Open Banking API Framework to Improve the Online Transaction between Local Banks in Egypt Using Blockchain Technology

Mohamed Hamed Mohamed Hefny *, Yehia Helmy, and Mohamed Abdelsalam

Business Information Systems Department, Faculty of Commerce & Business Administration, Helwan University, Cairo, Egypt; Email: ymhelmy@yahoo.com (Y.H.), dr.m_abdelsalam@commerce.helwan.edu.eg (M.A.)
*Correspondence: Mohamed.Hamed21@commerce.helwan.edu.eg (M.H.M.H.)

Abstract—**Blockchain technology is considered to have a high impact on the banking industry due to its potential to enable new ways of organizing and handling banking industry activities. It reduces costs and time associated with intermediaries and improves trust and security. This study explores how blockchain technology could enhance fund transfer transactions between local banks in Egypt by providing a blockchain-based framework to conduct instant payments and financial transactions. Due to its properties, blockchain is qualified to play a vital role in the financial sector by helping financial institutions protect their daily routine financial transactions with a more secure, instant, and low-cost model. The findings show that blockchain technology's characteristics (enhanced security, transparency, data integrity, information immutability, and instant settlement) and using open Application Programming Interface (API) architecture will give seamless integration of financial services and applications. This approach will improve Egypt's financial transactions between local banks as well as the growth of e-payments and digital transformation. The proposed framework, which uses blockchain and open banking API architecture in fund transfer between local banks, will provide a great opportunity and space for banks to improve and positively impact digital transformation strategy, financial inclusion, digitization of payments, online SME finance, increasing access points, partnerships with FinTech's, and using innovative technologies further to bring efficiency in banking and payments. By using a blockchain network for domestic remittance Automated Clearing House (ACH), banks should be able to offer customers a faster, cheaper, and more efficient service.**

Keywords—**blockchain technology, e-banking, e-payment, banking integration, open APIs**

I. Introduction

In recent years, a significant IT innovation known as blockchain technology has emerged as a potentially disruptive force. The concept of a global consensus ledger, which is kept and maintained on a distributed network of computers, lies at the heart of this technology. Since the introduction of bitcoin as a digital currency, blockchain technology has gained widespread popularity. Satoshi Nakamoto first introduced the bitcoin mechanism in 2008, in a paper entitled "Bitcoin: A Peer-To-Peer Electronic Cash System" [1]. This paper presented a novel approach to electronic payments, enabling funds to be transferred directly from one party to another without the need for intermediaries. The name given to the technology behind this groundbreaking innovation is blockchain.

A. Research Problem

The global financial system is massive, serving billions of individuals and businesses and facilitating trillions of dollars in transactions each day. Yet, while we can send an email around the world in a second, transferring money can take days to reach its destination. Financial intermediaries are required to transfer any sum of money, and each transfer incurs a service charge. Unfortunately, these intermediaries are also vulnerable to fraud, which results in increased regulation and higher costs for everyone involved. Blockchain technology offers a solution by reducing the number of middlemen involved, improving security, and lowering costs. By increasing the velocity of money, blockchain can boost cash flow and capital investments [2]. Financial institutions and banking systems should adopt blockchain technology to simplify both local and foreign payments and bond trading. Currently, international payments can take several days to reach their destinations and can be costly procedures. However, blockchain-based payment systems can overcome these challenges by offering a reliable, fast, low-cost, and secure system to transfer money from one party to another. Unlike bitcoin transactions, these transfers cannot be anonymous, as they must be traceable. Today's financial payment system relies largely on fund transfers, which, while well-implemented, take time and money to process and settle. Fig. 1 shows the number of days required to complete the direct debit transaction process and its settlement, as well as the time window constraints of the Automated Clearing House (ACH) network.

Manuscript received January 26, 2023; revised March 6, 2023; accepted March 31, 2023; published July 26, 2023.

doi: 10.12720/jait.14.4.729-740

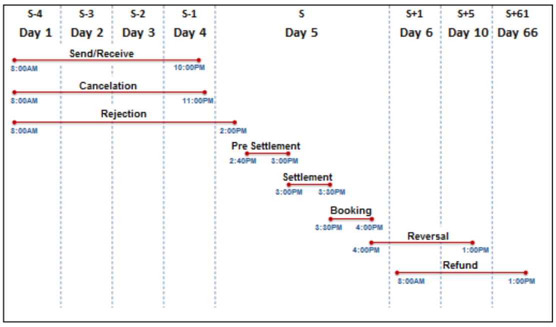


Figure 1. ACH direct debit window timing.

B. *Objective*

The main objective of this paper is to introduce a blockchain-based open banking framework designed to enhance the performance of the ACH transaction process between local banks in Egypt. Additionally, we aim to implement a blockchain payment-based framework to enable instant transactions between sources of funds such as bank accounts and cards, available around the clock 7×24.

II. Background and Related Work

A. *Blockchain*

Blockchain is a type of Distributed Ledger Technology (DLT) that has been defined as "an incorruptible digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value" [3, 4]. It acts as a shared database, with all copies synced and verified. While the technology is still in its initial stages, its potential to eliminate the need for third-party trust in exchange transactions is among its defining characteristics [5]. The potential uses of blockchain technology offer numerous expected benefits to the industry and can give birth to a new generation of services. Blockchain provides a robust cyber security solution and high-level privacy protection, making it an ideal technology for any form of asset [6]. In a blockchain-based model, there is no need to store information with third parties [7]. Nowadays, blockchain is becoming more significant to any business. According to Tan and Zhao *et al.* [8], since the advent of the internet, blockchain may have had the most substantial impact on information technology [9]. Distributed ledgers are public databases maintained by a group of people rather than centralized in one location. The information is processed on a distributed ledger that is spread over thousands of locations [10].

The distributed ledger cumulatively stores the complete transaction history of the entire system, from its inception to the latest entry [11]. The data of the transaction is not stored in a central database, but it is distributed to all participants of the network to be stored locally [12]. This approach each node in the network has the same access to the database, while running the blockchain on their systems. The term "public distributed ledger" refers here to a single shared truth [13].

The decentralized peer-to-peer system structure of a blockchain network is described in Fig. 2 [14].

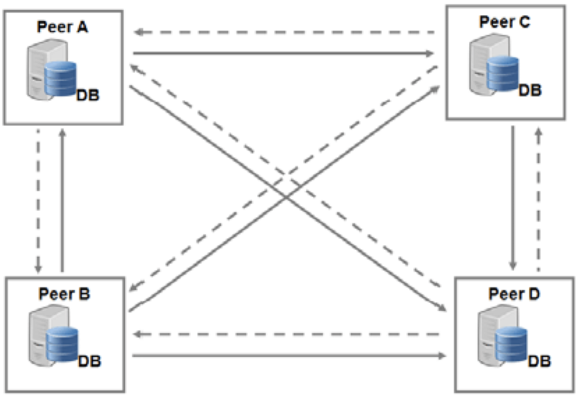


Figure 2. The decentralized peer-to-peer system structure.

