Vol. 6, No. 2 | July – December 2022

# Impact of Blockchain Technology in Modern Banking Sector to Exterminate the Financial Scams

Muhammad Ghazanfar Bhatti[1]*, Rizwan Ali Shah[2], Dr. Muhammad Asif Chuadhry[3]

**Abstract:**
The paper examined the use of blockchain in banking sector. With the increase of user's interest in banking sector, transactions are conducted online or via physical credit scanners. Banking sector is easy target for the hackers. Unauthorized person can hostage the bank data by using cyber security threats such as phishing attack, Ransomware attack, and Denial of Service (DoS). The only solution to secure the customer precious data is blockchain. It has the potential to considerably decrease costs and it can completely alter the banking industry. The present centralized banking system can be strengthened using blockchain technology. Due to the transparency, auditability, immutability, operational resilience and data encryption essential in blockchains, it can secure the cyber security, forbid crooked actions and perceived tampering of data. Blockchain technology will deal the movement in the banking industry and associated facilities in prevailing area. Correspondingly inspecting cases both at home and abroad, it might be recognized areas that blockchains are used aggressively, utilized in banking sections are growing into remittance, resolution, smart contracts and reliability. Multi-factor authentication (MFA) technique is used to find the legitimate users by demanding a user to conform multiple identification information. The username and password can easily be hacked by unauthorized person, so we create a new authentication method that can't be hacked with the help of Blockchain Techn ology.

**Keywords:** *Blockchain, Financial sector, Banking sector, Electronic Banking, Distributed Ledger Technology and E-banking*

## 1. Introduction

For last five decades, the banking sectors are using computer to improve its services and to provide easiness to its customer. Where the use of computers has provided easiness to the banks, it also causes different problem like cyber-crime which include hacking. A hacker can easily hack a system to steal a customer's personally identifiable information (PII). A hacker can use different malicious software (often used to steal data and destroy computer system like viruses, worm, spyware, mobile malware and Trojan) to gain illegal access to customer gadget or bank database. The injection of these software can be harmful for the entire banking network. Different types of software used to detect, scan, prevent and delete these harmful viruses to protect the computer system often known as antiviruses. But these antiviruses are not enough security precautions to control the hacker attacks. These security threats cannot reduce the interest of user in E-banking.

With the increase of user's interest in banking sector, transactions are conducted online or via physical credit scanners.

[1]Deputy Director Quality Assurance Agency, Higher Education Commission, Islamabad, Pakistan
[2]Deptt. Of CS & IT, The IUB, Bahawalpur, Pakistan
[3]Faculty Member, Shifa Tameer-e-Millat University, Islamabad.
Corresponding Author: asif.epm@gmail.com

Electronic banking (E-Banking) is making things easier, so consumers are increasingly avoiding cash and checks. Banking sectors are encouraging this tendency by enhancing portals and mobile applications or web banking. Basically, transaction can be performed through three different ways: (1) Web banking, (2) Phone banking, (3) Mobile banking.

i. Web banking (or internet banking) is accomplished through the internet. The bank gives access of personal computer and internet to its customer to overcome the security issues. Banking sectors provide extra devices like tokens, digital signature and specialized software to their customer which enhanced the online transaction.

ii. Phone banking provide the channel in which e-banking customer can gain online service from the concern bank. It is further split into two categories:

In first category a customer can call to the call center where a concern agent processed the service, where the customer can convey his issues. Firstly, the agent will identify the authenticity of the customer and then send the request for further task.

In second category customer voice can be recognized along Interactive Voice Response system (IVR). Client replies using voice message, the IVR identify the authenticity of the customer to reduce the security issues and then send the request for further task.

iii. The mobile banking performed its services via short message service system (SMS), mobile internet through mobile App. Each customer has installed the specialized bank app in their mobile devices for the security precautions.

