Software Requirement Specification Document for Egyptian Central Bank Digital Currency CBDC

Karim Tarek, Haidy Abdelmonem, Mennah Ayman, Habiba Muhamed Hefny
Supervised by: Dr. Mohamed Elemam, Eng. Salma Osama

May 1, 2024

Table 1: Document version history

Version	Date	Reason for Change
1.0	14-Dec-2023	SRS First version's specifications are defined.
1.1	15-Feb-2024	Updated SRS version to address feedback from committees

GitHub: `https://github.com/Habiba93/EgyCoin_mobile_app`

GitHub: `https://github.com/Habiba93/First-Egyption-Central-Bank-Digital-Currency-EGCBI`

Contents

Abstract

As the whole world especially Egypt is marching toward digitalization. Egypt is now discussing the idea of digital currency, mainly the central bank digital currency like many other countries. In this paper, we are adopting two problem statements from Egypt's fintech website that we aim to solve using CBDC and blockchain technology. The project's main goal is to improve university students' payment experiences by implementing a safe and effective digital currency on the Ethereum blockchain, fee payment will be revolutionized and made transparent and safe. The paper explores the concept of Central Bank Digital Currency (CBDC) and its historical background. Additionally, it assists female merchants and business owners in obtaining currency so they can buy and sell without having to go through the trouble of physically visiting a bank.

1 Introduction

1.1 Purpose of this document

Egypt's mobile application Central Bank Digital Currency (CBDC) project, intended for online trade and financial activities, is intended to be fully documented in the CBDC SRS document. It describes the primary objectives, constraints, and features of the mobile application CBDC system, including regulatory compliance, transaction processing, user account management, and security measures. The text places a strong emphasis on crucial technologies that are necessary for the CBDC to be implemented and run successfully in Egypt, including blockchain architecture and encryption protocols.

1.2 Scope of this document

The document's scope is to discuss CBDC-like systems from an academic and business perspective. It also includes an illustration of the system's scope, context, and overview, as well as the goals of the CBDC mobile application and user characteristics. This document also covers the object-oriented class diagram, software and hardware limitations, data design, and functional and non-functional requirements of the CBDC mobile application and system. Lastly, the operational scenarios of the system and the precise development timeline for this mobile application are covered in this document.

1.3 Business Context

To reduce the dangers related to cryptocurrencies in the expanding economy, the Central Bank of Egypt (CBE) is investigating the introduction of a Central Bank Digital Currency (CBDC). There has been a noticeable advancement in the investigation of CBDC applications by CBE committees working with foreign organisations. To make online account creation easier, CBE has also implemented the Electronic Customer Identification System (eKYC). In addition, a digital bank licencing framework is being developed; the Egyptian Credit Bureau is being consulted over e-wallet borrowing; and a mobile wallet-based digital savings and lending programme is being introduced. Acknowledging the role that digital banks play in financial inclusion, CBE seeks to improve electronic banking offerings, draw in new clients, and significantly alter the financial landscape of the country. CBE seeks to eliminate the need for intermediaries and reduce dependency on cash and printed money[1]. In order to accomplish these goals, CBE's leadership in committees collaborating with important ministries and national agencies is highlighted in their most recent financial stability report. The journey of Central Bank Digital Currencies (CBDCs) around the world is depicted in the following Figures 1 and 2, together with a status tracker that offers visual insights into the evolution and present state of CBDC implementations globally. [2]

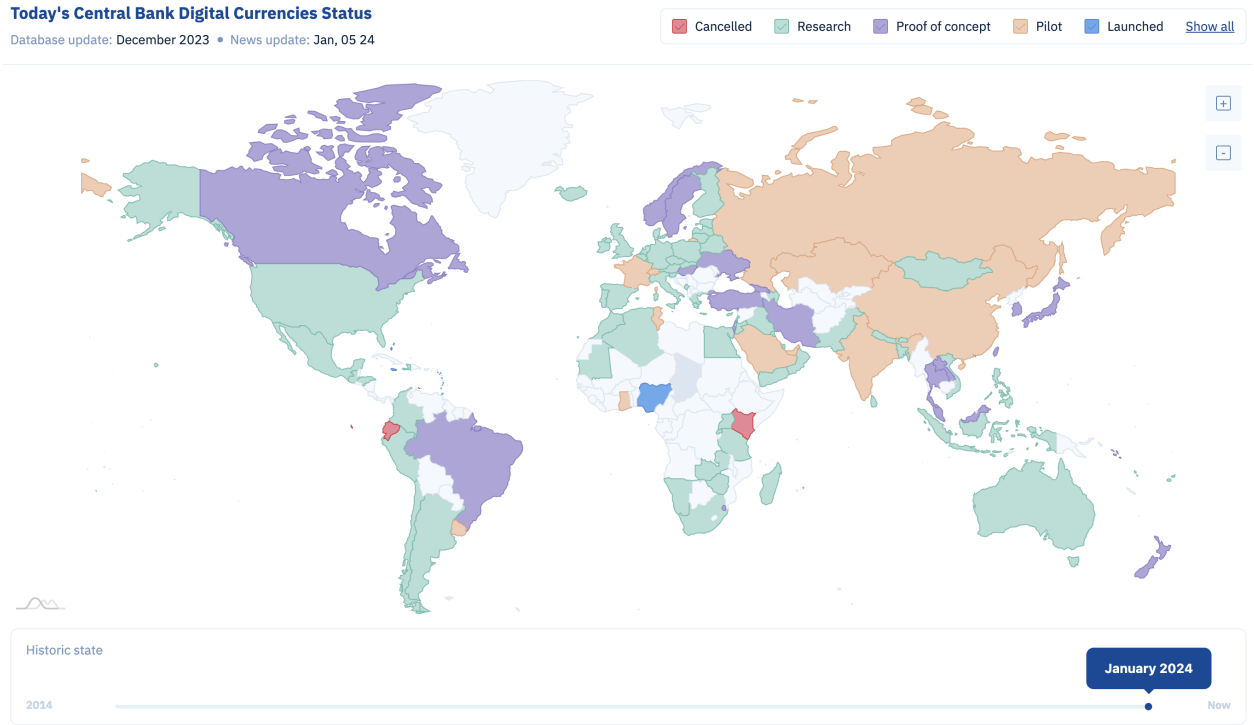

Figure 1: CBDC Tracker
[2]

