ISSN: 0067-2904

# Improving Security in E-Transaction Blockchain Systems by Segmenting Processes into Separate Zones and Using Smart Contracts Arbitration

**Wid Alaa Jebbar* and Mishall Al-Zubaidie**
*Department of Computer Sciences, Education College for Pure Sciences, University of Thi-Qar, Nasiriyah 64001, Iraq*

Received: 21/2/2024 Accepted: 5/7/2024 Published: 30/**6**/2025

**Abstract**

This study proposed an integrated security system for electronic transactions, first specifying the type of e-banking request using the two-phase commit procedure (2PC). The idea of micro-segmentation was then used to isolate individual e-transaction processes in different segments; after this, every segment was controlled by a smart contract. The Yellow Saddle Goatfish Algorithm (YSGA) was employed to detect whether the smart contract conditions were met optimally. Finally, if the customer receives approval, a distinct hash records the entire transaction procedure in the blockchain's main ledger. In a simulation environment, the proposed system was tested, and the results were: 0.0031 ns as a time to detect the smart contract's terms, an overall execution time between 0.001 ns and 0.005 ns, and a level of immutability equal to 5. The results of the analysis of the proposed system may inspire researchers/developers to apply it to e-banking institutions and benefit from the robust security features and high performance of the proposed methods.

**Keywords:** 2PC, Blockchain, E-Banking, Eclipse attack, FinTech, ProVerif.

# تحسين الأمان في أنظمة Blockchain للمعاملات الإلكترونية عن طريق تجزئة العمليات إلى مناطق منفصلة واستعمال تحكيم العقود الذكية

**ود علاء جبار، مشعل حمد عواد**

قسم علوم الحاسبات، كلية التربية للعلوم الصرفة، جامعة ذي قار، الناصرية 64001، العراق.

**الخلاصة**

في هذا البحث، تم اقتراح نظام أمني متكامل للمعاملات الإلكترونية، حيث تم أولاً تحديد نوع طلب الخدمات المصرفية الإلكترونية باستخدام إجراء (2PC). ثم تم استعمال فكرة التجزئة المايكروية (micro segmentation) لعزل العمليات التي تم تحديدها على انها تحويل مالي في قطع مختلفة، بعد ذلك تم التحكم والسيطرة على كل قطعة بواسطة عقد ذكي. تم استعمال خوارزمية (YSGA) لاكتشاف ما إذا كانت شروط العقد الذكي قد تم استيفاؤها على النحو الأمثل ام لا. في النهاية، تم تسجيل إجراءات التحويل المالي كاملة في الـ blockchain وحمايتها برقم مميز يدعى ال hash. في بيئة محاكاة وعلى نظام التشغيل اوبنتو وباستعمال لغة البرمجة جافا، تم اختبار النظام المقترح وكانت النتائج: 0.0031 ns كوقت للكشف عن شروط العقد الذكي، ووقت التنفيذ الإجمالي بين 0.001 ns و0.005 ns، وقد تم الحصول على immutability بمقدار 5

* Email: widalaa23co4@utq.edu.iq

للنظام. وبالتالي فان نتائج تحليل النظام المقترح قد تلهم الباحثين/المطورين لتطبيقه على المؤسسات المصرفية الإلكترونية والاستفادة من الميزات الأمنية القوية والأداء العالي للطرق المقترحة.

**الكلمات المفتاحية:** 2PC، البلوكجين، البنوك الرقمية، هجوم Eclipse، FinTech، ProVerif.

## 1. Introduction

The goal of today's financial institutions and banks is to fully automate all of their financial transactions, data, and information [1]. This goal, nevertheless, is dangerous because automation exposes data to threats and hacking as long as it's accessible online. Financial organizations are always under pressure to strike a balance between system security, pricing, and the speed at which procedures may be finished because confidence and security are important concerns for stakeholders as well as consumers [2]. It will be simpler to fend off attacks if banks and other organizations have a thorough awareness of all the threats to which their systems could be vulnerable [3]. One of the types of attacks that banking systems are exposed to is online fraud known as distributed denial-of-service attacks (DDoS), which can make websites load more slowly, especially those run by banks and other financial organizations. DDoS attacks occur when an overwhelming number of systems overload a targeted system's bandwidth or resources. According to the research Evolution of DDoS: Return of the Hacktivists, there was a 22% surge in DDoS assaults on financial institutions in 2022. This is particularly true in Europe, where attacks have increased by 73%, and financial institutions are the target of 50% of DDoS attacks. Peer-to-peer networks are susceptible to a type of attack called a Sybil attack [4], in which a node purposefully assumes multiple identities simultaneously, hence weakening the credibility and influence of reputation systems. This attack's primary goal is to obtain the majority of the network's influence and use it for illegal actions within the system. A single entity, a computer, is capable of creating and managing several identities, such as user accounts and accounts based on IP addresses.

Another kind of double-spending attack is the Finney attack. If someone approves an unconfirmed transaction, what might happen on the network? According to Finney, it is possible for an attacker to create a block that contains a transaction from address A to address B, both of which belong to him. The attacker will then send a second payment from address A to address C, which is owned by a different user, using the identical currencies. The attacker can release the block holding his or her initial transaction if the user accepts it without waiting for network confirmations. Studies on the safety of internet banking and the quality of customer care show that consumers prefer these services over traditional banking setups.

Employee mistakes or deliberate acts are the primary source of the majority of cyberattacks that impact businesses. This suggests that everyone who works for the company, including contractors, should be aware of the importance of cybersecurity in addition to the IT department. Thus, the engineers began improving the online services and creating new systems in order to safeguard user data and enable simple access to bank accounts. One of these improving methods is blockchain technology (BCT).

### 1.1. FinTech

In banks and financial institutions, technological and electronic methods have gradually replaced conventional methods due to the rapid advancement of technology. FinTech is the term for the application of technology in international corporate organizations to provide customers with improved financial services.

The term FinTech refers to a broad category of technologies that are continuously communicating inside a shared infrastructure. That is why FinTech has been presented as a fast, easy, and efficient way to make people electronically access their bank accounts. It also gives people the advantage of accessing their accounts 24 hours a day, 7 days a week. Figure 1 gives a brief overview of the FinTech scheme.

As clarified in Figure 1, blockchain is a main branch of FinTech; it is an evolutionary method that eliminates the need for a third party to complete any transaction. The upcoming section illustrates blockchain's mechanism and the importance of this technology in financial organizations.

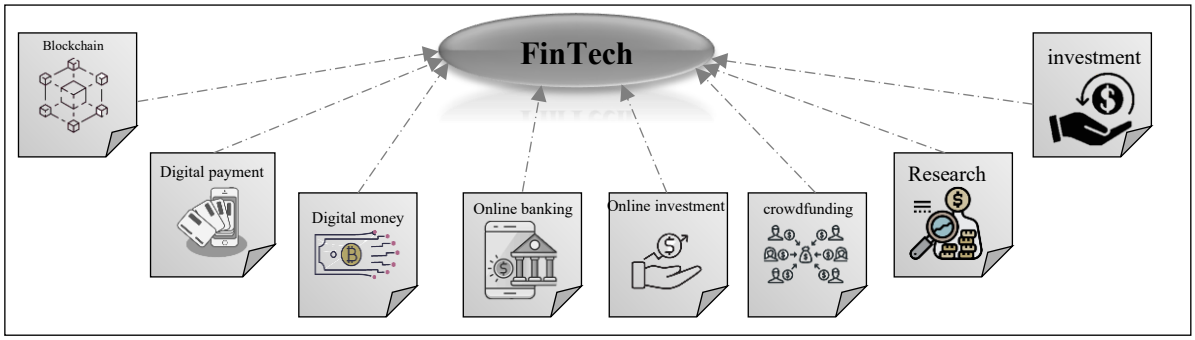



**Figure 1:** FinTech scheme

### 1.2. Blockchain Technology in Banks

Blockchain was invented as a revolutionary way to store banking transactions and carry out financial transfers. This technology relies on the principle of a distributed ledger, which is in the form of blocks interconnected with each other as chains, containing all information about customers and their accounts. Blockchain technology is highly important to the banking industry and financial institutions. It is a decentralized database or ledger that is shared by nodes in a computer network [5]. The data is saved in blocks, where each block consists of the date, hash, and hash of the preceding block. With the existence of blockchain technology, there is no need for a third party to complete the process; blockchain will play that role and send the money as a P2P, and the whole process will be saved, as clarified in Figure 2.

