A BLOCKCHAIN-BASED SYSTEM TOWARDS OVERCOMING FRAUD IN FINANCIAL INSTITUTIONS

[1] ADAM QURAN, [2] MOHAMMAD QATAWNEH

[1] Department of Computer Science - The University of Jordan, Jordan

[2]Department of Computer Science - The University of Jordan, Jordan

E-mail: [1]Adamq82@yahoo.com, [2]mohd.qat@ju.edu.jo

ABSTRACT

One of the key activities of financial institutions is lending, the lending activities are dependent on trust between clients and financial institutions. Financial institutions are continuously in the process of growing and expanding to meet the needs of their clients. Therefore, they need to establish an integrated system to reduce risks, and improve lending processes. This paper proposes a new blockchain system architecture, which provides a feasible solution for overcoming fraud in financial institutions through secure exchange of existing and potential client data. The proposed system architecture was implemented and evaluated using real data of National Microfinance Bank (NMB) clients in Jordan. The results show that the system architecture has a strong security level and makes it difficult for attackers to impersonate a legitimate validator, and high performance in terms of less time needed to validate, upload, and appending transactions and blocks to blockchain system.

Keywords: *Blockchain, Consensus Algorithm, Financial Institutions, Fraud.*

1. INTRODUCTION

Financial institutions have an important role in the world economy, with financial loans being importance in advancing the economy in all countries, for many reasons. First, the outstanding financial loans are indicators of financial and economic stability of any country. Second, for financial institutions, loans are considered one of their main income. In the current financial system in various countries, the borrower has to visit a bank to ask for a loan, and in turn, the bank need to check on the clients' financial statements from other financial institutions [1]. The process of checking such information happens over a centralized data system, where the data is uploaded by all financial institutions. However, the problem with centralized data is that it can be modified, manipulated or deleted through the use of several techniques [2][3].

Bank loans provided by the financial institutions play an essential role in advancing the economy of the world's countries, for many reasons. First, the outstanding financial loans are indicators of financial and economic stability of any country. Second, for financial institutions, loans are considered one of their main income. In the current financial system in various countries, the borrower has to visit a bank to ask for a loan, and in turn, the bank need to check on the clients' financial statements from other financial institutions [4]. The process of checking such information happens over a centralized data system, where the data is uploaded by all financial institutions. However, the problem with centralized data is that it can be modified, manipulated or deleted through the use of several techniques [5]. In addition, the systems currently in use do not live up to the ambitions of digital financial services. Therefore, financial institutions need to establish secure, reliable, immutable and distributed system to reduce the fraud and risk in bank-lending [6] [7] [8] [9].

The future of Digital Financial Services (DFS) depends on finding a mechanism that guarantees the protection of financial data for clients [10] [11]. Because the risk of modifying such data may lead to financial fraud and use of these financial data in illegitimate [12] [13]. Consequently, a new technology that guarantees transfer data without interference third party (central authority) and keep data secure and immutable is highly needed to handle the issues previously mentioned [14].

Blockchain technology can be used to address such drawbacks, because BC technology has several features that can mitigate fraud risk such as security, transparency, and integrity. Hence, using blockchain technology can yield the potential for transparency, traceability, and increase in touchless transactions.

- This paper proposes a new blockchain system to overcome fraud in financial institutions by ensuring the validity, integrity, and immutability. The paper's contribution is as follow: Discussing recent articles that investigate the use of blockchain in financial institutions.
- Proposing a new blockchain system architecture to reduce the risk and fraud in Jordanian financial institutions.
- Proposing a new consensus algorithm for the proposed system structure.
- Evolution the BC system architecture using a real dataset of National Microfinance Bank (NMB) clients.

The rest of the paper organized as follows. Section 2 presents the theoretical background of BC technology, literature review and related works. Section 3 presents the proposed system. Section 4 presents Simulation results and discussion. Section 5 present a compression between our proposed consensus algorithms with other consensus.

2. THEORETICAL BACKGROUND

A Blockchain technology (BC) can be defined as a decentralized, distributed, immutable, and shared a ledger that maintains a continuously growing list of blocks that are linked and secured using cryptograph [14]. The issues of integrity and trust between the different parts of distributed system is considered as one of the most important challenges that should be take into consideration when designing such systems. BC technology can deal with these issues [20] because it uses cryptography and security techniques like hashing [21] [22], digital signature, and time stamping. Digital signature and hashing are used to achieve data integrity due to their features like collision resistance and one-way function [23] [24].
Blockchain technology has the following essential features of BC:

A. **Decentralization**: The BC is a decentralized system, which means that there is no single point of control responsible for security of the system, the control of the system is shared and managed through many independent entities such as computers or enterprises. To keep decentralization going every BC system must have a consensus algorithm to help the system make decisions, or else the core value of it is lost.

B. **Distributed Ledgers:** the ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.

C. **Immutability**: Immutability of BC means that the blocks which contain data or transactions can't be altered retroactively without the alteration of all subsequent blocks and the consensus of the system.

D. **Consensus**: Every blockchain thrives because of the consensus algorithm. The architecture is cleverly designed, and consensus algorithms are at the core of this architecture. Every blockchain has a consensus to help the network make decision.

E. **Faster settlement**: Blockchain offers a faster settlement compared to traditional systems.

All of these features made a BC highly secure system and thus it became a good candidate to address many issues such as *security*, *privacy*, *counterfeiting*, *transparency* and *trustless* in several domains of our life like supply chain management, health care, education, financial services, real estate, smart environments, e-voting systems, etc. [24][25][26][27].