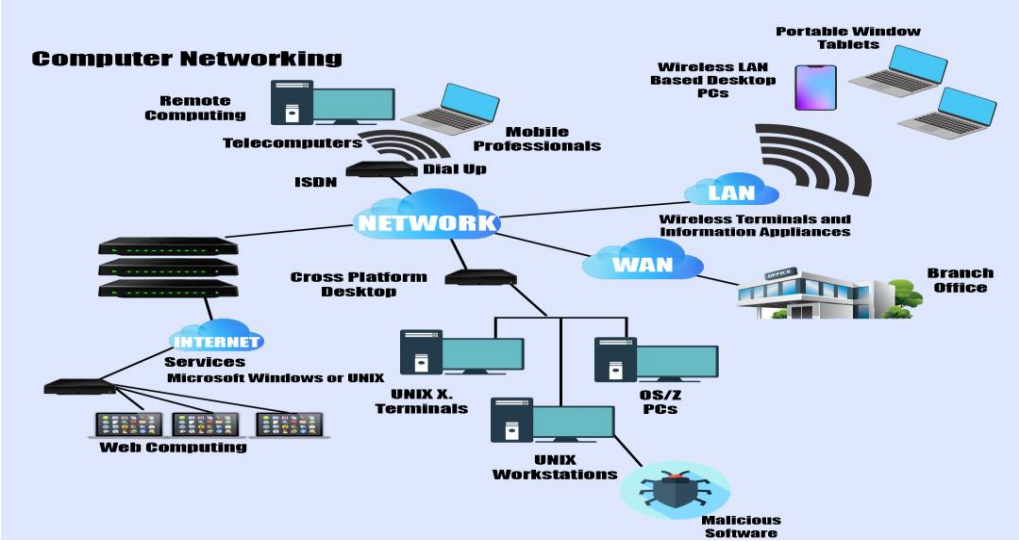


**Fig. 1.** A Malicious Software attacking the whole organization

The major purpose of these portal and application enhances user comfort and experience. Such software also adds the cyber security risks. Due to these reasons, financial sector is easy target for the hackers. Hackers can illegally earn from theft, fraud and treachery by attacking banks, banking sector can be used as ideological and political leverage for hacktivists. Unauthorized person can hostage the bank data by using cyber security threats such as phishing attack, Ransomware attack, and Denial of Service

(DoS) (See Fig. 1). When bank data is taken hostage, a bank has to pay thousands of dollars to recover the data that causes sizeable damage to bank and its clients.

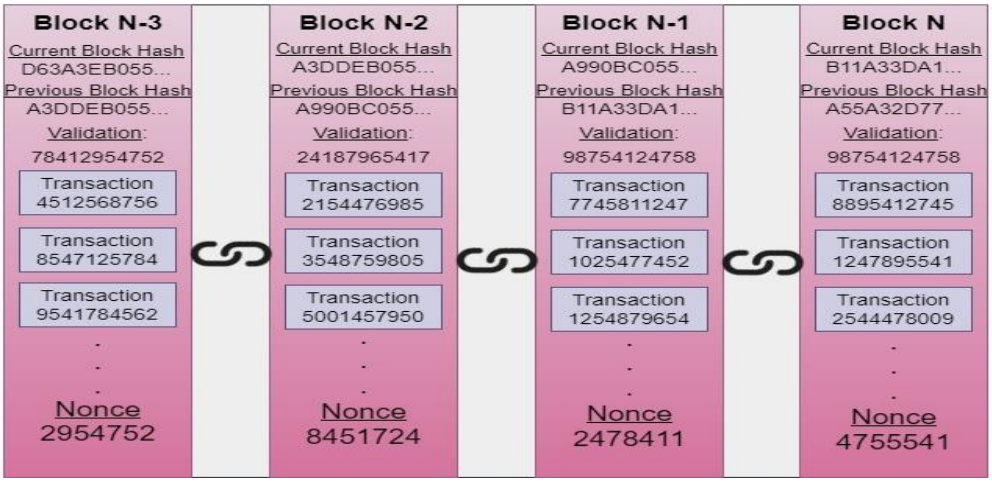


**Fig. 2.**Demonstrating the block ingredients. Transactions are assembling inside the block structure

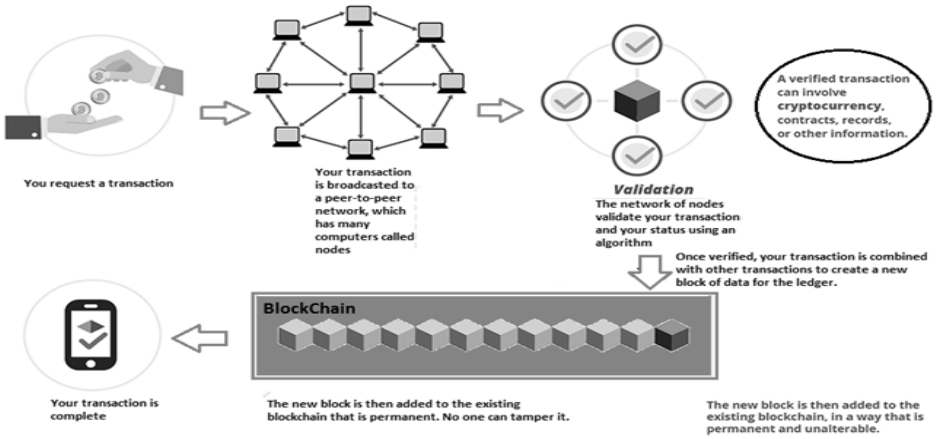


**Fig. 3.** Complete process of a transaction get into the Blockchain

It is the bank's responsibility to protect the data of its clients. Without suitable security, clients can lose valuable data along with their investment. Banks data can be protected through blockchain. It provides a novel approach to storing information, executing transactions, and performing functions. These days, blockchain has gained interest in different industries and academia. Blockchain contain chain of block which consist large number of data where a block contains multiple transactions. It represents complete ledger record, all block holds a timestamp, parent block has the value of hash of preceding blocks, and the hash is verified by a nonce. Hash value are unique, these value change

immediately when the blocks in the chain are changed. Fig. 2 and Fig. 3 showing the block structure as well as the whole process of execution of Blockchain technology.

