International Journal of Research in Engineering and Science (IJRES)
ISSN (Online): 2320-9364, ISSN (Print): 2320-9356
www.ijres.org Volume 13 Issue 4 ǁ April 2025 ǁ PP. 10-15

Enhancing the Traceability and Security of Bank Transaction using Elliptic Curve and Chaotic Map

Adeolu Seun Obamehinti[1], Adekunle Eludire[2], Araoluwa Simileolu Filani[3], Fadare Oluwaseun Gbenga[4]

[1]*Joseph Ayo Babalola University, Nigeria, lebiobamehinti@gmail.com*
[2]*Joseph Ayo Babalola University, Nigeria, aaeludire@jabu.edu.ng*
[3]*Joseph Ayo Babalola University, Nigeria, asfilani@jabu.edu.ng*
[3]*Joseph Ayo Babalola University, Nigeria, fadareadelodun90@gmail.com*

Abstract
Bank transaction security is one area in the banking sector that is very crucial. Over the years due to rapid increase in fraudulent activities perpetrated, by unscrupulous element has made the existing method of security architecture used by banks to protect every transaction initiated to be at risk. The banks are the actors who have overall responsibility for financial transaction, thus placing them in a position of responsibility for realizing the traceability demands. Hence the need for chaotic map and elliptic curve to serve as a security mechanism for every transaction that is performed in the bank sector.

Keyword; *Elliptic curve, Chaotic map, traceability, bank, algorithm*

Date of Submission: 27-03-2025 Date of acceptance: 07-04-2025

I. Introduction

Traceability has been acknowledged as an effective tool for achieving sustainability objectives in a number of businesses. This is caused by the constantly increasing demand from consumers for responsibly sourced and produced products together with the obligations by regulatory framework to improve transparency and tracking in supply chains (Anderson, 2017). Although other sectors, industries, countries, and regions have already started implementing traceability, bank sector are yet to tap into it despite their massive numbers and assimilation in the global economy. The traceability system of blockchain technology also facilitates the detection of fraud and secures the integrity of the supply chain globally (Agungi, 2022). In the context of blockchain technology, this study seeks to understand the traceability of bank transactions in other to prevent the menace of fake alert. Using Nigeria as a case study based on existing information technology-based systems and leverage on blockchain technology to provide a traceable transaction system in the bank sector. This research looks into what various sectors used different technologies for traceability, and its limitations and the need to adopt blockchain technology for traceability of transactions. Blockchain smart contract will serve as the driving force in the area of policy guidance in the transaction network. Smart contract is an executable code which helps to secure every transaction, that is carried out in the blockchain network system. The agricultural sector has already proposed a number of blockchain-based solutions to livestock data management Reilly (2016) along with food traceability and safety (Das, 2018). However, this research mainly delves into how banks can implement blockchain technology-based traceability in their business context by identifying and exploring key factors that are crucial to the effective application of the systems in the traceability of transactions.

The prevailing challenge of fake alert have been on for over the years and has driven many to depression or loss of businesses and this is largely caused by lack of traceability of transactions. After extensive review of related approaches to tackling this issue which has not properly addressed the challenges, it therefore drives the motivation to provide a solution to fake alert transactions.

Traceability of bank transactions in Nigeria have been challenging over the years, a lot of fraudulent activities are being carried out on transactions and this is largely due to lack of effective traceability of transactions from the source to the destination account. The predominant fraud that poses a threat to financial institutions at the moment is the issue of fake alerts.

According to Omogbolahan (2023) found that a Point of Sale (PoS) customer lost over 200,000 naira due to fake alert. Furthermore, Ayobami et al. (2022) found that, between 2014 and 2017 the financial institution has lost over 3 billion naira due to fraudulent activities perpetrated by fraudsters.

