An Improved Banking Application Model Using Blockchain

Muhammad Khalid Khan (mkhalidkhan@gmail.com)
Pakistan Air Force Karachi Institute of Economics and Technology https://orcid.org/0000-0001-6580-1624
Kashif Nisar
Faculty of Computing and Informatics, University Malaysia Sabah
Yumna Farooq
PAF KIET: Pakistan Air Force Karachi Institute of Economics and Technology
Shamsheela Habib
PAF KIET: Pakistan Air Force Karachi Institute of Economics and Technology
Muhammad Danish
PAF KIET: Pakistan Air Force Karachi Institute of Economics and Technology
Iram Hyder
University Malaysia Sabah

Research Article

Keywords: Consortium Blockchain ledger, Hyperledger, Smart Contract, On-chain, Off-chain, Database, and banking system

Posted Date: July 20th, 2021

DOI: https://doi.org/10.21203/rs.3.rs-582543/v1

Abstract

Every field is improving day by day as technologies become advance. The banking industry needs to improve as well, due to face lots of pressure for their backward system and having a lot of issues, such as data storage, privacy, scalability, and transparency. These issues, forced to drive the banking system towards advancements. We know that the banking system is the core of finance. So, banking should adopt blockchain technologies due to their characteristics, such as decentralization, data privacy, immutability, transparency, etc. which could help the banking industry to cope with the issues of the traditional centralized banking system. There are many systems already proposed to the banking industry, that are based on blockchain techniques like transaction, auditing, trading, data sharing, off-chain, and on-chain systems. But there is no proper solution base system for banking that carries out the banking process flow using consortium and ensures to solve all issues discussed above. Keeping these problems, we proposed a theoretical model for the banking sector. This model uses the techniques of on-chain and off-chain transactions based on a consortium blockchain. In which, a user ID, with the public key, and a private key are provided to each banking user. In this model, data stored in a third-party database as an off-chain mechanism, and mapped using (public\private) Keys and user ID as an on-chain mechanism, which will be updated and validate periodically using Smart Contract. So, if data will tamper between two periodic checks, then this tempering gets caught. This technique ensures security. In this model consortium, P2P (Peer-to-peer) protocol is also applied to ensure data privacy and partial transparency. Also, three more services provide by this model are, registration, transaction to contractual party, and transaction to the customer from the bank. The first two services are handled off-chain and the third service is handled on-chain, which ensures authentication of registered clients. In this regard, as we mentioned above, that still no banking system proposed an idea to use the consortium technique yet. So, we compare our model with the previously proposed transaction models. Our proposed model covered almost all aspects required for a banking system. This model will help to implement a blockchain-based banking system, which is more robust, secure, transparent, and scalable.

Introduction

Today’s computing is intrinsically distributed. Many industries and companies operate on a global scale, with thousands or even millions of machines on all continents. Data is stored in many distributed computers and data centers. Distributed systems have many benefits such as reliability, availability, and parallelism. In 2009, “Bitcoin: A Peer to Peer Electronic Cash System” was published pseudonymously by Satoshi Nakamoto, which comes to the advent of distributed ledger blockchain technology. The word Blockchain comprises of two sections, the blocks: means the digital data and the chain: which means all the digital data are interconnected like a chain. In other simple words, it is the digitalized recordkeeping technology that uses a public database to keep that record [1]. Blockchain is a secure decentralized distributed ledger technology that has the characteristics of immutability, transparency, and trust verification. Since the appearance of blockchain technology, it has successfully disrupted many industries including blockchain. A public ledger of blockchain technology has all the executed transactions. All the records of transactions made in blockchain are stored in blocks and maintained by all the systems that are linked in a peer-to-peer network. These blocks are similar to individual bank statements.

As discussed earlier, blockchain is immutable and any past transaction record cannot be modified [2]. Each block contains a hash of the previous one and changing the hash of the block will result in the breakage of links among blocks. There are many categories of blockchain, based on permission models. such as permission,

permissionless, and consortium blockchain. The concept of blockchain technology has initially appeared as the foundation of Bitcoin cryptocurrency, which is a type of permissionless model.

In the public blockchain-based transaction structure, all clients share one common public ledger which removes the need for central authority but raises the need to acknowledge data reliability and accuracy issues in this process. Various consensus algorithms included POW, POS are used with blockchain technology to solve nodes consistency issues in the absence of central authority. Distrustful nodes make a trust relationship using consensus. On different payment scenarios, blockchain uses digital currency like Bitcoin.

Permissionless models are not controlled by any organization or company. It has complete access to everyone who is a part of the relevant blockchain. Anyone can participate in the network. All the participants are unknown to each other [3]. The permissionless model requires an incentive to pay to the nodes who verify the transactions, which is also called mining incentives. Juri [3] has further discussed the permission system, which is because of the trustless environment in the permissionless model. All the nodes on the permission model are known to each other and can be trusted to vote, honestly. There is no need to provide any mining incentives, which makes it less complicated and trusted as compared to permissionless systems. In permissioned systems, only a particular member can publish a block of transactions which makes it less transparent and more restricted. Thus, private (permissioned) blockchain is not very decentralized and a consortium blockchain is semi-private, they have a spot between fully decentralized and fully-centrally controlled systems. Having these advantages many people are encouraged to use blockchain by replacing the traditional banking system. The traditional banking system has several issues and risks. While blockchain is the open ledger for all transactions in the network and the record of blockchain cannot be deleted or altered. So, there is no possibility of corrupted data. A system of blockchain cannot be controlled by a single person because it is a decentralized distributed ledger.

In centralized banking, all the personal information of the account holder is stored at a central server and all the branches of banks are connected to the central hub. Failure in the central server can affect all the branches. Currently, all information about cards and transactions is stored in banking servers in their centralized databases. Because in the modern world many applications or programs are working under heavy loads, special requirements of servers are needed. One server that cannot do such machines will need dozens, while the need to transfer large amounts of data. Distributed databases are increasingly finding their use. Distributed databases (DDB) are a set of copied, shared, and synchronized digital data, geographically distributed in different places by the institution [4].To reduce the cost, consumption of recourses and to enhance performance banks must use digital technologies. The risks of intruders are increasing day by day. Each bank needs the protection of data storage, confidentiality, integrity, in the process of change of information and control of the boundaries of internal information leakage. However, this task is complicated because of the presence of branches, cash dispensers, and other services. Banks are vulnerable to fraud and crimes. The estimated percentage of vulnerability is around 45.[5]It is now an urgent task to maintain the uniqueness, integrity, and security of the information circulating in distributed databases of banking infrastructure, using the capabilities of innovative information technologies, in particular, the Blockchain technology [4].