Now only solution to secure the customer precious data is blockchain. Although, conventional banks started presenting Internet financing in response to consumer demand and market rivalry, its effects are also not reassuring. Therefore, banks have also begun to look to new technologies that can secure the user data. It can be expected that a new technology block has the potential to enhance banking infrastructure in data storage and transmission. Blockchain has the potential to considerably decrease costs and, it can completely alter the banking industry. The present centralized banking system can be strengthened using blockchain technology. Financial institution can get rid of need intermediary, as blockchain provide transparency, security and immutability.

### 1.1 Research Objectives

Following points was consider before to start the working of this article.

i. To govern an inquisition into the existing scenario of modern Banking Sector.

ii. To inspect the possibility of employing Blockchain Technology in banking and its security exercises inside the Banking Sector.

iii. To establish a model that employs Blockchain Technology to shelter data storage in modern banking databases and to punch scams.

iv. To regulate the feasibility of the proposed Blockchain Application Model.

## 2. Literature Review

Many authors have discussed issues related to relevant field in different scenarios. Banking sector is already facing cybersecurity risks in result of fraud and operational failures from both outsiders and insiders. The sector faces this problem due to lack of awareness by computer users, technical resources, paucity of financial and attacks from different hackers such as viruses that attack on the weaknesses in legal framework which has strengthened recent time.

### 2.1 Blockchain adoption aspects in Banking Sector

Blockchain technology can play a (WEF, 2015) traditional or vital role in digital advancements and governments sector mostly attain an active facilitation style preferably than one of a leader. The adoption of blockchain in banking sector can changed the price and models for exchange rates. Chief factors that support acceptance of blockchain based on values of the business that are provided to economical and banking subdivisions like interest of using the new technology and through literature as opportunities. The factors identified by the researchers are:

#### 2.1.1 Enhanced data exploration:

In (ENISA, 2016), new emerging blockchain technology shall predict and alleviate new liability frauds in banking sector because of the regiment copying mechanism. In (Higginson et al., 2019) the author describes different prospect of blockchain like secrecy,

cryptography, safety and capability to store tremendous amount of data. This huge amount of data can allow the single bank or all members of network to see various information stored on a distributed ledger network added maintain by some other banks. This provide banks with other bank customer data, that provide more informative results, quick decision making and allocate credit process, which lower the banks credit risks.

#### 2.1.2 Regulatory compliance:

According to (ENISA, 2016), the blockchain technology will increase level of compliance automation, and improved the authorization transaction validity. Where (Accenture, 2017) probably evaluate 30-50% reserves on agreement via blockchain. (ENISA, 2016) additionally include that for adaptation taking place constructively, monetary structure used governance toolkit for audit, regulation and internal controls.

### 2.1.3 Refining KYC procedure:

(Lang, 2017) state that was data-sharing is secure through blockchain technology, it allows to create a central shared depository of updated customer identity information among various banks. It shall increase KYC procedure and appropriately AML procedure, enhanced interaction between various financial sector and banks. It minimized the departmental costs and minimized the reputation of data that shall decrease required underpinning price. (Hassani et al., 2018) estimates the KYC maintain up to 60-500 million USD per annum.EU Money Laundering Directive or financial sector needs to monitor, update, insert customers' information where GDPR control internal security through consumer security. (Hassani et al., 2018) argues if blockchain implemented correctly it can be useful to observe with these standards, where the KYC based blockchain registries got all banks refusing to accept data verification from outside sources.

### 2.1.4 Enhanced transactions speediness:

(Smith, 2018) state promptly and valid blockchain data increase the effectiveness of time. during transaction. The author also states that if new advisory function introduced, it will challenge the traditional roles like intermediaries. (Lang, 2017) argues the faster, simpler and secured blockchain payment method which directly transacted the corporates and both individuals. (Hassani et al., 2018) foresees transaction rate of typical blockchain to be 1,000–2,000 transactions every second (TPS), where the banking sectors done no agreement related to transaction blockchain capacity. (Marr, 2018) recommended that the blockchain await to be slower and inconvenient with time complexity as it expands large due to cryptography, distributed features of blockchain and complexity. The author emphasized evaluation in engineering and increased the processing speed, which should be developed in future. (Accenture, 2017) estimates savings of 50% on operational procedure's expenditure.

