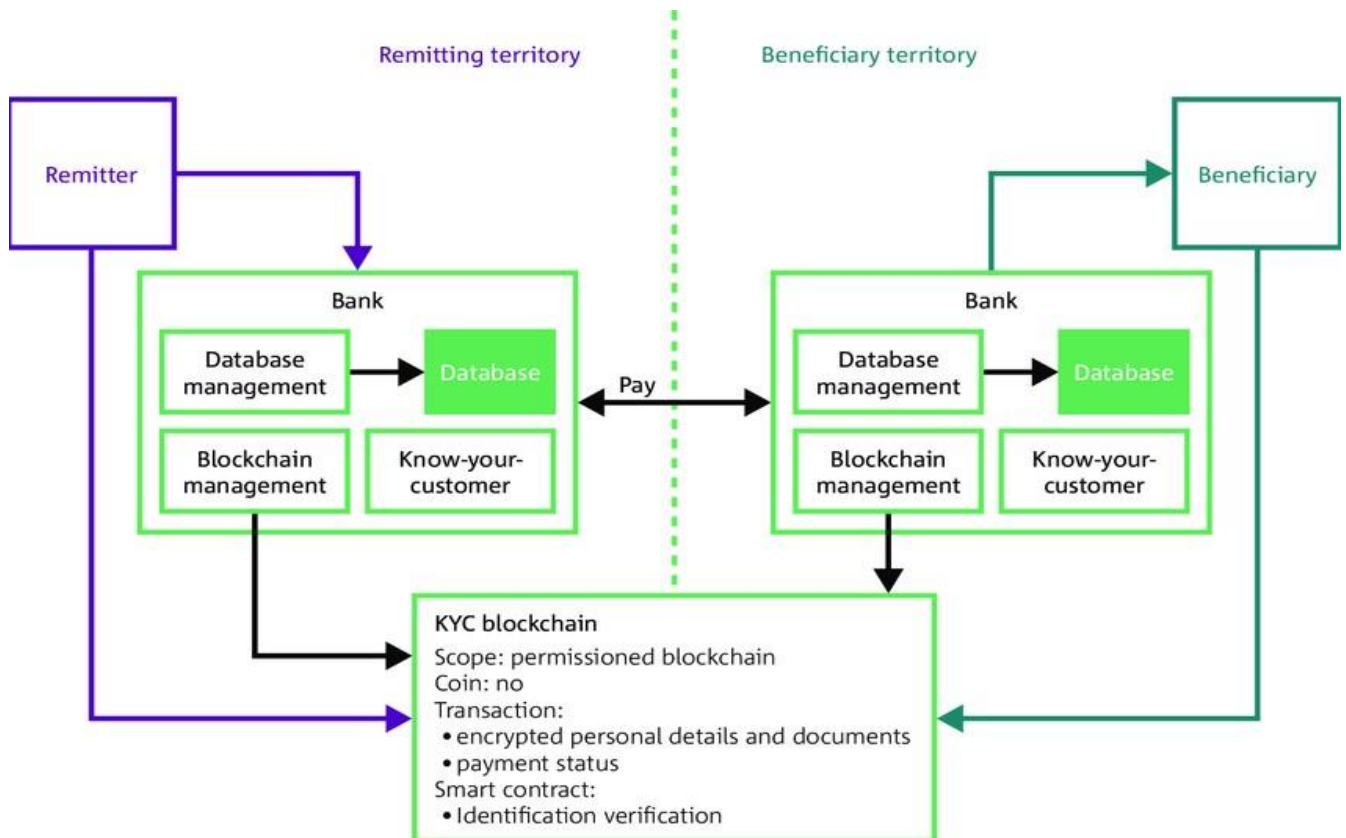
3.2 DATA:

- Data Collection Procedure:** The data collection procedure for studying the implementation of KYC (Know Your Customer) using blockchain involves several steps. Initially, a comprehensive review of relevant literature will be conducted to establish a foundation of existing knowledge. Subsequently, data will be collected through a mixed-method approach, comprising both quantitative and qualitative techniques. The quantitative phase will involve surveys distributed to financial institutions and organizations that have adopted blockchain-based KYC systems. In the qualitative phase, in-depth interviews will be conducted with experts in the fields of blockchain technology and KYC compliance within the financial sector. Additionally, document analysis will be performed to review any relevant reports, regulatory documents, and case studies. Data collection will be conducted over a specified timeframe to ensure the most up-to-date and accurate information is

obtained.