In the current financial industry, it is very difficult to synchronize a large amount of data that is segregated in silos. So much manual effort is involved in this process which is time-consuming and costly [6]. Traditional banks run their service freely and independently but, in this system, it is really hard to share information for the specific purpose of specific customers. Open banking is a system that also includes small businesses to allow sharing data securely and mutually across different banks. In the case of a third-party service provider, it also allows secure

communication and data sharing. Third parties can create mobile applications, and these applications provide a variety of services and grant user requests quickly and easily. Moreover, this process is very transparent, which improves bank credit. But, open banking is difficult because many problems can occur [7]. First, mutual authentication is hard to be transparently managed. The second is privacy provides services that enable the user to control and share personal data by customizing the access control list, and the third is provenance and regulation are necessary for accountability. To solve this type of issue blockchain is the best solution to assure none of these problems happen. Blockchain technology also makes it possible to reduce the number of intermediaries between participants in a transaction. Considering the advantage of this new technology, much research has been done on cryptocurrencies. Up to 700 currencies have been proposed yet including (CAD-Coin) the digital version of the Canadian dollar, RSCoin proposed by the Bank of England, De Nederlandsche Bank (DNB-Coin) prototype which was experimented with the Dutch Central Bank. The Central Bank of China had been studying the feasibility of the issuance of digital currency since 2014 and then published many research reports [8].

Az Azrinudin Alidin. [5] has proposed a process of integrating Saadatin (a core banking system in Malaysia) with blockchain. Three types of Muamalat contracts were included in Saadiqin which are Sale Based, Lease based, and Equity-Based. The successful integration and implementation of Saadiqin and blockchain have brought efficiency and effectiveness to the new system.

World Economic Forum (WEF) 2015, estimated that 10 percent of total Gross domestic product (GDP) will be stored on blockchains or blockchain-related technology by 2025 [9]. The banking industry is making significant strides into the blockchain with the upcoming innovations, researches, and developments. Bank-based blockchain projects are expected to transform the financial services industry, IBM-backed Hyperledger Fabric project, the Utility Settlement Coin (USC), and R3's blockchain consortium are few such examples (Harsono, 2018). The forex settlement giant, Continuous Linked Settlement CLS has partnered with IBM in creating a blockchain app store for banks [10]. Though, there is also evidence of resistance towards the adoption of blockchain in banking. For example, Whilst Visa is exploring the possibilities with distributed ledger technologies, its Chief Executive Officer (CEO) stated that it does not currently see the potential for blockchain in its core business (Kulkarni, 2018) [11] Despite the potential, opportunities, and new dimensions created by Blockchain in financial services, it is still in earlier stages. According to an interview with Oversea-Chinese Banking Corporation (OCBC), a Singapore Bank, adopting Blockchain in current financial services faced with many challenges. Blockchain real-life applications to local currencies are still in the infancy stage.

Many financial institutions including banks have already started to focus on the concept of digital currency for their regulatory processes. Bitcoin is one of the famous cryptocurrency which uses Proof of Work (POW) as their consensus model for the verification of transactions but POW requires huge computational cost. Other famed digital currencies, such as Ripple network, LiteCoin, PeerCoin are famous to use a hybrid version of Proof of Stake (POS) and POW consensus, but the implementation of these currencies has limitations of supervision, privacy, scalability, and computation cost. The transaction speed is also a big challenge, like bitcoin, only 7 transactions could be handled per second while an online payment system (PayPal) can handle 400 transactions per second (TPS) and an American multinational financial services corporation (Visa) can handle 20,000 (TPS). Security is an opportunity as well as a challenge in the implementation of blockchain in the banking industry. Satoshi Nakamoto highlighted the 51 percent attack in POW which means if half of the computers working as nodes to service the network tell a lie, the lie becomes the truth [12].

Developing a blockchain-enabled system is a high-cost affair. The cost of storage and mining is yet another growing concern for blockchain technology in banking. Bauerle discussed the costing issues of bitcoin, as it stands, each bitcoin transaction costs about 0.20 USD and can only store 80 bytes of data [12]. It is estimated that the long-term storage cost per gigabyte for a Bitcoin node will exceed 22 million USD or more and the energy required to mine bitcoin is equivalent to more energy than 159 countries consume in a year [11].

Block size issues, expanded chain size, and electronic mark size are also a few other issues that have arisen with the implementation of blockchain. These issues are called scalability issues one of the most significant issues in the blockchain. Some researchers have begun to look into the creation of another blockchain that allows for tradeoffs and improved scalability. A bank can exist without mining, connecting the entire infrastructure with a peer-to-peer network. The network is controlled by the bank, while blockchain technology retains its mechanism and all its advantages. Due to structural hashing on the Merkel Tree (a hash-based data structure), all transactions in the block are protected from changes, information remains confidential and reliable. Besides, using Merkel root, you can create simplified nodes only by block headers, while two interacting nodes can ensure that transactions are correct only by their headers. In this paper, we proposed a theoretical model for banking application using consortium blockchain based on the concept of on-chain and off-chain transactions to encounter the implementation issues of blockchain in banking systems with the consideration of basic blockchain challenges that give much more secure and reliable services.

The remaining paper comprised of the following sections: Sect. 2 presents the previous works published on blockchain implementation in the banking industry, Sect. 3 presents the system architecture of the proposed blockchain model, Sect. 4 discusses the major services of this model, Sect. 5 shows the comparative analysis of our proposed system with previously presented schemes and its results and Sect. 6 concludes the paper and highlights the open issues.

Related Work

In traditional banking systems, banking industries have to deal with multiple issues related to data security and integrity due to various aspects, such as centralization, data security, data privacy, etc. Blockchain is the most prominent technology to be employed in the banking industry to cope with the issues of traditional banking systems based on its characteristics including decentralization, immutability, data privacy, etc. Blockchain provides decentralized P2P (peer-to-peer) services between distrustful nodes with the surety of data integrity and transparency. Many publications have yet been presented, which proposed the blockchain-based models for the banking system and highlighted the implementation issues of blockchain in banking applications. Some of these researches are mentioned in this section. Sun, He, et al [8] presented the Multi-Blockchain based Central Bank Digital Currency (MBDC) model for the proper regulation of digital currency in the central bank and overcoming some blockchain implementation issues including user's privacy protection, transaction execution speed, and supervision. In this model, permissioned blockchain is used to ensure that only central banks could produce digital currency and with commercial banks and other agencies could manage this network. The authors also proposed transaction protocols for Inter-bank, Intra-bank communication, and feedback transactions. The model's simulation result showed that MBDC is scalable and can increase the transaction speed. In one paper [14], the blockchain-based inter-bank application model has been proposed and explored for payment areas and Inter-bank bill transactions. The proposed model was combined with the centralized credit matching system (XSwap) of China to testify its performance. Also, the technical aspects of blockchain and their application scenarios in the financial