The blockchain consists of blocks and transactions. The transactions are the events created by nodes (enterprises) and blocks record these transactions in the correct order and have not been tampered with [15]. Based on data management, BC can be categorized into three classes:

2.1 Permissionless Blockchain (Public)

In a permissionless BC network, anyone can read and write to the blockchain without authorization [15], this type of BC is the most commonly used and popular and was invented in 2008, by Satoshi Nakamoto [8] to underpin the Bitcoin cryptocurrency. In public BC anyone can participate without permission and can be a miner. This type of BC can use consensus protocols such as Proof of Work and Proof of Stake algorithms.

2.2 Permissioned Blockchain (Private)

This type of BC limits participation to specific people or organizations and allows finer-grained controls [15]. The participants require permission to join, as there are restrictions as to who can participate within a network. This blockchain can be used within a single entity internally or between entities of the same mother company.

2.3 Consortium Blockchain

This blockchain is a mix between public and private blockchain. It has the restricted access of private blockchain and can be used by several entities as the public blockchain. However, these entities are predefined and can be grouped to operate a single node of the network [16] [17].

Presently, blockchain technology has been applied in financial institutions and finance management. Hence, several research works and papers have been proposed in such area. David Doe Fiergbor [18] proposed a blockchain framework to be implemented in mutual funds management in Ghana. The proposed framework allows the investors and fund managers from any institution in Ghana to monitor investment performance, transaction accuracy and accountability. Using this framework, the can get a reduction on cost of movement and fees on transactions, which make more revenue for them and share it between the investors. Maria Todorof [19] presented a framework that describes how blockchain technology can support Islamic banks to be convoyed with the trend on technology in financial institutions. Maria Todorof [19] mentioned that Islamic banking products should be modified to support the lending of Shariah loans to clients. The aim of the proposed framework is to reduce lending costs, and provide the ability to measure the clients' capability of repaying loans by monitoring transactions on the block.

Vladimir Soloviev [3] presented another framework for Russian banks, which integrates the blockchain technology with conventional core bank system to create new services that can be provided to the clients which benefits both bank and financial institution. The proposed framework takes into consideration the following factors: Reducing cost of lending, reducing cost of money transactions and reducing cost of bank branches setup.

Rui Wang, Zhangxi Li and Hang Luo [27] presented and suggested how to use the blockchain in bank credit and (small and medium-sized enterprises) SME financing. The main idea was based on creating a risk pool for the blockchain based on lending and borrowing. Hence, if SME companies have defaulted loans, the records will appear on the blocks and they will not get any more loans from others.

3. THE PROPOSED SYSTEM ARCHITECTURE

This section presents a proposed system architecture. Before introducing the proposed system architecture, it is important first to present a BC decision path that can use to determine whether the BC system is justified and, if so, which type of BC technology to use as shown in figure 1 and table1.

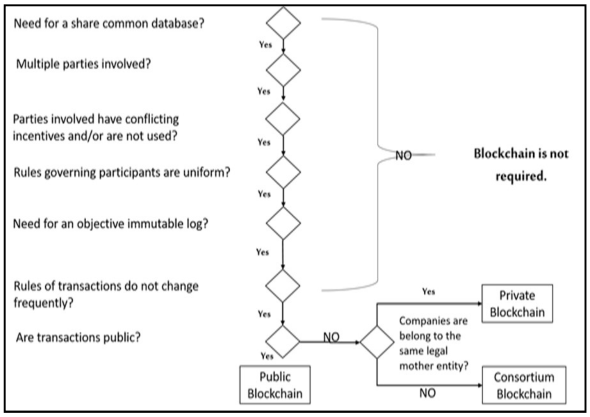

Need for a share common database?
Yes
Multiple parties involved?
Yes
Parties involved have conflicting incentives and/or are not used?
Yes
Rules governing participants are uniform?
Yes
Need for an objective immutable log?
Yes
Rules of transactions do not change frequently?
Yes
Are transactions public?
Yes
Public Blockchain
NO
NO
Blockchain is not required.
Companies are belong to the same legal mother entity?
Yes
Private Blockchain
NO
Consortium Blockchain

Figure 1: BC Decision Path

Applying of the decision path shows that the appropriate type of BC for the proposed system architecture is consortium BC. A Consortium BC determines the participants' authority, where only the authorized participant can join, read and write. In addition, only the network operator can register the participants and define the validators, which based on a common database between all financial institutions, all participants are should compile with network operator, all data transferred over the system have to be immutable.

Table 1: Blockchain Decision Path Steps.

	STEP	EXPLANATION
1	Is there a need for a shared database?	Yes, a common database between all Jordanian financial institutions.
2	Are there multiple parties involved?	Yes, the Central Bank of Jordan (CBJ) and other financial institutions that are involved in this system to reduce the cost of lending and risk of frauds.

3	Do parties have conflicting incentives and/or not used?	Yes, participating parties of the system have different incentives whilst simultaneously targeting the same clients. The shared data gives transparency for each party to know if their clients also belong to another party.
4	Are the rules governing participants uniform?	Yes, the CBJ is the only regulator in Jordan and responsible for issuing regulations and instructions that govern the work of Jordanian financial institutions. Hence, the rules are uniform.
5	Is there a need for an immutable objective log?	Yes, all transactions on the system have to be recorded and immutable.
6	Do the rules of transactions not change frequently?	Yes, all financial institutions in Jordan are governed by the CBJ. Their rule do not change frequently, and if they do, the rules are to be applied by all parties.
7	Are transactions public?	No, according to predefined laws of the CBJ, transactions are not public.
8	Do the companies belong to the same legal mother entity?	NO, all participants don not belong to the same mother entity.