- **Data Analysis Procedure:** Data collected in this study will be subjected to a rigorous analysis procedure to derive meaningful insights. In the quantitative phase, survey data will be statistically analysed to identify trends, patterns, and correlations. Descriptive statistics and inferential techniques, such as regression analysis, will be employed to explore the relationship between various variables. In the qualitative phase, content analysis will be used to extract key themes and insights from interview transcripts. Data collected through document analysis will be reviewed and compared to provide contextual information. A triangulation approach will be used to cross-validate findings from both quantitative and qualitative data sources. The analysis will be performed using appropriate software tools, such as statistical packages and qualitative data analysis software.



- **Data Collection Instrument:** The primary data collection instrument for the quantitative phase will be a structured questionnaire, specifically designed to gather information on the implementation of KYC using blockchain technology. The questionnaire will include a combination of closed-ended and Likert-scale questions to obtain quantifiable responses. For the qualitative phase, semistructured interview guides will be developed to facilitate in-depth discussions with experts. These guides will include open-ended questions, allowing for detailed insights and discussions. During document analysis, regulatory documents, reports, and case studies will serve as the primary data collection instruments, providing documented evidence of KYC implementation using blockchain.

Types of Data Instruments:

Instruments	Overall purpose	Advantages	Challenges
1. Interviews	to learn more about their answers to questionnaires	<ul style="list-style-type: none"> Provides full information Develops relationship with respondent. 	<ul style="list-style-type: none"> Can take much time Hard to analyze and compare Costly Generalization is limited
2. Focus groups	To explore a topic in depth through group discussion, e.g., about reactions to an experience or suggestion.	<ul style="list-style-type: none"> Quickly and reliably obtain common impressions Can be efficient way to gather Full of information in short time Can convey key information about projects. 	<ul style="list-style-type: none"> Can be hard to analyze responses Need a good moderator to steer the discussion and provide closure Difficult to schedule 6-8 people together
3. Questionnaires and surveys	To quickly and/or easily obtain a lot of information from people in a non-threatening way.	<ul style="list-style-type: none"> Can complete anonymously Inexpensive to administer Easy to compare and analyze Can obtain lots of data 	<ul style="list-style-type: none"> Might not get careful feedback Wording can bias client's responses Impersonal In surveys, may need sampling and statistical expertise.
4. Observation	To gather accurate information about how a project actually operates, particularly about processes.	<ul style="list-style-type: none"> Can view operations of a project as they are actually occurring Can adapt to events as they occur 	<ul style="list-style-type: none"> Can be difficult to interpret behaviors can be difficult to categorize Can influence participant's behaviors Can be expensive

- **Appropriate Research Design:** The most suitable research design for studying the implementation of KYC using blockchain in the financial services sector is a Mixed-Methods Research Design. This design combines both quantitative and qualitative research approaches to gain a comprehensive understanding of the topic. The quantitative phase involves surveys to gather numerical data and analyse trends, while the qualitative phase utilizes interviews and document analysis to provide in-depth insights and context. By using mixed methods, this research design enables a more robust and holistic examination of the complex factors and nuances involved in the KYC and blockchain implementation within the financial industry.