According to the Blockchain implementation it is impossible to erase or alter the transaction once it was entered. Blockchain is a network and database that is safe and easy to use. Blockchain can create transactions based on mathematically specified and mechanically implemented rules. Cryptographic algorithms verify all transactions between users or counterparties, which are then grouped into blocks and added to Blockchain. Since the information in blocks is linked together, no one can alter it [15]. The private key is used to authorize a transaction and ensures that it cannot be changed once it's broadcast. If the transaction information is altered, the signature will be incorrect because the algorithm generates the same key from identical information. It also means that all copies of the distributed blockchain are up to date. The highest degree of hack resistance and security optimization is provided by blockchain, and its popularity is far from over [16, 17].

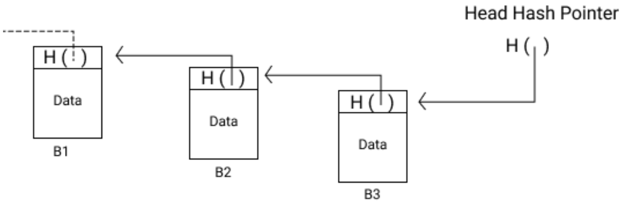


Figure 3. The blockchain structure.

Blockchain is a linked list that uses Hash Pointers to enable each node of blockchain to not only locate the next node but also verify whether the data in that node has been changed.

The blockchain structure in Fig. 3 typically consists of a series of linked blocks, where each block contains a cryptographic hash of the previous block, creating an immutable chain of blocks. The most recent blocks are stored at the end of the chain, and there is typically a Head hash pointer that points to the latest block added to the blockchain. Each block in a blockchain will store a pointer to the previous block and the hash of the contents of the previous block. This ensures that any tampering with a block will be easily detectable since it would invalidate all subsequent blocks in the chain. So, each block in a blockchain will have:

- Pointer to the block added just before it (previous block)
- Hash of the all the contents stored on the previous block (the one added just before it)
- Some data that needs to be stored (for example transactions data)

Any new blocks will be added next to B3 and will store pointer to B3 in this blockchain.

How is blockchain technology is tamper proof?

Suppose an attacker wants to change the data in the leftmost block B1 in the Fig. 4. But if the data in that block is changed, the hash pointer of the middle block will be invalid as presented in Fig. 4.

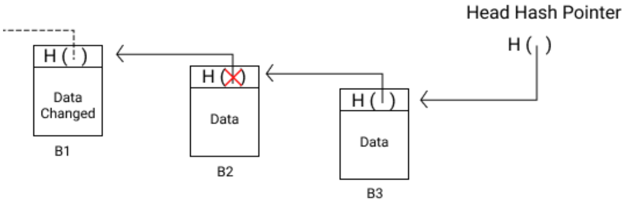


Figure 4. Invalid block in the blockchain structure.

To make the hash of a block valid, we need to update the hash of the previous block B1 that is stored in the current block B2, However, this will also change the hash of the current block B2, as well as all subsequent blocks in the chain. For example, if we want to remove block B1, we cannot simply delete it without invalidating the hash of the next block (B2). This is because the hash calculation for a block includes all the contents of that block. Therefore, any change to a block in the blockchain will be detected as long as we securely store the head hash pointer, which points to the latest block in the chain.

Blockchain networks are decentralized and do not rely on a central authority like a bank or government agency to regulate transactions. The decentralized nature of blockchain makes it difficult to tamper with data in the ledger since an attacker would have to change subsequent data in all predecessor blocks, making it theoretically impossible to make systematic changes, even with a large set of computational resources. This is why blockchain technology is considered to be tamper-proof, immutable, and secure.

Suppose person A wants to send 100 units of value to person B.

Step1: The transaction is first initiated by A and then broadcast to all participating members of the blockchain network.

Step 2: Every node in the network validates the transaction against predefined validation rules created by the creators of the blockchain network.

Step 3: Once the transaction is validated, it is stored in a block along with its own unique hash.

Step 4: The block is added to the blockchain after other nodes in the network verify that the block's hash is correct. Once the transaction is added to the blockchain, it cannot be changed in any way, making it an immutable record of the transaction."

According to blockchain architecture, new transactions are grouped into blocks. Each block is verified and validated by nodes (network participants) using complex cryptographic techniques, which may vary depending on the type of blockchain. In our transaction example, miners verify that person A is the owner of the 100 units of value. Once this is confirmed, the transaction is validated and visible to person B and other network participants, and person B becomes the owner of the units. All network participants perform necessary verification and approval tasks, and if there are any mismatches, the block is rejected. Otherwise, authenticated transactions in the block are timestamped and added to the transaction chain in a linear and sequential order, resulting in a chain of transactions that shows every network transaction in the transaction history of the blockchain. Fig. 5 shows the main transaction processing steps using blockchain technology.

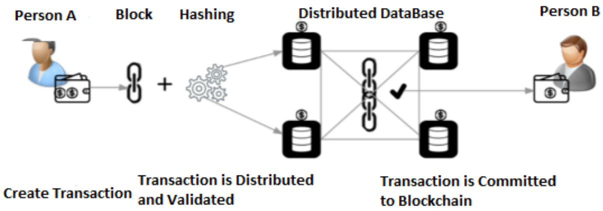

Person A
Block
Hashing
Distributed DataBase
Person B
Create Transaction
Transaction is Distributed and Validated
Transaction is Committed to Blockchain

Figure 5. Transaction steps of the blockchain.

B. *Consensus Algorithm Types*

Due to the high network delay in peer-to-peer networks, the order of transactions observed by each node may not be the same. Therefore, blockchain systems need to design a mechanism to agree on the order of transactions that occur within a similar period. A consensus mechanism is a program used in blockchain systems to achieve distributed agreement about the state of the ledger. Blockchain uses consensus algorithms to govern the network and verify every transaction. Commonly used consensus mechanisms for public blockchain networks are Proof of Work (PoW), Proof of Stake (PoS), Delegated Proof of Stake (DPoS), Practical Byzantine Fault Tolerance (PBFT), Proof of Elapsed Time (PoET), Proof-of-Weight (PoWeight), and Proof of Authority (PoA).

1) Proof of Work (PoW)

The concept of Proof of Work (PoW) was first introduced in 1993 by Cynthia Dwork and Moni Naor and later re-introduced by Satoshi Nakamoto in the Bitcoin whitepaper in 2008. The main idea of PoW is to require miners to use their computing power to solve a complex mathematical puzzle. Once the puzzle is solved, the miner broadcasts the new block to the network, and other miners can verify that the solution is correct before adding the new block to the blockchain [18].

The new blocks are validated by network members solving mathematical puzzles that are difficult enough to prevent malicious behavior, such as a miner attempting to validate a fraudulent transaction. Validating blocks uses a high level of electricity or processing power to decide what data gets added to the next block in a blockchain. The process of solving the crypto puzzle is called mining, and members earn rewards for completing the puzzle. When a node has a computing power of n% of the entire network, the node has a probability of n/100 to find the Block Hash.

