KTREND JOURNALS
Ktrend - International Journal of Computer Science and Artificial Intelligence (IJCSAI)

DOI: 10.5281/zenodo.20735327 **Volume:** 1 **Issue:** 1 **ISSN:** 3141-643X

Exploring Cryptographic Requirements of eNaira as Nigeria's Digital Currency

Saidu Isah Abubakar*, Buhari Mamuda, Sadiq Shehu

Department of Mathematics, Sokoto State University, Nigeria

Corresponding Author: siabubakar82@gmail.com

Abstract

The use of cryptographic algorithms in providing privacy and integrity of data to central bank digital currencies have been considered to be the most important infrastructure to be deployed by any nation as a requirement for safeguarding the system from cyber security attacks. This paper explores the goals of information security in relation to security of eNaira as Nigeria's digital currency, the architectural infrastructures/designs needed to be embedded in the eNaira system, and cryptographic algorithms required to make eNaira system tamper-proof and protect users' funds from double spending, counterfeiting and depend the eNaira system from security threats and malicious attacks such as side-channel, denial of service, persistent network attacks such as botnets and DDoS, spoofing, social engineering, information disclosure, repudiation among others.

Keywords: Cryptographic schemes, algorithms, eNaira, digital currency, CBDC, security threats, attacks,etc.

1 Introduction

Central Bank Digital Currency (CBDC) is one of the digital currencies that have emerged as a result of significant innovations and technological advancement in the financial system which offers efficiency in transaction. As technology evolves and advances, it is pertinent for central banks to continue to adapt and take advantage of these opportunities provided by new technologies. One of such new technologies is the Central Bank Digital Currency (CBDC). CBDC is a digital or fiat currency issued by central banks as a legal tender in order to provide financial inclusion and control the excessive use of cryptocurrencies. As more central banks begin researching for the possibilities of issuing a CBDC, there is a common concern around the

globe about its privacy. CBDC acceptance will therefore depend in part on users' trust in the privacy offered by CBDC. However, the notion of privacy is not consistent across the world and privacy preferences, policies and laws vary significantly by culture and region, [1].

The key motives of issuing retail CBDC include broadening financial inclusion, reducing the vulnerability of counterfeiting in paper currency, discourage illicit activity, enhancing government's ability to revenues and tax more efficiently, ensuring compliance with anti-money laundering/combating financing of terrorism and increasing efficiency and stability of payment systems. A well-functioning CBDC will require an extremely resilient, secure and performance new infrastructure with the ability to onboard, authenticate and support users on massive transactions across network. A CBDC is expected to address an innate tension between privacy and transparency, protecting user data from abuse while selectively permitting data mining for end-user services, policy makers, law enforcement investigations and interventions, [2]. The global adoption of digital currencies is rapidly increasing, with nearly 10,000 different digital currencies valued at over US$1.90 trillion as of March 2022. India leads with a 29% adoption rate, followed by Nigeria at 27% and Vietnam at 25%. As of November 2022, the global cryptocurrency market capitalization was US$1.01 trillion, with Nigeria having over 13 million crypto holders, [3].

Distributed Ledger Technology (DLT) has emerged as one of the transformational technologies which allows highly transparent, secure, tamper-proof transactions between parties and create trust and confidence even when parties have no reason to trust each other. As at the end of 2021, 90% of the 81central banks in Europe began to explore the CBDCs and by late 2023 over 130 countries across the globe are investigating CBDCs with the aim of modernizing their payment systems, promote financial inclusion and reduce the dominance of cryptocurrencies, [3,4].

Nigeria was the first country in Africa to explore CBDCs and implemented its digital currency known as eNaira. Nigeria's CBDC called eNaira was launched by Central Bank of Nigeria (CBN) in October 2021 as a digital currency with the aim of improving the availability and usability of central bank money, supporting a resilient payment system, encouraging financial inclusion, reducing the loss of processing cash, enabling direct welfare disbursement to citizens, increasing revenue and tax collection efficiency, facilitating Diaspora remittances and reducing the cost of cross-border payments. It gained acceptability during its early stage as of the launch, it was reported that approximately 840,000 people downloaded the e-Naira application with 270,000 active wallets, and transaction volumes exceeding N4.40 billion, [4,5].

In designing the eNaira, the CBN is expected to take into considerations four key design elements based on the recommendations from the World Economic Forum, Bank of International Settlements (BIS) and the Coalition of Central Banks on CBDC implementation. These design elements are architecture, infrastructure, access and inter linkages. The e-Naira infrastructure is based on DLT which support the two-tier model architecture which the CBN has adopted, [6]. Also, it was reported that cryptographic technology is the key to the technical security and credibility of CBDC. He opined that, cryptography should be used in the design of CBDC presentation format to ensure that it can be circulated and stored and cannot be forged, double-spend or repudiated by unauthorized party, [7].