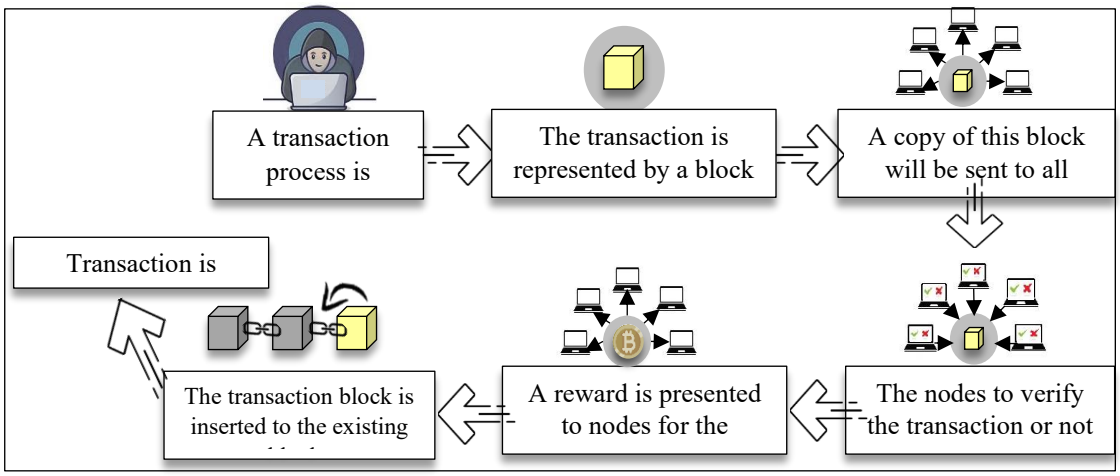



**Figure 2:** Scheme of Blockchain

Next, Table 1 [1] presents a complete classification of blockchain types.

**Table 1:** Blockchain classification

| Blockchain Type | Description |
|---|---|
| *Public Blockchain* | It is non-restrictive and requires no authorization to access; therefore, anyone with internet access can access this type of blockchain, which is why its primary benefit is that it is entirely independent. The majority of cryptocurrencies operate on public blockchains. |
| *Private Blockchain* | it is a kind of blockchain that is restricted, requires permission to access, and is controlled by a single institution. Only genuine users are allowed to access this kind of blockchain. |
| *Hybrid Blockchain* | This sort of blockchain is a hybrid of public and private, with some parts administered by a single organization and the rest accessible to the public. Permission is required for some elements of the system, but not for others. |
| *Consortium* | In which certain aspects are private and others are public, yet it can be regulated by several organizations [2]. |

But as explained above, as long as the data is on the Internet, it is vulnerable to hacks and attacks. For this reason, researchers consistently strive to integrate blockchain technology with various other technologies, methods, and principles to enhance security and fortify the system against cyberattacks. The suggested solution in this manuscript is exceptional in that it incorporates different methods together to obtain an integrated system that combines security with prompt action execution in real-time. Thus, the suggested system achieves the following primary accomplishments:

### 1.3. Main Accomplishments

- Improving the duration and execution time of the designated e-banking procedure, was achieved by relying on YSGA's characteristics, which are among the fastest.
- Strengthen customer confidence in the system by accelerating the process of financial transfers by reducing the period required to verify the terms of the smart contract, which gives speed to the entire system.
- Using the micro-segmentation approach for the first time with financial systems to isolate each process in a separate segment would improve security since it keeps the other segments safe and isolated if one segment is attacked.
- Implementing two authentication phases, the first during the condition's detection of smart contracts and the second during hashing and ID detection on the blockchain, will strengthen the authentication process. No unauthorized person will be able to access the system unless they have been validated in both stages.

## 2. Related Work

This section will provide a comprehensive overview of the previous studies.

Anatoliy et al. [1] clarified that the most valuable asset of a bank is its clients' trust. But this trust is compromised when it comes to cybersecurity. Technological developments and changes in data governance in the banking sector could lead to new cybersecurity risks. Cyberattack risks arise from various new and altering organizational contexts, such as the implementation of remote office technology, cloud migrations, automated decision-making models, and the revival of key systems. Using a zero-trust strategy, banks can effectively future-proof the security of their digital assets. However, the problem with this study is that it never suggested a practical model to improve banking sector security.

Dhoot, A.N. Nazarov, et al. [2] presented a security risk model that safeguards a customer's online banking account from hacking by utilizing inline biometric protections. It helps identify any unauthorized transactions that take place on their account without their awareness. The data is secured by the use of biometric identification mechanisms, such as face and fingerprint

recognition. The model makes it possible to create effective cybersecurity defenses for the financial system at the canonical, logical, and physical levels of representation, but in order to make the model more user-friendly, it still has to be protected against a variety of potential cyberattacks.

Popoola et al. [3] examined the possibility of using sensitive information, such as personal identification numbers (PINs) and credit cards, as a stand-in for present ATM security measures. Every possible transaction is considered in real time by the bank account holder. System maintenance and implementation seem to be simple. The paper, however, does not define or describe the formal verification procedure.

Khatri and Kaushik [5] addressed how blockchain technology will affect banking in the future and highlighted how distributed ledger-based transactions are becoming more and more significant for the banking sector. Ultimately, the goal of this study is to encourage more active participation from academics, researchers, and bankers by compiling research work that has been published in many credible databases and is not a practical study at all. A thorough analysis of the literature results in a detailed evaluation of blockchain use in banking to date and across geographic regions.

Qingquan He [6] described the features of blockchain technology, its effects on the management and operations of conventional commercial banks, and its potential applications in commercial banks, all of which were thoroughly examined in his research. However, their study was theoretical and did not contain practical evaluations.

Chaudhry and Hydros [7] presented a model based on the principle of zero trust. Zero trust is defined as a collection of ethereal concepts and guidelines intended to eliminate uncertainty while enforcing precise and limited resource access for users. ZTA is a cybersecurity strategy that involves access control, productivity planning, and essential communications. It may be implemented by any firm that follows zero-trust principles. However, they did not assess or address the time aspect of their suggested model. In this kind of application, time management is seen as crucial to completing banking tasks within the allotted time.

Lamba and Verma [8] demonstrated how transactions can be made via a trustworthy and secure blockchain-based network, doing away with the need for middlemen. Their paper, which is review-based, offers details on the potential applications of secure blockchain technology in the financial sector. Every transaction on a blockchain has a digital signature, which attests to the chain's legitimacy. In India, banks are some of the most reputable, well-established, and important financial intermediaries. The banking industry has seen a few significant yet significant changes as a result of modernization. When applied properly, blockchain technology has the potential to completely transform the banking industry's future.

Gupta and Ansurkar [9] investigated four studies that have been conducted on consensus algorithms for blockchain technology. The concept and architecture of the blockchain are used in their study to investigate and comprehend the workings of this technology. The benefits and drawbacks of this platform as it applies to the banking industry are the main subject of their study. Table 2 will provide an illustration of all the previously mentioned points.

**Table 2:** summary of previous studies

| Study | Methodology | Drawbacks |
|---|---|---|
| [1] 2018 | This study considered bank trust crucial, but cybersecurity risks arise from technological advancements and data governance changes. A zero-trust strategy can help future-proof digital asset security by; addressing cyberattack risks from remote office technology, cloud migrations, and automated decision-making models. | The study did not propose a practical model to improve security in the banking sector. |
| [2] 2020 | The study introduced a security risk model that uses inline biometric protections to safeguard online banking accounts from hacking, enabling effective cybersecurity defenses at all levels of the financial system. | The model needs to be safeguarded against various potential cyberattacks to enhance its user-friendliness. |
| [3] 2021 | The study explored the use of sensitive information like PINs and credit cards as a replacement for current ATM security measures, focusing on real-time account holders and the simplicity of system maintenance. | The paper lacks a clear definition or description of the formal verification procedure. |
| [5] 2021 | This study explores the future impact of blockchain technology on banking, emphasizing the increasing significance of distributed ledger-based transactions and encouraging active participation from academics, researchers, and bankers. | This study provides a comprehensive evaluation of blockchain's use in banking across various regions, despite not being a practical study. |
| [6] 2020 | The research thoroughly examines the features, effects, and potential applications of blockchain technology in the management and operations of conventional commercial banks. | The paper did not include any practical evaluations in the theoretical analysis. The suggested model's time aspect was not considered, which is crucial for completing banking tasks within the allotted time. |
| [7] 2021 | The study introduced a zero trust (ZTA) cybersecurity strategy, focusing on access control, productivity planning, and essential communications, which can be implemented by any firm following zero-trust principles. | The literature analysis provides a comprehensive evaluation of blockchain's current and geographically diverse use in banking. |
| [8] 2022 | The paper explores the potential applications of secure blockchain technology in the financial sector, highlighting its potential to eliminate middlemen and ensure transactions are legitimate. It highlights the potential for blockchain to transform the banking industry's future when applied properly. | This study is a theoretical model and not practical. |
| [9] 2022 | Four studies explore consensus algorithms for blockchain technology, focusing on its concept, architecture, benefits, and drawbacks in the banking industry. | It is just a review model. |

## 3. Essential Principles Applied in the Proposed System

**Here is a summary of the methods were used in the proposed system.**

### 3.1 Two-Phase Commit (2PC)

It is a distributed algorithm whose goal is to determine the type of e-banking process, which is done through two stages: the first stage is the initialization stage, and the second stage is the commitment stage. In the first stage, all participants are asked about the type of banking procedure that they want to achieve through the so-called organizer or coordinator. Then comes the next stage, which is called the commitment stage, meaning that the algorithm analyzes the

type of e-banking process through the words that the customer entered for his transaction, which sends requests to the organizer, who has the right to vote or not to complete the procedures of determining the type of bank transaction as in Algorithm 1.