The proposed system architecture as shown in figure 2 comprises the following components:

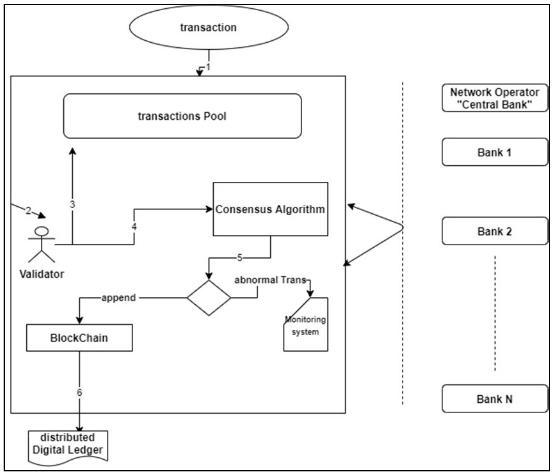


Figure 2: System Architecture

3.1 Network operator

Network operator corresponds to Central |Bank (CB), which responsible for registering participants (banks) and identifying the validators of the system. There are four attributes that are required to define a participant.

3.1.1 Institution ID

Each institution (bank) in the system has its own unique id.

3.1.2 Institution name

Name of the institution.

3.1.3 Registration date

The date of the bank's registration in the system.

3.1.4 Validator ID

A unique ID allocated to each financial institution registered in the system. This ID is randomly generated and assigned by the CB. The suggested format of the ID is composed of a total length of three characters; alphabet and digits.

3.2 Banks

Represents any participating institution authorized by the Network Operator. Once the bank is registered, it needs to submit all of its customer's data to the BC consortium system. The structure of the clients' data should entail:

3.2.1 Citizen ID

A unique ID for each client; in this case it is the Jordanian National Number with citizen password for citizen information privacy.

3.2.2 Outstanding Amount

The remaining principal loan amount.

3.2.3 Citizen Status

The status of loan (Good/Delinquent).

3.2.4 Expected Finish Date

The date of the last installment of the loan.

3.3 Blockchain Model

The blockchain model consists of the following elements:

3.3.1 Transaction

Represents the transaction from any financial institution authorized by the CB in the system. Below are the processes a transaction must undergo before being entered to the system:

- Each transaction is to be composed of four aforementioned attributes: Citizen ID, Outstanding Amount, Citizen Status, and Finish Expectation Date.
- The sender entity (associated financial institution), creates a HASH value for the transaction based on SHA1. The entity validator code is added on the HASH value in a random place.
- The transaction, along with its HASH is entered onto the system. Figure 3 illustrates the creation of a HASH value for a transaction.

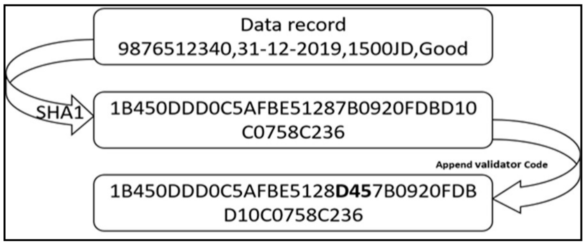

Data record
9876512340,31-12-2019,1500JD,Good
SHA1
1B450DDD0C5AFBE51287B0920FDBD10
C0758C236
Append validator Code
1B450DDD0C5AFBE5128D457B0920FDB
D10C0758C236

Figure 3: HASH value of Transaction framework

3.3.2 Transaction pool

A temporary area which contains all unconfirmed transactions in the system.

3.3.3 Validator

Each bank in the system has at least one corresponding validator. The validators validate new transactions and add them to the blockchain (global digital ledger) by running a consensus algorithm. The validator is randomly selected by the system network to start working on the transactions received in the transaction pool.

3.3.4 Blockchain consensus algorithm

The BC consensus algorithm requires validators to solve complex operations to add a block to the blockchain by following a set of consensus rules.

3.3.5 Blockchain

A chain of blocks where each block has a set of validated transactions. Each block stores the HASH values of both previous and next blocks in the chain. A new Accumulation HASH value is added, which represents the previous HASH value and the current blocks' HASH value. This value is used to check if any block on the chains has been attacked or modified.

3.3.6 Distributed Digital Ledger (DDL)

The existence of a similar copy of the data in institutions. It is a safety parameter for data, defending it from any fraud or illegal modification.

3.3.7 Monitoring System

A log system that stores any unauthentic transactions and validators in order to help the system monitor, determine and fix errors.

3.4 Hand by Hand Check (HHC) Consensus Algorithm

This session presents a new consensus algorithm, which called HHC for the proposed system architecture. The proposed HHC algorithm is used to validate the transactions and maintain the security of the blockchain system by allowing a new transactions to be added to the blockchain system without compromising the integrity of data stored in the ledger. The HHC uses HASH value (SHA1) of the transaction, where the HASH value is appended with validator ID of the predefined valuators by the network operator (Central Bank). This type of HAHS value is used to improve the performance of the system and no more time needed to finds the identical HAHS value of the transaction. Also, it used to append the transactions received from participating financial institutions into BC. Figure 4 explains how the HHC algorithm works.