PoW's security relies on the principle that no entity should gather more than 50% of the processing power because such an entity can effectively control the system by sustaining the longest chain [19].

2) Proof of Stake (PoS)

Proof of Stake (PoS) is another consensus algorithm which was first introduced by Sunny King and Scott Nadal in 2012 with the aim to reduce the computational requirements of PoW and introduce an energy-saving alternative to PoW. Instead of a competitive process that depends on energy consumption, PoS is based on a selection process that considers the validators' stake. The validators in a PoS system are the equivalent of miners in a PoW system. The selection process allows the network to choose the node that will validate the new block by proving its ownership of an amount of coins using the coin age metric [19]. The nodes with a higher amount of cryptocurrency have higher chances to be selected. Once a validator is selected, they check if the transactions in the block are accurate. If so, they add the block to the blockchain and receive cryptocurrency rewards for their contribution [20].

3) Delegated Proof of Stake (DPoS)

Delegated Proof of Stake (DPoS) is a consensus algorithm similar to a board vote. The algorithm allows token holders to vote for a certain number of nodes and delegate them for block verification and accounting. The main difference between PoS and DPoS is that PoS is a direct democratic process, while DPoS is a representative democratic process, where token holders elect delegates to generate and validate blocks. With fewer nodes involved in block validation, blocks can be confirmed quickly, resulting in faster transaction confirmation times. DPoS can greatly improve the efficiency of block validation compared to PoS, but it comes at the expense of some decentralization features [21].

4) Practical Byzantine Fault Tolerance (PBFT)

The Practical Byzantine Fault Tolerance (PBFT) is a state machine replication algorithm in which the service is modeled as a state machine, and the state machine performs replica replication at different nodes of the distributed system. A copy of each state machine saves the state of the service and also implements the operation of the service [22].

5) Proof of Elapsed Time (PoET)

In PoET, each participating node generates a random wait time and waits for that duration. The node that waits for the shortest time becomes the leader and creates a new block. The block is then broadcast to the network and validated by other nodes. PoET relies on Trusted Execution Environments (TEEs) to ensure that nodes cannot cheat by manipulating their wait times. These TEEs are special hardware components that can securely run code and prevent tampering or external interference. Therefore, the algorithm has additional checks to ensure that nodes are using TEEs properly, rather than checks to prevent nodes from always winning the election or generating the lowest timer value.

6) Proof-of-Weight (PoWeight)

Proof-of-Weight (PoWeight) is a consensus algorithm that uses a node's weight to determine its chances of being selected to create a new block. In a PoWeight system, a node's weight is determined by the number of coins it holds and the length of time it has held them [21].

7) Proof of Authority (PoA)

The Proof of Authority (PoA) is a consensus algorithm that allows only predefined authorities to validate transactions and add them to the Blockchain. This algorithm consists of designating a set of nodes to be validators and gives them the authority to update the ledger and secure the Blockchain. This leads to a kind of centralized agreement in the hands of a small number of validators [19]. The Proof of Authority (PoA) provides an efficient solution for blockchains, specifically private ones. Table I summarizes the advantages and disadvantages of each algorithm [22].

TABLE I. THE ADVANTAGES AND DISADVANTAGES OF THE CONSENSUS ALGORITHMS

Consensus Algorithm	Advantage	Disadvantages
PoW	Decentralization High security	Energy consumption Poor performance
PoS	Energy efficient Fast	Complex implementation Poor security
DPoS	High scalability Energy efficient	Centralization
PBFT	High security Energy efficient	Inefficient for large networks
PoET	Energy efficient Easily scalable	Computability (reliance on Intel hardware)
PoWeight	Energy-efficient Customizable	Incentivization can be a challenge.
PoA	Fast Energy efficient	More centralized It is better suited to a private blockchain than a public one.

C. Open Banking API Architecture

The open banking API provides a secure method of integration that allows third parties to access a user's financial information, including balances, customer data, cash flow, and transaction creation. This integration and communication method is referred to as the open banking API. In the United Kingdom, banks are required by law, specifically by PSD2 (Payment Service Providers Directive), to provide account information about their customers to companies in other sectors, such as payment initiators or account aggregators. To comply with PSD2 regulations, banks must establish processes that enable third-party providers to integrate safely, efficiently, and quickly with the bank's services and data on behalf of their customers, with their consent.

The emergence of open platforms (based on Open API architecture) is facilitating the direct connection between buyers and sellers of core services without the involvement of intermediary institutions. These systems offer companies a simple onboarding process through application programming interfaces (APIs), while allowing consumers to easily search for and access the banking services they require. Fig. 6 illustrates the Open API architecture.

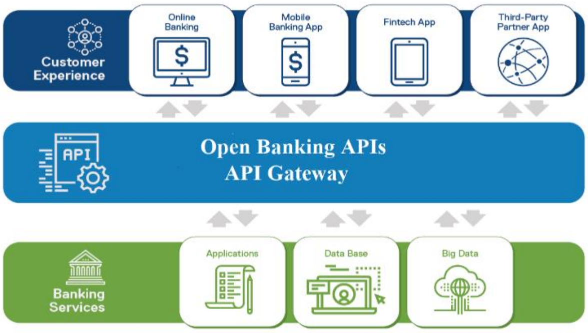


Figure 6. Open API architecture.

D. The Main Methods of Money Transfer in Banking Industry

- ACH Transfers (Automated Clearing House)
- Wire Transfers
- Electronic Transfers
- Direct Deposits
- E-Checks
- ACH Check Conversions

Each money transfer method has its own advantages and disadvantages. For instance, wire transfer is faster than most other methods listed in this section, but it is typically the most expensive option. As our proposed framework will use ACH transfer as the fund transfer method, we will now examine the pros and cons of this method.

- ACH Transfer

The ACH Network is a highly reliable and efficient nationwide electronic funds transfer system that is managed and authorized by the Central Bank of Egypt. It enables the inter-bank clearing of transactions among participating financial institutions, as well as the exchange of electronic transactions in batches of direct debit and direct credit payment instructions between participants. The Egyptian Automated Clearing House (EG-ACH) is the ACH infrastructure used in Egypt, which can be used to transfer funds between customers' bank accounts, whether it is for direct credit, direct debit, single payments, or recurring payments. The low transaction cost could be considered as the main advantage of accepting EG-ACH transactions [23]. To summarize, the main advantages and disadvantages of ACH transactions are as follows:

Advantages:

- ACH transfers are typically less expensive than other payment methods.
- ACH supports batch payments, which is useful for payroll and other similar transactions.
- ACH also supports recurring payments, such as monthly bills.
- There is no need to write or send physical checks.
- ACH transfers eliminate issues with missing or forged checks.
- Transactions can be easily tracked using the trace ID number, which is issued by the sending institution and can be provided to the receiving institution to track the transaction.
- ACH transfers are more efficient than using physical checks.
- ACH transfers are more environmentally friendly than using paper checks.