3.3 Functionality Probabilities

Certainly, the implementation of KYC (Know Your Customer) using blockchain technology offers several strengths and weaknesses, as well as considerations related to the technologies used, hardware requirements, and costs. Here's an overview:

1. Strengths:

- **Enhanced Security:** Blockchain technology provides robust security features, such as cryptographic encryption, decentralization, and immutability, which can protect sensitive customer data from unauthorized access and tampering.
- **Efficiency:** Automation of identity verification and compliance checks through smart contracts can significantly reduce the time and resources required for KYC processes, leading to increased efficiency.
- **Reduced Fraud:** The immutability of blockchain records and transparency can help reduce fraudulent activities by providing a tamper-proof audit trail of customer data and transactions.
- **Data Privacy:** Blockchain can offer customers greater control over their personal data by allowing them to grant or revoke access, enhancing data privacy and regulatory compliance.
- **Interoperability:** Blockchain can facilitate interoperability between different financial institutions and regulatory bodies, making it easier to share KYC data securely.

2. Weaknesses:

- **Regulatory Challenges:** The evolving regulatory landscape for blockchain and cryptocurrencies can present challenges for KYC implementation, as institutions must adapt to changing compliance requirements.
- **Integration Complexity:** Integrating blockchain-based KYC with existing legacy.

systems can be complex and may require significant investment in infrastructure.

- **Scalability:** As the number of customers and transactions increases, blockchain systems must be scalable to handle the load, which can be technically challenging.
- **Data Standardization:** Achieving data standardization for cross-institutional data sharing can be challenging due to differing data formats and protocols.
- **Cost:** The initial setup costs for blockchain infrastructure and ongoing maintenance and compliance expenses can be high.

3. **Technologies Used:**

- **Blockchain Technology:** Public or private blockchain networks, with variations like Ethereum, Hyperledger, or Corda, are used for storing and securing customer data.
- **Smart Contracts:** Smart contracts, often built on blockchain platforms, are employed for automating KYC processes and regulatory compliance checks.
- **Encryption:** Cryptographic techniques are used to secure data at rest and in transit within the blockchain network.

4. **Hardware Requirements:**

- **Nodes and Servers:** Hardware nodes and servers are required to run blockchain networks.
- **Storage:** Sufficient storage capacity is needed for storing the blockchain's distributed ledger.
- **Security Hardware:** Hardware security modules (HSMs) can be used for cryptographic key management and data protection.

5. **Cost:**

- The cost of implementing KYC using blockchain can vary significantly based on factors such as the chosen blockchain platform, the scale of implementation, and the complexity of integration.

- **Costs can include:**
- **Initial Setup:** Acquiring and configuring blockchain infrastructure, including nodes, servers, and network components.
- **Development:** Costs associated with developing and customizing blockchainbased KYC solutions and smart contracts.
- **Maintenance:** Ongoing maintenance and updates to keep the system secure and up-to-date with evolving blockchain technology.
- **Compliance:** Costs associated with ensuring adherence to regulatory requirements.
- **Data Storage:** Costs related to storing and maintaining blockchain data.
- **Training:** Expenses for training staff and users on the new KYC system. It's important for organizations to carefully assess the costs and benefits of KYC implementation using blockchain to determine whether it aligns with their operational and budgetary considerations.

CHAPTER-4 Conclusion

This paper has suggested an IS to reduce the aggregated cost of KYC in a jurisdiction by means of DLT. The main efficiency gain that this IS proposes is the avoidance of the same tasks being duplicated by different financial institutions. Additionally, this paper has shown how it is possible to distribute the costs of the core KYC verification process proportionally among those financial institutions, solutions that require the verification process be carried out for one given customer, and has defined a series of conditions that the IS in question needs to fulfil in order to ensure the correct incentive structure for the participating institutions. The maximum total cost saving per customer generated by the proposed IS can be measured as $\sum_i m_i \times (k_i - 1)$, where m_i is the cost of conducting ensures that all participating FIs remain up-to-date in terms of the validity of the KYC status of any customer. Additionally, we prove the concept by means of an artifact—coded a full core KYC verification for a customer i , and k_i is the number of financial institutions that conduct business with customer i .