Cryptographic primitives are mathematical algorithms used to ensure secrecy and integrity of data in the presence of eavesdroppers. They also concern themselves with three purposes of authentication, confidentiality and integrity of data. Based on the security needs and the threats involved, various cryptographic methods such as symmetric key cryptography, public-key cryptography, and hash functions can be used during transportation and storage of data. In addition, a homomorphic encryption allows various computations to take place on encrypted data without requiring the data to be decrypted for processing. It has been said that, no digital currency will remain operable and in use for long without satisfying the three fundamental properties of information security which include Confidentiality, Integrity and Availability (CIA). Interestingly, with advancement of cryptography, newer systematic and mathematical methods to achieve privacy, ensuring data reaches its destinations without being altered by unauthorized parties (integrity) and responding to users promptly when requested to retrieve data or perform some actions (availability) are being developed using cryptographic techniques, primitives and protocols. The securities of all these cryptographic schemes relies on the difficulties of solving complex mathematical problems.

Security is considered to be one of the most crucial and important factors in determining whether CBDC will work properly and be widely accepted by the populace or not. To win people's trust and confidence, the system of eNaira shall be able to resist hackers' attacks and be anti-counterfeiting. Distributed ledger technologies and other cryptographic methods have been considered by many researchers and system developers because they can reduce the risk of a single point of failure and make the CBDC system resistant to collapse, hackers attacks, physical damage and natural disasters. It can also support decentralized digital management to prevent large-scale data leakage in the system. Also, eNaira as Nigeria's CBDC is expected to rely on cryptographic schemes such as asymmetric cryptography and hash function to secure transactions in digital channel by creating a secure, immutable and untamperable records on decentralized ledgers. Mathematical techniques are also used for Privacy-Enhancing Technologies (PETs) to balance user privacy with Anti-Money Laundering (AML) and Counter Terrorism Financing (CTF) regulations; allow a secure offline transactions and pear-to-pear transfer without too much reliance on the system, [8,9,10].

Research on eNaira as Nigeria's digital currency have been conducted and reported by many researchers. Majority of these researches centred on the monetary policies, financial inclusion, economic gains, opportunities and risks/challenges of adopting eNaira and acceptability/adaptability of eNaira. A survey was conducted on factors that determine the adoption of eNaira in Nigeria as reported in [11]. One of their findings was the fear of fraudsters and online crimes (cybercrimes) by Nigerians as a result of security threats which posed a challenge for the wider adoption of eNaira as a digital currency issued by the Central Bank of Nigeria (CBN). In another research, the author reported on the eNaira as a tool for financial inclusion where he investigated the challenges of implementing the digital currency in Nigeria, [12]. Similarly, another research carried out its investigation on the determinants of intention to adopt eNaira as digital currency in Nigeria for financial transactions where one their findings was lack of trust (insecure digital channel) by Nigerians as a results of fraudsters and cybercrimes, [13]. Furthermore, a research was conducted research on the evaluation of people's perception,

knowledge and adoption of eNaira in rural communities as reported in [14]. Many researches on eNaira can be found in [15,16,17,18].

From the literature on eNaira as captured above, it was observed that there was scanty research focusing on exploring the cryptographic schemes, primitives and protocols of eNaira as a Nigeria's digital currency issued by the CBN. Most of the researches reported in their findings that people's fear on the activities of hackers and other cybercrimes as one the major challenges facing the adoption, operations and effective utilization of the eNaira system. In order to retain public trust, have wider acceptability and adoption of enaira, this research is aimed at exploring the cryptographic requirements of eNaira as its relate to the security of enaira which must be built on the concepts of three goals of information security which are: Confidentiality, Integrity and Availability (CIA). The security of CBDC is built on advanced mathematical principles, basically on number theory, cryptography, algebra and distributed ledger technologies. These mathematical formulations ensure that enaira is privately secured, tamper-proof while facilitating verifiable transactions by the central bank without intermediaries/third parties, [14].

This paper is motivated by the scanty works on cryptographic requirements of eNaira as Nigeria's digital currency and it is aimed to exploring these cryptographic algorithms and their functions/roles in providing confidentiality and integrity of data in the eNaira system in order to address the problem of lack of trust and users fear of potential attackers in the system. The paper is organised as follows. The goals of information security as its relates to the security of eNaira as a Nigeria's CBDC is contain in Section 2. Framework of its architectural components, and cryptographic schemes/algorithms and their roles in relation to privacy of eNaira are captured in Sections 3 and 4 respectively. Section 5 of the paper discusses security threats associated with eNaira and finally conclusion offers solutions on how to leverage these cyber threats.