Disadvantages:

- It takes at least one business day to be completed.
- Sometimes it may take 2-4 business days to be completed.
- ACH transfers are typically used only for domestic payments.
- Mistakes can occur when making ACH payments.
- Recurring transfers may result in overpayment.
- There is a risk of overdrawn accounts.

Although sending money between banks via ACH can be convenient, there are several limitations to the system:

- Amount limits:

ACH transfers may have restrictions on the amount of money that can be transferred within a specific period, such as a day or month. Additionally, there may be limits on the amount of money that can be transferred per transaction. These restrictions can be a limitation for businesses or individuals who need to transfer larger amounts of money quickly.

- Cut-off times:

ACH transfers may not be processed outside of certain hours or on weekends or holidays. For example, if a transfer is submitted on a Friday evening, processing may not begin until the following business day. This delay in processing can be a limitation for businesses or individuals who need to transfer money quickly.

- Insufficient funds fee:

If there are insufficient funds in the account, the bank may charge an insufficient funds fee and cancel the transaction.

- Not allowed for international transfers:

ACH transfers are typically only available for domestic transfers within a country and are not often available for international transfers. Banks may offer other methods for international transfers, such as wire transfers or international ACH transfers, but these may come with additional fees and longer processing times.

Blockchain technology has shown potential in the banking industry for money transfers due to its similarity to the general inner workings of the money transfer process. With these similarities, blockchain deployment seems suited to the task, and new blockchain-based services from FinTech's promise lower-cost services and implementations. However, it should be noted that blockchain is still a relatively new technology in the financial industry and requires further development and regulatory clarity before it can be widely adopted. The ACH fund movement flow is depicted in Fig. 7.

For domestic remittances, blockchain technology has the potential to provide customers with a quicker, more affordable, and more transparent service than traditional banking methods. Several new solutions are emerging that aim to transform the area by connecting various partners in different markets to enable more effective payments.

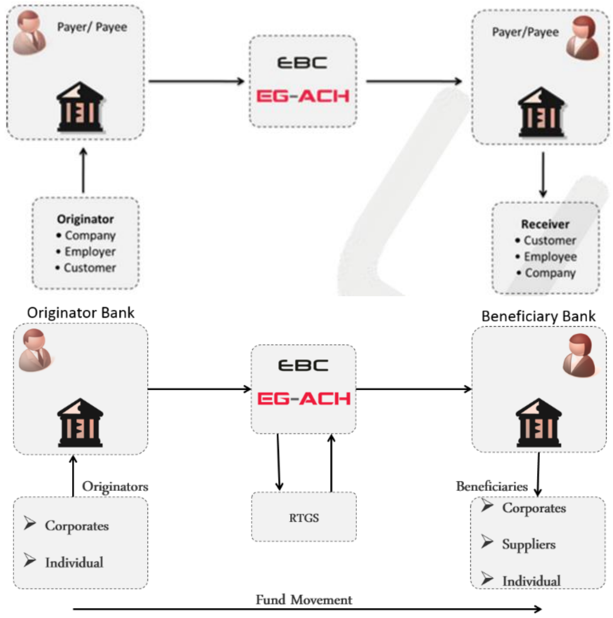


Figure 7. ACH Fund movement flow.

But to be successful, blockchain platforms must focus on increasing the number of participants to improve the efficiency of their networks. This is also an opportunity for traditional money transfer operators to change the way they operate and restructure their business models around the benefits enabled by blockchain technology.

The proposed framework that uses blockchain technology aims to minimize delays during the transfer process by effectively removing intermediary entities and providing guaranteed, real-time transactions. Additionally, the clearing and settlement processes would be near-real time, enabling businesses to access funds paid through the system immediately. Applying distributed ledger technology to ACH money transfers will allow verified participants to transact openly, reducing the risks and costs associated with mitigating fraud.

E. Related Work

The number of e-payment transactions is rapidly increasing in the financial sector, and blockchain technology has the potential to enhance the transaction process to build a more secure and unbiased financial system.

According to Kallugudde *et al.* [24], the global financial system is inefficient due to the high costs and long processing times associated with traditional financial intermediaries. Although billions of traditional financial transactions are facilitated globally through the banking system, a much smaller number are conducted through electronic payments.

Garg *et al*. [25] provides an overview of blockchain technology applications in the banking sector, highlighting the challenges and expected benefits. According to the authors, blockchain technology has the potential to transform the banking sector by making transactions more secure, transparent, faster, and cost-effective.

Bashir [26] supports the notion that blockchain technology is applicable to financial sector transactions and is being widely adopted by financial institutions around the world. Many companies are looking to use blockchain technology to save costs, time, and protect sensitive banking data.

Tapscott and Tapscott [27] explains why blockchain technology is well-suited to the banking and financial sector. Niranjanamurthy *et al.* [28] compares the performance of transactions conducted using blockchain technology with those of other traditional systems, showing that blockchain transactions do not take too much time compared to other traditional systems. Financial institutions can use blockchain technology for any type of transaction without performance issues.

According to Zhu and Zhou [2], the blockchain programmable features increase flexibility and reliability in different business application use cases.

According to Guo and Liang [29], blockchain technology offers technological advantages over banks as credit intermediaries and can be used to improve payment systems and overcome settlement process issues.

According to Dan [30], many international banks such as UBS and ING are exploring the potential of blockchain technology. The discussion suggests that blockchain technology is highly promising for addressing current challenges in financial transactions.

Notheisen *et al.* [31] provide a comprehensive overview of different financial and non-financial applications of blockchain technology. Brandon [32] presents the potential business fields where blockchain technology can be applied.

Sven [33] compares Rabobank and fintech start-up Ripple to filter out implications for the business model of traditional banks integrating blockchain technology to process international payments. The study suggests that blockchain technology is less likely to be successfully implemented by traditional banks in isolation. Instead, it will be more viable for banks to integrate with fintech organizations to capture value from blockchain technology on a larger scale.

Morkunas *et al.* [34] explore the different types of blockchain technology, including private and public applications, and their benefits for different business sectors. The study shows that blockchain technology has the potential to play an important role in solving traditional system problems such as improving financial transaction processes, reducing costs, managing currency exchange, payment systems, supply chain management, and reducing operational risks.

Overall, the discussed literature highlights the applicability of blockchain technology to financial sector transactions, particularly in the banking industry. Blockchain technology has the potential to overcome current challenges in e-payment transactions, making them more secure, transparent, faster, and cost-effective.

III. PORPOSED FRAMEWORK IMPLEMENTATION

In this section, we will explain the implementation of the ACH payment model using the proposed framework based on the open API and blockchain architecture.

A. *The Implementation Assumptions*

The local banks have established Open API gateways that are connected to the blockchain network.