**Algorithm 1: 2PC in the proposed system**

Start
Input: $R \leftarrow$ request
Output: $M \leftarrow$ type of request
1. **Initiation Phase: Coordinator Initiation:** A user, initiates the procedure by sending "request" message to the system.
2. **Voting phase:** If the request is e-banking process, sends "Yes" message back to the coordinator. Otherwise, it sends a "No, FAIL" message.
3. **Committing** or **decision-making phase:** The coordinator analyzes the votes from the above step.
- **Transaction process:** If respond with "Yes," then $M \leftarrow$transaction process, call micro segmentation procedure to isolate it in separate zone.
- **otherwise:** If any responds with "No FAIL," the coordinator decides to neglect the request and never specify a zone.

End

### 3.2 Micro-Segmentation

Micro-segmentation is a security strategy that pertains to the idea of creating distinct zones within a network, each with its own set of regulations, which is entirely distinct from network-segmentation, which is hardware-based, and network micro-segmentation, which requires software-based. As a result, the primary goal of this strategy is to create a secure system by isolating each zone. Even if an attacker manages to breach one, the remaining zones will remain safe and secure. Figure 3 illustrates the process of segmenting the entire system into zones. Each zone is entirely autonomous. For instance, if an intruder manages to access Zone 1, they remain confined within that zone without any influence on the other zones. Comparing micro-segmentation to more traditional techniques, designed and developed for locations with fortified perimeters, reveals several technological benefits.
Restricting the attacker's ability to move through the system due to the segmenting process into zones, therefore raising the level of security.

- Provides high ease in terms of maintenance and integration with other applications.

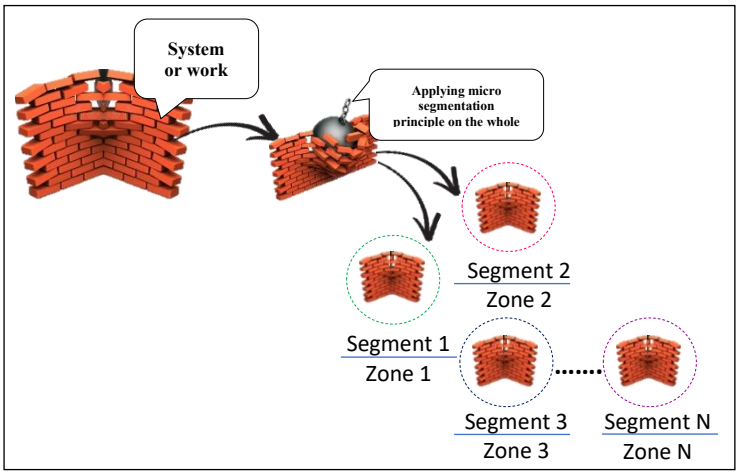



**Figure 3:** Micro segmentation scheme

- Closes possible gaps in security coverage that could lead to vulnerabilities by tying policies to workloads rather than network segments.

Where the implementation of this technique in the proposed system is explained in Algorithm 2.

Algorithm 2: Micro segmentation implementation in the proposed system

Start
**1- Initializing phase**
Input $T$← type of the e-transaction process
Where $T$ is the output of the 2PC procedure
**2- Identifying and isolation phase**
Identify zones based on the type of the e-transaction process $Z_i$
$i$← number of process
3- Isolate each zone $Z$ by a code-based condition (Smart Contract)
4- Output $Z_i$← isolated zones based on e-banking process type
End

### 3.3. Smart Contract

A decentralized piece of software called a smart contract has been presented as being extremely similar to the concept of a contract in real life. This suggests that every transaction between two peers is managed and identified by the smart contract following a set of predefined criteria; if they are met, the transaction is approved; if not, it is rejected. Thus, the implementation of a smart contract might be advantageous for any financial transaction or the execution of material that is controlled according to certain guidelines [7]. Simply put, a smart contract is a piece of code that, upon meeting specific criteria, initiates an activity. They lack any legal language, clauses, or commitments. The smart contracts are self-executing programs. The following are some of the many benefits of using smart contracts in financial systems in conjunction with blockchain technology: Table 3 presents the benefits of smart contracts [10].

**Table 3** Smart contract's benefits

| Aspects | Description |
|---|---|
| ***Independence*** | smart contracts don't need to be verified by agents or other middlemen, they eliminate the chance that third parties will manipulate the agreement. Additionally, since smart contracts eliminate the need for an intermediary, they save money. |
| ***Safety*** | A smart contract's self-reliance feature makes it regarded as having a high level of security. |
| ***Speeding up*** | Smart contracts save hours of job duties in a range of financial procedures by automating functions using computer protocols. |
| ***Trustworthy*** | Errors that result from filling out many forms by hand are removed with the use of smart contracts. |

#### *3.3.1 Smart Contract's in banks*

This section will review every stage the digital contract undergoes, from its creation to its approval and completion. Figure 4 illustrates the main smart contract phases, which are as follows: First, the creation phase involves two parties agreeing on a set of conditions to create a smart contract, which a software engineer then transforms into clear code. During the setting-up phase, the parties involved announce the terms of the smart contract and store them on a blockchain. All banking operations are closed to prepare for the next stage, the execution and validation phase, in which an auto-execution of the smart contract is accomplished. The verification phase commences by determining the fulfillment of the smart contract's conditions. Lastly, we initiate the completion phase by opening the lock for banking operations and initiating execution if the conditions are satisfied [8].

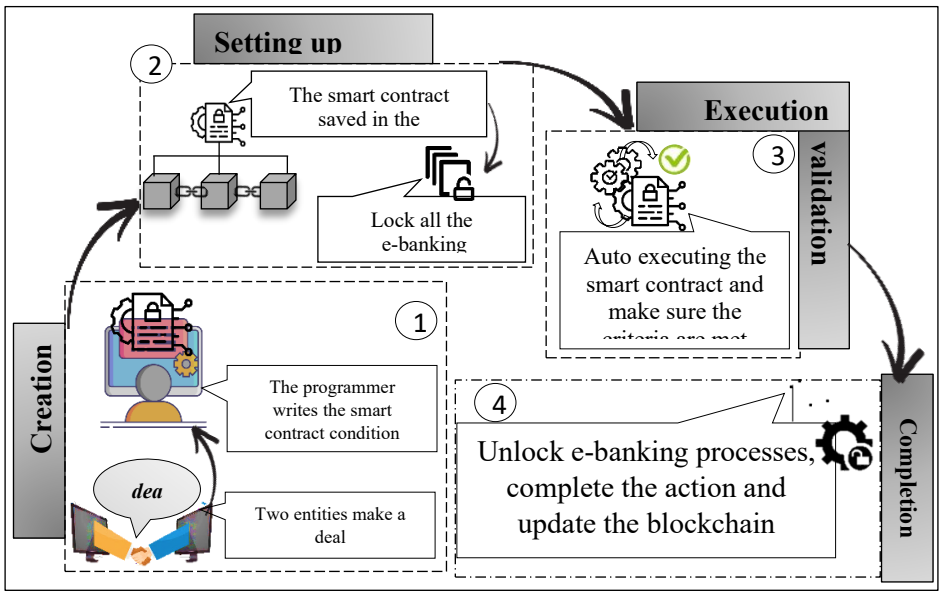



**Figure 4:** Smart contract life cycle

*3.3.2 Smart contract procedure in the proposed system:*

The procedure of the smart contract in the proposed system starts directly after the recognition of the type of e-banking process, which means directly after the 2PC procedure as follows in procedure 3.

