# SECURED AND PRIVACY PRESERVING E-KYC SYSTEM USING BLOCKCHAIN

**RAVI KIRAN KUMAR TERA 1, KOKKONDA NAVITHA 2, PENJARLA MANUDIKSHI 3, D NEHA 4, NAYIKINI GEETHA BHARATHI 5,**

**ASSISTANT PROFESSOR 1, UG SCHOLAR 2,3,4&5**
**DEPARTMENT OF CSE, MNR COLLEGE OF ENGINEERING AND TECHNOLOGY,**
**MOHD.SHAPUR, TELANGANA 502285**

**ABSTRACT** A Blockchain technology guarantees to be highly trending and empowering in financial domain computing programs. The virtual economic system is becoming an fundamental a part of present day life. in order the use of the digital global increases there are more probabilities of lower is the safety stage. So greater using digitization more the frauds and less the safety. In a few cases of personal information, leakage has brought back into the focus the security troubles with the extraordinary identification sharing mechanisms. A client is predicted to provide his identification for authentication by means of unique agencies. So the KYC process offers with the identity of the user. And in flip, provides the desired security. The KYC strategies which are used by the banks are absolutely dependent on the encryption that's sluggish and it is able to result in the lack of patron info to other their birthday celebration economic establishments. This device can be efficient by means of using Blockchain technology, which has the ability to automate numerous manual approaches and it's also proof against hacks of any type. The immutable blockchain block and its distributed ledger is the best complement to the system of KYC. With the addition of clever contacts, fraud detection may be computerized. For KYC identification info garage, we are able to employ any types of KYC. So, the banks can develop a shared non-public blockchain within the financial institution premise and the equal can be used for verifying the documents. This permits the user to get control in their touchy files and also makes it easier for banks to reap the documents they want for compliance.

**Keywords:** Blockchain, Banking, Digital Certificate, Digital Wallet, Decentralized Identity, Distributed Ledger Technology, Verifiable Credential.

**I.**

**INTRODUCTION** A Blockchain-based totally protection management device is for offering security to the bank transactions and to implement the KYC manner in a easier and secured manner. Blockchain technology is a brand new technology which is based totally on Mathematical, cryptographic and monetary concepts for preserving a database among diverse contributors without the need of any 0.33 party or central authority. it is a secured distributed database, tamper obvious, in which the validity of a transaction may be demonstrated by means of events in the transaction. Blockchains are normally managed by using a peer-to-peer (P2P) laptop network to be used as a public allotted ledger, wherein nodes together adhere to a consensus set of rules protocol to add and validate new transaction blocks. Al even though blockchain facts are not unalterable, considering the fact that blockchain forks are possible, blockchains can be considered secure via design and exemplify a distributed computing system with high Byzantine fault tolerance. know Your client (KYC) strategies performed through banks on their clients are needless, unmanageable and highly-priced. therefore, a gadget is proposed to automate unskilled obligations and allow sharing of facts related to KYC. Blockchain technology, with its concept of dispensed database, time-stamped ledgers, can correctly assist banks enhance their KYC technique. one of the most important duties of the bank is to make certain facts protection of data of the customers, confidentiality and the country in their account to assure their safety and integrity, inside the method of alternate and processing of records. for that reason, by means of the use of the competencies of innovative facts generation i.e., the Blockchain generation information protection may be performed.
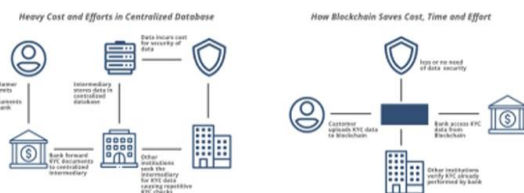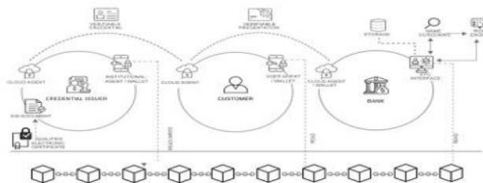