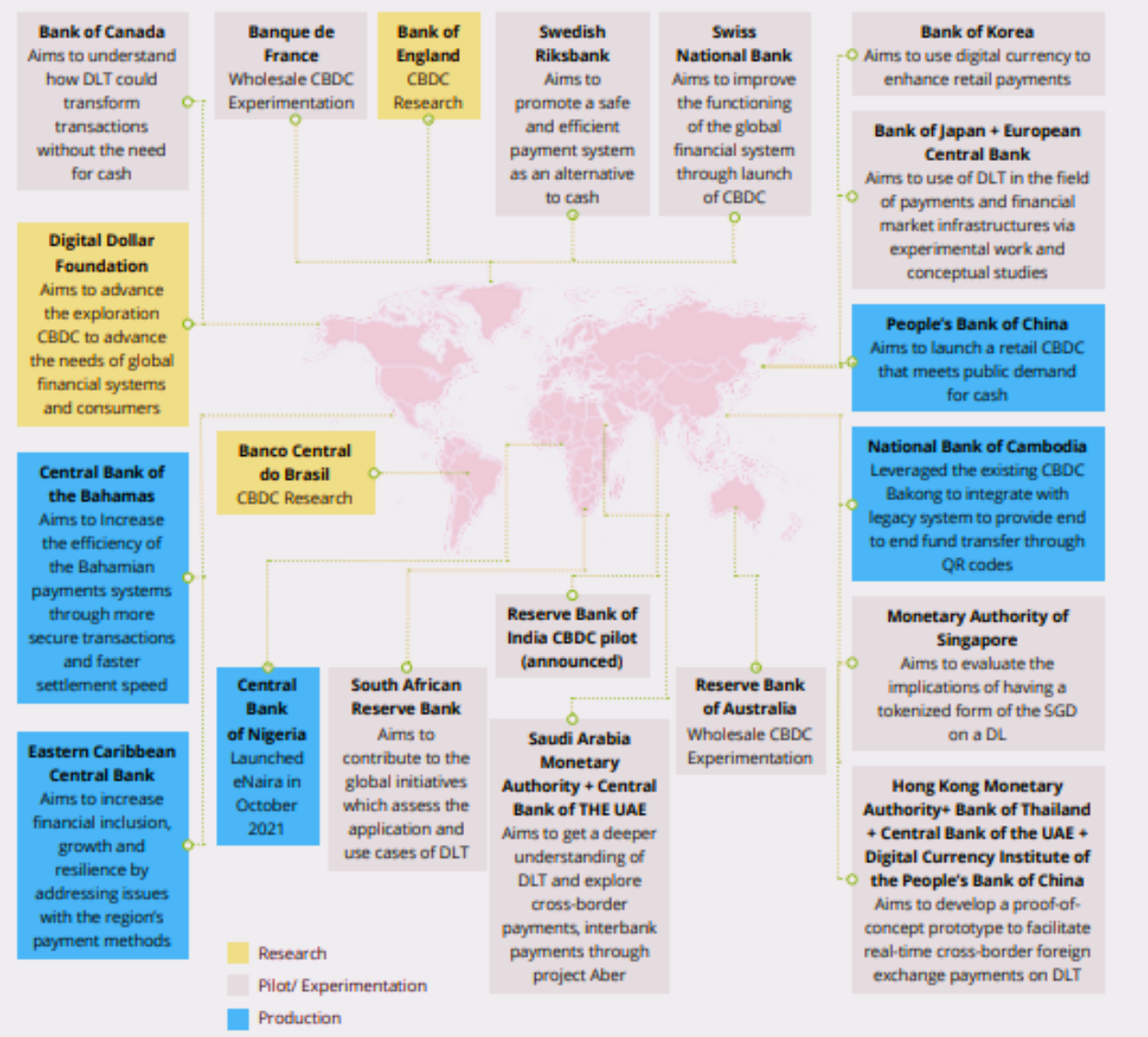

Figure 2: Global Snapshot of CBDC's Journey
[3]

2 Similar Systems

2.1 Academic

The paper [4], describes the evolution from virtual currencies to Central Bank Digital Currency (CBDC), highlighting the benefits of CBDC over physical currency. The study emphasizes how important it is for CBDC research to have an innovative technical model and an extensive theoretical framework. By combining account and UTXO schemes, the proposed CBDC scheme seeks to improve efficiency using the DPOS-BFT algorithm. To discuss the combination of UTXO and account schemes as shown in Figure 3, which represents the modular concept that splits the system into six levels to enhance regulatory oversight for central banks and governments, ensure effi-

cient transaction processing, and maintain reasonable construction difficulty and cost. The alliance chain design that has been suggested utilizes the use of a POA-PBFT consensus mechanism for secure block production, which optimizes data management and transaction performance. With a comprehensive storage plan and an operation mechanism that guarantees transaction security, the model improves security. Increased throughput, enhanced supervision, and controlled decentralization are the main features of this all-inclusive system. The hybrid approach shows a faster consensus speed of over 51.8%, a 16.4% processing rate improvement over UTXO, and a 26.3% increase in transaction processing speed via network design. The researchers should be more concerned about the limitations of smart contract installation and exploration. Further experiments are required to verify the optimization effect of the smart contract theory. The use of the system for national currency regulation and investment was also ignored, despite the fact that this is an important consideration in the field of digital currency systems.