### 2.1.5 Canny agreements:

In (Smith, 2018) states the used of blockchain canny contract can resolve or reduced the issues with substantial efficiency and improve the cost, furthermore establish automatic contractual procedures. Conferring to Accenture Technology Vision report, as per quoted by (Hassani et al., 2018), conducted a survey on blockchain and smart contracts in which 60% of surveyed participants believe that next three decades will be critical intended for blockchain. In (Hassani et al., 2018) the author warns the backing sector to implement smart contraction solution to overcome their responsibilities for handling contracts in coming future.

### 2.1.6 Amplified Transparency:

(Smith, 2018) examine consensus, the process of encryption and blockchain security fundamentals can increased in real-time scenario rather than historical and where compared random sampling can produced 100% transaction using traditionally. He sees a role of auditors in decision-making processes and data security policies. (Hassani et al., 2018) foresees the emerging technology blockchain can make the transaction more secure and transparent that the previous security processes. In order to achieve high transparency all parties can access the blocks and access to historical data, which can benefit the authorization process. This can provide easiness to the real time auditing, compliance violation or swift action, automated financial reporting and real-time communication between regulators and banking sector.

In (Catota et al., 2018) suggested the creation of Computer Security Incident Response Teams (CSIRT) a system for exchanging information that can share technical information about uncertainty threats which decrease the information security incidents. This approach can aware about opposed security attack but this is not a perpetual solution. The banking organizations care more about their investment and asset, which are easily stole through cyber-attacks. Big Data is a term often used describe the enormous amount of organized, unorganized, and semi-structured information that is simply too time- and resource-intensive to stack into a relational database for analysis. Big Data be a fashion in the technological advancement that

has initiated the door to a fresh method for comprehending and judgement.

In (Humberto et al., 2022) proposed a model of data analytical environment for the security of data in financial sector. The model implemented on data lake which allow the security gaps in identification repository and identify the high risks regarding critical data in financial institution.

To control the security threats (Dhoot, 2020) proposed a model which use digital signature and biometric impression for the transaction. The method used biometric recognition, data learning and machine learning techniques which is more secure and minimize the threats.

In (Klee et al., 2019) proposed a technique to handle PII (personal identifiable information), which are user sensitive information such as username, password of account, first name, last name, social security numbers and bank card numbers. The author demonstrates that their PII detection algorithm removed original information about the user from the dataset and then recall the useful information from the previous knowledge.

In (Narayanan et al., 2022) proposed a Secure Authentication and Data Sharing in Cloud (SADS-Cloud) method that can handle the data security issues. The method consists three processes. Firstly, in big data outsourcing, the user subscribes to a center using hashing algorithm SHA-3. The SALSA20 encryption algorithm is applied on input file which are split into same size of block using MapReduce model. The big data sharing retrieves the secure file of user sensitive data like ID, password, secured ID and existing timestamp, email id is hashed, then contrast alongside original data stored within database. With this there are three further process in big data management Indexing using Fractal Index Tree, Compression using LZMA and Clustering using DBSCAN.

Table 1 used to show the major work completed using Blockchain technology till so far, reflecting the pros and cons of each activity.

TABLE I. STRENGTH AND WEAKNESS OF PRIOR WORK IN THIS DOMAIN

| **Author** | **Methodology** | **Strength** | **Weakness** |
|---|---|---|---|
| (Dhongade, 2019) | It represents the blockchain potential in business application over India. | Blockchain has secured and faster banking sector. | The research is particularly implacable to the domain of this country only that is i.e. India. |
| (Cucari et al., 2022) | ABI lab is used for analysis Interbank spunta project. | Blockchain and DLT played vital role to strengthen the banks. | The research is particularly implacable to the domain of Italian Banking Sector. |
| (Osmani et al., 2021) | A database is made which is relevant to academic-based research. | This study proclaims different characteristics and benefits of blockchain like risk and cost, | The result show that the use of blockchain is lower in banking sector than other sectors. |
| (Collomb, 2016) | New transactional model DLT essential aspects are present. | Evaluate impact of DLT on financial market. | Blockchain can be used in stock market for settling trade. |

| | | | |
|---|---|---|---|
| (Yoo, 2017) | The paper highlights the use of blockchain in financial sector. | Financial sector is expended when blockchain application is applied to settlement, security, remittance and smart contracts. | The research is particularly implacable to the domain of this country only that is i.e. Republic of Korea. |
| (Klee et al., 2019) | The proposed technique handle PII (personal identifiable information). | PII detection algorithm removed original information about the user from the dataset and released keystroke database into the public domain. | The utility of proposed scheme is limited. |
| (Catota et al., 2018) | Suggested the creation of Computer Security Incident Response Teams (CSIRT). | sharing application that can share technical information about uncertainty threats which decrease the information security incidents. | This approach can aware about opposed security attack but this is not a perpetual solution. |
| (Narayanan et al., 2022) | Proposed a Secure Authentication and Data Sharing in Cloud (SADS-Cloud) method. | The method can handle the data security issues using big data distribution, big data organization and big data contract out, | High Time complexity for encryption and decryption of data. |

## 3. Methodology

The electronic banking is facing security protocol issues, the transmission of data over the internet is unsecured. One of the most crucial components of the system is data, it must be secured. Unauthorized person can access database storage, which increase the vulnerability of cyber-crime. Due to the transparency, auditability, immutability, operational resilience and data encryption essential in blockchains, it can secure the cyber security, forbid crooked actions and perceived tampering of data. The main objective is to implement blockchain technology in financial sector and its security threads within the banking sector for examine the feasibility. A two-way authentication model is designed that can secure the database and frauds within electronic banking.