industry were analyzed and discussed in the paper [14]. For testing, the authors build the prototype of distributed ledger named Narrow Bookon XSwap system in which two local Chinese banks made over 300 transactions with the price of 3.01 which is stored in the blockchain ledger. After analyzing the results, the paper concluded and suggested that such credit systems based on the blockchain can reduce regulatory cost, transaction, and settlement time which makes the process efficient and removes the need to rely on central authorities. Arantes et al [15] highlighted the implementation difficulties of blockchain in financial institutions by proposing a blockchain-based process for development projects of public financing in the Brazilian Development Bank (BNDES) and also discussed the ways to tackle these issues. The proposed solution is the payment system to deal with intermediaries in the process of BNDES. To track public funding, smart contracts were used in the solution with a proprietary token named BNDES token which is equal to one flat Brazilian currency. The proposed model is based on the Ethereum blockchain and used ERC-20 (Ethereum token) standards as a foundation. Many issues were raised with the use of BNDES token that how credit relationship will establish. To understand the gap in research and development into blockchain-based big data in the banking system, Hassani et al. [11] summarized the opportunities and challenges of banking from a banker's perspective and presented a comprehensive review of the impact of blockchain in banking and the impact of big data in the blockchain on banking data analytics in the future and evidence of successful implementation of blockchain in few banking industries. In one paper [4], Popova, Natalia A et al. presented the use of Blockchain technology without tokens by proposing a solution to the problem of maintaining the uniqueness of information in distributed databases to protect information about banking transactions, transfer amounts, card details, names of participants, etc. For this purpose, the protection mechanisms of distributed databases were analyzed. Another paper [2] proposed and implemented the secure and reliable model for banking systems based on Ethereumblockchain to cope with the issues of centralization, data tempering, security, and server crashes of the traditional central server-based banking system. The authors of this paper simulated their model on the Ethereum test network called Rinkeby and testified the smart contracts on Mocha (a JavaScript-based automated\manual testing framework). Alidin et al. [5] discussed in their paper that the structure of their implemented model which integrates their financial institution, Saadiqin (an industrial solution for Islamic banking) with Blockchain technology. The authors first discussed the existing problem with financial services particularly Islamic financial and the benefits of Blockchain implementation in financial services and then presented the feasibility of the proposed model. The initial version of this model has been implemented on the Hyperledger platform which integrated with Saadiqin core system and client interface using MuleSoft (an integration module). Lu et al [15] highlighted the issue of banking loans to micro organizations, as we know these organizations contribute in GDP (Gross domestic product) increments and provide job opportunities, but these organizations face difficulties in taking loans from banks and have several issues for banks, like higher credit cost, etc. To cope with this issue, the author proposed a novel study of BIS (Bank-tax interaction systems) that is based on blockchain technology. The author solves this issue by maintaining a tamper-resistant building bases smart contract in a distributed environment and it will support the peer-to-peer exchange of data among smart devices and IoT (internet of things) based devices. Xu et al [7] stated in their paper when one organization wants to connect with other organizations, they need to share data and exchange information with the mutual contract, but exchanging this data requires higher authentications and provenance of the participants. In solution, a blockchain-based data sharing scheme for open banking named a provenance-provided data sharing model (PPM) is proposed to meet the above-mentioned requirements. Chu et al [16] in their paper identifies the problem of manual processing when an audit letter for the third party that is being audited and the final result may be corrupted, slow processed, and outdated. To solve this issue, they proposed a machine learning-based technique, which consists of two processes that were data authorization, and data acquisition. These processes are integrated with the smart contract to become automated. Zheng et al [17] identified in their paper when financial institutions disclose their

application programming interfaces to third-party providers. The main issues arise, like malicious attacks, data leakage, data tampering, privacy disclosure, etc. In solution, a blockchain-based data sharing scheme for open banking blockchain named OBBC is proposed, in which blockchain saves the Application Programming Interface (API's) information. So that it is not dominated by anyone.

Besides the implementation issues of blockchain, including transaction cost, throughput, and storage capacity in real-world applications [18], some specific issues also exist in banking applications related to the implementation of blockchain. Banking industries require that business secrecy to some private information should remain in their application [15]. So as the characteristic of the public blockchain, the transparency of the entire information to the whole networks including customers and other contractual companies is not suitable in this context neither the complete privacy of transaction information is acceptable by customers. Considering this challenge, many papers proposed blockchain-based models using consortium blockchain which benefits the decentralization of public blockchain with the privacy and transaction efficiency of the private blockchain. But some papers pointed out the issues of data storage and query inefficiency in consortium blockchain, which caused network overhead and service delay [19].

In this paper, we are going to propose a theoretical model for banking applications using consortium blockchain, based on the concept of on-chain and off-chain transactions to encounter the problems discussed above. In this model, the transactions related to the customers will be process and store on-chain, while the transactions between the bank and other regulatory parties will be process and store off-chain. Only the index of the stored information will be saved in on-chain which can decrease the consumption of storage capacity and increase query efficiency in consortium blockchain, reduce the transaction processing overhead from the network and increase throughput in terms of TPS (transaction per second) on-chain. Also, a very minimum cost per transaction will be required for off-chain data processing. This model tries to overcome the problem of disputes that may occur in off-chain transactions, due to anonymity by optimizing the solution proposed and used in Raiden Network [20], which is based on Ethereum blockchain, in the context of banking applications. In Raiden Network [20], the payment channel between the counterparties must be opened on-chain before off-chain transactions to verify the balance of the sender's account, but this network presented the solution in the context of the public blockchain. In this model, the authentication and verification of transactions of information including documents or other types of data will be done directly through a smart contract, while for the transactions including tokens exchange. The counterparties must open an account on-chain for balance proof and authenticity.

Proposed System Architecture

Considering blockchain characteristics, current banking industries need to adopt blockchain technology which provides services like decentralization, data privacy and integrity, and immutability. But in researches that have been done yet in this area, pointed out some issues related to blockchain implementation for a real-world banking application. Therefore in this paper, an optimized theoretical model using consortium blockchain is proposed for banking application which uses the concept of on-chain and off-chain transactions to cope with the specific limitations of blockchain implementation in the banking industry including data privacy and partial transparency along with the basic scalability issues of blockchain including transaction speed, security, cost, storage capacity, and query inefficiency.

In this section, the system architecture of the banking application model is proposed and discussed. The proposed system architecture is divided into four layers as shown below in Fig. 1.

3.1 Data Storage Layer

In the proposed system, the bank's customer transactions are processed on-chain and the transactions between the bank and counterparties including other banks, companies, or regulatory parties are processed off-chain to be kept private. The data storage of both on-chain and off-chain transactions is held and Blockchain maintained separately which reduces the storage consumption of consortium blockchain and improves querying efficiency. The data type of the on-chain transactions input is always integer or some token values as in Bitcoin and the format of on-chain transactions is standardized according to banking standards and rules. Therefore the data processed from on-chain transactions is stored in distributed ledger associated with each payment channel.

The off-chain transactions depending on the data type are stored in third-party relational databases, e.g. MySQL, Azure, and SQL Server. It is recommended to use distributed database like MongoDB or Azure to store data. In distributed databases, the data is replicated on multiple nodes and reduces the chance of data loss in case of failure of a single node. Also distributed databases have strong querying capabilities and cheap storage for large amounts of data compared to blockchain. The transaction ID and transaction hash of off-chain data are stored in an on-chain ledger which is updated and validated periodically using a smart contract so that if data is tempered between two periodic checks, then this tempering is caught.

3.2 Network Layer

In the network layer, the consortium blockchain peer-to-peer in the network layer, the consortium blockchain peer-to-peer protocol is applied which creates links between customer-to-bank and bank-to-counterparty communication. This consortium blockchain can be applied by the mutual association of multiple banks or several branches of one organization. This distributed protocol allows the customer to send transactions to any other peer including bank authorized person or another customer. Each member node of this network either bank's authoritative users or customers has one local copy of distributed ledger associated with their payment channel. This means that customers can only have a ledger of their payment channel which is distributed between nodes associated with that channel while authorized user nodes are associated with each payment channel so they have a complete ledger of the network. This technique ensures data privacy and provides partial transparency to customers who are related to the transaction. Only users who are registered in the system off-chain are allowed to be a part of this network. These users are identified in this network with their public key generated at the time of registration.