***Algorithm 3:*** *smart contract procedure*

**Start**
**Input:**
$M \leftarrow$ Transaction specified process by 2PC
Output:
***Transfer function:***
*Successful transfer:* Updates the balances of sender and receiver in the blockchain ledger.
*Unsuccessful transfer:* Reverts the transaction (no changes made).
1- Initialize parameters:
2- Sender: Address of the transaction initiator.
3- Receiver: Address of the transaction recipient.
4- Amount: amount to be transferred.
5- Develop Smart Contract Functions:
6- Transfer (receiver, amount): Requires sender to call this function.
7- Verifies the terms if sender has sufficient balance (check sender's account on the blockchain).
8- If sufficient balance:
9- Deducts the amount from the sender's balance.
10- Adds the amount to the receiver's balance.
11- Updates the state with the new balances.
12- Announce a "Transfer Success" event with details.
13- If insufficient balance:
14- Reverts the transaction.
15- Security Considerations:
16- Implement access control checks.
17- Validate all inputs to prevent manipulation (amount is positive and sender address is valid).
End.

### 3.4 Yellow Saddle Goatfish Algorithm

The scientific community was drawn to the remarkably fascinating hunting behavior observed in a group of yellow saddlefish [11]. As a result, the fish mentioned were found to hunt in groups, with each group consisting of a single fish known as the chaser fish and the remaining fish belonging to the same group known as the blocker fish based on fitness value. As a result, an optimization technique has been developed for this type of behavior. This technique is thought to be a fairly potent, quick, and smart algorithm that is utilized for both scientific study and best practice determination. The entire hunt space is broken into distinct zones, and each population of fish in these zones will initialize a specific quantity, then apply a calculation of the fitness value of each particle and compare it to the global best value to identify which fish are the blocker fishes and which are the chasers, leading the hunting process [12].

- *YSGA usage in the proposed system*

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

- This algorithm relies on the technique of breaking or dividing the whole system into zones, the matter that is considered suitable for the micro-segmentation principle of isolating the threats.
- The easy-going procedure of calculating the values leads to an easy and fast result.

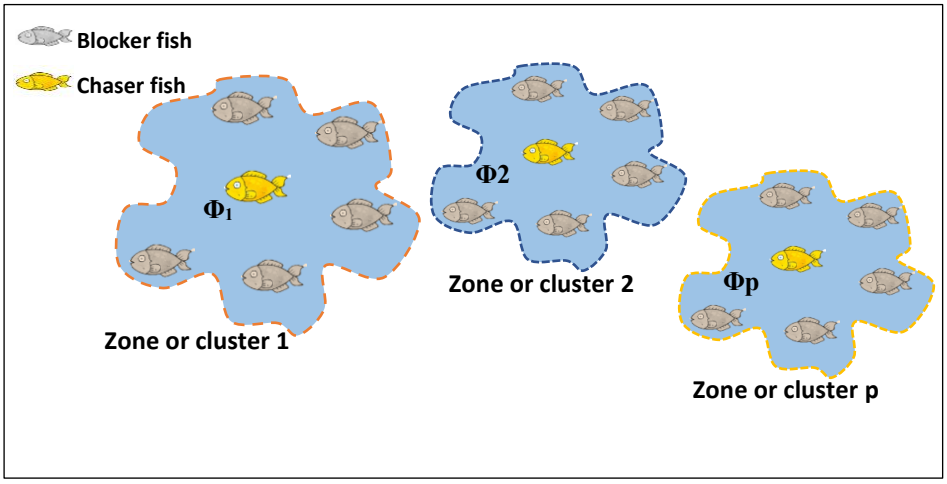



**Figure 5:** YSGA hierarchy

As illustrated in Figure 5, the yellow fish represent chaser fish with the highest fitness value, while the grey fish represent blocker fish. The authentication process ensures a quick and secure module. This algorithm plays a great role in detecting smart contract conditions and whether they are fulfilled or not, as shown in Figure 6, where the whole algorithm steps are specified.

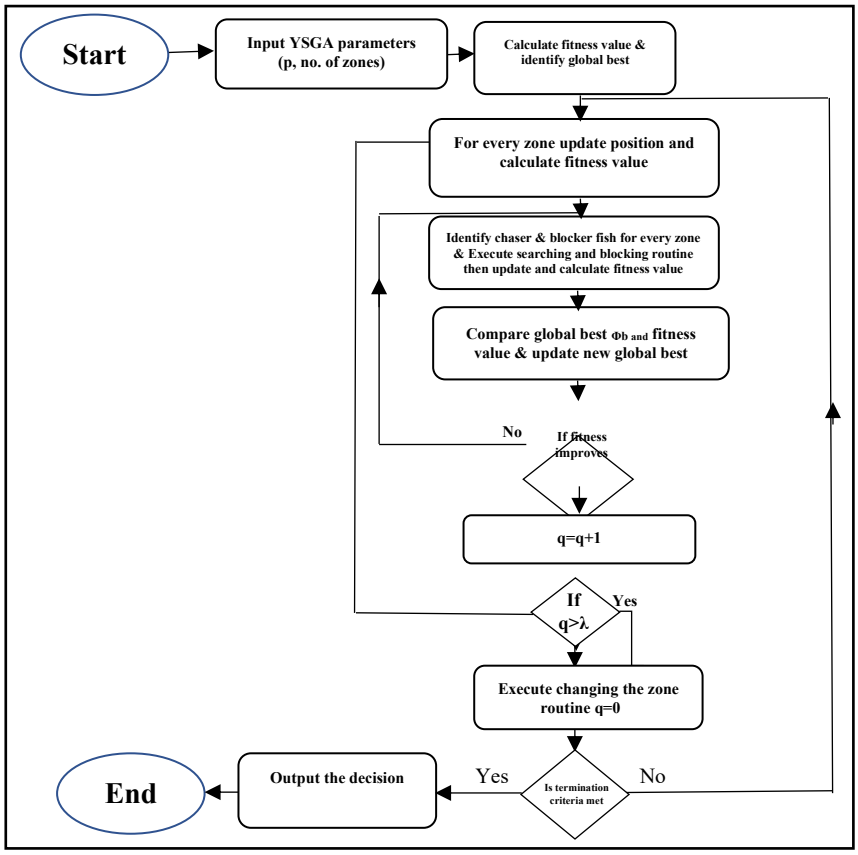



**Figure 6:** YSGA scheme

**Algorithm 4: YSGA**

Start

Input the goatfish population $P \leftarrow \{p_1, p_2, p_3, p_4 \ldots p_m\}$ number of the rules, "terms" of the smart contract.

Output the best search value in case of the proposed system if the terms are fulfilled or not ($\Phi_{best}$).

1- Calculate the fitness value of each particle ($p$)
2- Identify the global best $\Phi_{best}$ the terms detection value
3- Partition the population p into k zone $\{Z_1, Z_2, Z_3, Z_4, \ldots Z_k\}$
4- Identify the chaser $\Phi_c$ and the blocker $\Phi_b$ fish for every zone
5- For every zone $Z_i$
6- Execute hunting routine for chaser fish
7- Execute blocking routine for blocker fish
8- Calculate the fitness value for each goatfish
9- If the calculated $\Phi_g$ has better fitness than the $\Phi_i$
*10-* Exchange the $\Phi_i$
*11-* If the calculated $\Phi_i$ has better fitness than the $\Phi_{best}$
12- Update $\Phi_{best}$
13- If the fitness value of $\Phi_i$ has improved
*14-* $q \leftarrow q+1$
15- Execute routine for changing zone
*16-* $q \leftarrow 0$
17- Output the $\Phi_{best}$ which carry the identification decision

End

As previously stated and as depicted in Algorithm 4, the entire population will first be initialized as $\boldsymbol{p_k}$; in the case of the proposed system, $\boldsymbol{k}$ is the smart contract terms and $\boldsymbol{i}$ is the number of terms, while the global best value $\boldsymbol{\Phi_{best}}$ will be specified so that a comparison can be made with it. Following this, the population will be divided into zones, and in each zone, a specification will be activated for the chaser fish, $\boldsymbol{\Phi_C}$, and the blocker fish, $\boldsymbol{\Phi_b}$. Next, the hunting routine will compare the global best $\boldsymbol{\Phi_{best}}$ and the obtained $\boldsymbol{\Phi_i}$, and it will decide whether to replace the fish and carry out further for other terms detection, or end the hunt and terminate the detection.

### 3.5. Sequence of Work in the Proposed System for E-Transaction

The proposed system depends on dividing the processes using the micro-segmentation principle into separated zones after the process type is determined using the 2PC to reduce the chances of being hacked, as long as the processes are isolated from each other. Then strengthen these zones by using smart contracts, where every zone will be governed by particular guidelines and regulations. No action will be taken, which means no data sharing, financial transactions, buying, or selling through the financial system will take place unless these guidelines are detected as having been followed. After distinguishing these operations, we use one of the newest recognition algorithms, YSGA, to verify the conditions of the smart contract. This algorithm's simple calculations and lack of complexity, which are big advantages, give the system rapid and reliable performance. Once these stages are successfully completed, the final step involves storing the data on the blockchain, thereby concluding the banking process definitively. Figure 7 shows a wide overview of the proposed system.

