Mesopotamian journal of Cybersecurity
Vol.4 No.2, **pp**. 1–19
DOI: https://doi.org/10.58496/MJCS/2024/005; ISSN: 2958-6542
https://mesopotamian.press/journals/index.php/cybersecurity

Research Article

Transaction Security and Management of Blockchain-Based Smart Contracts in E-Banking-Employing Microsegmentation and Yellow Saddle Goatfish

Wid Alaa Jebbar ,[1], Mishall Al-Zubaidie ,[1] *,

[1] *Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq*

ARTICLE INFO

Article History

Received 08 Feb 2024
Accepted 30 Apr 2024
Published 09 May 2024

Keywords

Authentication

Blockchain Transaction;

E-banking

Microsegmentation

Smart contracts

ABSTRACT

The process security of money transactions is considered an important issue in e-banking. Additionally, it is an enormous problem if never controlled. particular, security should be a combination of fast and sturdy characteristics, which is the subject of previous studies suffered from. Our research attempts to improve the system in which banks deal with the security of financial transactions. This research leverages the idea of microsegmenting the entire system into designated zones to concentrate on security, where each zone has its own rules and limitations. These rules are managed by a smart contract, which decides whether they have been observed to verify the legitimacy of the customer. First, the two-phase commit algorithm (2PC) was used to specify the type of e-banking request. After this, the microsegmentation principle was applied to isolate each type of e-transaction process alone in a separate segment. Then, the yellow saddle goatfish algorithm (YSGA) was used to determine whether the smart contract conditions were optimized. Finally, if the customer is authorized, then the entire transaction process is saved in the blockchain's main ledger and secured by a unique hash. The blockchain application makes our system capable of dealing with large numbers of users in a decentralized manner. In addition, using a hash with each block prevents fraudulent transactions by adversaries. Our system has been examined against several recent well-known assaults/attacks, such as falsification, advanced persistent threat, bribery, spoofing, double spending, chosen text, race, and transaction replay attacks, and has proven to overcome them. In terms of the performance evaluation, we obtained an execution time of approximately 0.0056 nanoseconds, 3.75% complexity, and 1500 KB of memory and disk drive, which is considered low compared to that of state-of-the-art research. Thus, our proposed system is highly acceptable for banking sector applications.

1. INTRODUCTION

Currently, the goal of financial institutions and banks is to automate their information, data, and money transactions [1]. Moreover, this goal is facing many challenges because automation means many dangerous assaults and hacking as long as the information is available on the internet or through e-banking. Thus, trust and security are extremely important between customers and stakeholders. Banks and different financial organizations are constantly under pressure to strike a balance between system security, costs, and the ability to complete procedures in real time [2], which is a major challenge because cyber threats are increasingly developing and taking new forms continuously, resulting in breakthroughs, endangering data accessibility and putting banks' reputations on the edge [3, 4]. This section, which includes Subsection 1.1, will summarize the cyber threats that have been highly prevalent in the financial industry. Subsection 1.2 explains the motivation for using blockchain technology in e-banks, and Subsection 1.3 explains our main contributions.

1.1 Threats of the Financial Sector

A better understanding of assault vectors in the financial sector will enable banks and other organizations to develop better cybersecurity infrastructure [5]. Several common cyber threats are highly prevalent in the financial industry. For instance, falsification, bribery and spoofing refer to the act of someone or something impersonating another person or thing to gain access to a user's system, steal money or data, or distribute malware. Email, caller identifier (ID), text message, internet protocol (IP), facial, and other types of assaults are examples of spoofing and falsification assaults [6, 7]. These types of assaults cause considerable damage to banks and financial systems, such as loss of data, reputational damage, loss of intellectual property, loss of customers, financial penalties, loss of productivity, and money loss. For instance, in the first

*Corresponding author. Email: mishall_zubaidie@utq.edu.iq

quarter of 2022, spoofing assaults mimicking corporate social networking websites accounted for more than half (52%) of all assaults worldwide, based on the cyber security vendor's 2022 Q1 brand spoofing report. Additionally, according to 2022 reports, 9 out of 10 (91%) email phishing/spoofing assaults were successful in removing UK firms [8]. Furthermore, there is a possibility of race assault when two transactions are made simultaneously with the same funds, which is considered highly dangerous and is the most common assault affecting the financial sector, where the most affected are American, Argentinean, Brazilian, and Chinese banks. By the end of 2022, 566 breaches had occurred worldwide in the finance and insurance sectors, resulting in more than 254 million records being exposed. Moreover, assaults such as double spending, chosen text, and transaction replays were being used by assaulters/hackers in an attempt to steal $1 billion from the central bank of Bangladesh in February 2016; even with the majority of transactions banned, $101 million vanished. Figure 1 shows security assaults in various sectors [9], as financial institutions suffer from the largest percentage of security breaches.

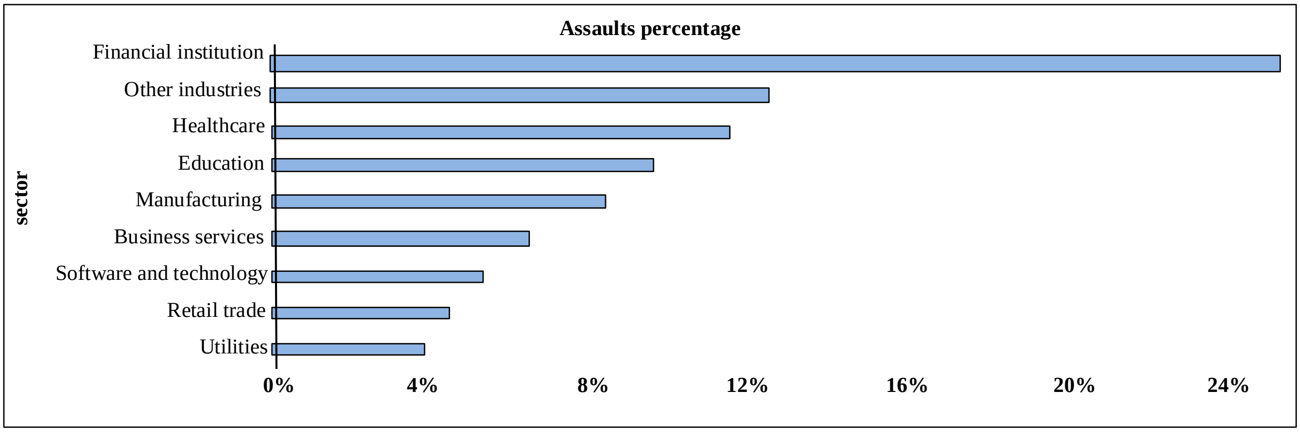


Fig. 1. Assault percentage in various sectors

1.2 Financial Sector's Technology

Blockchain technology (BCT) has been proposed as an evolutionary technology for estimating security goals, protecting data [2], and eliminating third-party roles during money transactions [10]. Transactions are performed via a peer-to-peer (P2P) process. Then, the whole process is saved on a decentralized ledger using the hashing principle; thus, since the creation of BCT, this technology has continued to make an exceptional decrease in cost compared to the considerable advantages that it offers [11]. According to studies on the safety of online banking and the standard of customer care, people prefer online banking services over traditional banking systems. However, in the interim, staff members' accidental or intentional mistakes account for the majority of cyberattacks that affect enterprises. This implies that not only is the information technology (IT) department worried about cybersecurity, but employees at all levels also need to be cyber aware. Additionally, people outside contractor areas should be aware of the importance of cybersecurity [12]. As a result, developers/researchers have begun to improve online services and create new systems that can safeguard user data and provide simple access to bank accounts. One of these amazing technologies and systems was BCT, which can be combined with other technologies such as identity management and business rules [13].

1.3 Main Contributions

Our contributions are as follows:

- The level of security can be increased by using the microsegmentation principle for the first time with financial systems to isolate each process alone in a separate segment, where if one segment is affected by an assault, then the other segments will remain isolated and safe. To the best of our knowledge, this contribution has not been previously studied.
- Two phases of authentication are applied: first, smart contract condition detection, and second, hashing and ID detection in BCT. This procedure will make the authentication process more powerful. There will be no entrance to the system from any assaulter unless he/she is verified in both phases.
- The increase in the time consumption and execution time of the specified e-banking process depended on the properties of the YSGA, which is considered one of the fastest search algorithms. To the best of our knowledge, this approach has not been previously applied in e-bank systems.

The content of this paper is as follows: in the introduction, we discuss e-banking and security risks in Section 1. In Section 2, we summarize the related works e-banking. Section 3 provides a preliminary overview of the methods used in our proposed system. Section 4 describes the design of our proposed security system in detail. Section 5 describes the security analysis against several well-known assaults, Scyther analysis, and performance evaluation. Section 6 addresses the limitations of the study. Our conclusions are presented in Section 7. Finally, future work will be described in Section 8.

2. RELATED RESEARCH OF E-BANKING SECURITY AND MANAGEMENT

An in-depth investigation of recent research on the topic of our study is provided in this section.
Taloba et al. [3] presented an Internet of Things (IoT) system with multimedia, such as user images and X-ray diagnostic medicine transactions between normal users and suppliers secured using BCTs, especially using hashes where every action taken by anyone inside the system is encoded in blocks by a specific number for a hash. Thus, any changes from any assaulter cause a change in the number of hashes, which leads the system to stop. However, their suggested framework never discussed the length of the hashes and never compared that to the percentage of accuracy. Thommandru and Chakka [10] presented a scheme that also addresses the security issue first and focuses on the problem of money laundry, which used distributed ledger BCT technologies. Their paper considered know your customer (KYC) principle to be an important consideration. They used KYC with BCT in this specific form because their scheme proposes that knowing whom the system is dealing with produces a safe system, and their scheme is considered fast in execution according to the analysis they mentioned. Unfortunately, they never mentioned how they protected the money and the customers' information. Additionally, they presented the KYC principle as the basis of their results without providing a detailed analysis of how it improves security. Similarly, Sai et al. [14] offered a method by which customers can immediately access microcredit from lenders directly, based on adding the KYC to BCT and then requesting authentication for the KYC number to determine access. A polygon network is used in this strategy and not Ethereum. However, this strategy is similar to that used in the study in [2], which means that no new technique was used, and no principles were mixed to support high performance. Javaid et al. [2] illustrated and explained BCT and its main importance for financial services. Following previous work, BCT also provides high security for transactions between customers and stakeholders. They presented a high and accurate security system related to using two types of keys, a public key and a private key, but the analysis of their system performance did not reveal high performance. Similarly, [15] suffers from a high complication rate, while [16], [17] and [18] presented a secured system but suffer from resource consumption problems. Moreover, e-banking schemes [19], [20], and [21] lack distributed and decentralized approaches to the security and management of user accounts in electronic banks.