The following API is available in the banks:

- ✓ Account details API
  (Get account details by account number)
- ✓ Customer Details API
  (Get customer information by customer ID)
- ✓ ACH fund Transfer API
  (Create ACH fund transfer operation)
- ✓ ACH Fund transfer reversal.
  (Reverse the fund transfer operation)
- ✓ ACH transaction status inquiry.
  (Check the status of the fund transfer operation)
- ✓ Transaction history
  (Get the transactions history of specific account)

- The required APIs are available 24×7
- All APIs are published in the banks' API gateway.
- The APIs are synchronies APIs.
- The API for debit/credit bank accounts and cards is up and running in the bank's API Gateway, and it is exposed to the network.
- The logical network architecture, as depicted in Fig. 8, assumes that two API Gateways are required for API security, with one located in the DMZ and the other in the green zone.

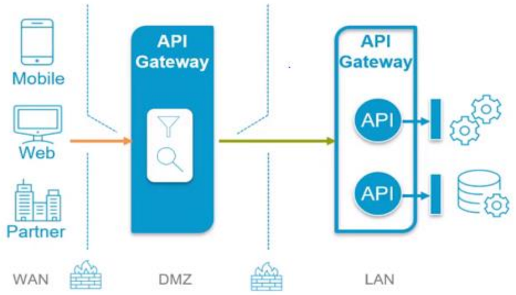


Figure 8. The logical architecture of the open banking API.

B. *The Main System Components*

1) *Blockchain network*

The blockchain network is used to connect all the banks in the network and store the transactions as a block in the distributed general ledger.

2) *API gateway*

The API Gateway serves as the primary external integration point for a bank's services and applications. It can be used to manage and secure the APIs that are exposed by the bank's internal systems. Depending on the use case, some APIs may be published as open APIs in the network, leveraging the security capabilities and API management provided by the API Gateway software, while others may be kept private.

3) *ESB/Integration layer*

The Enterprise Service Bus (ESB) is used as an internal integration layer to handle transaction orchestration, business rules, queuing, and internal monitoring for the bank's internal core systems, as well as the Service-Oriented Architecture (SOA) and service bus of the internal APIs.

4) *The core banking systems*

The core banking systems are used to retrieve customer information and transaction balances. All core banking systems are accessible through APIs published in the internal integration layer (ESB). The main system components are depicted in Fig. 9.

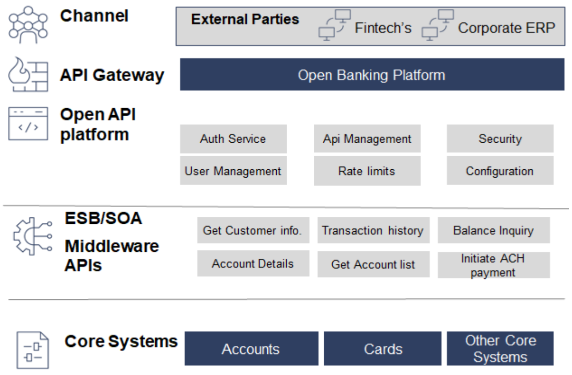


Figure 9. The framework system architecture.

C. *The Enterprise Blockchain Design*

This section will explain the main steps to build and expose a blockchain as a service, in order to design and implement enterprise blockchain technology for a specific business use case, as illustrated in Fig. 10:

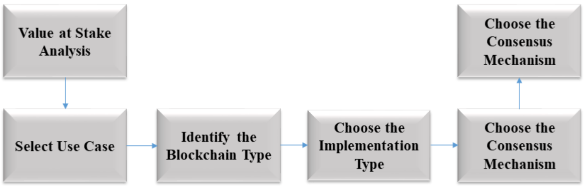

Value at Stake Analysis
Select Use Case
Identify the Blockchain Type
Choose the Implementation Type
Choose the Consensus Mechanism
Choose the Consensus Mechanism

Figure 10. Blockchain design steps.

✓ Step 1 Select Use Case

Select a use case by conducting a value-at-stake analysis to identify the most important business use case, based on selection criteria related to the market, internal environment, technology readiness, and added value of the use case. As we explained earlier, using a blockchain network for domestic remittance would allow banks to offer customers a faster, cheaper, and more transparent service. Therefore, we have selected ACH domestic fund transfer as the use case for our implementation.

✓ Step 2 Identify the Blockchain Type

Based on the selected business use case and the nature of the data used, we will choose between a public blockchain and a private blockchain.

- Public Blockchain

In a public blockchain, anyone is allowed to send transactions and participate in the consensus process. In this case, the ledger is available to all participants in the network [35].

- Private Blockchain

On the other hand, in a private blockchain, a new member in the network needs an invitation and validation from the other participants in the network to be accepted as a part of the private blockchain network [36]. Every network member is restricted to only certain transactions according to their permission and access rights. As per our use case requirements, we have selected a private blockchain to be able to control the permissions and accessibility of the sensitive data of the fund transfer transactions.

- ✓ Step 3 Set the Architecture and Centralization Level

In this step, we need to decide if the implementation will be fully decentralized or partially centralized (hybrid). In a hybrid approach, we can keep sensitive data as private and make the rest of the data as public [37], depending on the business rules of the selected use case. In our implementation, we will use the hybrid approach to protect the sensitive data of the transactions and the customers of the banks. However, the public implementation will be used for data that needs to be shared among all the banks in the network.

- ✓ Step 4 Select the Consensus Mechanism

The choice of consensus mechanism depends on the previous steps, the implementation type, the level of security, and the selected architecture. Each consensus algorithm has its pros and cons, so we need to select the appropriate consensus mechanism to implement according to the nature of the business model and the selected use case.

- ✓ Step 5 Exposing the Blockchain

The final step is to expose the blockchain as a service and make it available to the concerned parties in the network.

The decentralized nature of blockchain technology is one of the reasons for its growing popularity. The proposed framework using blockchain technology is similarly decentralized and aims to enable both the sender and recipient to track the exact location of their money. It also aims to minimize delays during the transfer process by removing intermediary entities and providing guaranteed, real-time transactions. Additionally, the clearing and settlement would be near-real time, enabling businesses to access funds paid through the system immediately. Applying distributed ledger technology to ACH money transfers will enable verified participants to transact openly, reducing the risks and costs associated with fraud mitigation. In the next section, we will use ACH domestic fund transfer as a use case for our implementation.

D. Security Controls

Keeping customers' financial data secure has always been a top priority. While opening APIs to third parties is essential in our implementation, we need to manage them with tight controls and security. Our proposed framework uses an API gateway that protects against security threats with DMZ-level protection. We can securely expose APIs to third-party developers, partners, and other consumers. In this section, we will explain the security policies required to be implemented at the API gateway level used in our proposed framework as a communication and integration layer between all APIs published in the network to perform the fund transfer and related inquiry functions used in the fund transfer journey.

1) Threat protection policies

We will implement threat protection policies in the API Gateway, which will limit the maximum message size, maximum number of concurrent requests, and maximum number of calls. For example, we will configure a global denial of service policy in the API Gateway to prevent DoS attacks. A DoS attack occurs when a client creates many concurrent requests to consume server resources. We need to limit the number of requests that the API Gateway accepts within a specified time interval and the number of requests that it can process concurrently. Setting these limits is crucial to protect the system from DoS attacks.