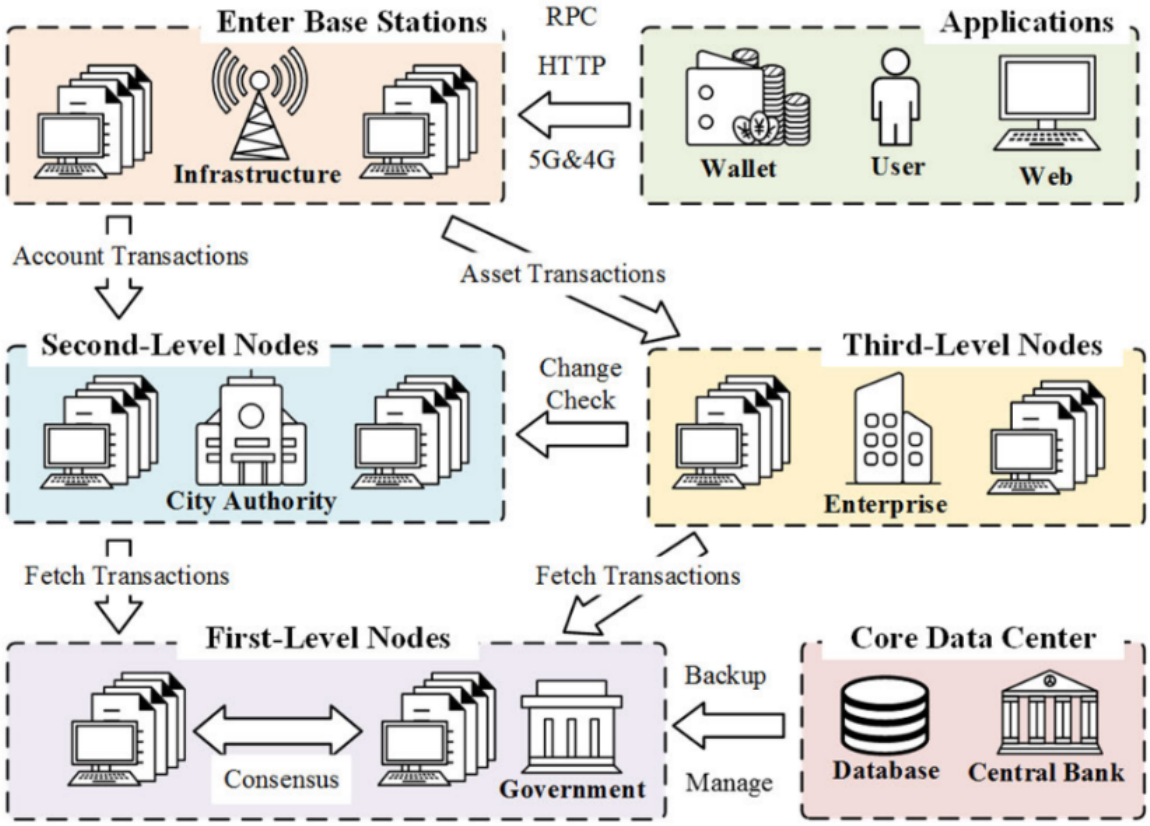

Figure 3: Overall architecture
[4]

In this article [5], The implementation of CBDCs requires central banks to overcome a number of important challenges, including the requirement for a sufficient technological infrastructure, assurance of privacy and security, the creation of a clear regulatory framework, interoperability, financial inclusion, public acceptance, international cooperation, and analysis of the monetary policy implications of CBDCs. They came to the conclusion that blockchain technology is not a viable option for financial infrastructures. With these prototypes, the researchers have experimented with various consensus and validation mechanisms. They have created prototypes of DNBcoin/Dukaton and RScoin, two blockchain-based CBDCs, also the researchers polled CBDCs from 65 central banks across the globe, Additionally, they have examined the trial and deployment of CBDC, as well as how monetary and financial concerns are handled by central banks using blockchain, the researchers have talked about difficulties and unresolved problems with blockchain-based CBDCs, they also have examined CBDC's requirement, scenarios, and possible blockchain uses in CBDC, and they have carried out an extensive examination of current blockchain-based CBDC programs. Researchers have reached that the two stages demonstrate how a blockchain-based wholesale payment system can help central banks by cutting expenses and increasing efficiency. Adoption of blockchain in CBDC design is still debatable, blockchain technology still faces numerous obstacles to be solved, including problems with scalability and security.

In response to the development of private digital currencies, this article[6] explores Central Bank Digital Currencies (CBDCs). It emphasizes how important central banks are to monetary policy and how important it is to reduce any possible instability caused by private digital currencies. With an emphasis on financial inclusion and the effectiveness of domestic payments, more than 70% of the central banks surveyed are investigating CBDCs. Through the organization and comparison of international wholesale CBDC studies as shown in Figure 4, the article functions as a complete resource. Twenty-six Central Bank Digital Currency (CBDC) experiments were originally found by the study using databases from WhitepaperDatabase.com, IEEE, BIS, WEF, and IACR. One experiment was screened and disqualified from the preliminary selection because of linguistic limitations. A secondary screening process was used on the remaining twenty-five papers for further evaluation. The research actively investigates Distributed Ledger Technology's (DLT) possibilities for Financial Market Infrastructures (FMIs), placing a focus on permissioned DLT platforms and teamwork. Nevertheless, arbitrary screening standards, a lack of empirical support, and a narrowly focused future orientation are possible critiques.