In this network to communicate with other nodes, the user has to request for the transaction which is broadcasted only in his payment channel and validated by authorized users. The approved transaction is added to the blockchain. The best-suited blockchain which incorporates the proposed model requirements is Hyperledger Fabric [21] which is an open-source permissioned blockchain for enterprise-level institutions. It allows creating separate payment channels between members by calling chain code (user-defined smart contracts). With the payment channel creation, the genesis block (first block of a blockchain) is created for the channel ledger which stores information about members, validators, and policies [22].

3.3 Services Layer

This is the main layer of the proposed model from a business perspective which integrates the blockchain services with the banking application's business logic and services. This system consists of three major services i.e. registration, bank to contractual party transaction, and bank to customer transaction. The first two services are handled off-chain and later service is handled on-chain by using the blockchain services. Users must register in the

system whether they are customers, bank authorized employees, or any contractual party. Only the authenticated users who are registered in the system can get an application account and blockchain account. The administrators of this application are registered as authorized users to this blockchain and use smart contracts (chain code in case of Hyperledger Fabric) to declare other employee nodes as authorized validators. Users first log in to the system's application and then log in to a blockchain account. On the creation of a new account, the user must have to buy some tokens for allowing them to do payment-based transactions. As this system is based on permissioned blockchain architecture, only the authorized users can take part in validating the transactions. Any transaction fee is not involved in the execution of this consensus. The transactions are selected from a pool, based on a first come first serve strategy. The voting-based consensus is formed between the validators to approve transactions in which 2/3 majority votes are respected to be Byzantine Fault Tolerance (BFT). This can be achieved using smart contracts but for strong security concerns, the consensus algorithm should be used to validate and authenticate the transactions by following complete procedures.

Hyperledger Fabric provides support for pluggable consensus protocols. For the proposed system, Practical byzantine fault tolerance (PBFT) [23] or Tendermint [24] consensus algorithms are the most suitable BFT protocols. In PBFT, one node is selected as a primary node which initiates the voting process. It is a three steps process namely pre-prepared, prepare, and commit. This algorithm can handle up to 1/3 of the ratio of the faulty nodes. The practical implementation and performance analysis of PBFT with Hyperledger Fabric has already been presented in [25] that emphasis us strongly to used of PBFT in this model implementation.

Tendermint is a punishment-based BFT algorithm that is based on three steps namely pre-commit, pre-vote, and commit. In this algorithm, validators have to lock their coins before the consensus round start and the node punished them who found dishonest [26].

For off-chain communication between the bank and contractual parties, a smart contract is triggered by authorized users who process and store the transaction off-chain and save its transaction ID and transaction hash in an on-chain ledger. The basic format of smart contracts for off-chain transaction processing is generated at the time of application development based on banking standards and policies. These contracts are editable by authorized employees who can revise the contracts according to the transaction format. These contracts include authentication and validation rules, policies, and also include other contractual terms which can be needed for off-chain transaction security. The contractual parties have to open an account on-chain for a payment-based transaction. But their transactions are operated off-chain, because these transactions may have to follow some rules or different types of format rather than basic transaction format.

To accomplish secure processing of transactions using smart contracts off-chain, it must be ensured those smart contracts are executed in a secured framework. For this concern, the Crypt let Fabric [8], the service provided by Microsoft Azure, can be used as its implementation is based on an off-chain transaction. In this framework, the smart contract is built and executed outside blockchain in a shared attested environment trusted by both parties. This can reduce the complexity of building and maintaining the smart contracts on-chain. All the business logic of smart contracts is written using Crypt let framework. The output of this execution is directly stored in off-chain databases.

3.4 Interface Layer

At the interface layer, the application interface is implemented from where the customers and contractual parties, and bank employees interact with the system. This provides a way to access the system services. A separate

interface is provided for the bank customers and contractual parties as the execution of their transactions are done through different procedures. The authorized user interface has more options than other users as most of them may play the role of administrator of this application. After entering the application, the user can access the blockchain network using his private key.

System Detail

In this section, the system's major processes, including registration, customer transaction (on-chain), and contractual party's transactions (off-chain) and their communication flows are discussed in detail.

4.1 Registration and Blockchain Account Process

In the proposed system, the registration service plays a key role in the authentication of users within and outside the blockchain. The authentication provided by this process of registering, personal details of users in the system help to avoid the malicious or unauthorized users being a part of the blockchain. Also, it reduces the chance of illegal token exchange outside the blockchain which minimizes off-chain transaction disputes such as money laundering. Throughout the system, bank customers are identified by User Id (UID) and the contractual client identified by Client ID (CID).

When a new user accesses the system as a customer to open an account in the bank, he first has to register his details. on above, Fig. 2. shows the complete process that how the customer information is being processed in the system. The personal details provided by the customer will validate and authenticate first and then this information is store in off-chain servers on successful registration. Otherwise, the system discards the given details and informs the user about the status.

On successful registration, a system account and blockchain account will open and assign to the customer by providing him UID for the application's account and private\public keys for the blockchain's account. The private and public keys were automatically generated with UID. On the creation of a blockchain account, a separate payment channel is also created in the customer's account to ensure privacy between the authorized user's node and the receivers of the transaction. The wallet address is also assigned to a user for a blockchain account which is also operated by using a private key. The customer's private key and UID are used to generate his Wallet address which could be verified by comparing with his private key. To initiate the transactions' execution from this blockchain account, the customer must have to buy some token to maintain the account balance. The tokens are some digital numbers that will be associate with the customer's account, on buying them by using local currency. It is assumed in this system that one token equal to one local currency. The transactions throughout the blockchain will do by using these digital tokens.

The contractual client's registration will be done somehow differently from the bank customer as shown in Fig. 3.

The contractual client including other banks to be added to consortium blockchain authority, any company for making some agreement for token exchange, and any regulatory party like Audit Company deals with the system's authorized users through off-chain transactions.

To initiate this process, the client provides its institutional details which are authenticated and validated off-chain. On successful registration, the client's provided information will store in off-chain servers, and the system account will assign to the client by providing him CID. If the client wants to execute transactions that involve token

exchange then it has to request for the blockchain account to the authorized users. The request will authenticate based on institutional details and transaction type. The private and public keys will generate automatically and assign to the client on its system account in case the request has been accepted. However, the transactions will execute off-chain for a client account. A client has to buy some tokens to initiate transaction execution from its account.

4.2 Customer Transactions Process

Customer's transaction execution and processing will be done within consortium blockchain using specific payment channel associated with the customer account and their results will also store on-chain. These transactions are validated by authorized users through the BFT consensus algorithm. The flow of transaction processing within the system is shown in Fig. 4.

To access the blockchain account, the customer first login the system using UID and then access the blockchain account by using his private key. The public key will use as a public address for the identification of the user on-chain. The customer has to digitally sign the transaction before executing it. The transaction must include the sender's public key, receiver's public key, digital signature, and transaction amount. Before processing the transaction, the sender's balance account will check against the transaction amount.