2) Identify and access policy

For inbound authentication, we are using JSON Web Token (JWT) and API key to verify the client's identity against the predefined list of applications for the specified API. On the other hand, WS-Security username token will be used for outbound authentication.

3) Routing policy

The routing policy is set to ensure that incoming requests are routed directly to the correct service endpoints as expected.

4) Transformation policy

We can apply a transformation rule to the request received by each bank in order to add specific parameters that are unique to each bank, or to validate certain business rules that are configured on the API gateway before passing it to the internal systems.

- Traffic Monitoring

TABLE II. THE MONITORING EVENT TYPES IN API GATEWAY

Event Type	Description
Transaction	Each time an API is invoked.
Error	When error occurs during API invocation
Lifecycle	Each time API gateway Started or shutdown
Threat Protection	Each time Global threat protection policy is violated
Performance Metrics	Generated for every API at specific intervals, this report provides information about the overall performance of the gateway. For example, it includes the total number of calls for the API within the specified interval, as well as the average, maximum, and minimum response times of the API.

This policy enables the logging of requests and responses to the internal data store (Elastic). Additionally, other information about the requests and responses, such as the API name, operation name, timestamp, and response time, is also logged. Table II explains the main monitoring event types that should be implemented in the API gateway. All of these action types need to be monitored at the API gateway level for fraud protection, support, and troubleshooting purposes.

5) Response processing—Data masking

Sensitive information can be protected and secured by using data masking techniques when the actual data is not required.

After implementing the required security measures in the API gateway, we will explain the transaction process flow based on our proposed framework.

IV. Methodologies

According to our design, the data flow for the ACH transaction using blockchain technology and open banking architecture will include the following steps, as shown in Fig. 11:

- Client Initiates a Transactions
- Internal Validation Before Sending the Transaction
- Signing the Transaction and Sending for The Network Approval
- Network Verification
- The Transaction is Verified and Committed
- Updating Across All Nodes

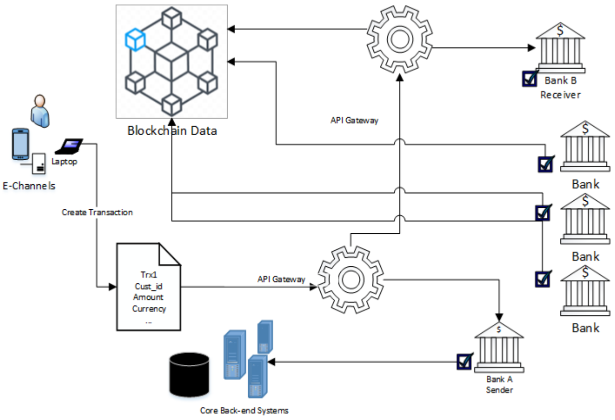


Figure 11. Process flow of the fund transfer transaction.

A. *Client Initiates a Transactions*

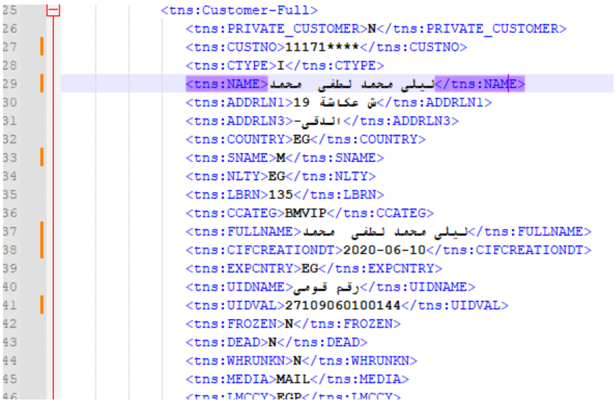
To initiate a transaction, the customer needs to log in to Bank A's channel (ATM, ERP, or mobile app) and request to make a fund transfer transaction from their account in Bank A to another account in Bank B. Using the e-channels, the client creates a properly formatted transaction that includes the main required data to initiate the transaction, such as the receiver account number, transaction amount, transaction currency, and the receiver bank code.

B. *Internal Validation before Sending the Transaction*

Before sending the transaction to the network, the initiating bank needs to validate its internal business rules, such as transaction limits, authorizations, and other internal business rules. The validation step is the main internal action that needs to be performed before sending the transaction details to the network. The sender bank uses the validation API, which is published in the API gateway level of each node (bank) in the network, to process all the required business rules of the transaction. For example, the following APIs need to be implemented to get the prerequisite data to initiate the transaction and perform the necessary validation:

- ✓ Obtain customer data.
- ✓ Obtain a list of customer accounts
- ✓ Retrieve customer account details, including account type and account number.
- ✓ Retrieve customer account balance.
- ✓ Validate the transfer amount (M) and its currency.
- ✓ Identify the account number of the payee (the receiver)
- ✓ Identify the bank code of the payee (the receiver's bank)

The system should prepare all the necessary data, which will be sent to the API gateway using the create ACH transaction API. A set of APIs needs to be implemented to validate the internal business rules of the bank that initiates the transaction before it is sent to the network. Fig. 12 shows a sample response of one of the validation APIs (the Get Customer Details API) used to validate customer data before the transaction is sent.



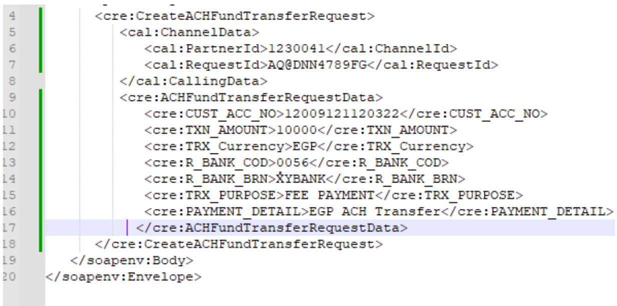
```
        <tns:Customer-Full>
           <tns:PRIVATE_CUSTOMER>N</tns:PRIVATE_CUSTOMER>
           <tns:CUSTNO>11171****</tns:CUSTNO>
           <tns:CTYPE>I</tns:CTYPE>
           <tns:NAME>ليلى محمد لطفى محمد</tns:NAME>
           <tns:ADDRLN1>19 ش عكاشة</tns:ADDRLN1>
           <tns:ADDRLN3>الدقى-</tns:ADDRLN3>
           <tns:COUNTRY>EG</tns:COUNTRY>
           <tns:SNAME>M</tns:SNAME>
           <tns:NLTY>EG</tns:NLTY>
           <tns:LBRN>135</tns:LBRN>
           <tns:CCATEG>BMVIP</tns:CCATEG>
           <tns:FULLNAME>ليلى محمد لطفى محمد</tns:FULLNAME>
           <tns:CIFCREATIONDT>2020-06-10</tns:CIFCREATIONDT>
           <tns:EXPCNTRY>EG</tns:EXPCNTRY>
           <tns:UIDNAME>رقم قومى</tns:UIDNAME>
           <tns:UIDVAL>27109060100144</tns:UIDVAL>
           <tns:FROZEN>N</tns:FROZEN>
           <tns:DEAD>N</tns:DEAD>
           <tns:WHRUNKN>N</tns:WHRUNKN>
           <tns:MEDIA>MAIL</tns:MEDIA>
           <tns:LMCCY>EGP</tns:LMCCY>
```

Figure 12. The Response of the get customer details API.