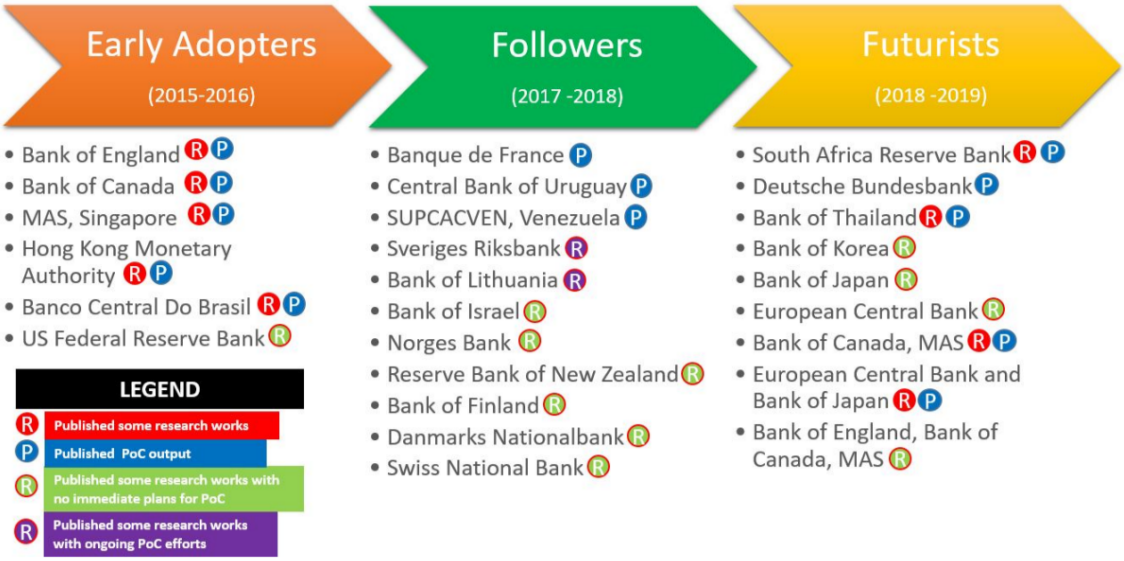

Figure 4: CBDC Experiment Landscape
[6]

2.2 Business Applications

2.2.1 Central Bank Digital Currency - the Digital Dirham (CBUAE)[7]

As part of the Central Bank Digital Currency Strategy, or Digital Dirham, mBridge will be soft launched to enable real-value cross-border CBDC transactions for the settlement of international trade.It will strengthen the UAE's payment infrastructure by providing additional robust payment channels and ensuring a resilient reliable financial system [8].Additionally, proof of concept work will be provided for bilateral CBDC bridges with India as well as for the issuance of domestic CBDCs for both wholesale and retail use.

2.2.2 Nigeria CBDC project (eNaira)[9]

Nigeria launched its CBDC project on October 25, 2021. President Muhammadu Buhari led the currency's launch, which goes by the name of the eNaira. The Central Bank of Nigeria issued the eNaira as legal tender. It is a central bank digital currency (CBDC) that is supported by the law and Nigeria's entire sovereignty.The eNaira is a liability of the CBN and may be transferred digitally to anyone in the world who has an eNaira wallet at almost no cost [10].It functions similarly to cash and is the naira's digital equivalent. The digital storage device that houses the eNaira is called an eNaira wallet. To access, store, and utilise eNaira, you must have an eNaira wallet. The eNaira serves as a medium of exchange, a store of value, and an accounting unit.

3 System Description

3.1 Problem Statement

When it comes to online payment for university fees experience, students may encounter various challenges. Students who are underserved by the banking system face difficulty paying their university fees. Moreover, for international students, exchange rate inconstancy and currency conversion fees may increase the cost of their tuition, which can lead to unforeseen expenses and make planning a budget for other expenses like tuition challenging.