If the account balance is not enough for the transaction, then the transaction will reject. Otherwise, the transaction will add to the pool for authentication using a consensus algorithm. Meanwhile, the transaction amount is also subtracted from the sender's account and add to the receiver's wallet address for preventing double-spending problems as used in [8]. To validate the transaction, all the authorized users take part in voting-based consensus. If 2/3 majority of voters approve the transaction, the transaction will be added to the block associated with the sender's account payment channel. For each payment channel, a separate ledger will maintain which distribute only among valuators, channel owners, and channel receivers, which increases the transparency of the transactions to the users, associated with those transactions and ensures data privacy between different bank customers. The consequences of this solution would be to increase the maintenance complexity for a large network, but this problem could be resolved by sharing the maintenance task among authorized users of the consortium.

4.3 Contractual Party Transactions Process

The transactions between the bank and contractual clients will process and store off-chain to minimize the blockchain network complexity and thus increases the on-chain transactions throughput, minimize overall cost and reduce the network storage consumption. To execute the transaction, a client has to log in to the system using CID as shown in Fig. 5.

Then it requests for the transaction off-chain which will process through the integrated off-chain framework executing smart contracts. On the transaction request execution, a smart contract will trigger, which authenticates this request and checks whether the transaction request includes token exchange. If the transaction amount is not included in the transaction request, the request will pass to authenticated users or administrators on their system account. Then the user-defined smart contract will execute by authenticated users on the transaction, which validates the transaction against policies and standards. If the transaction amount is included in the requested transaction then the client's on-chain account will create in case of the new client. The asymmetric key pair (cryptographic key) will generate and assign to the client on its system's account. If the client already has a blockchain account then it has to include the blockchain account's address in the transaction for account

validation. Then account will be cross-checked by smart contract for balance proof. If the account has a sufficient balance that equals to or greater than the transaction amount, then the transaction amount will subtract from the client's account and add to the bank's wallet address and the transaction will process off-chain in the same way as discussed above. The output of this execution will directly store in the off-chain database, its transaction ID and transaction hash will automatically write in the ledger associated with the payment channel of the client's account.

Result And Comparision

The mechanism of most cryptocurrencies, public blockchain, is not suitable to the banking as it has a complete decentralization. Private Blockchain has the issues of centralization which raises many problems, in which major is the trust among the participants. A consortium blockchain is not a new concept in banking, many models have been proposed by previous studies. However, it raised some other issues, such as transaction speed, security, cost, and storage capacity. We have compared and analyzed five different proposed models with our model, under the attributes provided in Table 1.

According to Table 1. Our proposed model possesses features that other models may not have. Few approaches [14] [2] used the permissionless models in banking which raises the issues of transparency. Our proposed model uses the consortium blockchain model. Blockchain characteristics cannot be completely implemented into the banking industries, therefore an optimized model is proposed to cope with the challenges faced by the banking sector in the implementation of blockchain.

In models [14][2], the off-chain framework was not used due to which on-chain data capacity utilization increased. Our proposed model uses off-chain transactions for contractual parties' transactions, which allows banks to process and store the most confidential transaction outside the blockchain. Also, the off-chain solution solves scalability issues of blockchain as mentioned in [18]. With the ever-increasing problems of terrorism, KYC (know your customer), is now becoming a critical aspect related to the prevention of criminal use of banking funds and services in the form of money laundering.[28].

The chances of transaction-related disputes are very minimum in our proposed solution as all the members are registered including customers and contractual clients, by providing their necessary personal details before making any transaction and authorized persons can only validate the payment channel. All the transactions on the network can easily be monitored by authorized members. The registration process also helps to identify the members, because all the users must register, whether they are customers, the bank authorized employees, or any contractual party, thus providing the benefits of KYC, and eliminates the risk of anonymous transactions and restricts the malicious customer to join the network. Since the transaction ID and transaction hash of off-chain data stored in an on-chain ledger, which is updated and verified periodically by using a smart contract, this phenomenon helps to identify the data, which is tempered.

Off-chain security is not considered in most of the related models as mentioned in Table 1. Crypt let Framework is suggested for off-chain transaction security, which will secure distributed third-party off-chain framework for transaction processing. Each member has only one local copy of the ledger of their payment channel, which is distributed between associative nodes. However, authorized user nodes are associated with each payment channel. This helps to improve and ensure data privacy, and also provides partial transparency. Double spending is another problem, few of the research papers suggested the solution but some of the related models [14] [7] [16] do not consider the solutions. our proposed model also provides the solution to the double-spending issue. In our

model, the account balance of the sender will check before making any transaction, if there will be sufficient amount for the transaction, then the amount will be subtracted from the sender account and add to the receiver account as an unverified amount while waiting for the consensus process to avoid the double-spending problem. During the verification of transactions, the voting consensus is used, which requires a 2/3 majority of votes. PBFT and Tendermint consensus protocols are suggested to ensure the security of the network. PBFT can handle up to 1/3 of faulty nodes, and Tendermint is a punishment-based protocol, where validators have to lock their coin before going through the consensus mechanism. After the consensus mechanism and verification, the unverified amount of the receiver is converted to the receiver's account. The wallet will store the private keys of the user.

Table 1
Comparison between related models

Ref Proposed Work	**[8]**	**[14]**	**[2]**	**[7]**	**[16]**	**Our Proposed Model**
Type of Blockchain Used	Consortium	Permissionless	Permissionless	Consortium	Consortium	Consortium
Off-Chain Framework	Not Used	Not Used	Not Used	Used	Used	Used
Transaction Disputes Issue	Resolved	Resolved	Resolved	Resolved	Resolved	Resolved
Off-Chain Transaction Security	Not Considered	Not Considered	Not Considered	Not Considered	Not Considered	Not Considered
Transaction Fees	Not Required	Required	Required	Not Required	Not Required	Not Required
Transactions Transparency Issue	Resolved (Partially)	Not Resolved	Resolved	Resolved (Partially)	Resolved (Partially)	Resolved
Throughput (TPS) Expected	High	Low	Low	Not Mentioned	Average	High
T-Cost Expected	High	High	High	Low	Low	Low
Double Spending Problem	Resolved	No	Yes	No	Yes	Resolved
On-Chain Storage Capacity Utilization	High	High	High	Low	Low	Low
Maintenance Required	High	Low	Low	Not Mentioned	High	High

The cost of storage is still another concern regarding blockchain technology in banking. On the behalf of some careful statistics, that the long-term storage cost per gigabyte for a Bitcoin node will exceed up to 22 million USD or more. Related work [8][14][2] has high on-chain utilization, which not only increases the computational cost but also the storage cost. However, our proposed model has a low computational cost because of two reasons. First, the complex data processing is done off-chain which has a low cost as compared to process on-chain [18]. Secondly, the BFT consensus algorithm is used in this model which takes less processing time.

In models [14] [2] Ethereum blockchain network was used which has low transaction speed [29]. This proposed model can also help to improve transaction speed as it enables the banks to transact directly and view the same ledger of transactions after verifying through consensus. The transactions are select first in first-order (FIFO). BFT consensus algorithm is used on-chain which takes less transaction processing time and provides high throughput. The suggested BFT algorithms, PBFT and Tendermint, have a throughput of 50tx/s and 10tx/s respectively[26].

This can increase the transaction processing speed within the network. Also, smart contracts will operate and maintain outside the blockchain for complex transactions, which can reduce the network overhead and improve transaction processing on-chain.

One of the limitations of the proposed model is that more consideration is required for maintaining the multiple payment channels, but this issue can be solved by the distribution of maintenance tasks between multiple authorized bank employees of consortium blockchain.