II. Literature Review

According to Tschorsch (2016) chaotic maps can not only process currency transactions but can also ensure that transactions comply with programmable rules in the form of "smart contracts". All these transactions could be validated between parties who fully trust each other without relying on a trusted middleman". Honduras government has set up all land records on the Blockchain. Whenever there is a change of ownership of a property, it gets recorded openly (Karamitsos, 2018). The tamper proof and straightforward of the Blockchain technology make it fit for records, create transaction and keep record of such transactions. Presently, the majority of the establishments, such as firms, have received elliptic innovations to keep up discreet and secure databases. Chaotic map can be utilized as a legal official administration to make it simple and modest by connecting some required information with the record of transaction. Kosba (2016) noted that" There are different type of consensus mechanism, the most outstanding is the Proof-of-Work (PoW). it requires solving the problem of a computational procedure, like discovering hashes with explicit examples, for example a main number of zeroes Palang (2021), found to guarantee verification and undeniable nature". In the case of power of stake, it is not determined by their mining power, Proof-of- Stake (PoS) conventions split stake block according to the present abundance of miners (Paul, 2019). Thus, the determination is more pleasant and keeps the wealthiest member from overwhelming the system. Numerous elliptic, for example, Noyes (2016) found that ethereum are bit by bit moving to Proof of Stake (PoS) which usually requires miners to use high computational power and because of the noteworthy reduction in power utilization and improved adaptability. (Zhao, 2019). An extra layer, the compute interface, permits chaotic map to offer greater usefulness. For all intents and purposes, a elliptic stores a state which comprises for example of the considerable number of exchanges that have been made by the clients, in this way permitting the count of every client's equalization. Notwithstanding, for further developed applications we have to store complex states which are refreshed powerfully utilizing disseminated figuring, for example states that move starting with one then onto the next once explicit criteria are met. A unified chaotic is a cross breed mix of public and private elliptic (Buterin, 2015). In spite of the fact that it has comparable versatility and security assurance level with private chaotic map, their difference is that it has a set of hubs, named pioneer hubs, is chosen rather than a solitary element to check the transaction record. This empowers a mostly decentralized plan where pioneer hubs can allow authorizations to different clients. Kraft (2016) found that on the grounds that, notwithstanding established highlights, for example, the proprietorship and the executives of the data shared in the elliptic, we consider highlights, for example, transaction endorsement time, or security perspectives, for example, obscurity. The chaotic map innovation is highly secured and autonomous and also keep record of the unique finger prints of a computerized resource without putting away the advanced resource. Glaser (2019) "highlights all banks are currently engaged in developing a vision of what this technology means for their business". (Agungi, 2022) discussed that in research and practice that the main parameters for elliptic implementations such as security, data privacy, and usability are subject to select the best algorithm to ensure consensus and validity. Tschorsch (2016) discusses proof-of-work approaches that require high levels of energy but guarantee relatively high levels of consistency and protection against forgery by any actor in the network for example, in bitcoin, compete against less costly ones. Such alternative approaches require a portion of a trust in some elements of the network, such as actors based on the resources they put at risk during validation for example, the proof-of stake or in the manufacturers of devices that are used to validate transactions for example, proof-of-elapsed time in hyper-ledger saw-tooth lake. For the design and deployment of elliptic implementations Noyes (2016) found that there are different selection criteria or parameters that are required to be considered while designing and deploying the implemented chaotic map.

III. Research Methodology

This chapter discusses the methodology that will be used to achieve the objectives of this research work. It explains the method approach and algorithm framework to be adopted in this research. The method and algorithms are explained in the subtopics. Steps Approach to the methodology adopted as it is shown in the figure 3.1 is stated below;

i. **Chaotic map/elliptic curve:** The chaotic map and elliptic curve provide double verification which is often use in blockchain system. The encryption and decryption will serve as a cryptographic form of security. Once the fourth stage is concluded, every transaction is recorded in the transaction hash value which is the next stage.

3.1 Algorithm 1: Registration Phase steps

i. Input: User Identity (UID); Public Key ($ß_{Ki}$); Low entropy password (LPW_i)
ii. Process: Registration phase
iii. The Authentication Server (AS_i) elects to employ Elliptic Curve by possessing the Banking server (BSi) and identifies base points $G1(x1, y1); G2(x2, y2); G(x, y); E(a, b)$

Mathematical equation for elliptic curve $y^2 = x^2 + ax + b$

1. **Login (Authentication) Phase**

i. The login phase or user authentication phase is the gateway of the proposed system which execute authentication Inspection for the entire incoming users.

ii. The authentication phase involves user id (Uid), Device Identity (DID); Authentication Server with Data Administrator, and Banking server (BS_i). In this phase, the user tends to succeed in the authentication phase by furnishing the user id (Uid) with the Low Entropy password (LPW).

iii. The system creates a strong password based on the User's Low entropy password and extracts the Device Identity (Did) to validate the user's authentication.