The first step in online business is to authenticate the customer, whether the customer is authorized for the current account. Multi-factor authentication (MFA) technique is used to find the legitimate users by demanding a user to conform multiple identification information. The user's name and password can easily be hacked by unauthorized person so we create a new authentication method that can't be hacked. To get access the account user must give at least two multi-factor authentication. The first identification is based on multiple question about your past like "What is your place of birth", "What is the color of your first vehicle", and "What is name of your grandmother". The customer has to give the correct answers of any four questions out of five. If the customer answers all the questions, then the transaction request will be approved otherwise customer have to pass form the second identification which is based on the facial identification.

User face will be identified through the gadget the user is using for the transaction like mobile or laptop. If the user succeeds second time to identify himself than the transaction request will be approved otherwise request will be denial and an altering message will be delivered to the network that unauthorized person try to access the account. The image, IP address and location of an unauthorized person will be sent to the network. Network contains different authorized members of banking sectors.

After the request is approved, the transaction is represented as a block. The block will be broadcast to the network for the approval of the transaction. Fig. 4 elaborating the whole concept of proposed system in pictorial form. The network consists of four members, all these members are connected with peer-to-peer networks, two persons from the dispatch banks and other two from the receiving bank. When all 4 members in the network allow the transaction, block are added to the chain which provide record of the transaction. The transaction money will be deducted from the original money and the record will be saved in the block. Finally, the transaction will be sent to the receiver or party B.

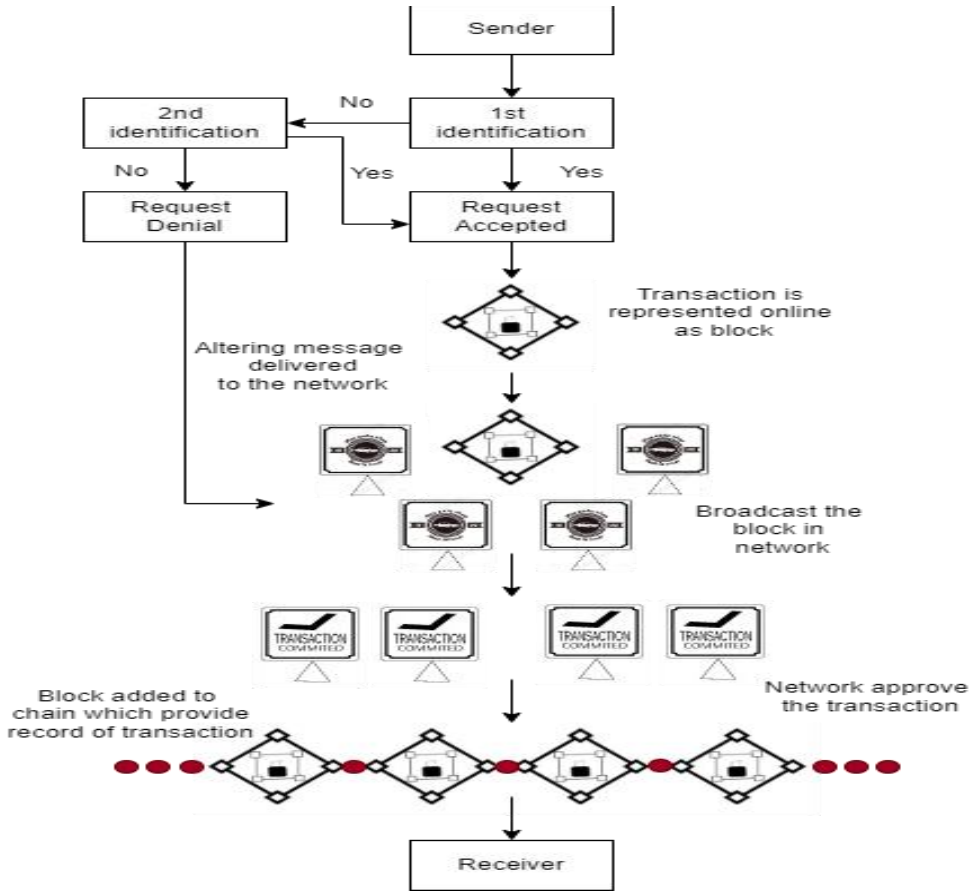


**Fig. 4.** Proposed Transaction Scenario in Banking Sector

In this article, the Linux Foundation's Hyperledger is used as a solution to build permissioned blockchain structure. A group of design tools Hyperledger Composer may be used to build a blockchain system. A part of the Hyperledger project, which is a group effort coordinated by the Linux foundation to generate open - sourced blockchain applications, is Hyperledger Fabric. Fig. 5 showing the block diagram of the Hyperledger Fabric components in this proposed solution.