**Figure 1**: Blockchain and e-KYC



**Figure 2**: Distributed Ledger

**II. LITERATURE SURVEY** This section of the literature survey eventually reveals some facts based on thoughtful analysis of many authors work as follows. Literature survey is the most important step in any kind of research. Before start developing, we need to study the previous papers of our domain which we are working and on the basis of study we can predict or generate the drawback and start working with the reference of previous papers. In this section, we briefly review the related work on Block chain technology. R.Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens present the concept between two arrangements of electric vehicles, which fundamentally diminish the effect of the charging procedure on the power framework amid business hours. This trading approach is also economically beneficial for all the users involved in the trading process. An activity-based approach is used to predict the daily agenda and trips of a synthetic population for Flanders (Belgium) [1]. Y. Xiao, D. Niyato, P. Wang, and Z. Han provide a study of the possible flow and functional factors that enable DET in communication networks. Various design issues on how to implement DET in practice are discussed. An ideal approach is created for delay-tolerant remote-controlled correspondence organizes in which every remote powered device can masterminded its information transmission and energy exchanging activities as indicated by present and future vitality accessibility [2]. J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain presents a work to accomplishes request reaction by giving motivating forces to releasing PHEVs to adjust nearby power request out of their own self-interests. Be that as it may, since exchange security and security insurance issues show genuine difficulties, they investigate a promising consortium block-chain innovation to enhance exchange security without dependence on a confided in outsider. A restricted P2P Electricity Trading framework with Consortium block- chain (PETCON) strategy is proposed to represent detailed activities of limited P2P power exchanging [3]. N. Z. Aitzhan and D. Svetinovic presents a work that address the issue of providing transaction security in decentralized smart grid energy trading without confidence on trusted third parties. We have developed a proof-of-concept for de centralized energy trading system using blockchain technology, multi-signatures, and anonymous encrypted messaging flows, enabling peers to anonymously negotiate energy prices and securely perform trading transactions [4]. M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now presents a work that shows decentralized computerized cash, called NRG coin. Prosumers in the smart grid framework exchange privately made
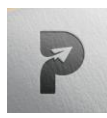
sustainable power source utilizing NRG-coins, the estimation of which is indented on an open cash trade advertise. Like Bit-coins, this money proposes various favorable circumstances over fiat cash, however not at all like Bit-coins it is made by infusing vitality into the matrix, as opposed to giving vitality on computational influence. Likewise, they make a novel exchanging worldview for purchasing and offering environmentally friendly power vitality in the smart grid network [5]. S. Barber et al presents a work that Bit-coin is isolated computerized cash which has pulled in a significant number of clients. They play out a top to bottom examination to comprehend what made Bit-coin so effective, while many years of research on cryptographic

emoney have not prompt a vast scale appropriation. They ask additionally how Bit-coin could turn into a decent contender for seemingly perpetual stable money [6]. I. Alqassem et al presents a work that Bit-coin is constantly improved by an open-source network, and different Bit-coin libraries, APIs, and elective usage are being created. All things considered, there is no up and coming convention contrast or design portrayal since the authority whitepaper was distributed. The work demonstrates an a la mode convention detail and design investigation of the Bit-coin framework. We play out this examination as the initial move towards determination of the cryptographic currency reference design [7]. K. Croman et al presents a work that the expanding fame of block-chain-based digital forms of money has made versatility an essential and earnest obligation. The work ponders how essential and incidental bottlenecks in Bit-coin restrict the ability of its present distributed overlay system to help generously higher throughputs and lower latencies. These outcomes propose that re-parameterization of square size and interruption ought to be seen just as a first augmentation toward accomplishing people to come, high-stack block-chain conventions, and real advances will moreover require a fundamental re-evaluating of specialized ways [8]. G. W. Peters and E. Panayi presents a work which give a diagram of the idea of block-chain innovation and its capacity to disturb the universe of managing an account through encouraging worldwide cash settlement, shrewd contracts, mechanized keeping money records and advanced resources. In such manner, they first give a concise outline of the center parts of this innovation, and in addition the second-age contract-based improvements [9]. L. Luu et al presents a work which gives another circulated understanding convention for authorization less block-chains called ELASTICO. ELASTICO

scales exchange rates straight with accessible estimation for mining: the more the calculation control in the system, the higher the quantity of exchange squares chosen per unit time. ELASTICO is productive in its system messages and permit com plex foes of up to one-fourth of the aggregate computational power [10].

**III. DESIGN OBJECTIVES** We discussed the current issues of the KYC manner and our derived goals with KYC professionals and an SSI expert. The interviews sought to evaluate the diagnosed layout targets regarding relevance and completeness. The KYC specialists worked in unique businesses and held exceptional positions, so that the objectives may be considered from unique perspectives. expert A showed the relevance of the derived targets and their associated necessities. as a result of the increasing expenditure on personnel and technology, the procedure's efficiency is indeed a important intention for banks. He careworn the significance of end-to-give up digital processing and recommended interbank cooperation within the KYC method, however diagnosed trust issues here, each among the banks and regarding patron believe in the confidentiality of their facts. according to him, the safety of purchaser privacy is likewise vital. in addition, he affirmed the relevance of increasingly strict rules and the need to comply with them. as an instance, patron records need to be stored by using banks for as a minimum 5 years. The expert also showed the need of inclusive of in addition MLA requirements. expert B also defined procedure performance because the maximum critical component, to make sure cost and time savings. The challenges apparently lie in particular in the high variety of guide process steps. This professional emphasized the importance of automation and digital processing of documents. He additionally showed the significance of shielding privacy. sensitive dealing with of consumer information is essential, and this must no longer be passed directly to third events, no longer even to cooperation partners. Like Ex pert A, he referred to the increasing significance of law and the want to comply with it. professional C emphasized the importance of a good consumer experience, due to the fact that many customers will not awareness at the structures' useful info. all through the implementation segment, unique care should be taken to make sure that the gadget is as intuitive as possible. requested approximately the architectural attitude, he mentioned backup and recovery abilities through cloud garage as a building block for person friendliness in case of statistics robbery or loss. professional C additionally confirmed the significance of the

GDPR and eIDAS. consistent with him, there may be nevertheless room for interpretation in the GDPR, as an instance regarding the position of encrypted or hashed in my view figuring out records. He recommended intending from the strictest possible interpretation of the GDPR. He pressured that, on a distributed ledger, data can't be deleted. A key project to the popularity of KYC documents attested via different banks, he stated the essential status quo of a trust relationship among the banks. but, he argued that connecting the e-KYC architecture to the eIDAS infrastructure can be a approach to this trouble. In sum, as a minimum one expert emphasized each of the design goals, and the experts generally taken into consideration the related requirements useful to evaluate an e-KYC framework from a financial institution's attitude.