The pseudocode for the blockchain-based authentication phase is illustrated

Table 3.1. Acronyms and descriptions

Symbol	Description
B_{Ui}	Block creation for user (Ui)
AS_i	Authentication Server
D_{ID}	Device Identity
H_{Bui}	Hash value generated for user
$H_{Bui(R)}$	Hash value registered for user
R_{KB}	Registration Key
B_{Ui}	Block creation for user (Ui)
SK_i	Session Key
T_1 — T_4	Time Stamp
N_1 — N_3	Nonce
E	Encryption
D	Decryption
SFA_{Ui}	Second Factor Authentication of User (U_i)
$CSFA_{Ui}$	Cipher Text of User's Biometrics Identity
$PSFA_{Ui}$	Plain Text of User's Biometrics Identity
F_{Ui}	Extracted Feature of User U_i
F_{UiR}	Registered Feature of User U_i

3.2. 1. Algorithm for Login (Authentication) Phase

Algorithm 2: Login (Authentication) Phase

1 Input: User Identity (U_{id}) Low Entropy Password (LPW)
2 Output: Session Key (SKi)
3 Process: Authentication Phase
4 The user provides the user identity (U_{ID}) along with the low Entropy Password (LPW)
5 $CA_i = E_{pKi}(U_{ID}, LPW, D_{id} || T_3)$
6 The Network administrator verifies the matching of the basic authentication credentials
7 if (U_{id}) = U_{IDR}
8 {
9 If (LPW -= LPW_R)// Perform Credential matching
10 Else
11 Deny login phase with report, "User ID not registered"
12 {
13 If (H_{Bui}= $H_{Bui\ (R)}$)
14 {

15 Deny login phase with report, "Password Wrong"
16 Session Key $SK_i = E_{\beta k \beta}[(r_i \backslash\backslash D_{ID} \backslash\backslash U_{ID}) \| N_2]$
17 else
18 {
19 Requesting for second Factor Authentication (SFA_{Ui})
20 SFA_{Ui}: ($CSFA_{Ui}$) = $E_{CMCD}(FU_i[B_{Ui}], N_3)$ // Chaotic Map confusion and diffusion of Biometric authentication
21 SFAUi: (PAFuI) = d_{cmcd} (FUi[B_{UI}], N_3)
22 if ($F_{Ui} = F_{UR}$)
23 Update hash value in blockchain
24 Session key $SK_i = E_{pKB}[r_i || D_{ID} || U_{ID}), N_2]$
25 Access Granted
26 Else
27 Deny login request
28 End if
29 End if
30 End if
31 End if
32 End

The mathematical equations for chaotic map; 1

$$x_n + 1 = -m(x_n + 2/m) \qquad 1$$
$$x_n + 1 = mx_n \qquad 2$$
$$x_n + 1 = -m(x_n - 2/m) \qquad 3$$

The user Ui on providing proper authentication credentials will be granted with the service. In turn, the observation of different service pattern from the users tends to variation in the hash value leading to the requisition of the Second Factor Authentication (SFA_{ui}) of the authenticated user.

3.3. Chaotic Map Confusion and Diffusion Process

i. The chaotic map algorithm is employed in the proposed system of securing the multi-factor authentication process. The deviation in the hash value leads to the second factor authentication, to which the user has to provide the biometric identity.
ii. The input biometric identity is treated with chaotic map confusion and diffusion process to misalign the features of the input biometric identity. In turn, the banking server (BSi) performs the reverse decryption process Of Chaotic map diffusion and confusion process to retrieve and to perform second factor authentication verification process.
iii. The confusion and diffusion process are depicted in Figure 3.4. The confusion process involved "m" number rounds and diffusion process with "n" rounds of rotation with chaotic code generated by the chaotic code generator. The secret key for the encryption is the user's private key (pKi) while the secret key for the decryption is the private key of the banking server.
iv. After the process of confusion and diffusion, the resulting pattern is again rotated for "x" rounds for further rotation of the input plain biometric feature. The purpose of executing this confusion and diffusion process is to safeguard the biometric features during the transmission in the insecure cloud channel.
v. The encryption and decryption process are bounded to 256 bits. The decryption process is a reverse process of encryption in which the diffusion process is followed by the confusion process with "n" and "m" number of rotational rounds respectively. The algorithm for chaotic map encryption and decryption process is illustrated in Algorithm 3 and Algorithm 4 respectively.