Riad et al. [11] presented a hierarchy for controlling access to open banks. When an honest customer requests access to cloud-hosted financial data, first, a unique customer identifier (CID) is assigned to the customer by the bank web server. After that, the authentication servers will either authenticate the CID or not based on the branch policy, fraud detection entities, username, password, or any other credentials provided by the customer. Next, the BCT contract's functions are initialized for the authenticated customer identified by CID. A block that has been mined will be included in the synchronized blockchain. Subsequently, the customer will use the synchronized peer network to obtain authorization. Finally, the data kept in the cloud are accessible only to approved customers. However, this process was considered along with the absence of high-level detection algorithms that affect the performance and cause a delay in execution, but this module presented a secure and safe method. Gamal and Aref [12] addressed BCT as a fundamental technology for providing security to the financial sector and banks, where researchers compared traditional processes and BCT-based banking processes and found that BCT was faster, more efficient, and more secure. At the same level, [22] categorized the importance of BCT through different applications, such as e-banking, e-healthcare, e-aircraft, e-car sharing, and e-voting. Additionally, this study focused on Ethereum as the most commonly used tool in building applications. However, it is not a suggested model as much as it is a study of BCT characteristics. Additionally, Jena [23] recommended a study that would aid decision-makers, government officials, and technologists in improving banking guidelines to utilize BCT. Their research proposed an expanded version of the unified theory of acceptance and use of technology (UTAUT) model. It is a theoretical model that shows analytics about the importance of BCT. However, this study is not practical because it only shows the importance of the blockchain. Chaudhry and Hydros [13] presented a security model based on the principle of zero-trust, which means that no one should trust either the user or the employees of the system itself. Hence, they combined zero-trust security side by side with the BCT algorithm to maintain a secure system. However, this principle is considered old compared to the modern attacks and threats that financial organizations deal with every day, which means that the system here does not have a high level of security. Although [24], [25], [26], and [27] investigated the security risks in e-banks and how to address them, they neglected important attacks such as falsification and spoofing.

Garg et al. [1] demonstrated the potential benefits that an organization could receive from BCT. These benefits include increased efficiency through quick response to transactions, faster transactions due to automated record keeping, reduced transaction time and operational costs, prompt settlements and payments without the need for third parties, enhanced third-party trust through the use of cryptography, and real-time information leading to transparency on both sides. Rjoub et al. [28] suggested a k-nearest neighbor algorithm based on an adaptive neuro-fuzzy approach. It is a way to select the best node (customer) during the transaction process or to classify the nodes according to the similarity depending on the amount of the variable *k*, which is accomplished by calculating the distance between two points. Then, the square root and diction are calculated after the classification. BCT is used to detect security risks. Nonetheless, this method analysis showed that it is excellent in terms of cost reduction, time, and safety, but the analysis was limited and did not show any improvement. Moreover, there is no verification phase before the classification; thus, the principle of knowing the customer is not detected. Ullah et al. [29] presented a model centered on the adoption of BCT for financial organization use in developing nations, utilizing the manner of technological acceptance as a basis. There are five multi-item components in their suggested model: saving money, intention, perceived ease of use (PEU), perceived usefulness (PU), and trust. These parameters were never considered as parameters for measuring the performance or security of financial systems.

Farah et al. [30] aimed to investigate the mechanism by which customers' perceived financial well-being is determined by blockchain-enabled banking. The researchers performed their investigation by surveying 283 people who had bank accounts. The study revealed that Pakistani banks can use BCT to increase security and transparency while also reducing costs and time consumption. However, the problem of this study is that it is a theoretical study that has never presented any enhancement of the base blockchain systems. Zook and Grote [31] proposed a framework that systematizes the analysis of BCT adoption in financial sectors using the concepts of space, agency, and scale. They concluded that, based on the limited information they gathered, it is inaccurate to characterize BCT as complex. Instead, BCT is a technology that can disrupt traditional business models by offering lower-cost alternatives and quickly overtaking incumbent _rms. Meanwhile, they did not provide any details about how they reduced the cost of their proposed system, nor did they provide detailed results about the extent to which their system carries out banking transactions on time, which never provided any temptations to customers to use their system. Agrawal et al. Garg et al. [32] provided a summary of blockchain capacity to foster organizational trust and guarantee transaction transparency. This study advances BCT's application in the banking sector from both a theoretical and practical standpoint. The main findings are as follows: First, before choosing to integrate BCT into the banking system, managers, decision-makers, and experts would particularly benefit from having a foundational view to measure business benefits. Second, the study is technically and socially relevant due to its combination of professional and theoretical use. Furthermore, BCT may be adapted to a banking ecosystem's requirements, which will assist in minimizing launch costs even further, but here, they never focused on security as a major issue in financial systems.

3. BACKGROUND ABOUT E-BANKING AND USED METHODS

This section is organized into subsections that offer details on e-banking procedures and security measures. We aim to safeguard transactions in e-banking apps to provide a fully subjective overview of e-banking strategies.

3.1 E-Banking Manners

Through time and because of the rapid movement of technological development, technical and electronic methods came to take place over traditional methods in banks and financial institutions [11]. Therefore, the term e-banking has been presented as a fast, easy, and efficient way to make people electronically access their bank accounts. Furthermore, it gives people an advantage to access their accounts 24 hours a day and 7 days a week.

3.2 Brief Summary of Blockchain Technology

Blockchain technology is important to the e-banking industry and financial institutions. BCT is a decentralized database or ledger that is shared by nodes in computer networks or the internet. The data are saved in blocks, with each block consisting of the date, hash, and hash of the preceding block. For example, suppose a customer aims to transfer money 2 bitcoins to a specific stakeholder where a customer has 5 bitcoins and the stakeholder has 2 bitcoins; in the presence of BCT, there is no need for a third party to complete the process where the BCT will play that role and send the money as a P2P, and the whole process will be saved, as clarified in Figure 2. The specific block has full information about the entire transaction process, and this information will be decentralized to all the nodes in the network.

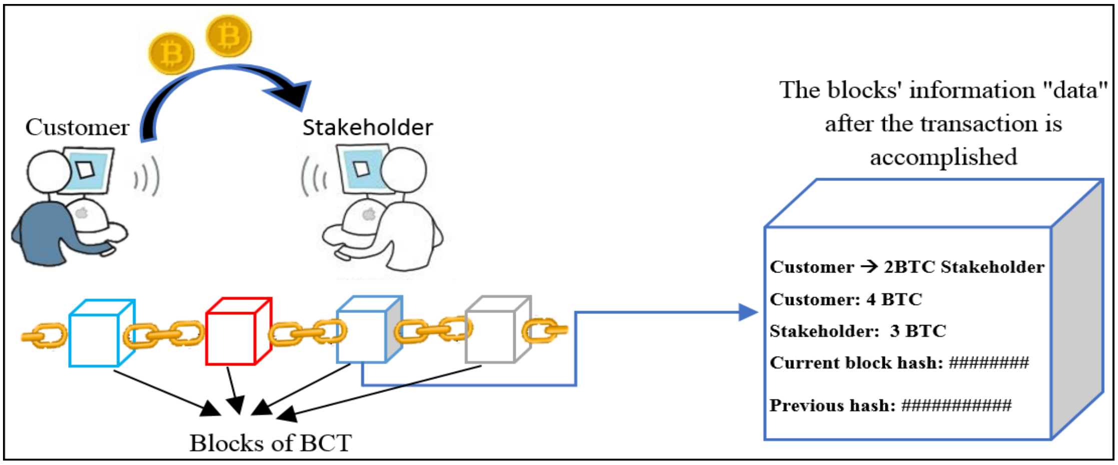

Customer
Stakeholder
The blocks' information "data" after the transaction is accomplished
Customer → 2BTC Stakeholder
Customer: 4 BTC
Stakeholder: 3 BTC
Current block hash: ########
Previous hash: ###########
Blocks of BCT

Fig. 2. Scheme of general BCT

Furthermore, BCT can be divided into the following main types [33].

- Public blockchain is nonrestrictive, and with this type of BCT, there is no need for permission to access; thus, anyone who has internet access can access this type of BCT. Therefore, the main advantage of this type of cryptocurrency is that it is completely independent, and most cryptocurrencies run on public BCT.
- A private blockchain is a restrictive type that needs permission to enter and is under the control of a single entity; only authentic users can access this type of BCT.
- Hybrid blockchain is a mix of public and private BCT where permission is needed, and it is a permissionless system of this type. Some parts are managed by one organization, but others are public.
- A consortium block is a creative approach in which some parts are public and others are private, but it can be moderated by more than one organization.

In our proposed method, private BCT is used because it offers enhanced privacy control and scalability compared to other types of blockchain. In finance, privacy is considered a very sensitive issue due to the sensitive data it deals with, which is why the private blockchain offers permissioned access that limits who can access the network and who can make a transaction. Additionally, a private blockchain allows faster transactions to meet the specific needs and requirements of a financial institution.

3.3 Smart Contracts

The smart contract (SC) has been proposed as a decentralized program that is considered very close to the idea of contracts in real life. This implies that any deal between two peers is controlled and detected by the SC based on a predetermined condition; if these conditions are accomplished, then the deal is done; otherwise, the deal is denied; consequently, any exchange of money or execution of any type of restricted content by specific rules can benefit from executing an SC [14]. The question is how these contracts work. The answer will be as simple as, if/when then, which means it is written code by a developer or programmer to ensure that there is no action taken unless the conditions are fulfilled. For example, if a customer (CR) wants to transact money to a stakeholder (SR), then an SC will be written as if the date is 21/10/2023 and the CR uses a specific password and then sends money to the SR, which means that the transaction process will never be performed unless the two conditions about the date and the password are fulfilled.

3.3.1 Steps of Smart Contracts

- Offer: The first component starts the deal. The first party uses a specific programming language to write a contract that includes an if-then clause. Then, the contract goes through the BCT.
- Negotiation: The contract is visible to all parties involved once it is posted on the BCT. The conditions of the contract are negotiable by the parties. Once it is signed, there is no turning back, so the involved ones check all the terms in this stage.
- Approval: Triggering events occur after all parties have given their approval to the conditions of the contract. The parties may designate other conditions as well, such as an expiration date, a due date, a strike pass or stop-loss, or another date. Following that, the agreement is accepted and finalized.
- Event of trigger: When the requirements are satisfied, the assets are transferred, or the underlying result takes place, the SC is activated.