By initializing the population in each zone, the best value of the YSGA will be obtained, which will regulate the detection process.

$$P = [p_1, p_2, p_3, \dots p_m] \quad (1)$$

Where $m$ is the number of the population. Then calculate the fitness value of each population in the zones to identify the chaser fish that will lead the searching process $\Phi_c$ to identify if the rules are detected or not, and also to identify the blocker fishes $\Phi_b$:

$\Phi_c = X$ $\Phi_b = y$

After this, a comparison is made between the fitness value, which means the best value to detect the rule, and the value of the search of the $\Phi_c$ If they are identical, then go to the next step of blockchain hashing and complete the action; if they are not identical, then terminate and reject the action.

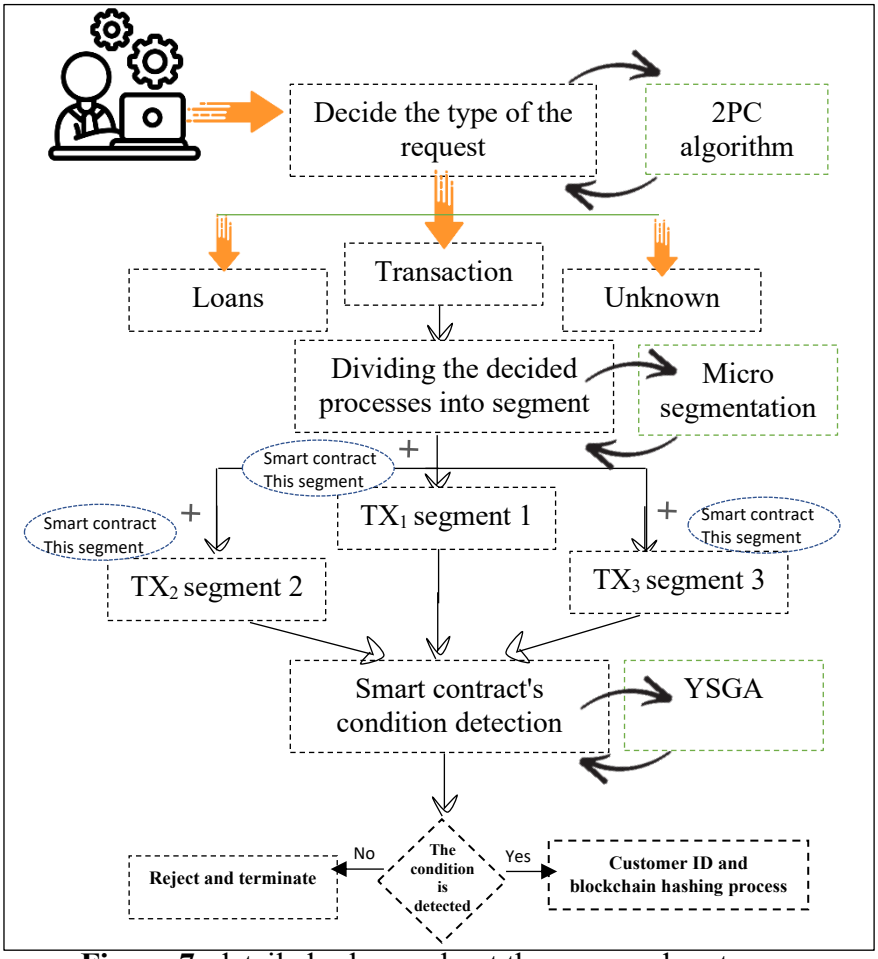



**Figure 7:** detailed scheme about the proposed system

## 6. Security examination of the E-banking risks

System security is considered very important in banking systems, where the system's ability to respond to attacks is considered essential [13] [14]. The following section provides a summary of the attacks that pose a threat to the security of the e-banking system, along with an explanation of how the proposed module effectively addresses these threats. Tables 4 and 5 will then present a comparison of the proposed system's and previous systems' responses to attacks within the research field.

**Table 4:** Attacks analysis on Blockchain system

| Attacks | Description |
|---|---|
| *Selfish mining attacks* | In most cases, a miner broadcasts their achievement to the entire network after successfully mining a block, ensuring synchronization and consistency all the way down the chain. But in the manner of the selfish mining attack, selfish miners create a situation where there are two versions of the truth: their private, undisclosed version and the version that the other members of the network are aware of by hiding their mined blocks. Otherwise, the proposed system for countering this type of attack is simple because it focuses primarily on the principle of verification using smart contracts rather than mining. |
| *Sybil attack* | It is a type of attack that operates multiple active fake identities (also known as Sybil identities) concurrently on a single node in a peer-to-peer network. This type of attack seeks to undermine authority or power in a trustworthy system by seizing the majority of the network's influence. The perpetrator creates numerous false internet personalities, similar to fake accounts. These fictitious personas are referred to as Sybil, after a novel about a multi-personality woman. The proposed system counters this attack by relying on the KYC principle, which mandates a unique ID for each individual entering the system, as well as the power of micro-segmentation, which limits any attempt to impact the entire system. |
| *51% attack* | Sometimes called a dominating attack, it occurs when one person or group of people owns more than 50% of the hashing power on a system based on blockchain technology. Reaching this degree of control could lead to rejected transactions and potential coin double-spending by manipulating and jeopardizing the integrity of the blockchain system. On the other hand, using the micro-segmentation principle, the proposed system divides e-banking operations into isolated zones and segments. Therefore, programmatically, it is extremely difficult to penetrate half of the network and obtain dominant control over it, as the risk will be isolated and specific. However, in terms of physical control, an intruder requires significant system resources to seize control of half of the network. |
| *Eclipse attack* | Eclipse attacks are a unique kind of cyberattack where the attacker surrounds a single node or client with a fake environment to persuade the targeted node into acting improperly. Eclipse attacks can cause fraudulent transaction confirmations and other network impacts by isolating a target node from its genuine adjacent nodes. Although these attacks isolate certain nodes, the underlying network's structure plays a major role in how well eclipse attacks disrupt traffic and network nodes. As a result, the proposed system's structure is already isolated, with each transaction process having its own segment, zone, smart contract rules, and verification process. As a result, the system structure is never suitable for such an attack, making the proposed system immutable against it. |
| *Finney attack* | This kind of attack, which goes like this, is known as a double-spending attack. Initially, a miner can produce a block that includes a transaction from address A to address B, provided that both addresses belong to the miner. The hacker can then use the same currencies to send a second payment from address A to address C, which is another user's address. The attacker can release the block containing his initial transaction if the recipient approves it without waiting for network confirmations. Because each process has its own set of smart contract terms that need to be confirmed before the transaction can begin, the suggested protocol does not allow for scenarios where a concurrent can be transmitted more than once. |
| *DDoS attack* | Blockchain systems are susceptible to a certain kind of denial-of-service assault. Instead of sending too many pings or requests, malicious actors can flood the network with spam transactions. The volume of valid transactions on the network is severely slowed down and clogged as a result. In the suggested system, these fake transactions will be highly detected due to the fast authentication using YSGA and the smart contract's terms, which means it will never slow the network and never affect the system. |
| *Long range attack* | An attacker can launch a long-range attack by splitting a blockchain chain and changing its history. The attacker can add more transactions when the new chain is longer than the legitimate one. Otherwise, the proposed system faces this type of attack by utilizing the KYC principle, which ensures the reliability of each entry through a unique ID and the immutability of the blockchain. |

**Table 5:** Comparison of attacks preventing between the proposed system and the related systems

| Attack | [4]2019 | [15]2022 | [16]2021 | [17]2023 | Proposed system |
|---|---|---|---|---|---|
| Selfish mining attack | ✔ | | | | ✔ |
| Sybil attack | | ✔ | | ✔ | ✔ |
| 51% attack | | | | | ✔ |
| Eclipse attack | | | ✔ | | ✔ |
| Finney attack | | | | | ✔ |
| DDoS attack | ✔ | | | ✔ | ✔ |
| Long range attack | | | | | ✔ |

## 7. Performance Analysis of the Proposed E-Banking System

The performance of the suggested system, which was constructed using Java programming language in an integrated development environment called "Eclipse" on the Ubuntu 16.04 LTS system, is covered in the sections that follow, both virtually and practically. The PC utilized for the study has the characteristics of an Intel CoreTM 3110M CPU and 4.00 GB of RAM. To examine the security of the suggested solution, two different tools, ProVerif and Scyther, have been employed. This is demonstrated in the next section.