3.2 System Overview

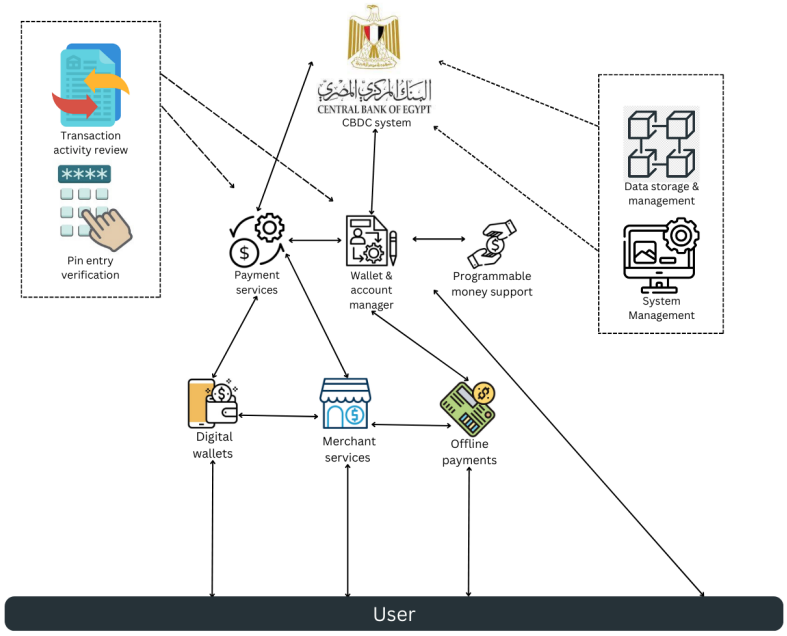

Figure 5: Overview diagram of the CBDC

A blockchain is a shared, unchangeable record where data of transactions is timestamped and kept in sequential blocks with distinct hashes. In the previous figure: Figure 5, the process outline provided in the schematic diagram illustrates how a Central Bank Digital Currency (CBDC) is transferred, providing a secure and effective means of conducting digital transactions. Users, commercial banks, the central bank, the CBDC wallet, and the underlying distributed ledger technology or blockchain comprise the key components. Starting with user initiation, the transfer process moves through ledger updates, validation, confirmation of transactions, and finalization. The diagram emphasizes how easily information and transactions flow between users and financial institutions by emphasizing their points of interaction. To ensure the integrity and confidentiality of the CBDC transfer mechanism, security features are incorporated. Authentication protocols and encryption are some of these features. Upon completion, the schematic diagram provides a visual representation of the CBDC transaction workflow that can be applied in presentations, documentation, and other contexts.

3.3 System Scope

1. Increased efficiency of transactions.
2. Reduced costs for the central bank (Decrease the cost of printing and circulating the physical money).
3. More secure for users.
4. Suitable for university students.
5. Easy for international transactions.

3.4 System Context

The context diagram for Central Bank Digital Currency (CBDC) shows the high-level connections and exchanges amongst important entities in the CBDC system. The CBDC system, which stands for the central bank-regulated centralized digital currency infrastructure, is at the center of the diagram. The CBDC system is surrounded by interconnected entities, including commercial banks, individuals, government, and businesses. In order to facilitate transactions and offer end users financial services, commercial banks are essential. Businesses and individuals use the CBDC system for digital transactions, and the government acts as a regulator by monitoring and guaranteeing adherence to the CBDC guidelines.

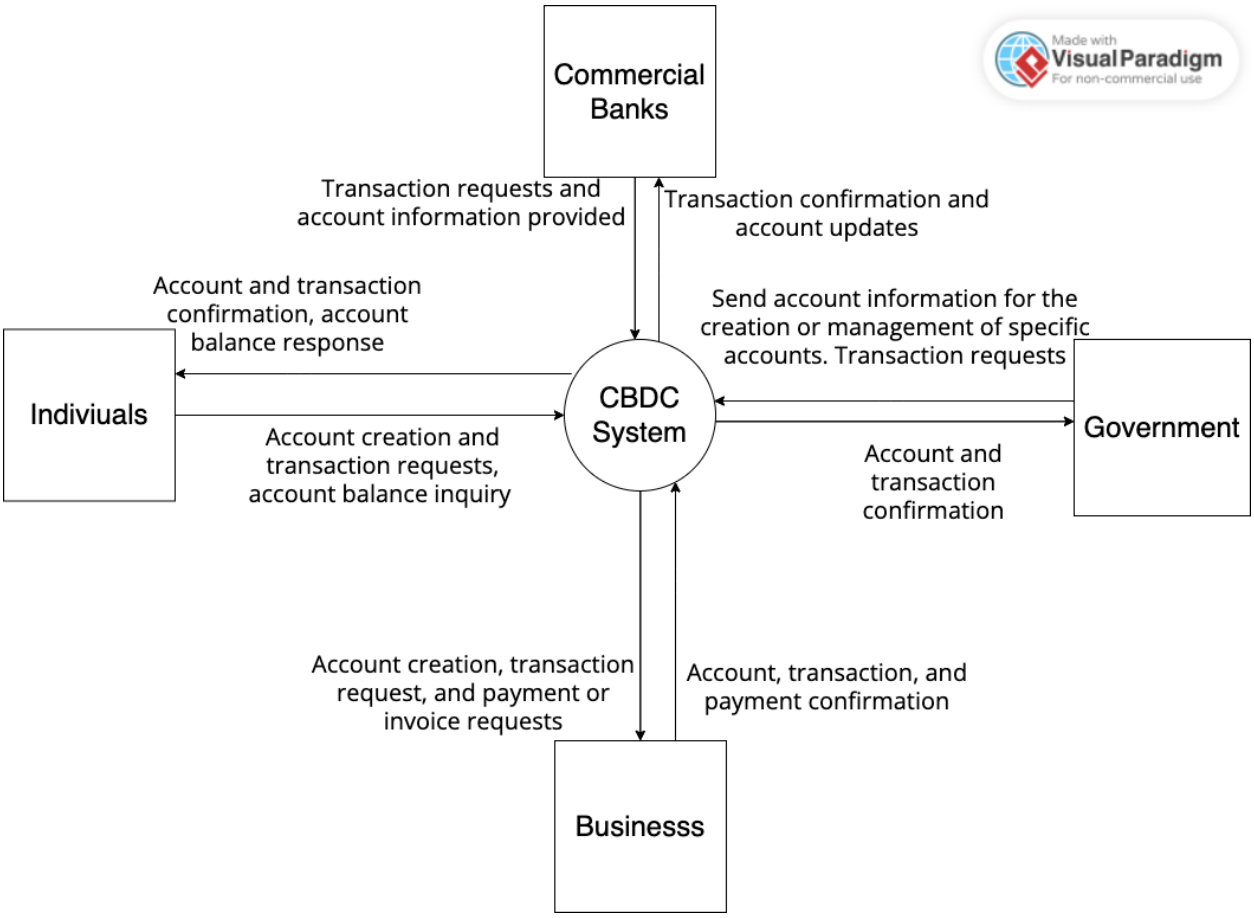

Figure 6: Context diagram of the CBDC

3.5 Objectives

The system aims to:

- Enhance the safety of customers when they transact virtually.
- Secure online buying environment.
- Design and assess features like escrow services and smart contracts integrated into CBDC transactions.
- Automatically releases funds to sellers upon the successful delivery of goods or services.
- Reduce the possibility of fraud and non-delivery especially for university students.
- Make the CBDC wallet usable and accessible to be suitable for a range of user demographics, including low-tech individuals.
- Determine and eliminate any barriers preventing female entrepreneurs from switching from cash to digital payments.