3.3.2 Positive Aspects of Smart Contracts

Using SCs alongside BCT in financial systems has numerous advantages, as follows:

- Self-reliance: SCs eliminate the possibility of third parties manipulating the agreement because they do not require brokers or other middlemen to verify it. Furthermore, there are financial savings with SCs because there is no middleman.
- Security: Because of their self-reliance, SCs are considered to have a high level of security.
- Acceleration: Using computer protocols, SCs automate tasks, saving hours of labor in a variety of financial processes.
- Reliability: By using SCs, errors that arise from filling out numerous forms by hand are eliminated.

3.3.3Smart Contracts vs Traditional Methods

For a detailed overview of our specific usage of smart contracts in the proposed system, a wide comparison is presented in Table I.

TABLE I. COMPARISON OF SMART CONTRACT AND THE TRADITIONAL METHODS

Aspect	**Smart contract**	**Traditional methods**
Efficiency	Automate execution of predefined terms and conditions when specific conditions are met, reducing manual intervention and streamlining processes.	Typically, rely on manual processing, which can be time-consuming, prone to errors, and require intermediaries.
Trust	Transactions are recorded on a transparent and immutable ledger, enhancing trust among the parties involved.	Lack the transparency of blockchain, relying on trust in intermediaries, which may lead to disputes and inefficiencies.
Security	Utilize cryptographic security measures and are tamper-proof once deployed, reducing the risk of fraud and unauthorized access.	Vulnerable to fraud, manipulation, and cyberattacks due to centralized storage of data and reliance on intermediaries.
Cost	Eliminate the need for intermediaries, reducing overhead costs associated with intermediation, verification, and enforcement.	Involve fees for intermediaries such as lawyers, brokers, and banks, increasing transaction costs.
Flexibility	Can be easily customized to meet specific business requirements and can execute complex logic, enabling greater flexibility.	Often rigid and require standardization, making it challenging to accommodate unique needs and changes in business processes.
Speed of execution	Execute transactions automatically and near-instantaneously once conditions are met, leading to faster settlement times.	Involve manual processing and multiple intermediaries, leading to delays in transaction execution and settlement.

Overall, smart contracts offer several advantages over traditional methods, including automation, transparency, security, cost-effectiveness, flexibility, and speed of execution.

3.4 Microsegmentation

Microsegmentation (MS) is a security technique that refers to the principle of dividing a network into a definable zone; each zone has its own rules and conditions, as shown in Figure 3. This approach is completely different from network-MS, which needs hardware, unlike software-based MS. Thus, the main purpose of obtaining a secure system in this technique is to isolate each zone by itself so that if the assaulter ($\mathscr{A}$) can reach a zone, the other zones will remain safe and secure. As depicted in Figure 3, in the process of breaking up the whole system into zones where these zones are completely independent, let us suppose that $\mathscr{A}$ makes access to green zone 1; then, the assault is trapped in that zone, and the other zones are never affected. Comparing MS to more established methods, which are created and intended for environments with reinforced perimeters, reveals significant technical advantages:

- Enhance security and management to prevent $\mathscr{A}$s from moving across the network.
- Rapid deployment, maintenance, and adaptation of policies integrated with the MS.
- Since MS keeps policies tied to workloads rather than segments of a network, potential gaps in security coverage that can create vulnerabilities are closed.

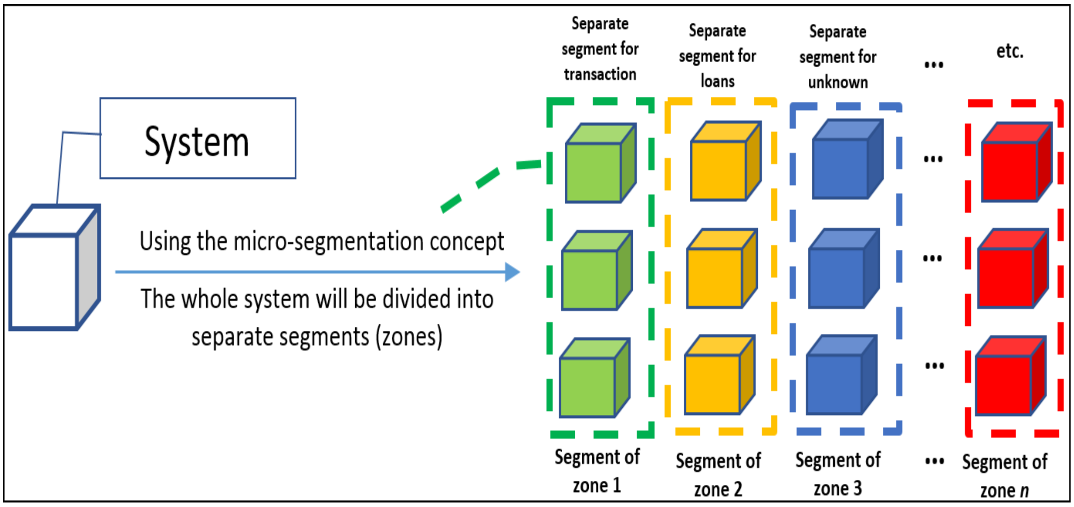

System
Using the micro-segmentation concept
The whole system will be divided into separate segments (zones)
Separate segment for transaction
Separate segment for loans
Separate segment for unknown
...
etc.
Segment of zone 1
Segment of zone 2
Segment of zone 3
Segment of zone *n*

Fig. 3. Scheme of microsegmentation

3.5 Yellow Saddle Goatfish Algorithm (YSGA)

The hunting behavior that has been found in a group of yellow saddle fishes is incredibly interesting and has attracted the attention of scientific communities [34]. Thus, the mentioned fishes were found to be hunting in groups. Each group has only one fish, called the chaser fish, and the others belong to the same group, called the blocker fish, according to the fitness value. Consequently, an optimization technique has been translated for this kind of behavior, which is considered a powerful, fast, and modern algorithm used for the purposes of scientific research and determining the best. The whole hunt space will be divided into specific zones, after which all the populations (fish) in these zones will initialize a specific quantity. Then, we calculate the fitness value of each particle. Then, a comparison will be performed between the global best value and the fitness value of each fish to specify which one is the chaser that will lead the hunting process and which is the blocker fish [35]. As shown in Figure 4, the yellow fishes are chaser fishes that have the best fitness values, and the other gray fishes are blocker fishes. The steps of the entire algorithm are shown in Figure 5.

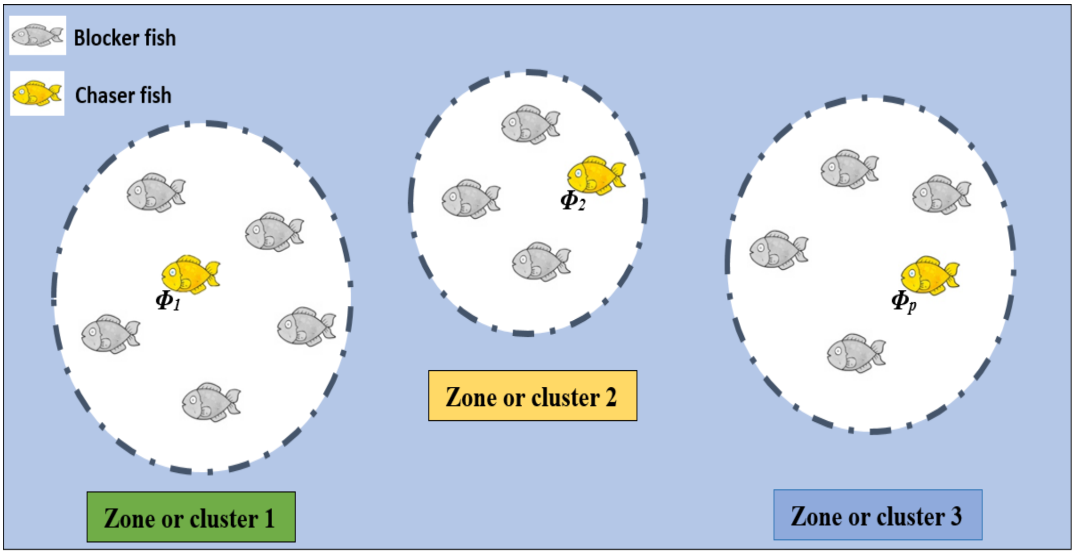


Fig. 4. YSGA hierarchy

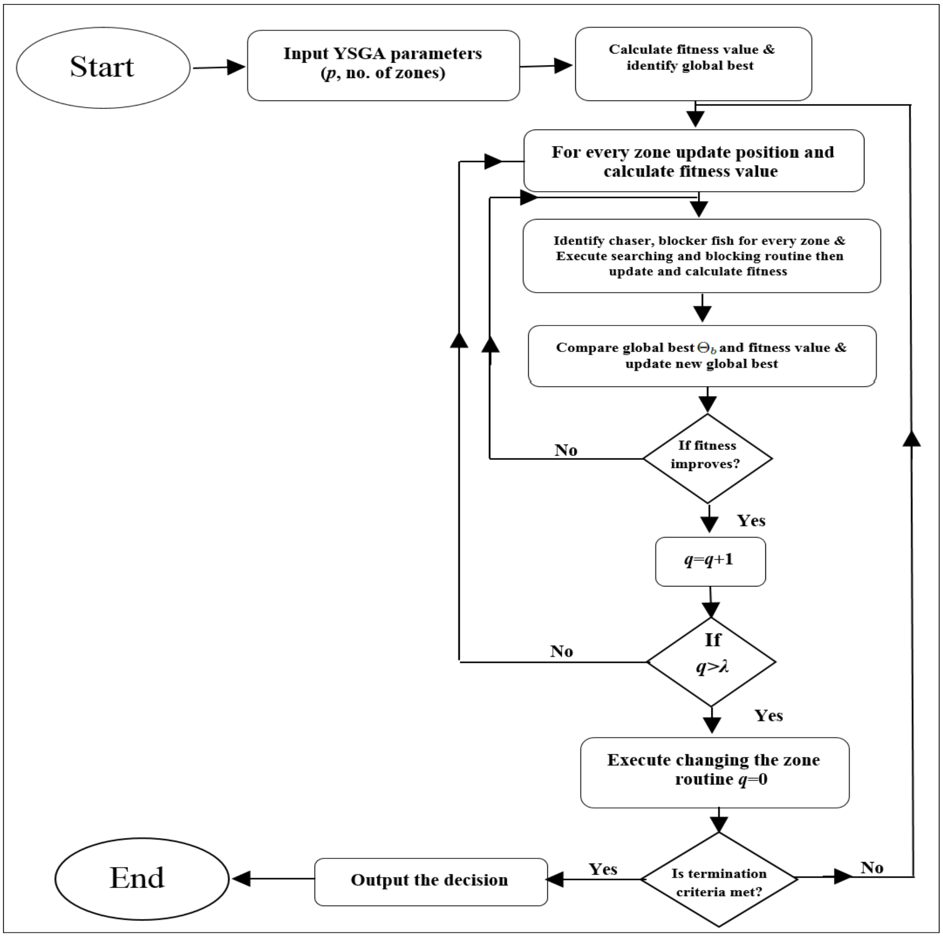

Start
Input YSGA parameters
(p, no. of zones)
Calculate fitness value &
identify global best
For every zone update position and
calculate fitness value
Identify chaser, blocker fish for every zone &
Execute searching and blocking routine then
update and calculate fitness
Compare global best Θb and fitness value &
update new global best
If fitness
improves?
No
Yes
q=q+1
If
q>λ
No
Yes
Execute changing the zone
routine q=0
Is termination
criteria met?
Yes
No
Output the decision
End