### 7.1 ProVerif Authentication

It is a software tool used to check the security characteristics of a cryptographic system. It automatically functions on a simplified symbolic model, which assumes that communication routes are unreliable and that adversaries can replay, inject, and eavesdrop on messages. ProVerif operates in the following manner: First, use logic-based rules to define participants, messages, communication channels, and necessary security features to specify the protocol that has to be verified. Considering the adversary's behavior, ProVerif employs automated reasoning techniques to investigate every scenario in which the protocol could be executed. ProVerif analyzes the data and evaluates whether the given security features (such as secrecy, authentication, and non-repudiation) hold for every scenario in which the protocol could be executed. Figure 8 displays the authentication results.

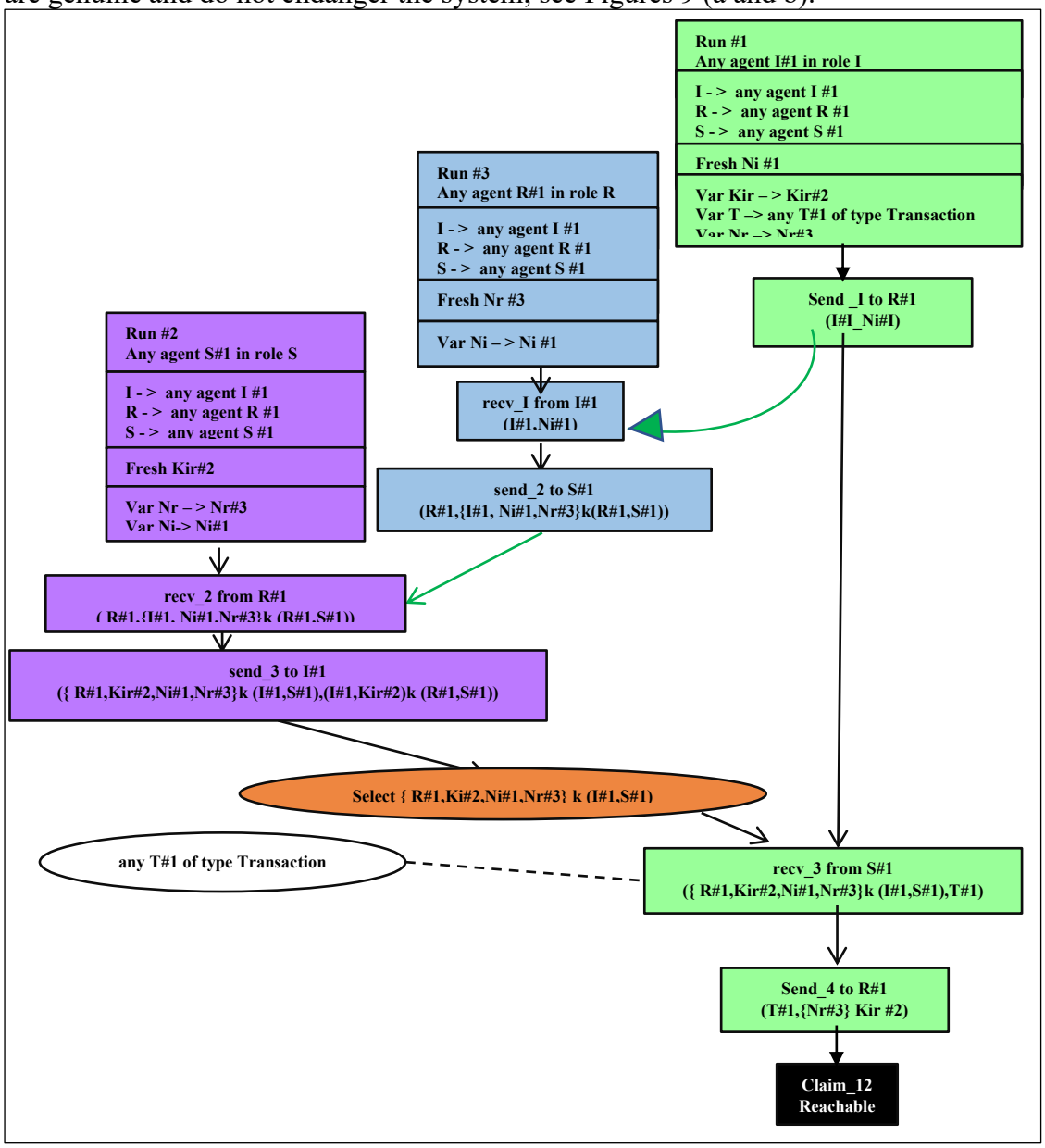
```
-- Transaction event
  event(sender_bitstring(d,(i_3,x1))) && event(reciever_bitstring(d,(i_3,x_3))) ==> x1 = x_3
  event(Counter(d,st2,st_1,i1)) && event(Counter(d,st2,st_1,i_3)) ==> i1 = i_3
  event(Counter(d,st2,st_1,i1)) && event(Counter(d,st2,st1,i1)) ==> st_1 = st1
 in process 0
-- Query not event(Attack) in process 0
Translating the process into Horn clauses...
Completing...
Starting query, not event(Attack)
RESULT not event(Attack) is true.
------------------------------------------------------------
Verification summary:
Query(ies):
 - Query not event(Attack) is true.
Associated axiom(s):
 - Axiom
  event(sender_bitstring(d,(i_3,x1))) && event(reciever_bitstring(d,(i_3,x_3))) ==> x1 = x_3
  event(Counter(d,st2,st_1,i1)) && event(Counter(d,st2,st_1,i_3)) ==> i1 = i_3
  event(Counter(d,st2,st_1,i1)) && event(Counter(d,st2,st1,i1)) ==> st_1 = st1
 in process 0.
----------------------------
Result
Transaction event is True
```

**Figure 8:** The verification result using ProVerif tool

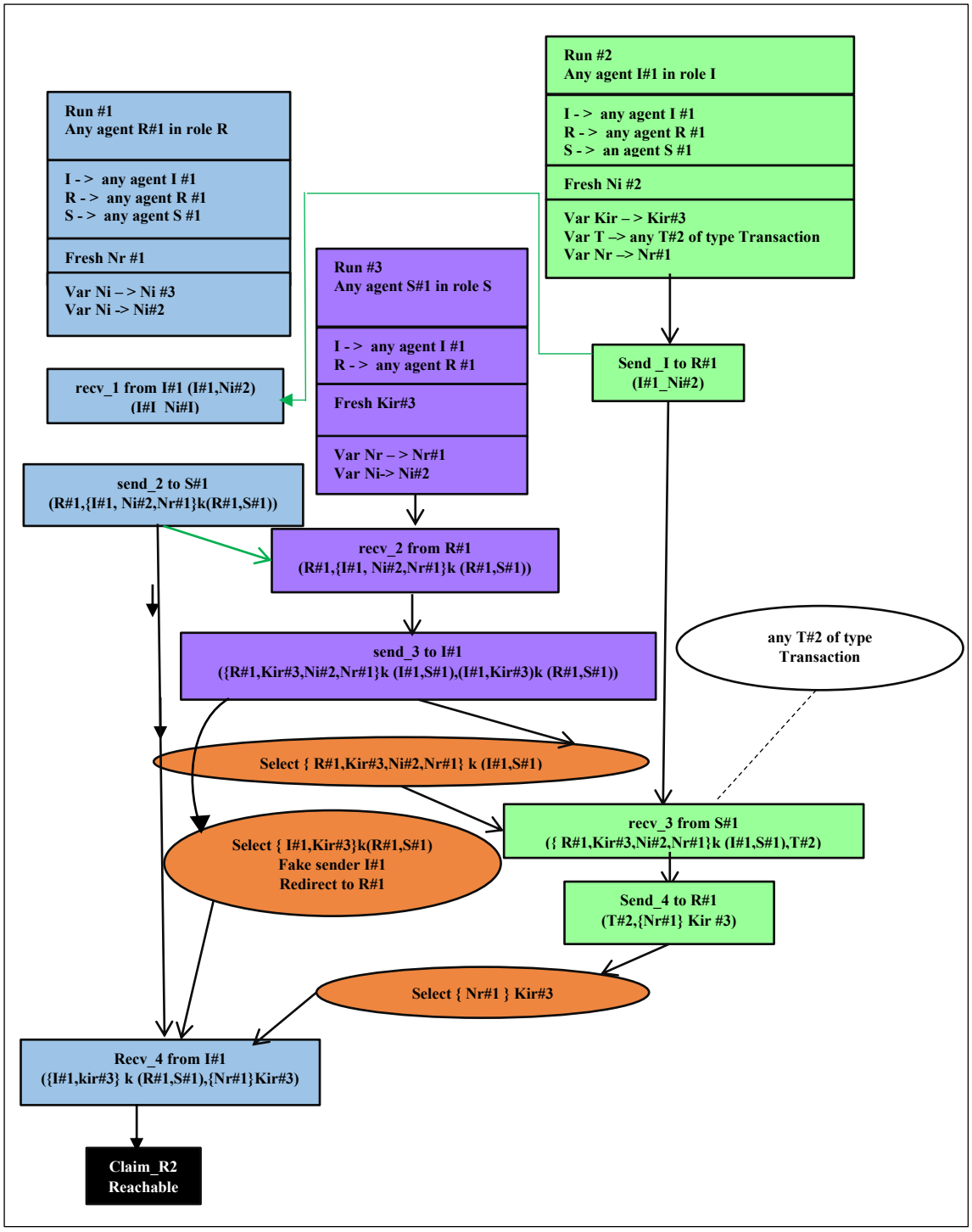
Figure 8 illustrates that the verification result following the transaction event was accurate.