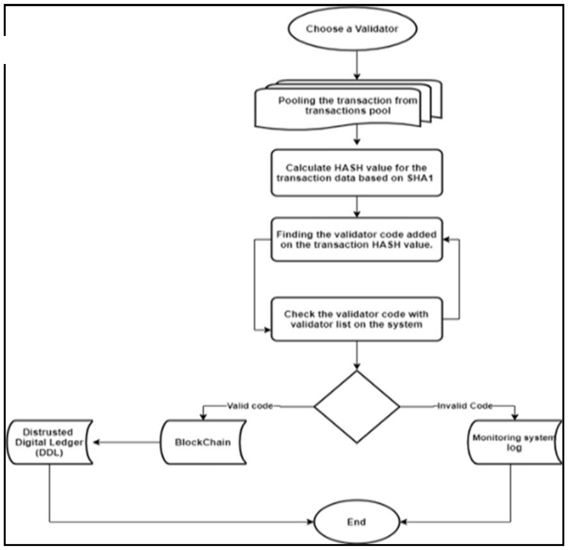

Choose a Validator
Pooling the transaction from transactions pool
Calculate HASH value for the transaction data based on SHA1
Finding the validator code added on the transaction HASH value.
Check the validator code with validator list on the system
Valid code
Invalid Code
Distrusted Digital Ledger (DDL)
BlockChain
Monitoring system log
End

Figure 4: HHC Consensus Algorithm

The network operator selects a validator randomly based on Round Robin concept every two minutes or when the block becomes full. The size of each block is around 1000 rows with 122 KB. Then the selected validator start pulling the transactions from the transaction pool and starts performing the validation process of transactions. The validated transactions are placed into a block and the HHC start performing the following steps:

1 **Calculate the HASH value for the transaction data**:

A transaction received by the transactions pool has two parts:

- Plaintext Data Record (Citizen ID, Outstanding Amount, Citizen Status and Finish Expectation Date).
- HASH value of the data record and Validator ID. The HHC recalculates the HASH value for the Plaintext Data Record based on SHA1 cryptographic function.

2 **Finding the validator code added on the transaction HASH value:**

As above mentioned, the HASH value of the transaction includes a validator code in a random place and the length of the code, where the length is three characters. The selected validator has to split

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

the HASH value into two parts; one has a length of three characters, and another is the rest of the HASH value.

3 Check the validator code with validator list in the system:

Compare the HASH value of the Plaintext Data record of the transaction with the result from step 4. By separating the part which is three characters of length, from the rest HASH value, we obtain the part that represents the validator code. It is then checked against the list of validator codes identified by the Central Bank on the system. Steps 2 and 3 will be repeated until the identical HASH value for the Plaintext Data Record and identical validator code; who was sent the transaction are found.

4 Adding the block into Blockchain:

After finding the identical HASH value and identical validator code in the previous steps, a new block will be added on the Blockchain. Once anew block is added, the HASH value of the previous block will be saved on this new block along with the Accumulation HASH value. To implement the concept of hand by hand, the chosen validator has to choose another validator in the network to append the transactions on the BC. This process based on the Round-Robin schedule concept to juggle the processes between the validators. After adding a new block into the chain, it will be reflected on all distributed digital ledgers for each associated financial institution on the system network.

Table 2 illustrates a comparison between the proposed HHC and other notable consensus algorithms.

Table 2: Comparison between HHC and Other Notable Consensus Algorithms.

Criteria	POW	POS	POA	HHC
Energy Efficient	No	Yes	Yes	Yes
Modern Hardware	Very important	No need	Yes	No
Forking	Yes	Yes- but difficult	Yes	No
Double Spending Attack	Yes	Difficult	No	No
Block Creating Speed	Low	Fast	Fast	Very Fast100 TB/s
Expandable	No	No	With a limit	Yes
Example	Bitcoin	Nextcoin	Microsoft Azure	-

5 Monitoring log system:

The monitoring log system is to record all transactions which made by unauthorized validators or intruders to keep the system safe by defining all types of attacks and intrusions. The HHC algorithm decides if the transaction is valid or not. If either the identical HASH value of the transaction or validator code are not found, a transaction deemed invalid. The following lists the data that will be stored on the Monitoring Log System:

- Fake transaction HASH value.
- Transaction Date.
- Fake validator ID.
- Validator ID that discovered the fake transaction and validator.

The HHC consensus algorithm has the following benefits:

1. Efficiency and velocity: The HHC algorithm is not complex in operating procedures.
2. No wasted validation time: Every two minutes the system network will randomly select a validator to work on transactions and no other efforts are needed.
3. No double validation processes on the transaction.
4. HHC is simple for validating transactions and complex for attackers.
5. The system processes transactions quickly to prevent system disruptions.
6. Zero forgeries.

3.5 Validation Process of Transactions

Each transaction enters into the transaction pool should calculate the HASH value with the validator ID as shown in figure 3. The validation process is started by the selected validator, as shown in figure 5 where the validator should perform the following steps for each receive transaction:

1. The validator has to pull the transaction from the transaction pool. The transaction consists of a client ID, HASH value, client status, outstanding amount, expectation finish date and HASH value of data record. As it appears in the data record, the client ID is HASHed with the client password for the sake of the client's privacy. Hence, banks on the BC system will not be able to inquire about any client without a client password.

2. Based on step one, the validator has to recalculate the HASH value for the data record in; equal to: acdded14efc7c7dd91944eb7a0080548d2214afd.

3. The validator has to use the inserted HASH value to check the transactions' validity; where the inserted HASH value has the validator ID for the transaction sender, as seen below: acdded14efc7c7dd91iuf944eb7a0080548d2214afd. In this example, the validator ID is "iuf", and the validator has to try to find this validator ID and match it with one of the validator IDs identified by the network operator.