Fig. 5. YSGA scheme

4. PROPOSED SYSTEM'S APPROACHES

In this section, the e-transaction hierarchy, two-phase commit, MS, and YSGA with BCT are adopted in our proposed system. All of these approaches are explained in detail in the following subsections.

4.1 Hierarchy of Our Proposed System for E-Transaction

In financial institution and bank applications, the matter of security and data availability is considered an enormous matter, as we mentioned previously, but as much as security is important, the fast process of obtaining both security and managing information in real time is important because *CR*s' trust is a major issue for banks. Therefore, it is important to propose a reliable system that gains both fast and secure system characteristics to clarify our proposed system, let us imagine that a *CR* wants to transact money to an *SR*. This process will be considered a request sent to the system. Meanwhile, the system will decide which type of e-banking procedure is money transactions, loans, or any other applications by using the two-phase commit algorithm. After the type of the requested procedure is detected, it is assigned to a segment that combines all the transaction processes. Then, this segment is divided into different rules/zones using the MS principle. These zones will be controlled by an SC. Then, the detection of the authentication and the SCs' decision will be decided using the YSGA. For further illustration, Figure 6 shows the proposed system's hierarchy. Initially, the proposed system determines the type of CR request based on the decision of the 2PC algorithm and then creates a separate segment for each type of e-banking process after the transaction processes are combined alone in a separate segment. The detection phase of the SC's conditions will start based on the fast detection of the YSGA result, as clarified in Figure 6.

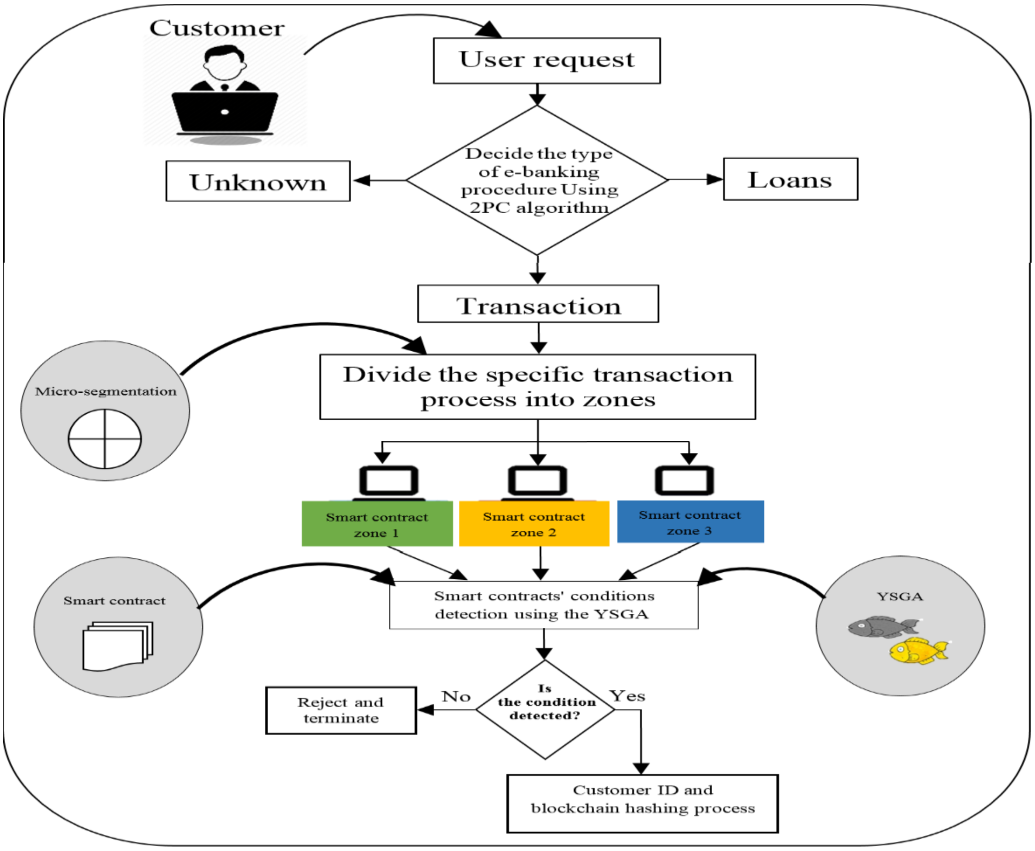

Customer
User request
Decide the type of e-banking procedure Using 2PC algorithm
Unknown
Loans
Transaction
Micro-segmentation
Divide the specific transaction process into zones
Smart contract zone 1
Smart contract zone 2
Smart contract zone 3
Smart contract
Smart contracts' conditions detection using the YSGA
YSGA
Is the condition detected?
No
Yes
Reject and terminate
Customer ID and blockchain hashing process

Fig. 6. Scheme of our proposed system

The detection process is controlled by obtaining the best value of the YSGA, which is completed by initializing the population in each zone: $P = [p_1, p_2, p_3 \dots p_m]$, where m is the number of the population.

Then, our system calculates the fitness value of each population in the zones to identify the chaser fish. The latter will lead the search process Φ_c: $\Phi_c = X$ to identify whether the rules are detected or not and to identify the blocker fishes Φ_b: $\Phi_b = Y$. Then, this process compares the fitness values, which is the best value for detecting the rule, and the value of the search of the Φ_c. If they are identical, then go to the next step of BCT hashing and complete the action; if not identical, then terminate and reject the action. Figure 7 depicts the whole operation of our proposed system from the CS request to the termination of the operation.

4.2 Two-Phase Commit Algorithm

2PC is a distributed technique that is used to guarantee the consistency of e-banking procedures among several databases or participants. This algorithm consists of two stages: preparation and commitment. All participants received a preparation request from the coordinator during the preparation phase to specify the type of e-banking procedure that should be applied and to commit to the procedure until the end. The next step is for each participant to vote, either to commit or to abort. In the commit phase, based on the participants' votes, the coordinator decides whether to commit or abort the e-banking procedure.

4.3 Micro-Segmentation in Our Proposed System

The MS technique, as explained previously plays a large role in providing the system with high security, and it needs to complete the transaction procedure safely and in real time. Our proposed system's main steps for MS are illustrated in Algorithm 1.

4.4 YSGA in E-Transaction

The YSGA was used in our proposed transaction module for the following reasons:

- This algorithm relies on the technique of breaking or dividing the whole system into zones, which is suitable for the MS principle of isolating threats.
- The easy-going procedure of calculating the values leads to an easy and fast authentication process to obtain a fast and secure module.

This algorithm plays a great role in detecting SC conditions if it is fulfilled or not, as in Algorithm 2. As clarified, the whole population will first be initialized as pi. Additionally, the global best value Φ_{best} that the comparison will ensure should be specified. After this process, division into zones occurs; then, for each zone, a specification is activated for the chaser fish Φ_c and the blocker fish Φ_b, and the hunting routine is used to compare the global best Φ_{best} and the obtained Φ_i to either replace them or continue the hunting process or terminate.

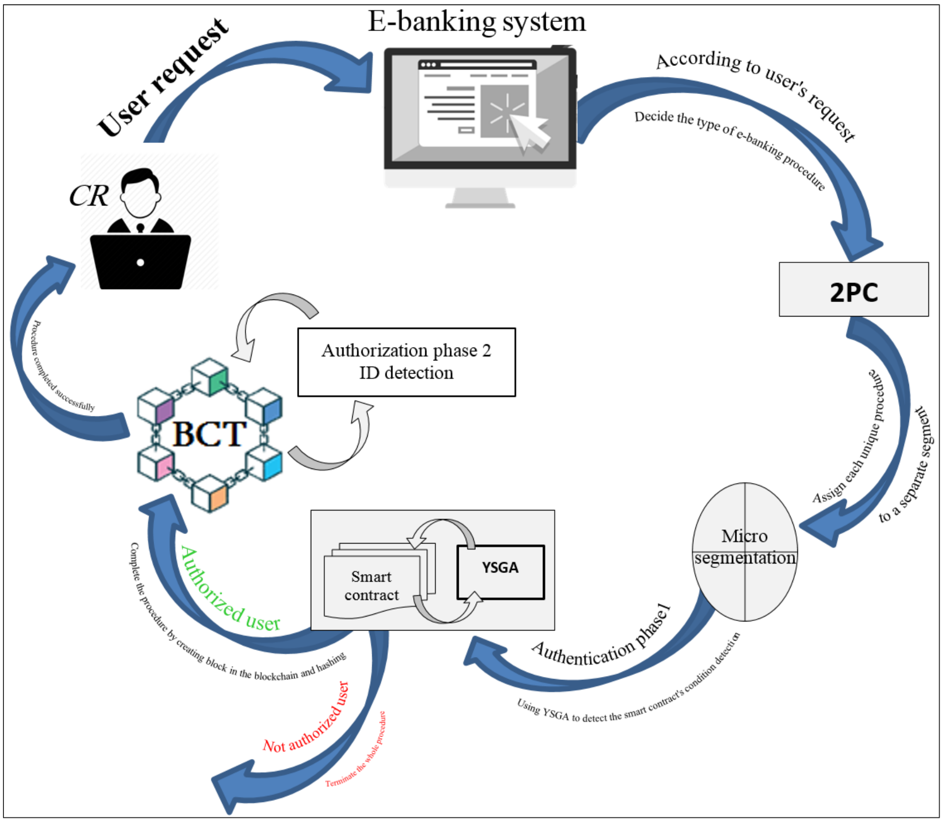

E-banking system
User request
According to user's request
Decide the type of e-banking procedure
2PC
Assign each unique procedure
to a separate segment
Micro
segmentation
Authentication phase1
Using YSGA to detect the smart contract's condition detection
Smart
contract
YSGA
Authorized user
Complete the procedure by creating block in the blockchain and hashing
Not authorized user
Terminate the whole procedure
BCT
Authorization phase 2
ID detection
Procedure completed successfully
CR