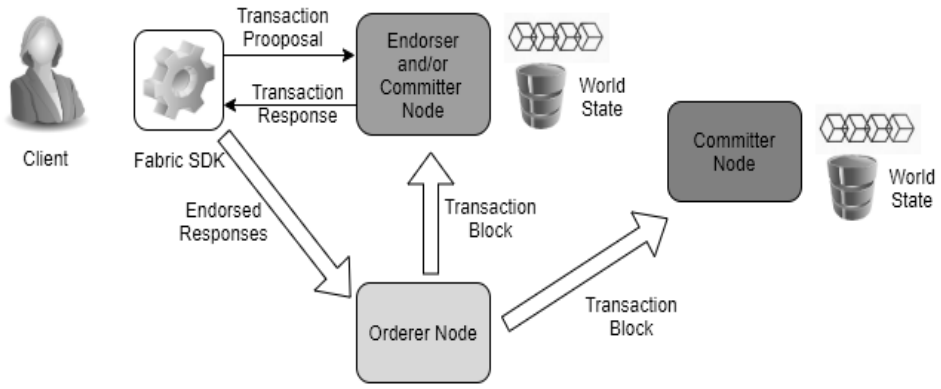


**Fig. 5.**Hyperledger Fabric Block Diagram

Fabric SDK allows clients to enter transaction recommendations, which are then forwarded to all Endorsing Peers. Read and Write sets are produced as output after these supporting peers authenticate and carry out all transaction. Customer is now given this response once again. Client compiles and delivers each peer's responses.

## 4. Implementation

As mention in Fig. 6, a Hyperledger Fabric-based network. This system is composed of four clients. The other three users are aware of any exchange that takes place between any two of the four clients. When creating a network, information about the network's Smart Contract instance and channel regulations are delivered.

Every peer is given Committer status by standard. A solitary peer may be given all duties. Every peer does have a logbook that consists of a World State as well as a blockchain. A smart contract is placed on each peer with an approving duty to verify transactions. A different Certificate Authority oversees each organization (CA). Transaction is recorded to ledger and global context is altered with Write data when confirming peer confirms the transaction. Fig. 7 use to show the integration of Smart code in Hyperledger Fabric Network.

Blockchain technology connects each one of these participants through a peer-to-peer network, eliminating all risks mentioned before and creating a transparent system. Synchronized data might be accessible to all users and kept in a "shared, immutable ledger," enabling monitoring of automobiles from point of production to final consumer. Blockchain ledger will record all business dealings concerning making, processing, and distribution of automobiles.

Typically, every company within a network has its own copy, which is synced through the network's complex protocols and technical layers (called peers). There is also an Ordering Service which compiles several concurrent processes. All these is used by all

participants to define the order and structure of transactions on the blockchain. A Membership Services Provider (MSP) is used to grant admittance to specific users on a network with lots of users.

Eventually, ledger accounts are used to document all transactions that took place during this procedure (e.g. data with ID, color, make, model, serial, version, etc.). This information is accurate and reliable. Now next stage following construction of blockchain network is to decide what sort of business transactions would take place inside blockchain architecture. Certain principles are really codified in legally binding contracts. Clearly, this is referring to a Smart Contract that is part of blockchain code (also called as Chain code from Hyperledger Composer)