2 Goals of Information Security as it Relates to eNaira Privacy

The major goals of information security are Confidentiality, Integrity and Availability (CIA). For any CBDC system including eNaira to be considered secured, its security architecture must be designed using cryptographic schemes while taken into consideration the CIA. These goals can further be explained below:

i. **Confidentiality:** This is one of the goals of information security designed to provide privacy for transactions, holdings and identities in digital eNaira. Information shall be kept secret and shall not be revealed to any unauthorized party. Leakage of confidential information increases the severity of a breach dramatically. Requirements such as Know Your Customer (KYC), Anti-Money Laundering (AML) and Anti-Terrorist Financing (ATF) may entail storing and linking Personally Identifiable Information (PII) to value stores and transactions.

ii. **Integrity:** This is another goal of information security that provides security by protecting the system against counterfeiting and double-spending of enaira in digital transactions.

It also ensures correctness and finality of all transactions. Counterfeiting of enaira can be stopped/eliminated with the use of digital signature while tamper-resistant hardware can be deployed by Central Bank of Nigeria in local store-of-value devices to avoid double-spending of enaira.

iii. **Availability:** This is one of the CIA triad that provides timely and reliable access of data, systems and resources to authorized users of eNaira when needed. This feature will strengthen the ability of eNaira design structure to withstand large-scale cyber-attacks. Disruption such as botnet attack, Distributed Denial-of-Service (DDoS) may be temporarily limited or disable access to the system. Standard and cryptographic cyber security techniques such as digital signatures, hashing and use of certificates can be re-enforced in public end-points and connected systems to prevent and cushion the impact of such attacks.

3 Framework of Security Architectural Design of eNaira

Furthermore, it has also been reported by [18, 7] that, while designing CBDC-eNaira system, the central bank must put into considerations the following components of security architecture in order to protect the system from intruders:

Layered defense: This design component enables eNaira system to accommodate and implement multi-factor authentication of the stakeholders, comprehensive cybersecurity framework and ensure regular system audits.

Identity management: The eNaira system shall establish security identification protocols in order to balance privacy with regulatory requirements.

Immutable ledger: The eNaira system design shall use technology that will prevent the system from intruders and eavesdroppers by ensuring that transaction records cannot be tempered with or deleted. This can be achieved by using strong encryption schemes and DLT.

Similarly, for security analysis, eNaira as Nigeria's CBDC system shall have the following two sub-functional components:

i. **The front-end component:** This component shall consist of a dedicated device, a software application running on a mobile app or a desktop platform, a web interface or a combination of them.

ii. **The back-end component:** This component may consist of a secure, private and resilient data storage system; a set of public-facing access points for connection to front-end component or a supporting and redundant components such as firewalls and backups.

4 Cryptographic Schemes/Algorithms

Cryptographic schemes are built using mathematical formulations, algorithms and techniques to provide security to information in digital communications. These schemes form the basis

for encryption methods, authentication, digital signature, key exchange and other mechanisms for information security which ensure privacy, integrity, authentication, availability and non-repudiation of information in the presence of unauthorized users. The security architecture of eNaira as Nigeria's CBDC shall be designed/built using combinations of cryptographic schemes for it to withstand the security threat of cybercrimes and other related attacks. These cryptographic schemes are as follows:

Symmetric encryption: This is a cryptographic algorithm that uses one key (private key) for both encryption and decryption of data. It provides end-to-end encryption and the trusted parties will agree on the use of one secret key which cannot be disclosed to anyone else. Examples of symmetric cryptographic include AES and DES. This algorithm is applicable mostly in data protection on media, VPN and file encryption.

Asymmetric encryption: This is one of the cryptographic algorithms that uses two keys where one is a public key and the other is a private key. The public key is always published for public use while the private key is kept secret. The private key is used to authenticate the user by signing while the public key is used to validates the user. This type of encryption algorithm is used for digital signatures which are intrinsic to any digital money asset and is the most widely used scheme currently by the leading cryptocurrency players and CBDCs as well. The eNaira system is expected to have these mechanisms of authenticating users to ensure privacy and built user's trust and confidence in adopting the eNaira wallet. In this algorithm, in-coming payments require the sender to know the recipient's public key which is always known as address. Conversely, the out-going payments require a digital signature through the use of private/secret key and can be validated with the use of public key. This public key is always recorded in a register of CBDCs. Also, anyone can send a payment to someone else, but only the specified payee can have access to spend the money/funds received. The payee's assets are directly tied to their private keys and are always secret and confidential. Examples of this encryption algorithm include RSA, ECC, ElGamal, DLP, ECDSA, etc. It is the most widely used encryption algorithm by CBDCs, business entities, cryptocurrency players among other and is applicable for digital signature, secure data transmission, non-repudiation, among others.