Fig. 7. Proposed system's procedures

Algorithm 1 Microsegmentation and 2PC steps

```
Input: $X$ keyword for the 2PC
Output: Separate e-banking procedure segments
Deciding the type of e-banking request using 2PC algorithm X ← type
If $X$ is a transaction?
Yes, create a new segment and migrate the system
No, if $X$ is loan?
Yes, create a new segment and migrate the system
No, migrate system into the existing segment
Applying SC condition to each segment
If the SCs conditions are identical
Yes, complete the request as its type
No, terminate
```

Algorithm 2 YSGA

```
Input: The goatfish population $P \leftarrow p_1, p_2, p_3, \dots p_m$
Output: The best search value ($\Phi_{best}$)
Calculating the fitness value of each particle ($p$)
Identifying the global best $\Phi_{best}$
Partition the population $p$ into k zone $Z_1, Z_2, Z_3, \dots Z_k$
Identifying the chaser $\Phi_c$ and the blocker $\Phi_b$ fish for each zone
For each zone $Z_i$
Executing of hunting routine for chaser fish
Executing of blocking routine for blocker fish
Calculating the fitness value for each goatfish
If the calculated $\Phi_g$ has better fitness than the $\Phi_i$
Exchanging the $\Phi_i$
If the calculated $\Phi_i$ has better fitness than the $\Phi_{best}$
Updating $\Phi_{best}$
If the fitness value of $\Phi_i$ has improved
$q \leftarrow q + 1$
Executing routine for changing zone
$q \leftarrow 0$
Output the _best which carry the identification decision
```

5. ANALYSIS OF THE PROPOSED E-BANKING SYSTEM

In this section, we evaluate our proposed system from both security and performance perspectives. First, we evaluate our system against assaults and use Scyther simulation to practically evaluate our system from a security perspective. Second, the performance of the proposed module, both conceptually and practically, will be covered next. Our proposed system was implemented using Java on the Ubuntu 16.04 LTS system. The computer used for the study was equipped with an Intel core^{TM} 3110 M CPU and 4.00 GB of RAM.

5.1 Security Examination of E-Banking Risks

Next, summarize the assaults that threaten the security of the e-banking system and how our proposed module effectively addresses them.

- **Falsification**: The goal of this assault is to have the message sent between the nodes forged. Fundamentally, this assault directly compromises data integrity, which is a crucial need for any system's security. In other words, when the message or data reaches its destination, precision decreases. Specifically, misrepresenting messages ultimately results in poor decision-making. On the other hand, our proposed approach will be faced and stopped because of the use of the SC conditions and the KYC principle, where there is a previous condition between the parts of the e-banking system that must be accomplished to complete the e-banking process; namely, the SC conditions will face these types of assaults.
- **Advanced persistent threat (APT)**: An APT, as its name implies, is a cyberattack that employs persistent, covert, and highly skilled hacking methods to penetrate a system and stay inside it for an extended length of time, often resulting in catastrophic outcomes. To gain access, APT groups often use a variety of advanced assault methods, including social engineering techniques, but in the case of our proposed module, there are a variety of algorithms that the proposed module includes; thus, in the use of the MS principle, APT assault will be detected and stopped.
- **Bribery**: The dishonest practice of offering, providing, accepting, or consenting to receive money or another valuable thing to influence a public official while they are doing their official duties. Bribery occurs when an official receives money in exchange for performing corrupt conduct. The official does not have to carry out the act for the offense to be considered committed. However, in the manner of the proposed module, this kind of threat has been overcome because our module is based on the idea of P2P with no third party. Additionally, the system is partitioned into segments, where each segment has its own role.
- **Double-Spending**: The possibility of using a cryptocurrency more than once is known as double-spending. In BCT, transaction data can change if certain requirements are satisfied. The requirements for altered blocks to be added to the BCT. If this occurs, the original alteration of the change may recover coins that have been spent. However, in the case of the proposed module, this cannot occur because the system consists of several layers before the data are completed and stored in the BCT. Hence, our module is considered safe.

- **Spoofing**: This assault is the act of disguising a communication or identity to give the impression that it is coming from a trustworthy and authorized source. Spoofing assaults come in a variety of forms, from the more common email spoofing assaults used in phishing operations to caller ID spoofing assaults, which are regularly used to commit fraud. In such a case, the proposed system will stop because of the use of the 2PC algorithm, which has two phases to detect the type of process and the isolation of each *CR* in a segment.
- **Chosen text**: This is a situation where $\mathscr{A}$ can select plaintexts P_i and see cipher texts C_i, which correspond to those encryptions. $\mathscr{A}$ selected plaintext differential assault can be transformed into a known-plaintext assault by using m pairs of texts for an n-bit block cipher. This will require $26n/2\sqrt{2m}$. This phenomenon does not exist in the procedure of our proposed module because we have no text. Our system has conditions controlled by the SCs and the YSGA.
- **Race**: This assault refers to the action of two events racing to obtain the same prize. In brief, it is two operations that occur at the same time, and they are racing to which one will execute first. For the following scenario, one *CR* with $2000 writes two checks: check *A* with $1000 and check *B* with $1500. The deposit starts here the racing assault could run at the same time leaving the bank account with -500$ at someone's *CR* bank account. Fortunately, our proposed module dealt with such a manner with the principle of MS, where each process has its own segment and its own time to run cannot conflict with the time of other processes.
- **Transaction replay**: To understand such assault, *CR* wishes to show *SR* who he/she truly is. *CR* obediently gives her/his password to *SR* when he/she asks for identification, possibly after hashing or even salting it. Meanwhile, $\mathscr{A}$ is listening in on the conversation and retains the password (or hash). Following their conversation, $\mathscr{A}$-posing as a *CR* connects with *SR*. When the *SR* requests identification, $\mathscr{A}$ provides him/her *CR*'s password (or hash) from their last session, which he/she accepts, giving $\mathscr{A}$ access. Such an assault can be stopped by the principle of giving each user or *CR* a unique ID, and this principle is embedded in the proposed system, the KYC principle. Table II provides a brief comparison between our system and recent transaction systems in terms of preventing assaults. We note from the table that our proposed system repels all attacks in the field of research, while some existing systems do not repel well-known modern attacks.

TABLE II. COMPARISON OF ASSAULT PREVENTION BETWEEN THE PROPOSED SYSTEM AND THE RELATED SYSTEMS

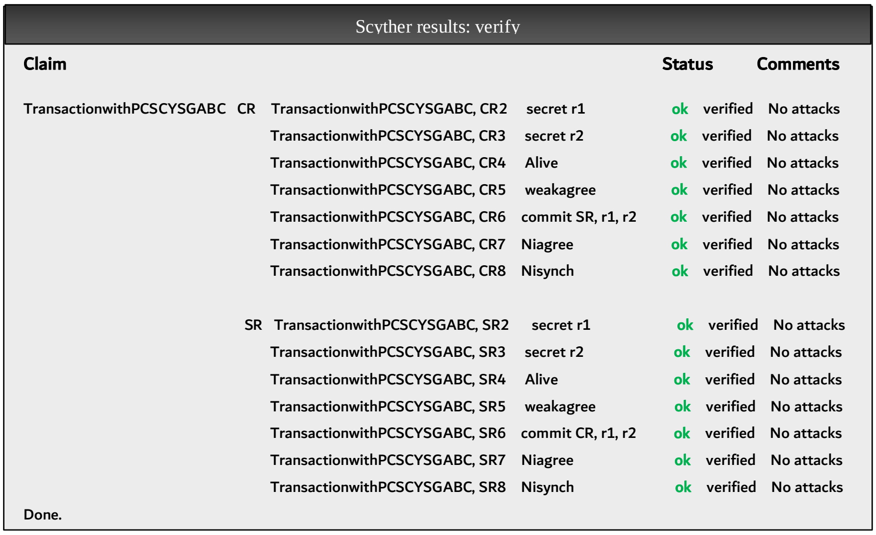
Assault	[3]	[11]	[24]	[25]	[26]	[27]	Proposed system
Falsification	✓						✓
APT			✓				✓
Bribery					✓		✓
Double-Spending					✓	✓	✓
Spoofing				✓		✓	✓
Chosen text		✓					✓
Race					✓	✓	✓
Transaction replay			✓	✓	✓		✓

5.2 Scyther as an Analysis Tool

We employ Scyther simulation as an effective tool for cryptographic system validation. With its cutting-edge features, attack/assault tracking, and verification speed, this tool is impressive. Without the need for approximation approaches, it efficiently checks the majority of systems and approaches for any number of sessions and ensures that all assaults detected are real and pose no threat to the system [4, 36]. Users (CRs and SRs) have the option to perform unfettered verification or use Scyther for assault detection. Among the various tools for scheme analysis, Scyther is unique in that it combines the benefits of model-checking techniques (such as identifying assaults and termination) with the strengths of theorem proving or abstraction-based approaches (unbounded verification). In addition, Scyther provides unique capabilities such as assault detection and full characterization that are absent from other tools. It can be utilized through the graphical user interface, the command-line interface, or as a backend for analysis programs that make use of Python interface functions. Scyther employs the analysis of security specifications for a range of approaches, identifying information assaults and confirming the confidentiality and authentication of these data, whether sending and receiving between a CR and SR or between businesses or organizations. This tool uses security requirement attributes to verify some of the authentication data, such as Aliveness, Nisynch, Niagree, and Weakagree.