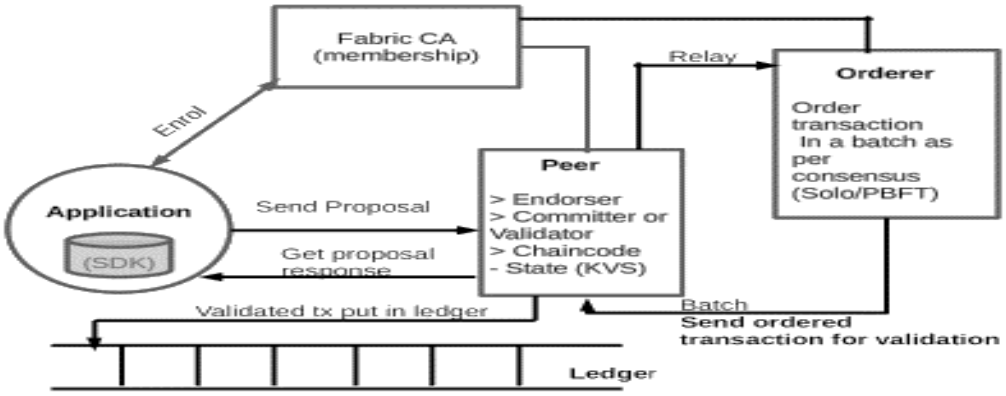


**Fig. 6.** Blockchain based banking transaction scenario based on Hyperledger Fabric

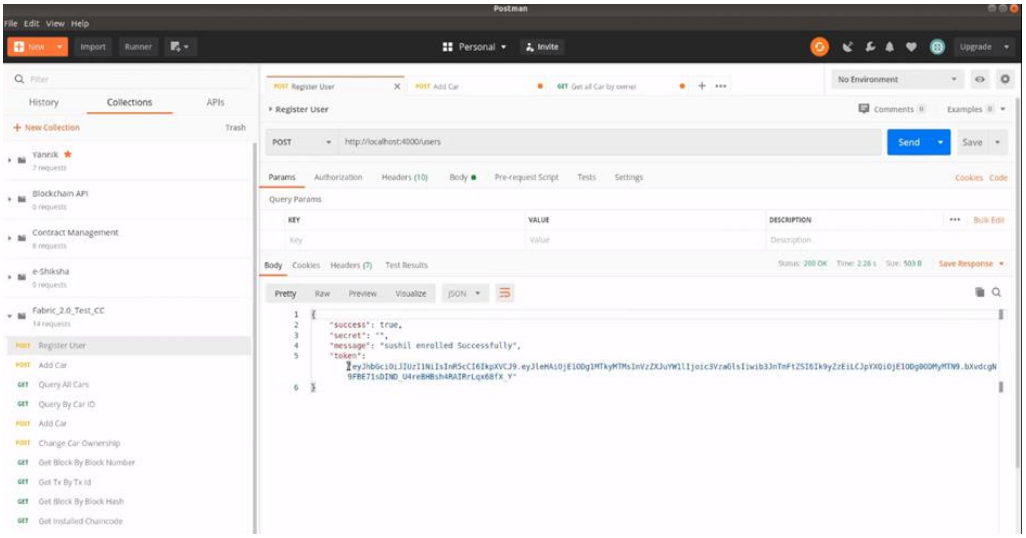


**Fig. 7.** Activity showing the Smart Code implementation

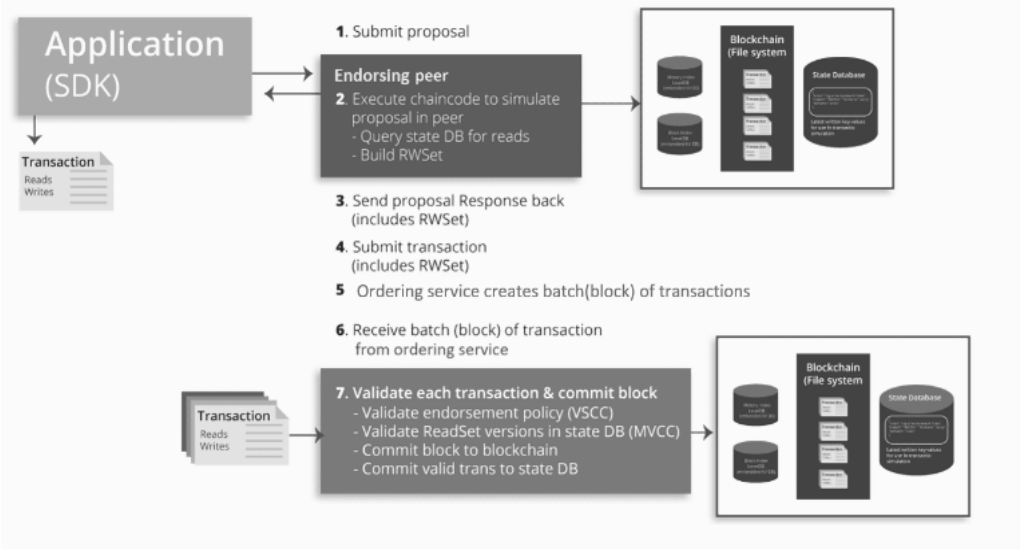


**Fig. 8.** Transaction Life-cycle of Hyperledger Fabric

The use of blockchain obviating the necessity of third-party transaction. In blockchain the information is saved in the blocks and then the information can share in a network. The network can save the whole transaction, because the transaction needs the approval of network. The major benefit of the designed method is to secure the whole transaction, only an authorized person can conduct the transaction. If hacker try to conduct the transaction illegally it informs to the active systems in a network and save the hacker personal information like image, IP address and location. This information can be used against the hacker for legal action.