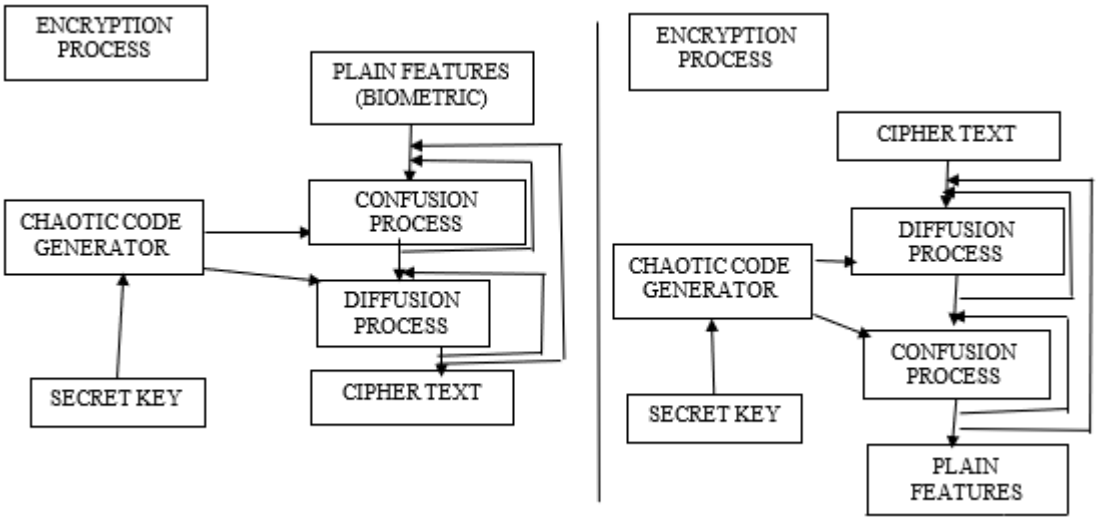

Figure 3.1 Chaotic Map Confusion and Diffusion Process (Jude, 2021)

Plain text is inputed as biometric feature which in turn generation and out of cipher text and the process this takes to work is the confusion and diffusion process. The chaotic code generator generates a unique security key for the blockchain user which serve as its pass-code. These procedures and repeated for double verification purpose as it is indicated in figure 3.4. the algorithm below further indicates how the chaotic map confusion and diffusion process works.

Algorithm 3: Encryption Process
1. **Input**: Plain Text (Biometric features)
2. **Output**: Cipher Text
3. **Process**: Chaotic Map Confusion and
Diffusion (Encryption)
4. procedure Confusion process
5. $F[X, Y]_{ixj-} = Bakersmap(\dot{p}_{Ki}, x_i, y_j)$
6. for j=1 to m; j=1 to n
7. do
8: x =X(ι) and y =Y(j)
9: C1 = swap[I(x, y)and *I*(i, j)]
10: end for
11: Close
12: procedure Diffusion process
13: $F[X,Y]_{ixj}$ = Bakersmap(pKi, Xi', yj')
14: for i=1 to n; j = 1 to m
15: do
16: x=X (*ι*) and y=Y (j)
17: C2=mod[X(i-1), Y(j - 1), 255]
18: end for
19: Close
20: procedure Rotation
21: $C(i, j) = mod[x \oplus C_1 \oplus C_2), 255]$
22: CSF A_{ui} C(i, j) // Cipher Text
23: end

Algorithm 4 Chaotic Map Decryption Process
1 : Input: Cipher Text
2: Output: Plain Text (Biometric features)
3: Process: Chaotic Map Confusion and Diffusion (Decryption)
4: procedure Diffusion process
5: $C[X, Y]_{ixj}$ = Bakersmap(pKUi, Xi', yj')
6: for i=1 to n; j = 1 to m
7: do