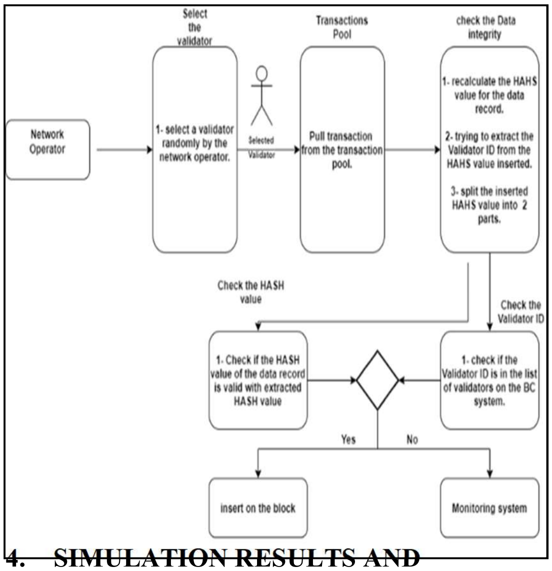
4. If the validator ID is matched and the HASH value for the data record is matched to the rest of the HASH value, the transaction will be inserted into the block; else it will be rejected and insert on the monitoring system.

5. Once the block has 1000 records, the block size is 122KB, or the two minutes are up, the validator has to request support from another validator on the BC system to add the block into BC.

6. The validator has to pull the transaction from the transaction pool. The transaction consists of a client ID, HASH value, client status, outstanding amount, expectation finish date and HASH value of data record. As it appears in the data record, the client ID is HASHed with the client password for the sake of the client's privacy. Hence, banks on the BC system will not be able to inquire about any client without a client password.

7. Based on step 2, the validator has to recalculate the HASH value for the data record in Figure 5; equal to: acdded14efc7c7dd91944eb7a0080548d2214afd.

8. The validator has to use the inserted HASH value to check the transactions' validity; where the inserted HASH value has the validator ID for the transaction sender, as seen below: acdded14efc7c7dd91iuf944eb7a0080548d2214afd.


Select the validator
Transactions Pool
check the Data integrity
Network Operator
1- select a validator randomly by the network operator.
Selected Validator
Pull transaction from the transaction pool.
1- recalculate the HAHS value for the data record.
2- trying to extract the Validator ID from the HAHS value inserted.
3- split the inserted HAHS value into 2 parts.
Check the HASH value
Check the Validator ID
1- Check if the HASH value of the data record is valid with extracted HASH value
1- check if the Validator ID is in the list of validators on the BC system.
Yes
No
insert on the block
Monitoring system

4. SIMULATION RESULTS AND DISCUSSIONS

Figure 5: Process of Validation Transactions

The system architecture is evaluated using a real dataset (55384 record) from National Microfinance Bank (NMB). This number of records corresponds to approximately 25% of NMBs daily data traffic. A sample of the dataset is presented in Table 3.

Table 3: NBMs Data Set Sample

National ID	Outstanding AMT	Delay Day	Last Installment date
9871018724	1000	0	05/12/2020
9662040750	268.01	0	04/02/2020
9932057326	154.5	96	04/09/2019
9712044632	41.625	278	04/01/2019
9902023722	51.7	95	06/07/2019
9711038796	469	4	04/04/2020
9751049165	3853.343	0	07/03/2021
9912000624	164	0	04/02/2020
9922027984	451.99	0	06/03/2020

The system architecture is implemented using JAVA and Oracle Tools for Users Interface. Figure 6 shows the simulation scenario of the proposed system architecture, where the number of registered banks is three. The system is ready to integrate with N number of banks.

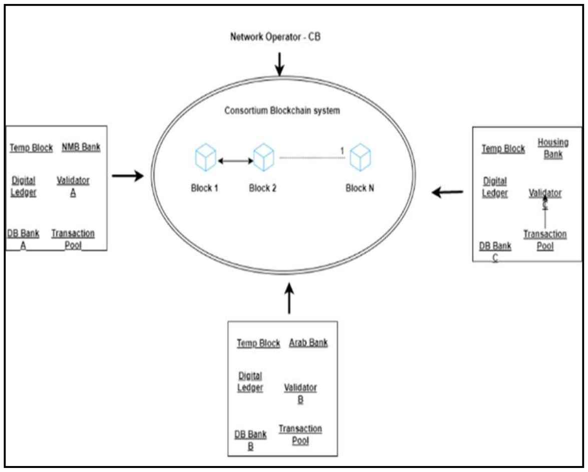


Figure 6 : Simulation Scenario

The Simulation scenario of the system architecture has been tested in several stages, to evaluate system performance, capacity and immutability. The aim of these tests is to ensure the ability of the system to absorb large numbers of transactions and system scalability to associate N numbers of financial institutions. In addition, to evaluate the ability of the system to validate and adding blocks of transactions into the blockchain. The system architecture is evaluated according to transaction upload time, validation time, time needed to add the block into the chain, impersonate the validator, client data privacy, and monitoring system.

4.1 Transaction Upload Time Into Bc

The proposed system architecture is based on an unlimited number of financial institutions participating in the network, which means that the system can handle the increasing number of transactions without delay in processing and uploading these transactions, where each financial institution in the network have at least one validator to work on the transactions and can generate large number of transactions.

Figures 7 and 8 show the time needed to upload different number of transactions from different number of banks with different data size (number of transactions). Figure 8 shows that as the number of transactions increases the load time is increased.