Conclusion

In this paper, we highlight the issues of traditional banking systems, like data storage, privacy, scalability, and transparency. To cope with these issues, we proposed a theoretical model based on new technology named blockchain for the banking industry. Our model used on-chain and off-chain techniques using consortium blockchain and comprised of four layers, a data storage layer, network layer, consensus layer, and application layer. Each layer has a unique purpose to ensure blockchain-based banking systems become secure, immutable, transparent, and decentralize. In these layers, three processes are followed, that guarantees authentication of the banking system. In the result, we compare our model with other proposed models and found that our proposed system is perfectly fitted in all aspects that were included in the problem statement. As each industry is growing and adopting new technologies, banking systems also need to upgrade themselves with new technology and our system provides a better solution to implement it practically. In the future, we can associate third parties and other transaction bodies in the banking system to completely replace the traditional banking system.

Declarations

Acknowledgment: The authors would like to thanks Professor Dr. Yong-Jin Park (IEEE Life member) Former Director IEEE Region 10 for his expertise, his valuable comments and suggestions to improve the quality of the paper.

Funding Statement: This research work is fully supported by College of Computing and Information Sciences, PAF Karachi Institute of Economics and Technology, Karachi, Pakistan.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Lu, Zhihui, et al. ”Bis: A Novel Blockchain Based Bank Tax Interaction System in Smart City.” 2019 IEEE Intl Confon Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Confon Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech).IEEE, 2019.
2. Bakaul, Masum, Nipa Rani Das, and Madhabi Akter Moni. ”The Implementation of Blockchain in Banking System using Ethereum.” International Journal of Computer Applications 975:8887.
3. Mattila, Juri. ”The blockchain phenomenon.” Berkeley Roundtable of the International Economy(2016).
4. Popova, Natalia A., and Natalia G. Butakova. ”Research of a possibility of using blockchain technology without tokens to protect banking transactions.” 2019 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus). IEEE,2019.
5. Alidin, Az Azrinudin, Abdo Ali Abdullah Ali- Wosabi, and Zamri Yusoff. ”Overview of blockchain implementation on islamic finance: Saadiqin experience.” 2018 Cyber Resilience Conference (CRC). IEEE,2018.
6. Ding, Xiaowei, and Hongyao Zhu. ”Blockchain- Based Implementation of Smart Contract and Risk Management for Interest Rate Swap.”CCF China Blockchain Conference. Springer, Singapore, 2019.
7. Xu, Zhiyu, et al. ”PPM: A Provenance-Provided Data Sharing Model for Open Banking via Blockchain.” Proceedings of the Australasian Computer Science Week Multiconference.2020.
8. Sun, He, et al. ”Multi-blockchain model for central bank digital currency.” 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT). IEEE,2017.
9. World Economic Forum.. Deep shift: Technology tipping points and societal impact. m2015.
10. Harsono, Hugh. ”Bank-based blockchain projects are going to transform the financial services industry.” Tech Crunch: The latest technology news and information on startups(2018).
11. Hassani, Hossein, Xu Huang, and Emmanuel Silva. ”Banking with blockchain-ed big data.” Journal of Management Analytics 5.4 (2018):256–275.
12. Bauerle, Nolan. ”What are blockchain’s issues and limitations.” Accessed 15th July(2018).
13. Wu, Tong, and Xiubo Liang. ”Exploration and practice of inter-bank application based on blockchain.”2017 12th International Conference on Computer Science and Education (ICCSE). IEEE,2017.
14. Arantes, Gladstone Moises, et al. ”Improving the Process of Lending, Monitoring and Evaluating Through Blockchain Technologies: An Application of Blockchain in the Brazilian Development Bank (BNDES).” 2018 IEEE International Conference on Internet of Things (iThings)and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData).IEEE,2018.
15. Lu, Zhihui, Xiaoli Wan, Jian Yang, Jie Wu, Cheng Zhang, Patrick C. K. Hung, and Shih-Chia Huang. “Bis: A Novel Blockchain Based Bank-Tax Interaction System in Smart City.”2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress(DASC/ PiCom/ CBDCom/ CyberSciTech), 2019.
16. Chu, X. yan, Jiang, T., Li, X., Ding, X. wei.“Bye Audit! A Novel Blockchain-Based Automated Data Processing Scheme for Bank Audit Confirmation.”Second CCF China Blockchain Conference, CBCC2019.

17. Zhang, Q., Zhu, J., Ding, Q. OBBC:“A Blockchain Based Data Sharing Scheme for Open Banking.”Blockchain Technology and Application 2019.
18. Kim, Soohyeong, Yongseok Kwon, and Sunghyun Cho. ”A survey of scalability solutions on blockchain.” 2018 International Conference on Information and Communication Technology Convergence (ICTC).IEEE,2018.
19. Zhang, Qing, et al. ”Future OTC: An Intelligent Decentralized OTC Option Trading and E-contract Signing System.” CCF China Blockchain Conference. Springer, Singapore, 2019.
20. Raiden Network. ”cheap, scalable token transfers for Ethereum,”2018.
21. “Hyperledgerproject,”2015.[Online].Available: https://www.hyperledger.org/
22. “Hyperledger”.[Online].Available:https://hyperledgerfabric.readthedocs.io/en/master/channels.hml.
23. Kwon, Jae. ”Tendermint: Consensus without mining.” Draft v. 0.6, fall 1.11(2014).
24. Sukhwani, Harish, et al. ”Performance modeling of pbft consensus process for permissioned blockchain network (hyperledger fabric).” 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS). IEEE,2017.
25. Zheng, Zibin, et al. ”An overview of blockchain technology: Architecture, consensus, and future trends.”2017 IEEE international congress on big data (BigData congress). IEEE,2017.
26. Dib, Omar, et al. ”Consortium blockchains: Overview, applications and challenges. ”International Journal On Advances in Telecommunications 11.12(2018).
27. Blockchain, 2017. Bletchley The Cryptlet Fabric Evolution of blockchain Smart Contracts. Availableat: ¡https://azure.microsoft.com/en-us/blog/scanatomy-2/¿
28. Practical examples of how blockchains are used in banking and the financial services sector. Retrieved from https://www.forbes.com/sites/bernardmarr/2017/08/10/ practical-examples-of-how-blockchains-are-used-in-banking and-the-financial-services sector/f1b33831a116.
29. Ethereum 101- What is Ethereum. Retrieved from https://www.coindesk.com/learn/ethereum-101/who-createdethereum.