This system is based on previous system proposals and emerged through the application of DSR. Specifically, the system development process employed a series of loops of design, evaluation, and demonstration that served to improve the system's applicability to a real-life corporate environment and to resolve the inefficiencies of previously proposed systems. The major contribution of the system we propose has been that it eliminates the need for a TTP, making the system truly decentralized, and that it makes possible a distributed data storage architecture that is independent of the blockchain architecture, which makes implementation more cost efficient and easier for FIs. In our system the blockchain is only used to grant and manage the distributed database's reading permissions. This strengthens the incentive structure for participating FIs. Our system has made another vital contribution in that it allows each participating FI to dynamically update each customer's status, such that if an FI identifies—for example—a flaw with regard to the legality of a customer's activities, it can revise that customer's status and propagate this information through the system to those other FIs that work with that customer.

The implications of this are, in fact, crucial because this feature not only allows FIs to revise the status of any given customer, it also increases the quality of the information—in the form of KYC documentation—available to the network, which

in the language Solidity—that can be easily used by any interested individual to test and develop the concept, implement it in an experimental environment, and further develop it and adapt it in order improve its applicability and usefulness. We are convinced that the conceptual system and the PoC that we propose here can serve to improve the existing KYC process and that they constitute one necessary further step toward the adoption of blockchain-based systems in the corporate environment.

REFERENCES

- [1]. Prof. Venkatesh U. Rajput, “Research on Know Your Customer (KYC),” International Journal of Scientific and Research Publications, Volume 3, Issue 7, July 2013.
- [2]. Malhotra, D., Saini, P. & Singh, A.K., “How Blockchain Can Automate KYC: Systematic Review,” Wireless Personal Communication, vol. 122, pp.1987–2021, 2022.
- [3]. Parra Moyano, J., Ross, O., “KYC Optimization Using Distributed Ledger Technology,” Bus Inf Syst Eng, vol. 59, pp.411–423, 2017.
- [4]. P. Yadav and R. Chandak, “Transforming the Know Your Customer (KYC) Process using Blockchain,” International Conference on Advances in Computing, Communication and Control (ICAC3), pp. 1-5, 2019.
- [5]. Biryukov, Alex; Khovratovich, Dmitry; Tikhomirov, Sergei , “Privacy-preserving KYC on Ethereum,” Proceedings of the 1st ERCIM Blockchain Workshop Reports of the European Society for Socially Embedded Technologies, 2018.
- [6]. N. Sundareswaran, S. Sasirekha, I. J. Louis Paul, S. Balakrishnan and G. Swaminathan, "Optimised KYC Blockchain System," International Conference on Innovative Trends in Information Technology (ICITIIT), pp. 1-6, 2020.
- [7]. Vitalik Buterin “Ethereum: Platform Review: Opportunities and Challenges for Private and Consortium Blockchains,”<http://www.smallake.kr/wp-content/uploads/2016/06/314477721-Ethereum-Platform-Review-Opportunities-andChallenges-forPrivate-and-Consortium-Blockchains.pdf>, pp.1-44, 2016.
- [8]. Shakya, Subarna, and Smys Smys. "Big data analytics for improved risk management and customer segregation in banking applications." Journal of ISMAC 3.03 (2021): 235249.
- [9]. Kamel, Dr Khaled. “Wireless IoT with blockchain-enabled technology amidst attacks." IRO Journal on Sustainable Wireless Systems 2.3 (2021): 133-137.
- [10]. Ashok Kumar Yadav , Ramendra Kumar Bajpai, “KYC Optimization using Blockchain Smart Contract Technology,” International Journal of Innovative Research in Applied Sciences and Engineering (IJIRASE) Volume 4, Issue 3, September 2020.