- To support the transition to safer and more effective digital payment methods.
- Create educational initiatives and CBDC features that are specific to the needs of small business owners and female sellers.

3.6 User Characteristics

- Individuals of varied age groups, financial origins, and genders could access the system easily.
- A foundational understanding of English, which is the user interface's default language.
- CBDC system's user-friendly interface would allow wide range of users and their differing levels of digital competence.
- People who are at ease using mobile applications will find the CBDC system convenient as it also runs on a mobile platform.
- Basic comprehension of financial transactions and digital money is needed.
- Knowledge of security procedures, such as password management and device security, to guarantee secure online transactions.
- Users are knowledgeable about and ready to comply with the restrictions governing digital currency transactions in Egypt.

4 Functional Requirements

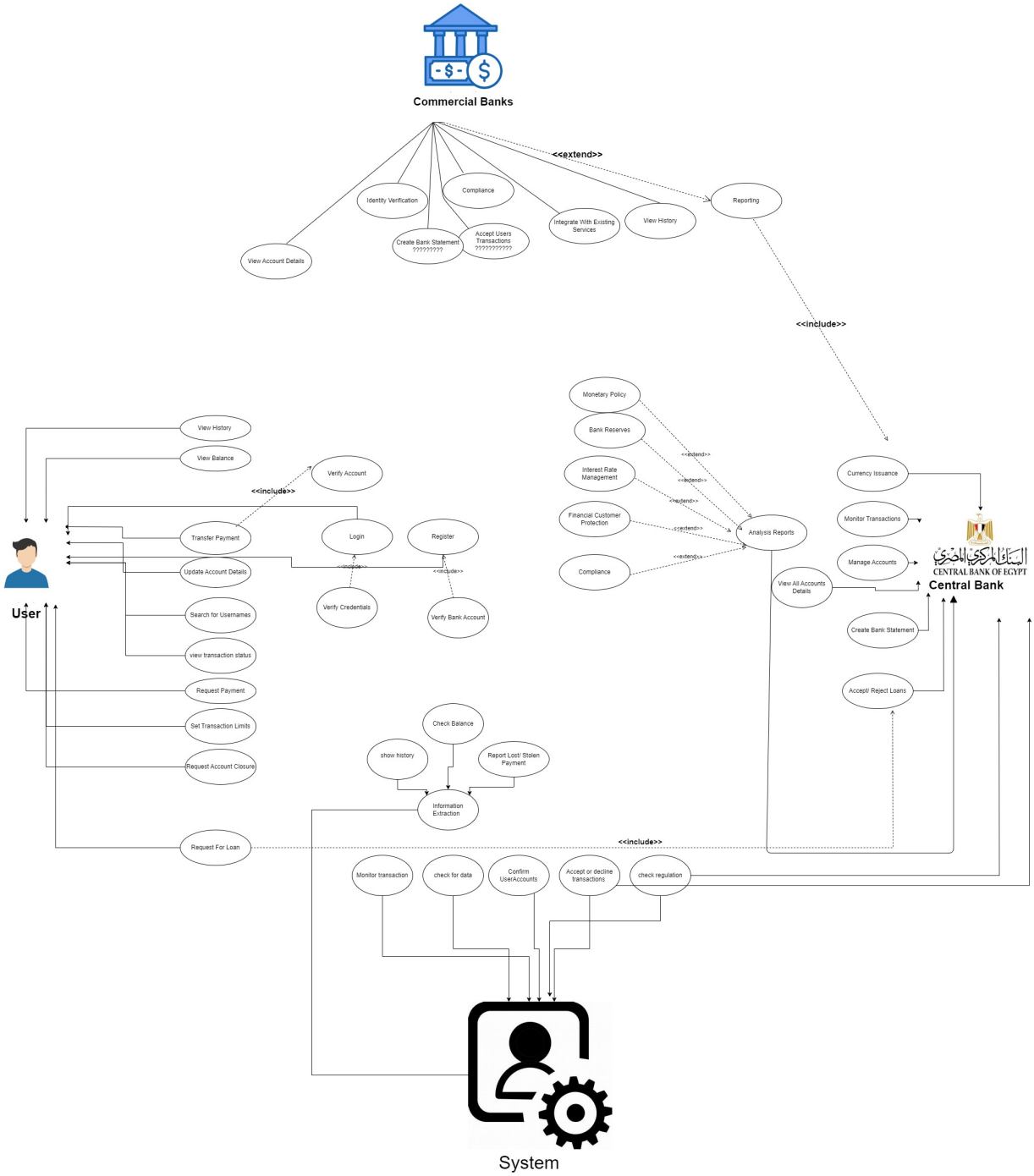

Figure 7: Use-case diagram of the CBDC

4.1 System Functions

- System have security measures, including encryption and secure authentication.
- System allows the user to make registrations.
- System allows the user to login.
- System allow the user to make transaction.
- System should support real-time fund transfers between users.
- System allow the notification to alert users.
- System allow the difficulty for any hacker to hack.
- User shall Login with account.
- User shall Edit account.
- User shall have access to a transaction history that provides details about their past transactions.
- User shall check his balance.
- User shall manage his account.
- User shall send money.
- User shall search for username.
- CBDC shall view and manage user accounts, including creating, modifying, or deactivating accounts as needed.
- CBDC shall have Transaction Monitoring.
- CBDC shall have a Security Configuration.
- CBDC shall conduct Account Verification.
- CBDC shall have Transaction Disputes Resolution.
- CBDC shall Support and have a Communication center.
- CBDC shall have Reports and Analytics.
- CBDC shall Set User Permissions and Roles.