Figures

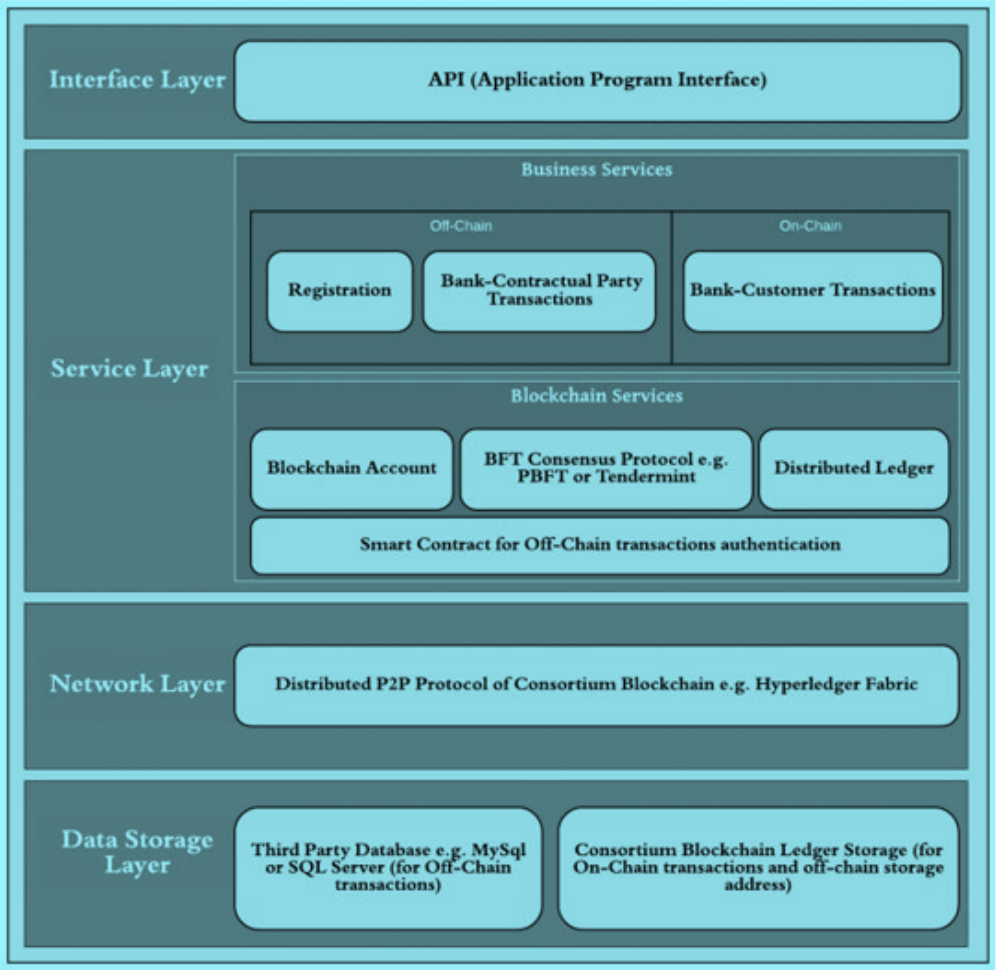

Figure 1

System Architecture for Banking Application based on Consortium Blockchain

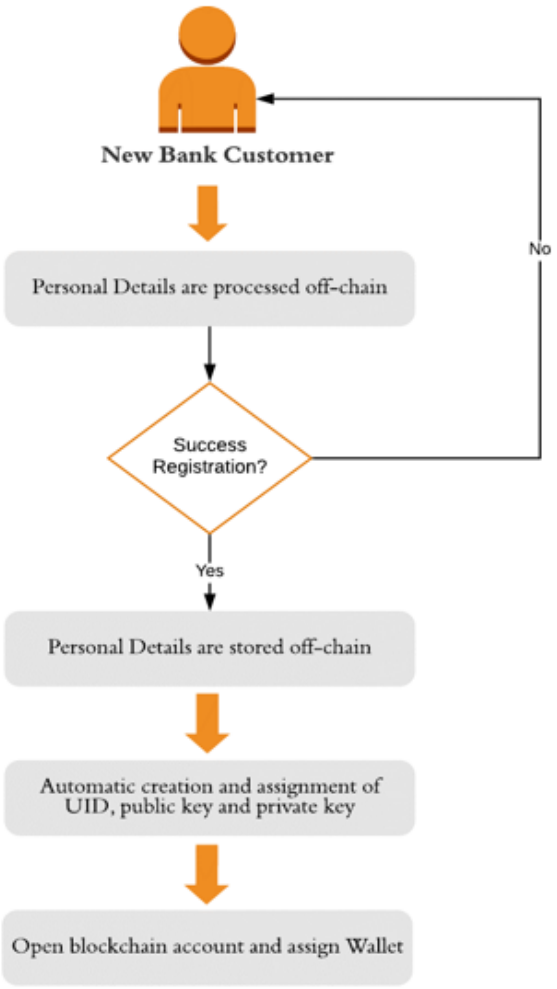

Figure 2

Customer registration process

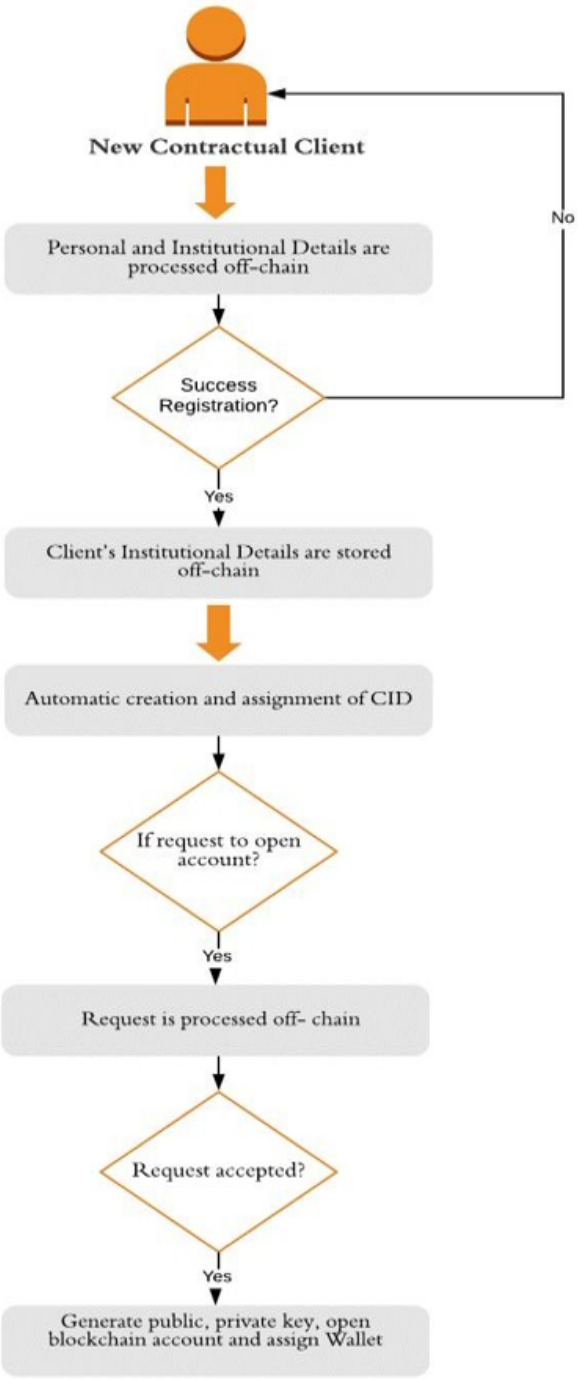