## 5. Conclusion

With the increase of user's interest in banking sector, transactions are conducted online or via physical credit scanners. Electronic banking (E-Banking) is making things easier, so consumers are increasingly avoiding cash and checks. Banking sectors are encouraging this tendency by enhancing portals and mobile applications or web banking. Where the use of computer has provided easiness to the banks, it also causes different problem like cyber-crime which include hacking. A hacker can easily hack a system to steal a customer's personally identifiable information (PII). A hacker can use different malicious software (often used to steal data and destroy computer system like viruses, worm, spyware, mobile malware and Trojan) to gain illegal access to customer gadget or bank database. The injection of these software can be harmful for the entire banking network. Unauthorized person can access database storage, which increase the vulnerability of cyber-crime. Due to the transparency, auditability, immutability, operational resilience and data encryption essential in blockchains, it can secure the cyber security, forbid crooked actions and perceived tampering of data. The objective is putting blockchain technology to use in banking sector its security threads within the banking sector for examine the feasibility.

A two-way authentication model is designed that can secure the database and frauds within electronic banking. The first step in online business is to authenticate the customer, whether the customer is authorized for the current account. Multi-factor authentication (MFA) technique is used to find

the legitimate users by demanding a user to conform multiple identification information. The second identification is based on the facial identification. User face is identified through the gadget the user is using for the transaction like mobile or laptop. The major benefits of the designed method is to secure the whole transaction, only an authorized person can conduct the transaction. If hacker try to conduct the transaction illegally it informs to the activated systems in a network and save the hacker personal information like image, IP address and location. This information can be used against the hacker for legal act.

## REFERENCES


[1] Catota, F. E., Morgan, M. G., & Sicker, D. C. (2018). Cybersecurity incident response capabilities in the Ecuadorian financial sector. Journal of Cybersecurity, 4(1), tyy002.

[2] Collomb, A., & Sok, K. (2016). Blockchain/distributed ledger technology (DLT): What impact on the financial sector? Digiworld Economic Journal(103).

[3] Cucari, N., Lagasio, V., Lia, G., & Torriero, C. (2022). The impact of blockchain in banking processes: The Interbank Spunta case study. Technology Analysis & Strategic Management, 34(2), 138-150.

[4] Dhongade, R. (2019). Blockchain Technology Basics. Spheregen. com.

[5] Dhoot, A., Nazarov, A., & Koupaei, A. N. A. (2020). A security risk model for online banking system. Paper presented at the 2020 Systems of Signals Generating and Processing in the Field of on Board Communications.

[6] Hassani, H., Huang, X., & Silva, E. (2018). Banking with blockchain-ed big data. Journal of Management Analytics, 5(4), 256-275.

[7] Higginson, M., Hilal, A., & Yugac, E. (2019). Blockchain and retail banking: Making the connection. McKinsey & Company.

[8] Hon, W., Palfreyman, J., & Tegart, M. (2016). Distributed ledger technology & cybersecurity. European Union Agency For Network And Information Securit (ENISA).

[9] Huamán, C. H. O., Fuster, N. F., Luyo, A. C., & Armas-Aguirre, J. (2022). Critical Data Security Model: Gap Security Identification and Risk Analysis In Financial Sector. Paper presented at the 2022 17th Iberian Conference on Information Systems and Technologies (CISTI).

[10] Huang, J., Klee, B., Schuckers, D., Hou, D., & Schuckers, S. (2019). Removing Personally Identifiable Information from Shared Dataset for Keystroke Authentication Research. Paper presented at the 2019 IEEE 5th International Conference on Identity, Security, and Behavior Analysis (ISBA).

[11] Lang, J. (2017). Three uses for blockchain in banking. IBM, October.

[12] Marr, B. (2017). Practical examples of how blockchains are used in banking and the financial services sector. Retrieved December, 18, 2017.

[13] Narayanan, U., Paul, V., & Joseph, S. (2022). A novel system architecture for secure authentication and data sharing in cloud enabled Big Data Environment. Journal of King Saud University-Computer and Information Sciences, 34(6), 3121-3135.

[14] Osmani, M., El-Haddadeh, R., Hindi, N., Janssen, M., & Weerakkody, V. (2021). Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis. Journal of Enterprise Information Management, 34(3), 884-899.

[15] Smith, S. S. (Producer). (2018, 02/10/2022). Blockchain, Disruption, and the Financial Services Landscape. Retrieved from https://www.ibm.com/blogs/blockchain/2018/02/blockchain-disruption-and-thefinancial-services-landscape/

[16] Syvänne, P. (Producer). (8/12/2016, 25/06/2022). Blockchain technology: How banks are building a real-time global payment network. Retrieved from https://www.accenture.com/us-en/_acnmedia/accenture/conversion-assets/dotcom/documents/global/pdf/consulting/accenture-banking-on-blockchain.pdf

[17] WEF (Producer). (2015, 01/10/2022). Deep Shift: Technology Tipping Points and Societal Impact Retrieved from http://www3.weforum.org/docs/WEF_GAC15Technological_Tipping_Points_report_2015.pdf

[18] Yoo, S. (2017). Blockchain based financial case analysis and its implications. Asia Pacific Journal of Innovation and Entrepreneurship