5.3 Scyther's Authentication Test Results

We demonstrate our e-banking approach test with the Scyther tool. The test results of our protocol are based on the following events: Alive, Niagree, Nisynch, Secret, and Commit. The outcome demonstrated that security parameters were exchanged between network entities (CR_i and SR_i) that were free from any threats or assaults. As shown in Figure 8, we designed a system that is resistant to assaults in our study area. Additionally, we completed a summary of characterizing roles of our proposed system, the results of which are shown in Figure 9, and the results of the respective paradigms are shown in Figures 9 and 10.



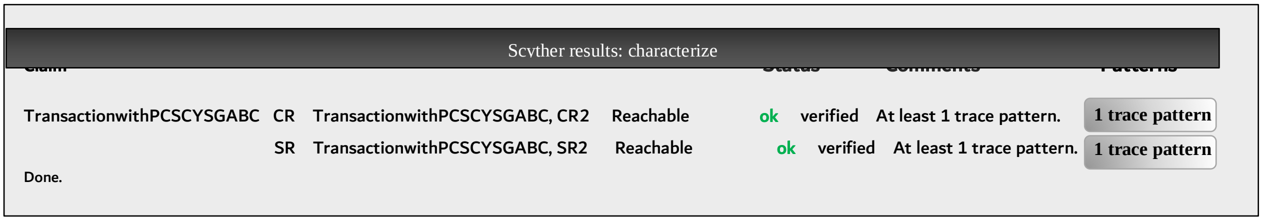
```
Scyther results: verify

Claim                                                                              Status        Comments

TransactionwithPCSCYSGABC  CR  TransactionwithPCSCYSGABC, CR2  secret r1           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR3  secret r2           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR4  Alive               ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR5  weakagree           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR6  commit SR, r1, r2   ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR7  Niagree             ok  verified  No attacks
                               TransactionwithPCSCYSGABC, CR8  Nisynch             ok  verified  No attacks

                           SR  TransactionwithPCSCYSGABC, SR2  secret r1           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR3  secret r2           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR4  Alive               ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR5  weakagree           ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR6  commit CR, r1, r2   ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR7  Niagree             ok  verified  No attacks
                               TransactionwithPCSCYSGABC, SR8  Nisynch             ok  verified  No attacks
Done.
```

Fig. 8. Depiction of the Scyther results



```
Scyther results: characterize

TransactionwithPCSCYSGABC  CR  TransactionwithPCSCYSGABC, CR2  Reachable  ok  verified  At least 1 trace pattern.  1 trace pattern
                           SR  TransactionwithPCSCYSGABC, SR2  Reachable  ok  verified  At least 1 trace pattern.  1 trace pattern
Done.
```

Fig. 9. Proposed system summary of the characterized roles

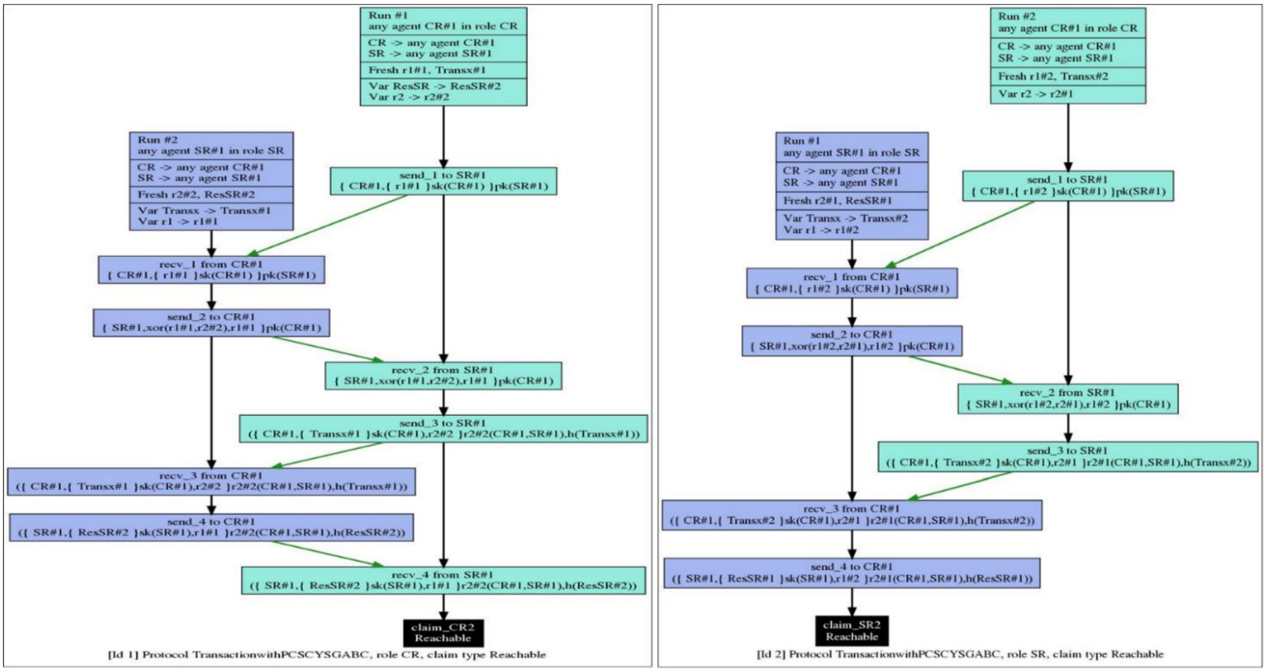

Run #1
any agent CR#1 in role CR
CR -> any agent CR#1
SR -> any agent SR#1
Fresh r1#1, Transx#1
Var ResSR -> ResSR#2
Var r2 -> r2#2
Run #2
any agent SR#1 in role SR
CR -> any agent CR#1
SR -> any agent SR#1
Fresh r2#2, ResSR#2
Var Transx -> Transx#1
Var r1 -> r1#1
send_1 to SR#1
{ CR#1,{ r1#1 }sk(CR#1) }pk(SR#1)
recv_1 from CR#1
{ CR#1,{ r1#1 }sk(CR#1) }pk(SR#1)
send_2 to CR#1
{ SR#1,xor(r1#1,r2#2),r1#1 }pk(CR#1)
recv_2 from SR#1
{ SR#1,xor(r1#1,r2#2),r1#1 }pk(CR#1)
send_3 to SR#1
({ CR#1,{ Transx#1 }sk(CR#1),r2#2 }r2#2(CR#1,SR#1),h(Transx#1))
recv_3 from CR#1
({ CR#1,{ Transx#1 }sk(CR#1),r2#2 }r2#2(CR#1,SR#1),h(Transx#1))
send_4 to CR#1
({ SR#1,{ ResSR#2 }sk(SR#1),r1#1 }r2#2(CR#1,SR#1),h(ResSR#2))
recv_4 from SR#1
({ SR#1,{ ResSR#2 }sk(SR#1),r1#1 }r2#2(CR#1,SR#1),h(ResSR#2))
claim_CR2
Reachable
[Id 1] Protocol TransactionwithPCSCYSGABC, role CR, claim type Reachable
Run #2
any agent CR#1 in role CR
CR -> any agent CR#1
SR -> any agent SR#1
Fresh r1#2, Transx#2
Var r2 -> r2#1
Run #1
any agent SR#1 in role SR
CR -> any agent CR#1
SR -> any agent SR#1
Fresh r2#1, ResSR#1
Var Transx -> Transx#2
Var r1 -> r1#2
send_1 to SR#1
{ CR#1,{ r1#2 }sk(CR#1) }pk(SR#1)
recv_1 from CR#1
{ CR#1,{ r1#2 }sk(CR#1) }pk(SR#1)
send_2 to CR#1
{ SR#1,xor(r1#2,r2#1),r1#2 }pk(CR#1)
recv_2 from SR#1
{ SR#1,xor(r1#2,r2#1),r1#2 }pk(CR#1)
send_3 to SR#1
({ CR#1,{ Transx#2 }sk(CR#1),r2#1 }r2#1(CR#1,SR#1),h(Transx#2))
recv_3 from CR#1
({ CR#1,{ Transx#2 }sk(CR#1),r2#1 }r2#1(CR#1,SR#1),h(Transx#2))
send_4 to CR#1
({ SR#1,{ ResSR#1 }sk(SR#1),r1#2 }r2#1(CR#1,SR#1),h(ResSR#1))
claim_SR2
Reachable
[Id 2] Protocol TransactionwithPCSCYSGABC, role SR, claim type Reachable

Fig. 10. Roles of the proposed system characterized roles

5.4 Assessment Process of Our Proposed E-Banking System

The execution time, complexity, and storage metrics are used in our proposed system to measure its overall effectiveness.

- **The execution time** or CPU time refers to the amount of time that the whole e-banking procedure needs to be performed. Our proposed module implemented it using code in Java, where we obtained the average execution time in milliseconds. The execution times of the implemented algorithms in the proposed system are shown in Figures 11, 12, and 13. As shown in Figures 11, 12, and 13, each execution was repeated 100 times. Additionally, the average execution time was fractions of a second, which means that our proposed module is considered to be fast compared with recent existing systems. If we focused on Figures 12 and 13 of the time taken for implementation, we would note that 0.0056 ns was repeated for more than one implementation, meaning that the time taken to implement the entire system was 0.0056 ns for more than one implementation; thus, it was calculated as the average time to implement the system. Our proposed module is fast compared with existing systems, as shown in Table III. Our proposed system provides an execution time of 0.0056 ns, which is ultrafast compared to that of other existing systems.