Figure 3

Contractual client registration process

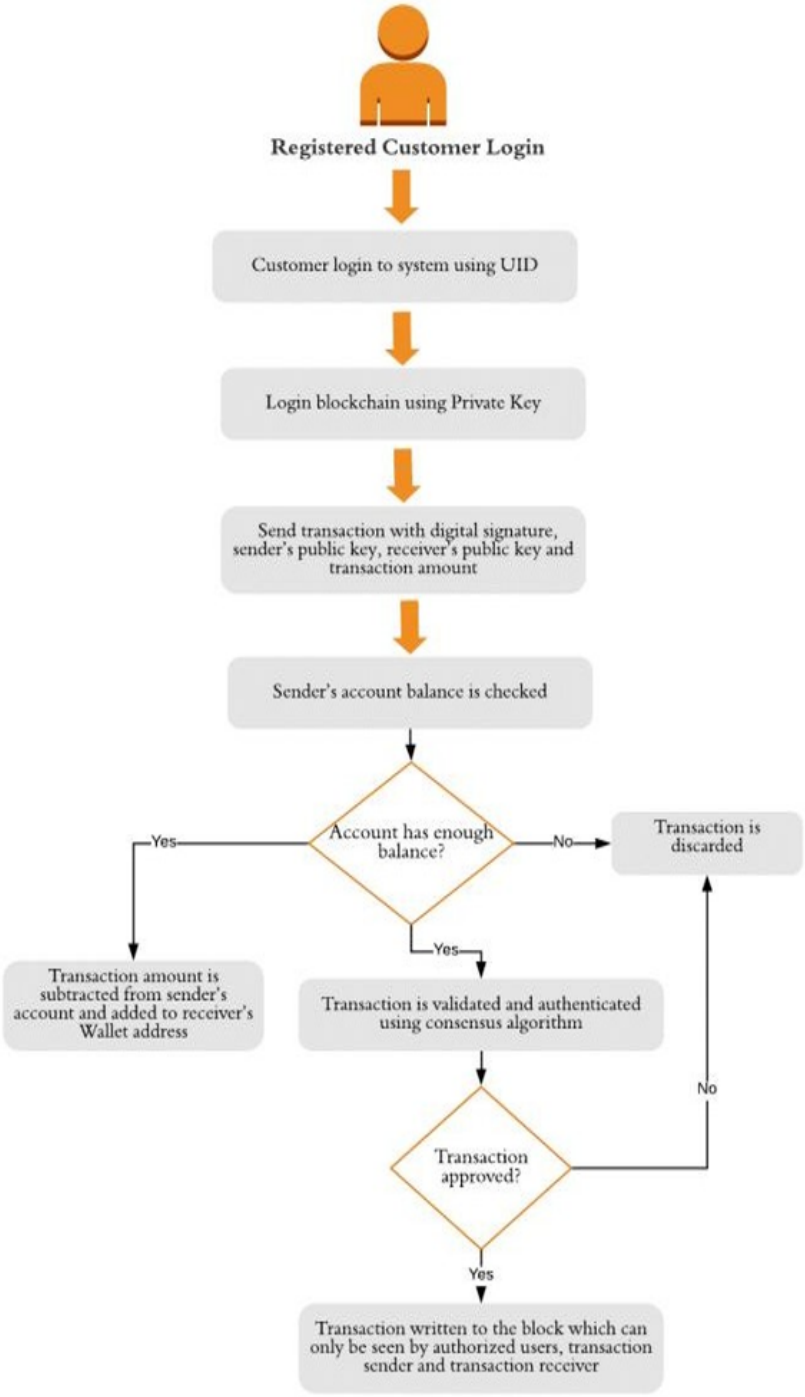

Figure 4

Customer transaction process flow

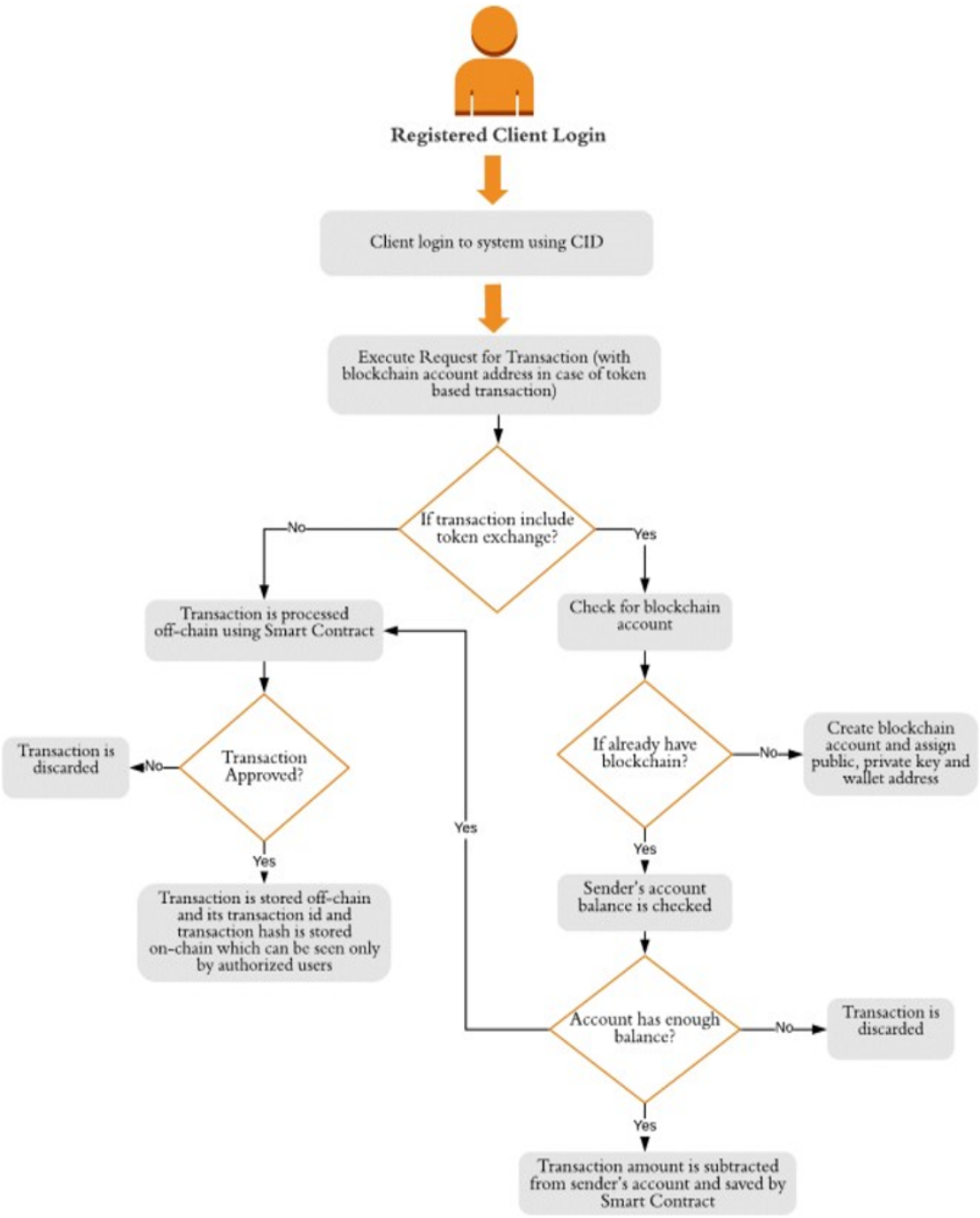

Figure 5

Contractual Client Transaction Process Flow