8: x = X(i) and y = Y(j)
9: P_1 = mod[X(i-1), Y(j - 1), 255]
10: end for
11: Close
12: procedure confusion process
13: $C[X, Y]_{ixj}$ = Bakersmap(pK_{UI},x_i, $y_{j)}$
14: for i = 1 to m; j= 1 to n
15: do
16: x = X(i) and y = Y(j)
17: P_2 = swap[*I*(x, y) and *I*(i, j)]
18: end for
19: close
20: procedure Rotation
21: P(i, j) = mod[x $\oplus P_1 \oplus P_2$), 255]
22: PSF A_{ui} P(i, j) // Plain Text
23: end

References

[1]. Adekanmbi.O. (2022) SMS Fraud Detector and Instant Fraud Prevention Call Alert International Journal of Information Science. 2(8) 1 12.
[2]. Agungi, M. W. (2022). The business blockchain promise traceability: practice, and application of the next Internet Technology. John Wiley & Sons, Inc., 128 (2), 1 16.
[3]. Anderson S. A. (2017). The traceability of fees payment through banks by student to various institutions. International Journal of Information Science. 275 (1), 1 12.
[4]. Atzori (2016). Blockchain bad architectures for the internet of things. Springer.
[5]. Azaria, A., Ekblaw, A., Vieira, T., & Lippman, A. (2022). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd International Conference on Open and Big Data 12(25) 1. 12
[6]. Azubuike, O. S. (2019). Banking sector a critical sector addressing the bottle necks. International of Advanced Trends in Computer Science and Engineering. 4 (9).
[7]. Bracci, M. E. (2021). Smart contracts: terminology, technical limitations and real-world complexity", Law, International Journal of Innovation and Jude, k. D. (2020). PayPal transactions effective towards payment to various sectors. International Journal of Information Science and Computing. 2(21) 1 13.
[8]. Karamitsos, I. P. (2018). Design of the blockchain smart contract; A use case for real estate. International Journal of Management Information Technology and Engineering. 8(4) 1 6.
[9]. Kosba, A. M. (2016). The blockchain model of cryptography and privacy preserving smart contracts. Proceedings of IEEE Symposium on Security and Privacy. 6(2) 1 18.
[10]. Kraft, D. (2016). Difficulty control of blockchain based consensus systems: peer to peer network and applications.
[11]. Miorandi, D., Sicari, S., Pellegrini, F.D. and Chlamtac, I. (2021) Internet of things: vision, applications and research challenges. Ad Hoc Networks. 10(7) 1497.
[12]. Oluwafemi, O. Yisa, O. (2020) Mobile spamming in Nigeria: Pirical Survey. International Conference on Cyberspace. https://doi.org/10.1109
[13]. Paul. (2019). towards a more democratic mining in bitcoin.
[14]. Presley, M. S. (2021) Understanding modern banking ledgers through blockchain. IEE.
[15]. Reilly, W. C. (2016). New kind on the block a strategic archetypes approach to understanding the blockchain. Dublin: 37th International Conference on Information System. 6(2) 1 19
[16]. Skarmeta, A. F. (2019). A decentralized approach for security and privacy challenges in internet of things. IEEE World Forum. 8(2) 1 12
[17]. Tom Wilson & Marc Jones, (2021) China proposes global rules for central bank digital currencies, Reuters https://www.reuters.com/article/us-cenbanks-digital-china-rules.
[18]. Tschorsch, F. A. (2016). The future of blockchain technology.
[19]. Weele, V.A. (2018). Cryptocurrency, smart contracts and artificial intelligence: AI Matters. Springer. 7(4) 1 12.
[20]. Urowayino Warami. (2022). Nigerian banks lose N12.30bn to fraud in 4 years NIBSS. https://www.vanguardngr.com/2018/06/nigerian-banks-lose-n12-30bn
[21]. Zhao, K. A. (2019). The blockchain model of cryptography and privacy preserving smart contracts. Proceedings of IEEE Symposium on security and privacy. 128(4) 1. 16 Technology. 269 (3) 1 14.