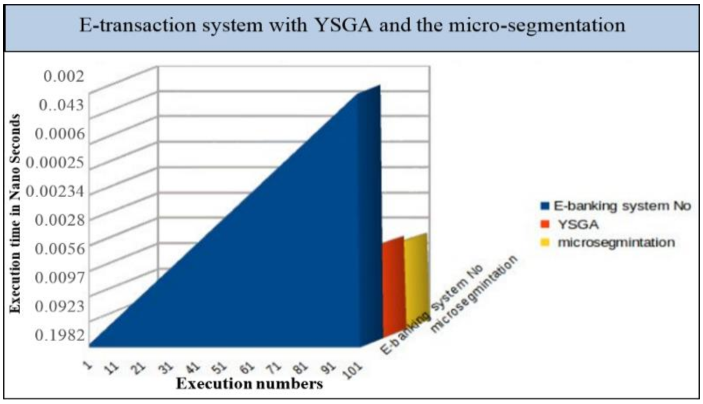


Fig. 11. Execution time average for YSGA and the microsegmentation

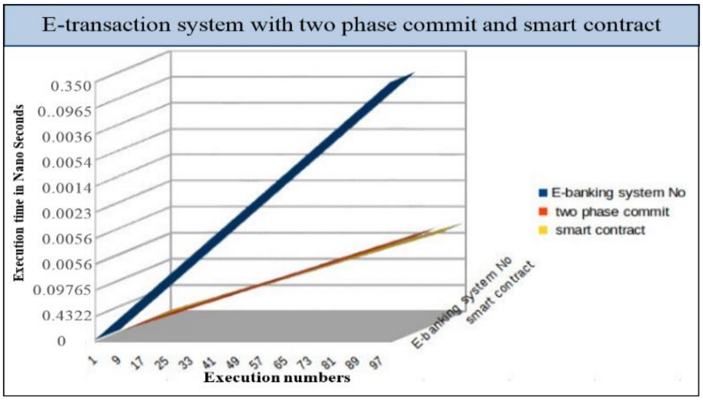


Fig. 12. Execution time average for 2PC and the smart contract

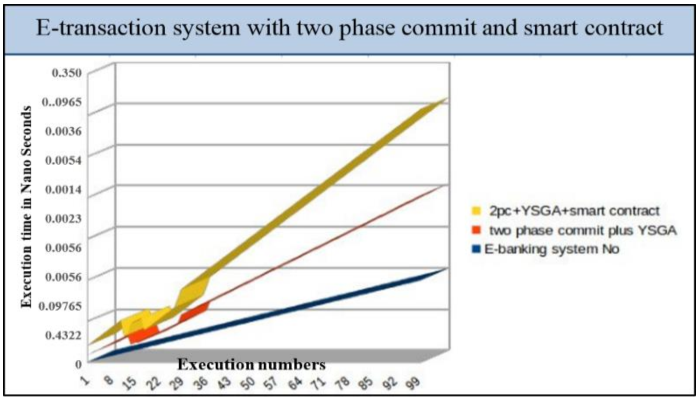


Fig. 13. Execution time average for 2PC plus the YSGA with the smart contract

TABLE III. COMPMARISON BETWEEN CURRENT SYSTEMS AND THE PROPOSED SYSTEM ACCORDING TO EXECUTION TIME

BCT-based system	Execution time
BCT-based hybrid platform [3]	60 s
BCT-based-revocation Access control [11]	49.67 ms
Ethereum BCT of _financial transactions [37]	15 s
Proposed system	0.0056 ns

- **Complexity**: A system or a model is supposed to exhibit complex behavior when its constituent parts interact in many ways and adhere to local laws, resulting in nonlinearity, unpredictability, collective dynamics, hierarchy, and emergence. When anything has numerous components that interact with one another in different ways to form a higher order of emergence that is more than the sum of its parts, the phrase is usually used to describe it. The analysis of these complicated interactions at many scales is the main goal of complex systems theory. Our proposed system has many layers. Figure 6 starts with the division of the whole e-banking process into separate segments using the principle of MS and the 2PC algorithm combined. Then, the next layer of the detection of the CR identity using the SCs and the YSGA combined, and the final layer of creating the blocks and hashing in the BCT. Thus, we have a complex system with many layers combined but with a smooth flow of the procedure that makes the e-transaction process easy, fast, authentic, and complete. As shown in Figure 14, the overall percentage of complexity is considered significantly lower than that in the research on the same topic, where the 2PC algorithm scored the highest complexity because it is an algorithm of two phases, while the other algorithms had a very small percentage of complexity. In general, after calculating the overall complexity percentage, 15000/4=3.75%, which is considered very low. This means that the system is easy to manipulate and update. Additionally, compared to the complexity rates extracted from previous systems, we found that our research has a much lower complexity rate than previous research, as summarized in Table IV. Our proposed system has a complexity of approximately $15 \times 10^{3,}$ which is lower than that of existing modern systems [15] and [38].

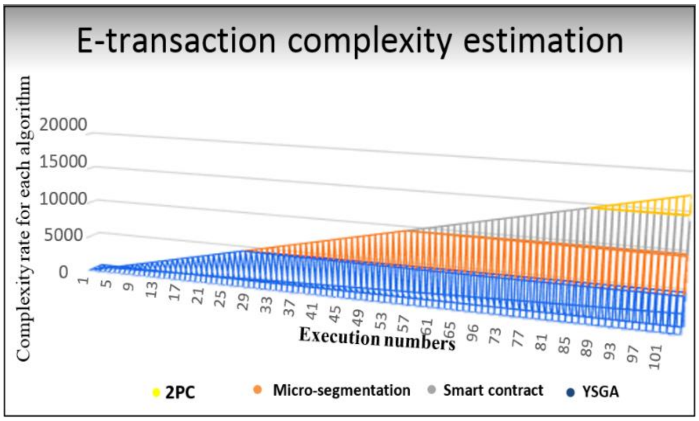


Fig. 14. Proposed system complexity estimation

TABLE IV. COMPARISON BETWEEN CURRENT SYSTEMS AND THE PROPOSED SYSTEM ACCORDING TO COMPLEXITY

BCT-based system	Complexity rate
Holochain blocks for distributed security in IoT [15]	10^6
Secure BCT-Driven Audit Trails [38]	5×10^7
Proposed system	15×10^3

- Storage: The allocation and management of memory resources to store data and code utilized by a specific module or system components is referred to as system or module storage. In computer/network systems, storage can be classified into two main types: primary storage and secondary storage. Primary storage, also known as main memory or RAM, is the temporary storage space used by the system or module to hold data and instructions during execution. It provides fast access to data and is directly accessible by the processor. Conversely, long-term storage systems such as network-attached storage (NAS), solid-state drives (SSDs), and hard disk drives (HDDs) are referred to as secondary storage. BCT relies on the principle of a distributed ledger. Specifically, this distributed ledger works as a database to store all *CR*s' information related to the banking operations conducted on their accounts, which are interconnected with chains in the form of blocks; thus, the process of storing and protecting those blocks is considered extremely important, meaning that the less load the system has on memory, the more data are protected from errors that affect the system as a result of excessive load on memory, which causes it to stop electronic banking systems. In the case of our proposed system, we estimated the overall storage, as shown in Figure 15. When we have a tremendous amount of system resources, the RAM and disk drive usage never skips 1030 KB, while executing the system 100 times showed that the system's resource usage rate was between 500 KB and 1000 KB; as a summation, it never crossed 1500 KB, guaranteeing fast, reliable and balanced usage of system resources. Figure 16 shows the storage sizes consumed by all our algorithms (MS, 2PC, YSGA, and SC) in the KB for ten implementations. This figure shows that our algorithms use low storage space. Table V summarizes a comparison of storage consumption between our suggested system and other recent systems on the same topic. This indicates that our system needs to consume 1500 KB of memory storage, which is small compared to the existing search results [16], [17] and [18].

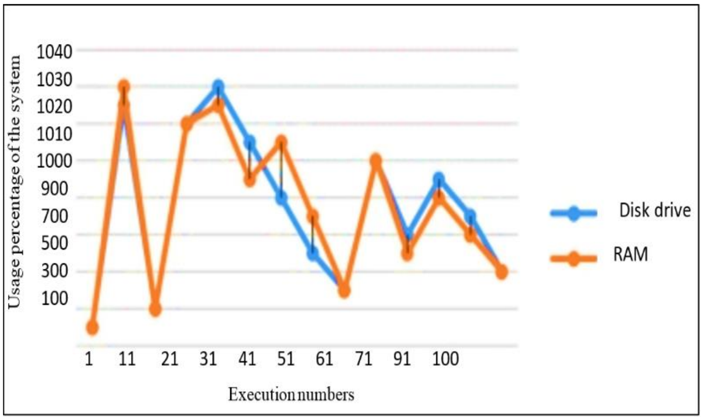


Fig. 15. Storage spending by the proposed module

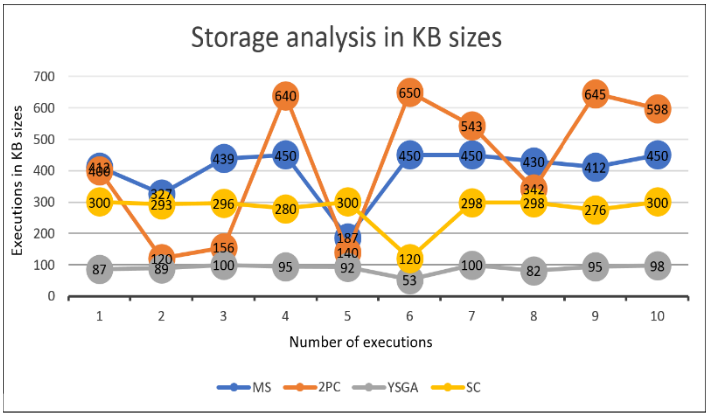


Fig. 16. Storage analysis for our proposed algorithms

TABLE V. COMPARISON BETWEEN CURRENT SYSTEMS AND THE PROPOSED SYSTEM ACCORDING

BCT-based system	**System resources use**
Analysis of BCT based storage systems [16]	512 MB
Development and evaluation of BCT based secure application [17]	470 MB
Flexible BCT with memory-optimized [18]	12000 KB
Proposed system	1500 KB

Table VI shows a complete general comparison between existing systems and the proposed system with the parameters of speed, security, efficiency, and control. This indicates that our system shows better efficiency than previous research systems.

TABLE VI. RELIABILITY PARAMETERS COMPARISON BETWEEN CURRENT

Parameter Current systems	**Current systems [19, 20, 21]**	**Proposed system**
Speed and security	Intermediate or fast with low security	Fast due to the speed of the used algorithms with a high range of security
Efficiency	Redundancy and duplication of tasks	Improve payment efficiency and flexibility of transactions
Control	Centralized	Decentralized with SC

6. LIMITATIONS

Our proposed system provides a new, fast, and secure method for data transactions. On the other hand, any study and suggestion to develop e-banking systems using BCT are considered quite challenging issues. The first reason is that BCT technology itself is considered a modern technology, and the second reason, as long as there is CR information we are dealing with, is that it is sensitive and has so many risks. Thus, the limitations of this study include the difficulty of updating the BCT information because, after creating the blocks in the BCT and hashing process, it is impossible to update the information. Moreover, another limitation is the issue of big, which requires many separate segments and, consequently, a large amount of space memory. Finally, the use of default hashes in BCT could be a reason for the relative decrease in performance, in addition to the possibility of attacks that are not covered within the scope of this research.