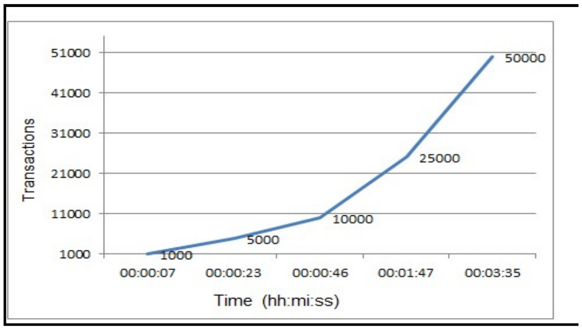


Figure 7 : Transaction upload time from one bank (NMB)

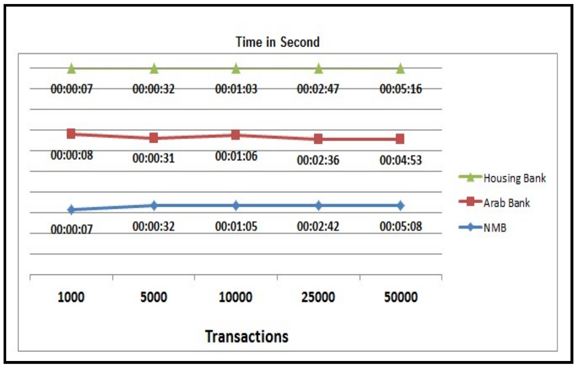


Figure 8 : Transaction load time from three banks (NMB, Arab Bank, Housing)

As seen in figure 8 the time needed to upload different number of transactions by three banks simultaneously is increased for each bank as the number of transactions increased. The upload time increases because the three banks are uploading the transactions simultaneously. The slight difference between the upload times required for each bank depends on the data complexity of each bank while inserting the transactions into transaction pool. Each transaction should calculate the HASH value of the transaction by SHA1 appended with the validator ID, which is generated randomly and appended in a random place in SHA1 value. This indicates that when the number of banks registered on the BC system increases, the performance of the BC system also increases.

4.2 Validation Time

Based on the result of the time needed to upload transactions, the validation time is increased simultaneously, which presents the system's capacity to work with the increased number of transactions with high performance and the capability to add N number of validators.

The time needed to validate the transactions is shown in Figure 9. It is clear from the figure 9 that as the number of transactions increases the validation time is also increased. This time represent the time needed to perform all steps in validation process.

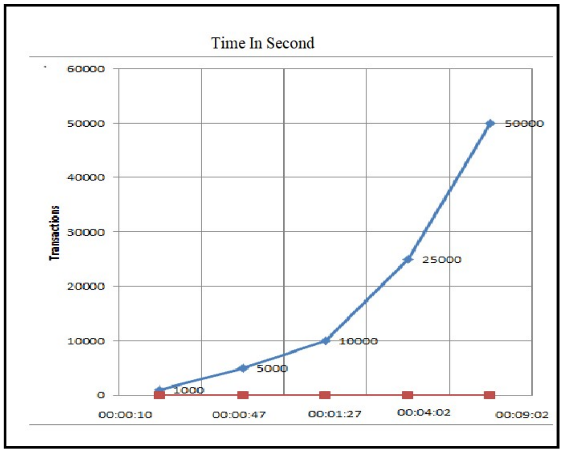


Figure 9 : Time to Validate and Appending Transactions into BC

4.3 The Time Needed To Append Block Into Bc

In parallel, when the number of transactions increases, the time needed to validate the transaction will increase, and this will also be reflected in the time needed to append the transactions block on chain, those first three points prove the performance and capacity of the system to handle the increases of the transactions by at least one validator for each participant on the network.

The time needed to append a block into BC is shown in Figure 10. The evaluation of this time is based on the block size which is 1000 records.

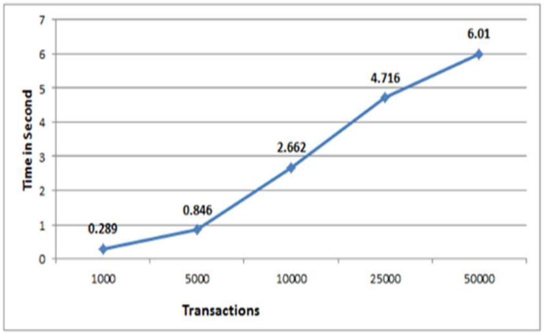


Figure 10 : Time needed to append block of transactions into BC

4.4 Impersonate The Validator

While the most important strengths of blockchain technology are the security, privacy, and immutability of the data, we are evaluating if there is any type of attack can happen, at this point, we test "authentication spoofing" if the attacker has the ability to add a fake validator on the system to make any fake transactions or validate any transactions by the fake validator.

This kind of attack requests to join the BC system network illegally. In this case, the attacker will go through many processes that need a lot of time to discover the Validator ID. The Validator ID is composed of a total length of three characters; alphabet and digits, which represent a very large number of possibilities (0 … 9, a … z and A…Z) represented in equation below:

Number of possibilities = $X! / (X-Y)$

Where X is the total number of digits and alphabets, and Y is the validator ID length. Hence, to find a potential validator is near impossible because the attacker has to find the used validator in the blockchain system with the random possible validators already predefined. This means that the proposed BC system has a strong security level and makes it difficult for attackers to impersonate a legitimate validator.

4.5 Client Data Privacy

Protection of a clients' financial information considered as one of the most important international standards of any system based on the distribution data mechanism. For this reason, the Client ID is stored as a HASH value in the proposed BC system, making it impossible to inquire any data about any random client. The only way to inquire about a client is to know the Client ID and the password of the client, calculate the HASH value of that ID, then query through that HASH value. Note that the HASH value is one-way data encrypted and therefore cannot be decrypted. Table 4 shows the data saved on the BC and DDL. When a transaction sniffed out by an attacker and tries to edit the data record, the validator will recalculate the HASH value for the transaction. However, the recalculated HASH value will not be matched with the sent HASH value so the transaction will be rejected and inserted into monitoring system, also alerting the network operator.