- ○ The transfer amount (Txn_Amount)
- ○ The sender's account number (Cust_Acc_Number)
- ○ The sender's bank code (S_Bank_Code)
- ○ The currency of the transfer (Trx_currency)
- ○ The receiver's account number (R_Account)
- ○ The receiver's bank code (R_Bank_Code)
- ○ The receiver's branch code (R_Branch_Code)
- ○ The eligibility of the transaction (IS_valid)
- ○ The transaction purpose (Trx_Purpose)

C. *Signing the Transaction and Sending for The Network Approval*

Each initiated transaction is signed by a digital signature of the sender, which is essentially the sender bank's private key. This is done to make the transaction more secure and prevent fraud. After signing, the transaction is sent to the network for the approval cycle. To accomplish this, we need to implement an API for fund transfer, which is responsible for the ACH fund transfer operation (ACH_FundTransfer). The primary function of the ACH_FundTransfer API is to take the input parameters of the ACH transaction with the required validation from the API gateway of the sender bank (the caller) and send it to the network (the API gateway of the receiver bank). Fig. 13 shows the input parameters of the ACH fund transfer API.



```
      <cre:CreateACHFundTransferRequest>
         <cal:ChannelData>
            <cal:PartnerId>1230041</cal:ChannelId>
            <cal:RequestId>AQ@DNN4789FG</cal:RequestId>
         </cal:CallingData>
         <cre:ACHFundTransferRequestData>
            <cre:CUST_ACC_NO>12009121120322</cre:CUST_ACC_NO>
            <cre:TXN_AMOUNT>10000</cre:TXN_AMOUNT>
            <cre:TRX_Currency>EGP</cre:TRX_Currency>
            <cre:R_BANK_COD>0056</cre:R_BANK_COD>
            <cre:R_BANK_BRN>XYBANK</cre:R_BANK_BRN>
            <cre:TRX_PURPOSE>FEE PAYMENT</cre:TRX_PURPOSE>
            <cre:PAYMENT_DETAIL>EGP ACH Transfer</cre:PAYMENT_DETAIL>
          </cre:ACHFundTransferRequestData>
      </cre:CreateACHFundTransferRequest>
   </soapenv:Body>
</soapenv:Envelope>
```

Figure 13. ACH_Fund transfer input parameters.

D. Network Verification

The transaction is now broadcast to the memory pool within the network. Network peers verify the transaction and execute it if they receive a transaction with a valid signature from a known peer. They can sign a proposal response, which can be passed to the wider network as a change to the state object. The responses are transmitted across the network and inspected independently by each node. Execution will take place after doing internal validation and verification using the validation APIs implemented in the API gateway, such as account details, customer information (receiver), and AML checks.

E. The Transaction is Verified and Committed

The transaction data is converted into a transaction record and passed to the ordering nodes to add it to the blockchain. The ordering nodes achieve consensus through a complex process known as Proof of Authority, which enables them to determine the order in which transactions should be added to the blockchain based on a predetermined hierarchy between known nodes.

F. Updating the Across All Nodes

Once the state object has been updated and the verified ledger is confirmed by the ordering nodes, each client node (bank) can now read the new information with confidence.

V. Results and Discussions

Based on the characteristics of blockchain technology, the proposed framework will improve the efficiency of ACH payments between local banks in Egypt and have a positive impact on the following:

- Accuracy of the Chain

The ACH transactions on the blockchain network are approved by a network of many computers. As a result, practically all human involvement in the verification process is eliminated, reducing human error, and ensuring that the transaction information is accurately recorded.

- Cost Reductions

The implementation of blockchain technology eliminates the need for third-party verification of transactions and associated costs, resulting in cost reductions.

- Decentralization

Blockchain does not store any of its information in a central location. Instead, a network of computers copies and distributes the blockchain. Every computer in the network updates its blockchain whenever a new block is added to the blockchain. By spreading that information across a network rather than storing it in one central database, blockchain becomes more difficult to tamper with. If a hacker obtained a copy of the blockchain, only one instance of the data would be at risk rather than the entire network. If any of the fields in a block are changed, then the entire hash of the block would change, causing the blockchain to be invalidated. If other nodes detect any changes to the blockchain, they will not accept those blocks. A malicious node attempting to alter the blockchain would need to change the previous hash field of the following block to make the attack successful, which would also change the hash of that block. Then, they would have to update the previous hash field of the next block and continue this process until they reach the last mined block, and then broadcast their chain to the whole network. This attack is known as a 51% attack.

- Efficient Transactions

Transactions processed through the existing ACH network can take several days to settle, while transactions processed through our proposed framework based on blockchain technology and open API architecture can be processed 24/7, 365 days a year, resulting in faster settlement times.

- Private and Secure Transactions

Once a transaction is recorded, its authenticity must be verified by the blockchain network (not banks). All network members should confirm that the details of the transaction are correct. Once network members have validated the transaction, it is added to the blockchain as a block. When the information on a block is edited in any way, that block’s hash code changes, and as a result, the hash code of the subsequent blocks also changes. This discrepancy makes it extremely difficult for information on the blockchain to be changed.

- Banking the Unbanked

According to the World Bank, an estimated 1.7 billion adults do not have access to formal financial services, such as bank accounts or any means of storing their money or wealth. Using blockchain technology can facilitate methods to improve financial inclusion by providing low-cost, secure, and fast fund transfers.

- Instant Fund Transfer

Using blockchain technology with instant open API integration can provide the quickest availability of funds because it allows for immediate real-time and final settlement.

VI. Conclusion

The purpose of this paper is to examine and highlight the potential of applying blockchain technology in financial transactions with the presence of an open API framework. In the current technology era, many industries are widely adopting blockchain technology to speed up processes, make them transparent, safe, and secure.

The proposed framework aims to provide banks with opportunities to improve various areas, including:

- Digitization of payments
- E-commerce

- Enabling data as a service model for consumption of analytical and other data needs by internal and external consumers.
- Facilitating instant transactions between all e-commerce business models, such as C2C (customer to customer), B2B (business to business), C2B (customer to business), and B2C (business to customer)
- Online SME finance
- Digital transformation
- Increasing access points, partnerships with non-bank FinTech's, and leveraging innovative technologies to bring efficiency in banking and payments.
- Reducing dependency on legacy core platforms through technology modernization
- Complying with regulatory requirements (e.g., PSD2, GDPR, data sharing laws, etc.)
- Enabling partners, such as corporate clients
- Reducing IT build and test effort/cost by developing reusable APIs for internal and external consumers
- Improving IT security by standardizing access to core systems via APIs.