- [11]. Maicon Azevedo da Luz and Kleinner Farias, "The Use of Blockchain in Financial Area: A Systematic Mapping Study," In XVI Brazilian Symposium on Information Systems (SBSI'20). Association for Computing Machinery, New York, USA, Article 3, pp.1–8, 2020.
- [12]. B. Rankhambe and Dr H. Kaur Khanuja, "Hassle - Free and Secure e-KYC System Using Distributed Ledger Technology," International Journal of Next-Generation Computing - Special Issue, Vol. 12, No. 2, April 2021.
- [13]. Patel, D., Suslade, H., Rane, J., Prabhu, P., Saluja, S., Busnel, Y. "KYC as a Service (KASE)—A Blockchain Approach," Advances in Machine Learning and Computational Intelligence, Springer, Singapore, 2021.
- [14]. Kapsoulis, N.; Psychas, A.; Palaiokrassas, G.; Marinakis, A.; Litke, A.; Varvarigou, T., "Know Your Customer (KYC) Implementation with Smart Contracts on a PrivacyOriented Decentralized Architecture," Future Internet, 2020
- Arasa R, Ottichilo L (2015) Determinants of know your customer (KYC) compliance among commercial banks in kenya. J Econ Behav Stud 7(2):162–175
- Arner D, Barberis J, Buckly R (2016) The emergence of regtech 2.0: from know your customer to know your data.
- J Financ Transform 44:79–86 Colladon AF, Remondi E (2017) Using social network analysis to prevent money laundering.
- Expert Syst Appl 67:49–58 Egelund-Mu'ller B, Elsmann M, Henglein F, Ross O (2017) Automated execution of financial contracts on blockchains.
- Business & Information Systems Engineering. <https://doi.org/10.2139/ssrn.2898670>
- European Central Bank (2012) Virtual currency schemes. <https://www.ecb.europa.eu/pub/pdf/other/virtualcurrencyschemes201210en.pdf>. Accessed 31 Oct 2017
- European Commission (2016) Reform of EU data protection rulesEuropean commission. http://ec.europa.eu/justice/data-protection/reform/index_en.htm. Accessed 31 Oct 2017
- European Security and Markets Authority (2016) The distributed ledger technology applied to securities markets. https://www.esma.europa.eu/sites/default/files/library/2016-773_dp_dlt.pdf. . Accessed 31 Oct 2017
- Freifeld K (2012) ING to pay \$619 million over Cuba, Iran sanctions. <http://www.reuters.com/article/us-ing-sanctions-idUSBRE85B12I2012061> Accessed 31 Oct 2017
- Glaser F (2017) Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis. In: Proceedings of the 50th Hawaii international conference on system sciences.

<https://doi.org/10.24251/HICSS.2017.186> Szabo N (1997) Smart contracts: formalizing and securing relationships on public networks. *Expert Syst Appl* 2(9) Thompson Reuters (2016) Know your customer (KYC) independent survey USA (1986) The money laundering control act of 1986 (public law 99-570) USA (1988)

The anti-drug abuse act of 1988, pub law 100690, 102 stat. 4181 USA (1992)

AnnunzioWylie anti-money laundering act of 1992 USA (1994) The money laundering suppression act of 1994 USA (1998) The money laundering and financial crimes act (1998) USA

(2001)

patriot act of 2001 (public law 107-156) (2004) Intelligence reform and terrorism prevention act of 2004 Viswanatha A, Wolf B (2012) HSBC to pay \$1.9 billion U.S. fine in money-laundering case. [http://www.reuters.com/article/us-](http://www.reuters.com/article/us-hsbcprobeidUSBRE8BA05M20121211)

hsbcprobeidUSBRE8BA05M20121211. Accessed 31 Oct 2017 Wood G (2016)

Ethereum: a secure decentralised generalised transaction ledger.

<http://gavwood.com/paper.pdf>. Accessed 31 Oct 2017 World Economic Forum (2016)

The future of financial infrastructure.

http://www3.weforum.org/docs/WEF_The_future_of_financial_infrastructure.pdf.

Accessed 31 Oct 2017