Table 4: Data Saved in BC and DDL

Previous Block Hash	1c2e893bd422da8c241daf5 a56e3f8e0e34bcbce		Block Serial
Client Hash	Data Record	Data HASH	Transaction Date Validation Date
f5d4af40cedf3aa38e24315ee818412ea213507d	f5d4af40cedf3aa38e24315ee818412ea213507d,Good,487.5,04/11/20	e0ad69c917bc0c327bf0e1dc0c250eb6d08225be	15/02/2020 18:40:55 15/02/2020 18:41:01
577e5930457f20500d0deddbc6fb650285e406ec	577e5930457f20500d0deddbc6fb650285e406ec,Good,776.992,05/12/20	d3eb5aecaed2e19560f5b5db3d2e9794d09b835c	15/02/2020 18:40:55 15/02/2020 18:41:01
ed4d05e2428284bb370c8d6bb787258aab82fe	ed4d05e24282854bb370c8d6bb7187258aab82fe,Good,457.495,04/08/20	54788df51f4e7b5ec883ed0fabcdcebc4bdff1ea	15/02/2020 18:40:55 15/02/2020 18:41:01
2b87b59c72901c708ceacea62931611b6c5ae2a0	2b87b59c72901c708ceacea62931611b6c5ae2a0,Good,693,05/12/20	249f80459d9970901ac4a7c8dbffaa0e0c63539c	15/02/2020 18:40:55 15/02/2020 18:41:01
2e04d3351a13afe88f0c6258a0648dca91c46b08	2e04d3351a13afe88f0c6258a0648dca91c46b08,Good,832.492,04/01/21	1263ce1b30c1b96293a633471371b71a90dd6fc3	15/02/2020 18:40:55 15/02/2020 18:41:01

The complexity of the transactions evaluated to measure the performance of validation time needed, which proves that the proposed architecture is working well in different kinds of transactions as show in table5.

Table 5: Total validation time

Transaction HASH value	Start Time	End Time	Validation time
d504918e89921ef1660f8c04	17:39:09:414	17:39:09:510	96 Msec

ce3zn22760fbc251e88			
d3zn504918e89921ef1660f8c04ce22760fbc251e88	17:45:13:290	17:45:13:373	83 Msec
d504918e89921ef1660f8c04ce22760fbc251e83zn8	17:42:06:419	17:42:06:518	99 Msec
d504918e89921ef1660f3zn8c04ce22760fbc251e88	18:09:43:801	18:09:43:896	95 Msec

As shown in table 5, regardless of the complexity of the validator place in HASH transaction, the validation times are closed, which proves the effectiveness of the proposed system.

4.6 Monitoring System

One of the most important advantages of blockchain technology is to keep data secure, distributed, and immutable. Any attempt by a fake participant in the system to modify data, the monitoring system automatically send an alert to all participants in the system informing them about illegal event in the system. The monitoring system stores the unauthentic transactions, fake validators, etc. as shown in Table 6, which can be as an evidence source for the digital forensics investigators [9].

Table 6: Monitor System Log

Fake Transaction HASH	Data Record	Transaction Date	Fake Validator	Discover BY
4bbpdw2728ecd3bc4aa6f4a6d5bb9892d10f340792c	1000000001,Good,900,31-AUG-20	09-FEB-2020	C	AB
c9d2e795b83503c8c27856cf6633749cc1d8f43zn10	,Good,713.7,04/11/20	11-FEB-2020	3zn	BC
2c3cf1e3zn2d95638ebe70247284dc51453f6f8d536	122211009,pad,780,01-JAN-21	06-FEB-2020	6	NMB
4bbpdw2728ecd3bc4aa6f4a6d5bb9892d10f340792c	1000000001,Good,900,31-AUG-20	09-FEB-2020	C	BC
4bbpdw2728ecd3bc4aa6f4a6d5bb9892d10f340792c	1000000001,Good,900,31-AUG-20	09-FEB-2020	C	BC
4bbpdw2728ecd3bc4aa6f4a6d5bb9892d10f340792c	1000000001,Good,900,31-AUG-20	09-FEB-2020	C	BC
4bbpdw2728ecd3bc4aa6f4a6d5bb9892d10f340792c	1000000001,Good,900,31-AUG-20	09-FEB-2020	C	BC

The results of the evaluation of the proposed system based on the selected evaluation criteria show that the system can reduce fraud in financial institutions by achieving high level of security, immutability of data.

4.7 Comparison Between Existing and Proposed Systems

The Table 7 shows the comparison between the existing and proposed systems, the comparison show the advantages of the proposed system over the others.

Table 7: Proposed system compared with other works

	Consensus algorithm	Reduce risk	Reduce Cost	Real data test	Log Monitor
Proposed System	YES	YES	YES	YES	YES
David Doe[18]	NO	YES	YES	NO	YES
Maria Todoref[19]	NO	YES	YES	NO	YES
Vladimir Soloviev[3]	NO	NO	YES	NO	NO
Rui Wang[27]	NO	YES	NO	NO	YES

5. CONCLUSION

The goal of this paper is to improve lending process and overcome fraud in Jordanian financial institutions. At the moment there is no system implemented in Jordan that address such challenges. As the financial institutions are continuously in the process of growing and expanding to meet the needs of their clients, the proposed architecture cam be used by them to achieve security, privacy, etc. Because he results show that the system architecture has a strong security level and makes it difficult for attackers to impersonate a legitimate validator, and high performance in terms of less time needed to validate, upload, and adding transactions and blocks to blockchain system. The contribution of this research must be considered in light of its limitations, which also build the basis for future research. Therefore, we argue that this system architecture could be applied in Jordan. In the future, tests will be pursued through the system's test by using data from different financial institutions and applying international financial standards regarding the security and protection of financial clients' data.