7. CONCLUSIONS

As time runs fast toward technology and there is new technology appearing daily, the banking sector will be affected, and the traditional procedure in banking organizations will be electronic and available to be completed online, which is known as e-banking. However, everything online is threatened by the $\mathscr{A}$s and assaults, and the result is data loss. Therefore, we propose a security e-transaction system that combines both safe and fast procedures for money transactions in e-banking. Our proposed module has the following characteristics and advantages.

- Fast: Because of the use of modern, easy, and accurate algorithms such as the YSGA and the 2PC, our proposed system guarantees that the e-banking procedure will be performed in real time.
- Safe and authentic: The proposed module is controlled by the SC conditions in which both the *CR* and the *SR* agree on and do not agree, the e-transaction procedure cannot be performed, and our proposed module can be considered safe and secure.
- Additionally, because of the usage of the principle of isolation for each process alone in a separate segment, the danger that threatens a specific segment will remain bounded by that segment, and the other segments will work normally.
- Integrating: The final layer of our proposed module is the hashing and creating blocks for each procedure. Each block has complete information about the whole transaction process plus the number of previous blocks. This approach provided our proposed module with an advantage in terms of integrity.
- Speed: Our proposed system is fast due to the speed of the algorithms used. Additionally, after the full analysis shown above, the time required to complete a full transaction is not more than 0.0056 nanoseconds, which is considered fast compared to other similar methods.

Based on our analysis in terms of security and performance, we conclude that our proposed system has efficient performance and is capable of repelling attacks within the scope of this study. Every single system, module, or scheme can be changeable and can developed because of the fast and challenging walking forward technology, and this study also needs to improve some aspects of our system. In future works, some machine learning algorithms can be applied to make some changes to the saved blocks of BCT, and data compression algorithms can be used to reduce the size of the segments or cloud storage can be used.

Conflicts of interest

The paper states that there are no personal, financial, or professional conflicts of interest.

Funding

The acknowledgments section of the paper does not mention any financial support from institutions or sponsors.

Acknowledgements

The author acknowledges the assistance and guidance received from the institution in various aspects of this study.

References

[1] P. Garg, B. Gupta, K. N. Kapil, U. Sivarajah, and S. Gupta, "Examining the relationship between blockchain capabilities and organizational performance in the Indian banking sector," Annals of Operations Research, pp. 1-34, 2023.

[2] M. Javaid, A. Haleem, R. P. Singh, R. Suman, and S. Khan, "A review of blockchain technology applications for financial services," BenchCouncil Transactions on Benchmarks, Standards and Evaluations, p. 100073, 2022.

[3] A. I. Taloba, A. Elhadad, A. Rayan, R. M. Abd El-Aziz, M. Salem, A. A. Alzahrani, F. S. Alharithi, and C. Park, "A blockchain-based hybrid platform for multimedia data processing in IoT-healthcare," Alexandria Engineering Journal, vol. 65, pp. 263-274, 2023.

[4] M. Al-Zubaidie and G. S. Shyaa, "Applying detection leakage on hybrid cryptography to secure transaction information in e-commerce apps," Future Internet, vol. 15, no. 8, p. 262, 2023.

[5] S. A. Yousiff, R. A. Muhajjar, and M. H. Al-Zubaidie, "Designing a blockchain approach to secure firefighting stations based Internet of things," Informatica, vol. 47, no. 10, pp. 09-26, 2023.

[6] M. Al-Zubaidie, "Implication of lightweight and robust hash function to support key exchange in health sensor networks," Symmetry, vol. 15, no. 1, p. 152, 2023.

[7] M. Al-Zubaidie, Z. Zhang, and J. Zhang, "REISCH: Incorporating lightweight and reliable algorithms into healthcare applications of WSNs," Applied Sciences, vol. 10, no. 6, p. 2007, 2020.

[8] P. Rawat, "How do phishing and spoofing attacks impact businesses?" 2023, https://www.infosectrain.com/blog/howdo-phishing-and-spoofing-attacks-impact-businesses/ (accessed on January 02, 2024).

[9] S. Bhanda and A. Taylor, "Fundamentals of cybersecurity in banks," 2023, https://www.qentelli.com/thought-leadership/insights/fundamentals-cybersecurity-banks (accessed on December 03, 2023).

[10] A. Thommandru and B. Chakka, "Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances by banks," Sustainable Futures, vol. 5, p. 100107, 2023.

[11] K. Riad, M. Elhoseny et al., "A blockchain-based key-revocation access control for open banking," Wireless Communications and Mobile Computing, vol. 2022, 2022.

[12] S. Gamal and M. M. Aref, "Challenges and opportunities of blockchain integration in the Egyptian banks: A qualitative analysis," Digital Economy, Business Analytics, and Big Data Analytics Applications, pp. 469-485, 2022.

[13] U. B. Chaudhry and A. K. Hydros, "Zero-trust-based security model against data breaches in the banking sector: A blockchain consensus algorithm," IET blockchain, vol. 3, no. 2, pp. 98-115, 2023.

[14] B. D. S. Sai, R. Nikhil, S. Prasad, and N. S. Naik, "A decentralised KYC based approach for microfinance using blockchain technology," Cyber Security and Applications, vol. 1, p. 100009, 2023.

[15] S. Zaman, M. R. Khandaker, R. T. Khan, F. Tariq, and K.-K. Wong, "Thinking out of the blocks: Holochain for distributed security in IoT healthcare," IEEE Access, vol. 10, pp. 37064-37081, 2022.

[16] P. S. Austria, "Analysis of blockchain-based storage systems," Ph.D. dissertation, University of Nevada, Las Vegas, 2020.

[17] E. Leka and B. Selimi, "Development and evaluation of blockchain based secure application for verification and validation of academic certificates," Annals of Emerging Technologies in Computing (AETiC), vol. 5, no. 2, pp. 22-36, 2021.

[18] A. Dorri, S. S. Kanhere, and R. Jurdak, "MOF-BC: A memory optimized and flexible blockchain for large scale networks," Future Generation Computer Systems, vol. 92, pp. 357-373, 2019.

[19] M. K. Ojha, C. P. Sharma, R. Farswan, and N. Prakash, "E-banking: Banking solution in modern era," Ilkogretim Online, vol. 20, no. 2, pp. 2510-2519, 2021.

[20] B. Lv, P. Cheng, C. Zhang, H. Ye, X. Meng, and X. Wang, "Research on modeling of e-banking fraud account identification based on federated learning," in 2021 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech). IEEE, 2021, pp. 611-618.

[21] F. Li, H. Lu, M. Hou, K. Cui, and M. Darbandi, "Customer satisfaction with bank services: The role of cloud services, security, e-learning and service quality," Technology in Society, vol. 64, p. 101487, 2021.

[22] K. Agrawal, M. Aggarwal, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "An extensive blockchain based applications survey: Tools, frameworks, opportunities, challenges and solutions," IEEE Access, 2022.

[23] R. K. Jena, "Examining the factors affecting the adoption of blockchain technology in the banking sector: An extended UTAUT model," International Journal of Financial Studies, vol. 10, no. 4, p. 90, 2022.

[24] T. N. Thakur and N. Yoshiura, "AntiPhiMBS: A new anti-phishing model to mitigate phishing attacks in mobile banking system at application level," in Intelligent Information and Database Systems: 13th Asian Conference, ACIIDS 2021, Phuket, Thailand, April 7-10, 2021, Proceedings 13. Springer, 2021, pp. 399-412.

[25] K. Lee and K. Yim, "Study on the transaction linkage technique combined with the designated terminal for 5G enabled IoT," Digital Communications and Networks, vol. 8, no. 2, pp. 124-131, 2022.

[26] S. Mollajafari and K. Bechkoum, "blockchain technology and related security risks: Towards a seven-layer perspective and taxonomy," Sustainability, vol. 15, no. 18, p. 13401, 2023.

[27] B. Saha, M. M. Hasan, N. Anjum, S. Tahora, A. Siddika, and H. Shahriar, "Protecting the decentralized future: An exploration of common blockchain attacks and their countermeasures," arXiv preprintarXiv:2306.11884, 2023.

[28] H. Rjoub, T. S. Adebayo, and D. Kirikkaleli, "blockchain technology-based FinTech banking sector involvement using adaptive neuro-fuzzy-based K-nearest neighbors algorithm," Financial Innovation, vol. 9, no. 1, p. 65, 2023.

[29] N. Ullah, W. M. Al-Rahmi, O. Alfarraj, N. Alalwan, A. I. Alzahrani, T. Ramayah, and V. Kumar, "Hybridizing cost saving with trust for blockchain technology adoption by financial institutions," Telematics and Informatics Reports, vol. 6, p. 100008, 2022.

[30] M. F. Farah, M. Naveed, and S. Ali, "Blockchain-enabled banking services and customers' perceived financial wellbeing: A structural nexus," in National Brand and Private Label Marketing Conference. Springer, 2023, pp. 41-49.

[31] M. Zook and M. H. Grote, "Blockchain financial geographies: Disrupting space, agency and scale," Geoforum, 2022.

[32] P. Garg, B. Gupta, A. K. 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, p. 120407, 2021.

[33] M. K. Shrivas and T. Yeboah, "The disruptive blockchain: Types, platforms and applications," Texila International Journal of Academic Research, vol. 3, pp. 17-39, 2019.

[34] D. Kashyap, B. Singh, and M. Kaur, "Chaotic approach for improving global optimization in yellow saddle Goatfish," Engineering Reports, vol. 3, no. 9, p. e12381, 2021.

[35] D. Zaldivar, B. Morales, A. Rodriguez, A. Valdivia-G, E. Cuevas, and M. Perez-Cisneros, "A novel bio-inspired optimization model based on yellow saddle Goatfish behavior," Biosystems, vol. 174, pp. 1-21, 2018.

[36] A. Hassan, I. Ishaq, and J. Minilla, "Automated verification tools for cryptographic protocols," in 2021 International Conference on Promising Electronic Technologies (ICPET). IEEE, 2021, pp. 58-65.

[37] P. S. Maharjan, "Performance analysis of blockchain platforms," Ph.D. dissertation, University of Nevada, Las Vegas, 2018.

[38] A. Ashar, S. Muhammad, A. G. Mohammed, and M. David, "Blocktrail: A service for secure and transparent blockchain-driven audit trails," IEEE Systems Journal, vol. 16, pp. 1367-1378, 2022.