While blockchain technology has the potential to revolutionize e-payment systems in the future, there are some challenges that must be addressed before it can be widely employed in the financial sector. These challenges include: the ability to manage a large number of users simultaneously is still a challenge for blockchain technology. In addition, the technology is complex and not easy to understand, so using it for critical operations like financial transactions requires well-trained and skilled technical staff to handle and manage the system and technical issues effectively.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Mohamed Hamed proposed the model architectures, conducted the research, and wrote the paper under the supervision of Prof. Yehia Helmy and Dr. Mohamed Abd ElSalam. All the authors had approved the final version.

References

[1] S. Nakamoto. (2008). Bitcoin: A peer-to-peer electronic cash system. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[2] H. Zhu and Z. Zhou, "Analysis and outlook of applications of blockchain technology to equity crowdfunding in China," *Financ. Innov.*, pp. 11–12, 2017.

[3] C. M. Christopher, "The bridging model: Exploring the roles of trust and enforcement in banking, bitcoin, and the blockchain," *Nevada Law Journal*, vol. 17, pp. 139–151, 2019.

[4] M. Fyrigou-Koulouri, "Blockchain technology: An interconnected legal framework for an interconnected system," *Journal of Law, Technology and the Internet*, vol. 9, pp. 14–15, 2018.

[5] D. Tapscott and A. Tapscott, "Blockchain revolution: How the technology behind bitcoin is changing money, business, and the world," *FIIB Business Review*, vol. 7, pp. 275–276, 2018.

[6] M. Swan, *Blockchain: Blueprint for a New Economy*, 1st ed. 2016, O'Reilly Media Inc., Sebastopol, CA, Ch. 3, pp. 145–148.

[7] N. Kshetri, "Can blockchain strengthen the inter-net of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[8] A. Tan, Y. Zhao, and T. Halliday, "A blockchain model for less container load operations in China," *International Journal of Information Systems and Supply Chain Management*, vol. 11, issue 2, pp. 39–53, 2018.

[9] K. Werbach, "Trust but verify: Why the blockchain needs the law," *Berkeley Technology Law Journal*, vol. 33, issue 2, pp. 13–16, 2018.

[10] A. Pinna and W. Ruttenberg, "Distributed ledger technologies in securities post-trading revolution or evolution," ECB Occasional Paper No. 172, pp. 4–7, 2016.

[11] R. Beck, J. S. Czepluch, N. Lollike, and S. Malone, "Blockchain—The gateway to trust-free cryptographic transactions," in *Proc. Twenty-Fourth European Conference on Information Systems (ECIS)*, Istanbul, Turkey, 2016, pp.7–9.

[12] J. Mattila and T. Seppälä, "Blockchains as a path to a network of systems," ETLA Reports No. 45, pp. 14–15, 2015.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," *IEEE Access*, vol. 4, pp. 31–32, 2016.

[14] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 13–19, 2018.

[15] M. Swan and P. de Filippi, "Toward a philosophy of blockchain: A symposium: introduction," *Metaphilosophy*, vol. 48, no. 5, pp. 603–619, Oct. 2017.

[16] D. Tapscott and A. Tapscott, *Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World*, Toronto: Penguin Canada, 2018, ch. 3, pp. 75–77.

[17] A. Pinna and W. Ruttenberg "Distributed ledger technologies in securities post-trading revolution or evolution?" ECB Occasional Paper, 2016, p. 172.

[18] A. Castor. (2017). A guide to blockchain consensus protocols. [Online]. Available: https://www.coindesk.com/markets/2017/03/04/ashort-guide-to-blockchain-consensus-protocols

[19] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," *ACM Computing Surveys*, vol. 1, no. 1, pp. 5–8, 2019.

[20] P. Vasin, *BlackCoins Proof-of-Stake Protocol v2*, 2018, p. 1.

[21] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE 6th International Congress on Big Data*, 2017, pp. 13–17.

[22] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proc. Third Symposium on Operating Systems Design and Implementation*, New Orleans, USA, February 1999, pp. 51–54.

[23] EBC. (2022). About Automated Clearing House (EG-ACH). [Online]. Available: https://www.egyptianbanks.com/automated-clearing-house-eg-ach/

[24] A. Mavridou and A. Laszka, "Designing secure Ethereum smart contracts: A finite state machine based approach," in *Proc. International Conference on Financial Cryptography and Data Security*, 2018.

[25] P. Garg, B. Gupta, A. Chauhan, U. Sivarajah, S. Gupta and S. Modgil, "Measuring the perceived benefits of implementing blockchain technology in the banking sector," *Technological Forecasting and Social Change*, vol. 163, pp. 11–13, 2020.

[26] I. Bashir, *Mastering Blockchain*, 2nd ed. Packt Publishing Ltd., 2018, ch. 2, pp. 39–42.

[27] A. Tapscott and D. Tapscott, "How blockchain is changing finance," *Harvard Business Review*, 2017, vol. 9, pp. 2–5.

[28] M. Niranjanamurthy, B. Nithya, and S. Jagannatha, "Analysis of blockchain technology: Pros, cons and SWOT," *Cluster Computing*, 2019, p. 22.

[29] Y. Guo and C. Liang, "Blockchain application and outlook in the banking industry," *Financial Innovation*, 2016, pp. 24–26.

[30] B. Dan. (2015). Blockchain Manoeuvres: Applying Bitcoin's technology to banking. The Banker. [Online]. Available: https://www.thebanker.com/Transactions-Technology/Technology/Blockchain-manoeuvres-applying-Bitcoin-s-technology-to-banking?ct=true

[31] B. Notheisen, J. Cholewa, and A. Shanmugam, "Trading real-world assets on blockchain," *Business Information Systems Engineering*, vol. 59, no. 6, pp. 425–440, 2017.

[32] D. Brandon, “The blockchain: The future of business information systems?” *International Journal of the Academic Business World*, vol. 10, pp. 33–40, 2016.

[33] M. Sven, “How blockchain affects business models in international banking,” in *Proc. 11th IBA Bachelor Thesis Conference*, Enschede, The Netherlands, 2018.

[34] V. Morkunas, J. Paschen, and E. Boon, “How blockchain technologies impact your business model,” *Business Horizons*, vol. 62, pp. 295–306, 2019.

[35] P. Jayachandran. (2017). The difference between public and private blockchain. [Online]. Available: https://www.ibm.com/blogs/blockchain/2017/05/thedifference-between-public-and-private-blockchain/

[36] V. Buterin, “A next generation smart contract and decentralized application platform: Ethereum,” *White Paper*, pp. 4–5, 2016.

[37] Q. Hua, B. Yanb, Y. Hana, and J. Yu, “An improved delegated proof of stake consensus algorithm,” in *Proc. International Conference on Identification, Information and Knowledge in the Internet of Things*, 2021, vol.187, pp. 341–345.