REFRENCES:

[1] P. S. Moekti, "Financial Inclusion in Indonesia: Moving Towards a Digital Payment System," Financial Inclusion in Asia, pp. 131-186, 2016.

[2] I. Barrès, "The Management of Foreign Exchange Risk by Microfinance Institutions and Microfinance Investment Funds," in Microfinance Investment funds, Berlin, Springer, 2006, pp. 115-146.

[3] V. Soloviev, "Fintech Ecosystem in Russia," in 2018 Eleventh International Conference "Management of large-scale system development" (MLSD, Moscow, 2018.

[4] S. Boris and K. Anton, "Comparison of ERP Systems with Blockchain Platform," Intelligent Systems in Cybernetics and Automation Control Theory, pp. 240-247, 2018.

[5] W. Shuang, "Research on the Collection Method of Financial Blockchain Risk Prompt Information from Sandbox Perspective," in 2019 International Conference on Virtual Reality and Intelligent Systems (ICVRIS), Jishou, China, China, 2019.

[6] Sarah Al-Maaitah, Mohammad Qatawneh, Abdullah Quzmar. E-Voting System Based on Blockchain Technology: A Survey. 2021 International Conference on Information Technology (ICIT).

[7] Sara El-Switi, Mohammad Qatawneh. Application of Blockchain Technology in Used Vehicle Market: A Review. 2021 International Conference on Information Technology (ICIT).

[8] Abdullah Quzmar, Mohammad Qatawneh, Sarah Al-Maaitah. Reducing Counterfeit Drugs with Blockchains: A Survey. 2021 International Conference on Information Technology (ICIT).

[9] Baker Alhasan, Mohammad Qatawneh, Wesam Almobaideen. Blockchain Technology for Preventing Counterfeit in Health Insurance. 2021 International Conference on Information Technology (ICIT).

[10] Z. Xiaoming, S. Bingying, N. Yingzi, R. Yifan and L. Rui, "Digital Finance—From Traditional Finance to Digital and Internet Finance," in Business Trends in the Digital Era, Singapore, 2016.

[11] K. Nir, "Blockchains and International Business," IT Professional, pp. 8-13, 2019.

[12] G. Dorfleitner and D. Braun, "Fintech, Digitalization and Blockchain: Possible Applications for Green Finance," in the Rise of Green Finance in Europe, Cham, Palgrave Macmillan, Cham, 2019, pp. 207-237.

[13] A. Dan, B. Zahn, D. C. James, D. Quentin, M. K. Jonathan and S. Richard, "Financial reporting fraud and other forms of misconduct: a multidisciplinary review of the literature," Review of Accounting Studies, p. 732–783, 2018.

[14] Z. Xueyun, H. Ninghua, Z. Junchen and X. Xuening, "A consortium blockchain paradigm on hyperledger-based peer-to-peer lending system," China Communications, pp. 38-50, 2019.

[15] I. Karagiannis, K. Mavrogiannis, J. Soldatos, D. Drakoulis, E. Troiano and A. Polyviou, "Blockchain Based Sharing of Security Information for Critical Infrastructures of the Finance Sector," Fournaris Computer Security, pp. 226-241, 2020.

[16] D. Huang, X. Ma and S. Zhang, "Performance Analysis of the Raft Consensus Algorithm for Private Blockchains," IEEE Transactions on Systems, Man, and Cybernetics: Systems, pp. 172-181, 2019.

[17] Q. Mohammad, A. Wesam and A. Orieb, "Challenges of Blockchain Technology in Context Internet of Things: A Survey," International Journal of Computer Applications, vol. 175, no. 16, pp. 13-20, 2020.

[18] D. D. Fiergbor, "Blockchain Technology in Fund Management," in International Conference on Application of Computing and Communication Technologies, Delhi, India, 2018.

[19] M. Todorof, "Shariah-compliant FinTech in the banking industry," pp. 1-17, 5 April 2019.

[20] Ahmad Bany Doumi, Mohammad Qatawneh. Performance Evaluation of Parallel

International Data Encryption Algorithm on IMAN1 Super Computer. International Journal of Network Security & Its Applications (IJNSA), Vol. 11(1), 2019.

[21]Heba Harahsheh, Mohammad Qatawneh. Performance Evaluation of Twofish Algorithm on IMAN1 Supercomputer. International Journal of Computer Applications, Vol. 179 (50), 2018.

[22]Areej Al-Shorman, Mohammad Qatawneh. Performance of Parallel RSA on IMAN1 Supercomputer. International Journal of Computer Applications, Vol. 180(37), 2018.

[23]Sanad AbuRass, Mohammad Qatawneh. Performance Evaluation of AES algorithm on Supercomputer IMAN1. International Journal of Computer Applications, Vol. 179(48). 2018.

[24]Asassfeh Mahmoud Rajallah, Mohammad Qatawneh, Feras Mohamed AL-Azzeh. Performance Evaluation of Blowfish Algorithm on Supercomputer IMAN. International Journal of Computer Networks & Communications (IJCNC). Vol. 10(2), 2018.

[25]Mohammad Qatawneh, Wesam Almobaideen, Mohammaed Khanafseh, Ibrahim Al Qatawneh, “DFIM: A New Digital Forensics Investigation Model for Internet of Things,” Journal of Theoretical and Applied Information Technology, Vol. 97(24), 2019.

[26]Orieb Abualghanam, Mohammad Qatawneh, Wesam Almobaideen, A Survey of Key Distribution in the Context of Internet of Things, Journal of Theoretical and Applied Information Technology, Vol. 97(22), 2019.

[27] M. Todorof, "Shariah-compliant FinTech in the banking industry," ERA Forum, vol. 19, no. 1, pp. 1-17, 2018.