### 7.2 Scyther Authentication

Scyther is another helpful tool in the realm of cybersecurity [18] [19], but it focuses on a different aspect compared to ProVerif. Scyther is a tool that looks at cryptographic protocols to find holes in them related to nonce usage and session concurrency. This is different from ProVerif, which works in the symbolic model and checks overall security properties. The proposed system's Scyther, with its cutting-edge features, attack monitoring, and quick verification, is excellent [20]. It successfully tests most protocols without the requirement for approximation techniques for an arbitrary number of sessions and verifies that all attacks found are genuine and do not endanger the system; see Figures 9 (a and b).




(a)




**(b)**

**Figure 9:** Role1 (a) and role2 (b) of the proposed system characterized roles

### 7.3 Parameters of performance analysis

The suggested system's overall efficacy has been assessed using the following parameters:

- Period analysis to verify the terms of the smart contract: The time it takes to verify smart contracts' terms depends on factors like the programming language used, the size of the smart contract, and the number of conditions to check. The efficiency of writing a smart contract depends on the algorithm used. To increase efficiency, the proposed system employs the YSGA algorithm, a modern, high-search-speed algorithm.

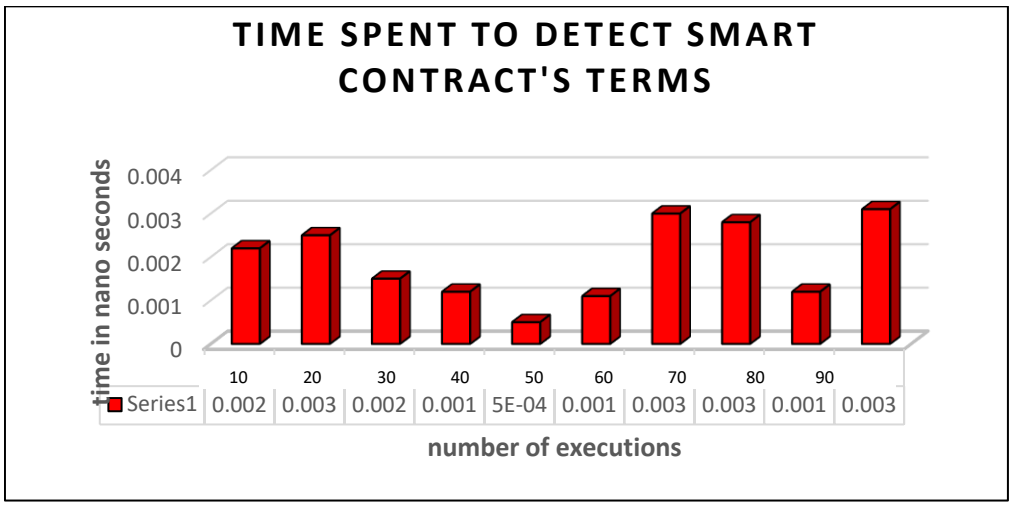



**Figure 10:** Time spent to detect smart contract's conditions

Table 6 below illustrates how the proposed system's smart contract verification process, compared to other digital contract research, is believed to be extraordinarily quick and simple.

**Table 6:** Time spent to detect the smart contract's terms

| Blockchain based smart contract system | Time spent to detect the smart contract's terms |
|---|---|
| *2021[10]* | 15 MS |
| *2024[21]* | 2.75 S |
| *Proposed system* | 0.0031 NS |

- Immutability of Data: Within the context of blockchain, it describes a fundamental property that, once recorded, keeps data unchangeable and irreversible [22،23]. This implies that once data is added to a blockchain, it cannot be changed, removed, or tampered with in any manner. It is like having a person's name permanently and irrevocably carved into the blockchain's history. Next is how this accomplishment is made possible:

Blockchains are tamper-proof systems in which each block contains data and a unique hash, similar to a fingerprint. Any alteration to the data would create a new hash, making the entire block invalid. Blocks are connected temporally, and any modification would invalidate all succeeding blocks' hashes and the block's own hash. Due to the importance of this measure in determining the quality of the system, it is considered one of the most important scales to evaluate blockchain performance. Immutability has been adopted to analyze the performance of the proposed system, where the following results mentioned in Figure 11 have been obtained:

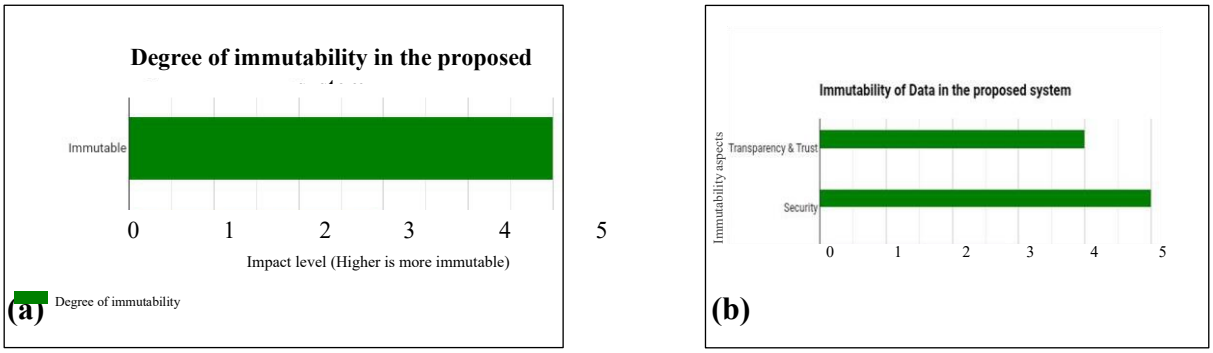



**Figure 11:** The level of immutability in the proposed system (a) and the aspects of immutability in the proposed system (b)

The level of immutability is 5 and recorded high performance in the aspects of trust and security, which is considered a very high scale in the systems based on blockchain. This scale is supported by the use of smart contracts and YSGA.

• Duration of execution: the time spent on the central processing unit (CPU), which is the amount of time needed to finish the suggested system's operation. The total time required was determined by running Java code that supplied the average execution time in milliseconds; see Figure 12.

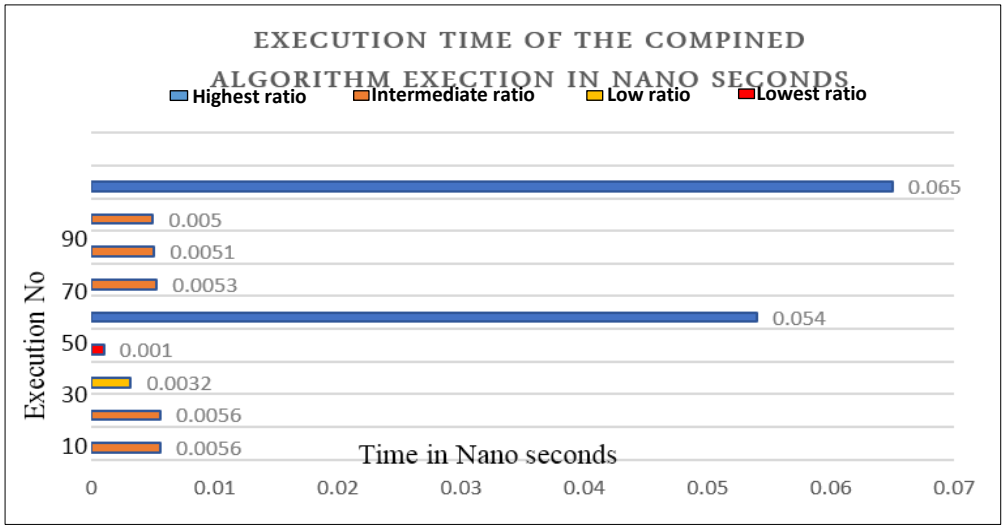



**Figure 12:** The execution time for overall proposed system

The execution was carried out 100 times. The average execution time was determined to be a fraction of a second. It was noted when extracting the results that the ratio the proposed system reached was between 0.001 ns and 0.005 ns, with a few results of 0.054 ns and 0.065 ns. In light of these findings, the proposed system is regarded as extremely fast in comparison to existing systems.