Hash function: This is a mathematical function that converts any digital data into an output string with a fixed number of characters. It is a one-way function that takes inputs of variable lengths to generate output of fixed length which makes the transaction ledger tamper-proof. This type of cryptographic algorithms is used for fingerprinting data making it more difficult to temper with the input without anyone noticing. It transforms arbitrary data into a fixed length fingerprint (inform of hash). It also ensures that records of transactions are not altered and any modification to the transaction data would result in a different hash. It is more applicable in data integrity verification and password storage. Examples of hash functions include SHA-256, SHA-3.

i. **Distributed Ledger Technology (DLT) and Consensus Algorithms:** DLT is one of the block chain technologies used by CBDCs to provide security in digital network. It was embedded using algebraic structures such as groups and fields to minimize simple points failures in distributed/decentralized ledger. While mathematical consensus algorithms

known as proof of works are designed and used to verify valid transactions and ensure only valid transactions are added to the ledger. This is used to protect double spending and counterfeiting of enaira as digital currency.

ii. **Zero-Knowledge Proof:** This is one of the mathematical encryption schemes that permits one party (a user) to prove to another party (a bank) of having enough balance in enaira wallet to complete a transaction initiated without disclosing the actual balance or identity of the user. It was built using advanced algebraic structures which make information mathematically irreversible. It works on four principles of completeness (witness) where the proofs works based on the secret data the prover possesses which makes the proof to be true/correct; the commitment where the prover undisclosed the witness and send the commitment; the challenge where the verifier sends a query randomly; and the response where the prover uses mathematical formulations such as modular arithmetic and elliptic curve to prove that the knowledge of knowing the witness without disclosing their identity.

Homomorphic encryption: This is one of the data protection encryption algorithms that allows processing of encrypted data without the need to decrypting it first. This ensures privacy of funds and enable the CBN to verify transactions conducted.

5 Security Threats Associated with eNaira

The eNaira as Nigeria's digital currency is vulnerable to face the following cyber security threats from attackers in their attempt to compromise the system and steal valuable information that might help them in having access to the system:

i. **Spoofing:** This is a malicious entity that pretends to be a legitimate user in violation of authentication.

ii. **Repudiation:** This is a threat where by the eNaira end-users could try spend their wallets in multiple places (double spending) as a digital counterfeiting. The eNaira portal/services may be spoofed by a malicious entity that a wallet connects to or is using as a relay to connect to a portal as a violation of non-repudiation.

iii. **Denial of service:** This is another type of cyber threat whereby malicious attackers could overwhelmed the eNaira system with requests, denying/preventing legitimate users having access to the services provided by the eNaira system. This could also be as a result of loss of funds through the use of damaged e-wallets. Similarly, insiders at the central bank could accidentally impact the system or make fraudulent transactions deliberately in violation of the availability as a security component of eNaira.

iv. **Authorization:** This is a form of threat whereby system operators and IT administrators trusted with the roles of having access to the system could freeze or withdraw funds from eNaira accounts without the consent of users which is an abuse of the trust reposed in them and a violation of authorization as one of the components of eNaira security requirements.

v. **Information disclosure:** This is another security threat whereby if an eNaira system collect large volume of data and does not provide privacy protection techniques/mechanisms which could be visible to system operators and if breached could lead to the disclosure of sensitive information that could be used by the attackers to compromise the system in violation of confidentiality as one of the components of eNaira security requirements.

vi. Persistent network attacks such as botnet and DDoS causing outage of critical services provided by the eNaira digital currency.

vii. Supply-side attacks against components used in infrastructure and end-user devices of the eNaira system.

viii. Side-channel attacks against end-users' devices and applications.

ix. Social engineering attacks against end-users of eNaira which can serve as an attractive avenue for organized crime.

6 Conclusion

The paper discussed goals of information security and their functions in relation to providing privacy to eNaira digital currency and cryptographic algorithms have been explained as the most essential components to be deployed by the CBN in order to ensure safety of users' fund in eNaira system. In other to protect the eNaira system from the security threats mentioned above, a combination of these algorithms need to deployed to give the best security in the eNaira ecosystem. Also, long and sufficient hashes should be used to protect assets from being stole while at rest in the eNaira wallets. Similarly, digital signature should be used to authenticate the tokens to be used through proof of ownership from the sender and wallet certificates are also used to ensure the authenticity of both the sender and the receiver as these certificates contain some identifiers which are derived from public key infrastructure as operated by the central bank.