4.2 Detailed Functional Specification

Name	**createGenesisBlock**
Code	Fn1
Priority	Extreme
Critical	Function in a blockchain system involves ensuring the integrity, security, and consistency of the generated genesis block. Here are the critical considerations for this function
Description	This function is responsible for generating and returning the initial or genesis block of a blockchain. The genesis block is the first block in the blockchain, and it usually has specific characteristics, such as a predefined hash ("0000") and no transactions.
Input	The function does not have any explicit input parameters. It is a self-contained function that generates the genesis block with predefined properties.
Output	It produce 6 output which are Index, Timestamp, Transaction, Nonce, hash, and the previous blockHash
Pre-condition	Availability of Date.now():
Post-condition	Genesis Block Creation Immutable Properties
Dependency	No dependency
Risk	None

Table 2: Create Gensis block

Name	**generateHash**
Code	Fn2
Priority	Extreme
Critical	These critical aspects are essential to ensuring the proper functioning, security, and reliability of a blockchain system
Description	It iteratively adjusts the nonce to find a hash that meets specific criteria, making it computationally expensive and time-consuming to produce a valid block.
Input	Takes three parameters: previousBlockHash of the block, timestamp and the pendingtransaction of the other users
Output	returns an object with two properties: Hash, nonce
Pre-condition	Must be Valid Inputs, Also a Valid SHA256 Implementation
Post-condition	It generate the Hash of the block and the Nonce
Dependency	Fn1
Risk	Dependence on SHA256: If there are vulnerabilities discovered in SHA256 in the future, it could impact the security of the blockchain.

Table 3: Generate hash

Name	**createNewTransaction**
Code	Fn3
Priority	Extreme
Critical	The function itself is not inherently complex, some considerations could be considered critical, depending on the context of its use within a broader system. Here are some critical aspects to consider:
Description	The function initializes a new transaction object (newTransaction) with the provided amount, sender, and recipient values.
Input	Takes three parameters: Amount: of the sender money Sender: name or verified account Recipient: name or verified account
Output	Does not explicitly produce any output or return a value. Instead, it modifies the state of an object (presumably a blockchain) by adding a new transaction to the list of pending transactions.
Pre-condition	Blockchain Object Exists:
Post-condition	Transaction Object Added to the blockchain. Also, the Array Length Increased
Dependency	Fn2
Risk	Input Validation must be right And check for Authentication and Authorization

Table 4: Create new transaction

Name	createNewBlock
Code	Fn4
Priority	Extreme
Critical	The criticality of these aspects depends on the specific requirements, use case and security considerations of the blockchain system.
Description	The function serves the purpose of creating a new block in a blockchain. In a blockchain system, a block typically contains a collection of transactions, a timestamp, a reference to the previous block (via its hash), and a hash that verifies the integrity of its contents.
Input	Key inputs:"this.pendingTransaction"
Output	New Block Object and Blockchain state Update of the new data added
Pre-condition	Blockchain Exists, Pending Transaction Existence, Previous Block Existence And Hash Generation Function
Post-condition	New Block Creation, Blockchain State Update, pending transaction clearing ("This.PendingTransaction") And Return The Value Of New Block
Dependency	Fn3
Risk	Input Validation must be correct And check for Authentication and Authorization

Table 5: Create new block

5 Design Constraints

5.1 Standards Compliance

The CBDC mobile application can work with any android smartphone.

5.2 Hardware Limitations

The user could access the mobile application from a smartphone that could successfully connect to the internet.

5.3 Other Constraints as appropriate

An dependable internet connection is necessary for the application to operate as intended.

6 Non-functional Requirements

6.1 Security

A digital currency system needs strong security measures, such as multi-factor authentication, access controls, and data encryption, to guarantee the integrity and confidentiality of sensitive data. The system's security and resilience are further enhanced by incident response plans, regular security audits, and regulatory compliance.

6.2 Portability

The CBDC mobile application will be accessible by all android smartphones.

6.3 Reliability

In order to maintain constant performance and ongoing availability under fluctuating operational conditions and possible network failures, the system must possess a high level of reliability. Throughout its life, its operational resilience must efficiently handle faults to ensure a consistent and reliable user experience.

6.4 Maintainability

The system must exhibit exceptional maintainability, facilitating the smooth incorporation of software upgrades, system enhancements, and security patches without interfering with essential operations. For long-term stability and adaptability, the architecture should make maintenance simple.

6.5 Manageability

It requires a strong and intuitive management interface to enable easy system monitoring and control. It should also facilitate effective updates, troubleshooting, and monitoring to guarantee top performance and flexibility.

6.6 Usability

To ensure that people with different levels of technological proficiency can interact and navigate the digital currency platform, it requires an interface that is both intuitive and user-friendly. To accommodate different user demographics, the system should also give priority to accessibility features.

6.7 Performance

For transactions to be processed quickly and securely, it must operate with stability. A dynamic financial environment should be met by it, as it should be able to support a large number of concurrent users with low latency.