**IV. SYSTEM OVERVIEW** [A] System Architecture  The system architecture provides the architecture for the proposed system in the form of different layers. In proposed system, we implement a block chain Based KYC system, in which each customer upload a data files and

encrypts these data with corresponding key. To implement both security preservation and relevant searches, we propose an effective search scheme. In this framework, the server is permitted to viably combine various encrypted records, and safely play out the pursuit without uncovering the user sensitive data, neither information documents nor the questions.
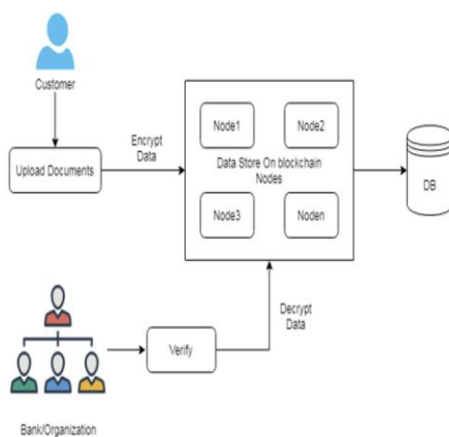


**Figure 3:** System Architecture

**V. CONCLUSION** In many approaches, Blockchain these days is similar to in which the net was in early 20s. The development of facts generation and digital business each day has an increasing number of tremendous impacts on all spheres of the modern existence. Blockchain generation is designed to alternate the conventional perception of how humans interact through

a network. the main benefit of the Blockchain technology is the whole synchronization of processes, integrity and area of expertise of all processed statistics, irrespective of mining and tokens. Blockchain era enables to improve allotted databases in terms of storage, synchronization, loss and integrity of information. Its early days, but industry leaders are sponsoring a wide variety of blockchain use instances supported with the aid of enterprise consortiums. Having seen the potential of this generation and the demanding situations, we think the opportunity is clear but the blue sky is too some distance off and businesses need to validate use instances and enterprise/technical viability before imposing blockchain. save you banks from being attacked or used on purpose or by chance by way of criminal elements for cash laundering activities. records changes can be tracked and monitored. when you consider that all data is saved in a homogeneous blockchain, resulting better governance. Direct get right of entry to the KYC information may want to save huge quantity of time for establishments. Ensures relaxed and authenticated transaction in joint bills.

## VI. REFERENCES

[1] R. Alvaro-Hermana, J. Fraile-Ardanuy, P. J. Zufiria, L. Knapen, and D. Janssens, "Peer to peer energy trading with electric vehicles," IEEE Intell. Transp. Syst. Mag., vol. 8, no., pp. 33–44, Fall 2016.

[2] Y. Xiao, D. Niyato, P. Wang, and Z. Han, "Dynamic energy trading for wireless powered communication networks," IEEE Commun. Mag., vol. 54, no. 11, pp. 158–164, Nov. 2016.

[3] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "En abling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," IEEE Trans. Ind. Informat., vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[4] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized en ergy trading through multisignatures, blockchain and anonymous messaging streams," IEEE Trans. Depend. Sec. Computer.

[5] M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. M. de Abril, and A. Now, "Nrgcoin: Virtual currency for trading of renewable energy in smart grids," in Proc. IEEE 11the Int. Conf. Eur. Energy Market, 2014, pp. 1–6.

[6] S. Barber et al, "Bitter to better-how to make bitcoin a better currency," in Proc. Int. Conf. Financial Cryptography Data Security, 2012, pp. 399–414.

[7] I. Alqassem et al., "Towards reference architecture for cryptocurrencies: Bit coin architectural analysis," in Proc. IEEE Internet Things, IEEE Int. Conf. Green Comput. Commun. IEEE Cyber, Physical Social Comput. 2014, pp. 436–443.

[8] K. Croman et al., "On scaling decentralized blockchains," in Proc. Int. Conf. Financial Cryptography Data Security, 2016, pp. 106–125.

[9] G. W. Peters and E. Panayi, "Understanding modern banking ledgers through blockchain technologies: Future of transaction processing and smart contracts on the internet of money," in Banking Beyond Banks and Money. New York, NY, USA: Springer-Verlag, 2016, pp. 239–278.

[10] L. Luu et al., "A secure sharding protocol for open blockchains," Proc. ACM SIGSAC Conf. Comput. Commun. Security, 2016, pp. 17–30.