References

[1] Privacy and Confidentiality options for Central Bank Digital Currency: Digital Currency Governance Consortium White Paper Series November 2021 published by World Economic Forum.

[2] Implementing CBDC: Lessons learnt and key insights policy report: Central Bank Digital Currencies Working Group (CBDC WG) October 2020 published by CEMLA FINTECH FORUM.

[3] Ozili, Peterson K. (2023), Using e-Naira CBDC to solve economic problems in Nigeria, Munich Personal RePEc Archive (MNPR), Online at https://mpra.ub.uni-muenchen.de/118805/ MPRA Paper No. 118805, posted 12 Oct 2023 11:32 UTC.

[4] Sarah Allen, Srđjan Čapkun, Ittay Eyal, Giulia Fanti, Bryan A. Ford, James Grimmelmann, Ari Juels, Kari Kostiainen, Sarah Meiklejohn, Andrew Miller, Eswar Prasad, Karl Wüst, Fan Zhang (2020). Design choices for Central Bank Digital Currency: Policy and Technical Considerations, Nber working paper series, National Bureau of Economic Research 27634, 1050 Massachusetts Avenue, Cambridge http://wwwinber.org/paper/w27634 August 2020.

[5] Ozili, Peterson K (2021), Central Bank Digital Currency in Nigeria: Opportunities and Risks, https://mpra.ub.un-muenchenidee/11029/

[6] Katrin Tinn, & Christophe Dubatch (2020), Central Bank Digital Currency with Asymmetric Privacy. McGill University, Desautels Faculty of Management (Finance).

[7] Jushua Ebere Chekwuere (2021): The e-Naira - Opportunities and challenges. Journal of Emerging Technologies, 1(1), 72-77.

[8] Oladoja Timilehin (2024): Exploring Central Bank Digital Currency in India: Opportunities, Challenges, and Fintech Solutions Leveraging Cryptography.

[9] Ahmed, A. A., Saidu, A. A., & Kawure, J. H. (2022). The Roles of Central Bank Digital Currency over Physical Currency. International Journal of Social Science, Education, Communication and Economics (Sinomics Journal), 1(2), 75-92.

[10] Kopaliani, A. (2022). The Digital Currency Revolution: A Cost-Benefit Analysis and Future Manifestations. Available at SSRN 4215586.

[11] Y. Sani, A.A.Shinkafi, Abdullahi, M, S.S.Kura & L.Y. Saleh (2025). A Survey of Determining the Factors of eNaira Adoption in Nigeria. International Journal of Intellectual Discourse (IJID),8(4), 17-33, ISSN: 2636-4832.

[12] Uchenna Anyamele (2024). The eNaiar as a Tool for Financial Inclusion: Challenges and Recommendations. NESG Economic and Policy Review Journal H1, 22(1).

[13] Marzuk A. N. A. Lee, N.A. Abdullah (2026). Exploring Industry 4.0: Sentiments Analysis on Behavioural Adoption of e-Naira Digital Currency in Nigeria Using SVM and XGBOOST Models. International Journal of Electronic Commerce Studies, 17(1), 95-111.

[14] A.T Usman, M.B.Bello, S, Balarabe, S. Sanusi (2025). Factors that Determine the Adoption of Nigeria's Central Bank Digital Currency. International Journal of Research and Innovation in Social Sciences, IX(VIII), ISSNNO. 2425-6128, DOI:http://dx.doi.org/10.47772/IJRISS.2025.908000580.

[15] Abraham, A. (2021). Challenges of the proposed e-naira. Retrived at: https://guardian.ng/opinion/challenges-of-the-proposed-e-naira/

[16] Said, A. (2019). The Economic Impact of Digital Fiat Currency (DFC): Opportunities and Challenges.

[17] Bernard Epharaim (2026). The Nigerian eNaira and Financial Inclusion: A Model for Boosting Financial Participation of the Unbanked in Rural and Hra-To-Reach Areas. Journal of Accounts and Finance, 1(1), 10-18, DOI: http://doi.dg/10.69739/jaf.v1i1.1488

[18] Peterson K Ozili (2026). Important Considerations for Designing and Issuing a Central Bnak Digital Currency (CBDC) in Africa. International Journal of Blockchains and Cryptocurrencies, 7(1), 71-90.