## 8. Conclusions

The regular introduction of new inventions and the swift progress of technology have had an impact on the banking sector. As a result, online electronic banking processes—also known as e-banking—have taken on the role of traditional banking practices. But since anything done online is susceptible to data loss, hacking, and attacks, a secure e-transaction system that combines a fast and secure way to conduct financial transactions has been proposed here. It is an integrated security system for electronic transactions, where initially, the two-phase commit (2PC) was used to specify the kind of e-banking request in this study. Subsequently, distinct e-transaction processes were divided into several parts using the concept of micro-segmentation, with each segment subsequently being managed by a smart contract. The Yellow Saddle Goatfish Algorithm (YSGA) was used to determine whether the smart contract's requirements were satisfied in the best possible way. Finally, if the customer is accepted, the entire transaction process is documented on the blockchain's main ledger and protected by a unique hash.

All results were analyzed and obtained through simulation using the Linux operating system and the Java programming language in the Eclipse environment. Where the following characteristics are gained:

- The proposed system ensures that the financial transfer is completed in real time and without delay, which enhances the customer's confidence in the system. The proposed system is considered rapid because the e-transaction's total execution time, from the start of the user request until it reaches the blockchain storage, did not exceed 0.0056 ns.
- The proposed system guarantees the security of customer data according to the results that have been gained in the analysis section above, in addition to the use of algorithms and procedures that enhance security, such as the principle of micro-segmentation and smart contracts.
- Raising productivity levels by using 0031 ns to detect the terms of the smart contract will increase the system's overall number of processed requests.

Finally, the analysis's findings may motivate researchers and developers to use the suggested system's strong security features and good performance in e-banking establishments.

**References**

**[1]** P. N. Anatoliy, V. A. Kristina, A. K. Elena, D. G. Vagiz and V. S. Aleksandr, "Technologies of safety in the bank sphere from cyber attacks," *2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*, Moscow and St. Petersburg, Russia, 2018, pp. 102-104, doi:10.1109/EIConRus.2018.8317040.

**[2]** A. Dhoot, A. N. Nazarov and A. N. A. Koupaei, "A Security Risk Model for Online Banking System," *2020 Systems of Signals Generating and Processing in the Field of on-Board Communications*, Moscow, Russia, 2020, pp. 1-4, doi:10.1109/IEEECONF48371.2020.9078655.

**[3]** O. Popoola, I. Jimoh, A. O. Adetunmbi and B. K. Alese, "Design of a Customer-Centric Surveillance System for ATM Banking Transactions Using Remote Certification Technique," *2020 IEEE 2nd International Conference on Cyberspace,* Abuja, Nigeria, 2021, pp. 104–111, doi**:** 10.1109/CYBERNIGERIA51635.2021.9428795.

**[4]** M. Saad, L. Njilla, C. Kamhoua and A. Mohaisen, "Countering Selfish Mining in Blockchains," *2019 International Conference on Computing, Networking and Communications (ICNC)*, Honolulu, HI, USA, 2019, pp. 360-364, doi: 10.1109/ICCNC.2019.8685577.

**[5]** A. Khatri and A. Kaushik, "Systematic Literature Review on Blockchain Adoption in Banking," *Journal of Economics, Finance and Accounting (JEFA)*, vol. 8, no. 3, pp.126-146, September 2021, doi:10.17261/Pressacademia.2021.1458

**[6]** Q. He, "Application of Blockchain Technology in Commercial Banks," *2020 International Conference on New Energy Technology and Industrial Development (NETID 2020)*, Dali, China, vol. 235, no. 03070, pp. 1-4, 2021, doi:10.1051/e3sconf/202123503070.

**[7]** J. T. Force, "Security and Privacy Controls for Information Systems and Organizations," *NIST Special Publication,* vol. 8, no. 53, pp.1-463, September 2021, doi:10.6028/NIST.SP.800-53r4.

**[8]** S. Lamba, S. Saxena and M. Verma, "Blockchain Technology in Banking Sector*," International Journal of Research Publication and Reviews (IJRPR),* vol. 3, no. 3, pp. 1786-1789, March 2022.

**[9]** A. Gupta, and G. Ansurkar**,** "Use of Blockchain in Banking System," *International Journal of Research Publication and Reviews (IJRPR)*, vol. 3, no. 11, pp. 2089-2091, November 2022**.**

**[10]** X. Ge, "Smart Contract Mechanism Based on Blockchain Smart Contract Mechanism," *Scientific Programming*, vol. 2021, pp. 1-12, December 2021, doi:10.1155/2021/3988070.

**[11]** D. Kashyap, B. Singh, and M. Kaur, "Chaotic approach for improving global optimization in Yellow Saddle Goatfish," *Engineering Reports,* vol. 3, no. 9, pp. 1-25, February 2021, doi:10.1002/eng2.12381.

**[12]** D. Zaldívar, B. Morales, A. Rodríguez, A. G. Valdivia, E. Cuevas and M. P. Cisneros, "A novel bio-inspired optimization model based on Yellow Saddle Goatfish behaviour," *Elsevier*, vol. 174, pp. 1-21, December 2018, doi:10.1016/j.biosystems.2018.09.007.

**[13]** M. Al-Zubaidie, "Implication of Lightweight and Robust Hash Function to Support Key Exchange in Health Sensor Networks," *Symmetry*, vol. 15, no. 1, pp.1-25, January 2023, doi:10.3390/sym15010152.

**[14]** M. Al-Zubaidie, M. Z. Zhang and J. Zhang, "REISCH: Incorporating Lightweight and Reliable Algorithms into Light Care Applications of WSNs," *Applied Science,* vol. 10, no. 6, pp. 1-36, March 2020, doi:10.3390/app10062007.

**[15]** K. Riad and M. Elhoseny, "A blockchain-Based Key-Revocation Access Control for Open Banking," *Wireless Communications and Mobile Computing,* vol. 2022, no. 3200891, pp. 1-14, January 2022, doi:10.1155/2022/3200891.

**[16]** S. Yoo, "Research on Security Threats Emerging from Blockchain-Based Services," *International Journal of Internet, Broadcasting and Communication*, vol. 13, no. 4, pp. 1-10, November 2021, doi:10.7236/IJIBC.2021.13.4.1.

**[17]** R. Chagantia, B. Bhushanb and V. Ravic, "A Survey on Blockchain Solutions in DDoS Attacks Mitigation: Techniques, Open Challenges and Future Directions," *Elsevier*, vol. 197, pp. 96-112, 2023, doi:10.1016/j.comcom.2022.10.026.

**[18]** M. Al-Zubaidie, Implication of lightweight and robust hash function to support key exchange in health sensor networks. *Symmetry*, vol. 15, no. 1, pp. 152, 2023.doi.org/10.3390/sym15010152.

**[19]** 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, December 2023, doi:10.31449/inf.v47i10.5395.

**[20]** C. Cremers, "Scyther User Manual", 2014, p. 52, [Online]. Available: mailto:https://www.scribd.com/document/510869159/scyther-manual.

**[21]** M. Faheem, H. Kuusniemi, B. Eltahawy, M. S. Bhutta and B. Raza, "A Lightweight Smart Contracts Framework for Blockchain-Based Secure Communication in Smart Grid Applications," *IET Generation, Transmission & Distribution,* vol. 18, no. 3, pp. 413-652, January 2024, doi:10.1049/gtd2.13103.

**[22]** S. A. Salman, S. Al-Janabi and A. M. Sagheer, " A Review on E-Voting Based on Blockchain Models," *Iraqi journal of science*, vol. 63, no. 3, pp. 1362-1375, March 2022, doi:10.24996/ijs.2022.63.3.38.

**[23]** F. Hofmann, S. Wurster, E. Ron and M. B. Schwafert, "The Immutability Concept of Blockchains and Benefits of Early Standardization," *2017 ITU Kaleidoscope: Challenges for a Data-Driven Society (ITU K),* Nanjing, China, 2017, pp.1-8, doi:10.23919/ITU-WT.2017.8247004.