6.8 Scalability

Scalability is essential in the dynamic world of digital currencies to manage increasing user numbers and transaction volumes. The system has to retain excellent operation while handling more traffic and processing transactions quickly.

7 Data Design

The Central Bank Digital Currency (CBDC) system's data design diagram illustrates the relationships between key entities in the ecosystem. The primary entities include "user," representing individuals, "user merchant" for merchants interacting with users, and "merchant" for businesses. Transactions are captured through entities like "payment," "wallet," and "currency," where the latter two connect to "user" and "merchant" to depict ownership. The system tracks transactions and currency flow with "blocks" and "transaction" entities, while tax-related information is managed through "taxin" and "taxout" entities. This diagram provides a comprehensive overview of the CBDC system's data structure, depicting the interactions among users, merchants, and the underlying financial components.

Figure 8: Egyptian CBDC DB Schema

8 Preliminary Object-Oriented Domain Analysis

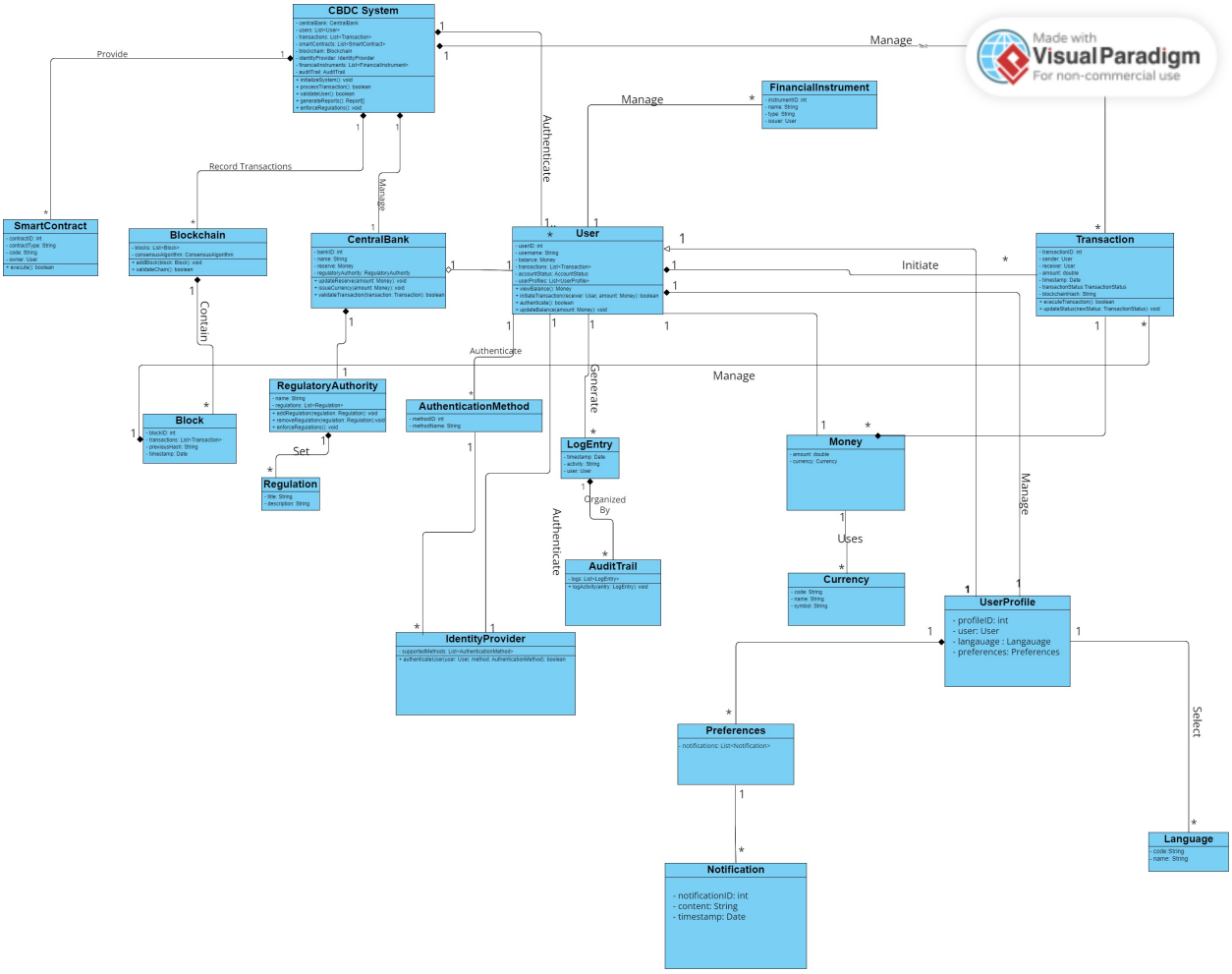

Figure 9: Initial Class Diagram

9 Operational Scenarios

- **Scenario 1**
  The user will login into the CBDC system using their credentials. Once logged in the user navigates to the "Transactions" section of the CBDC system. The user fills in the necessary details for the transaction including recipient's CBDC account details and transaction amount. To authorize the transaction, the user provides the necessary authentication (e.g., pin).

- **Scenario 2**
  The user logs into the CBDC system using their credentials. Once logged in, the user navigates to the "Account" section of the CBDC system and then the system displays an overview of the user's account, including the current balance and recent transactions, the user specifically selects the option to "Check Account Balance", the CBDC system retrieves and displays the user's current account balance.

- **Scenario 3**
  The CBDC system verifies the user's request for a fund transfer by verifying the recipient's authenticity and account balance. After validation, the system figure out each financial institution's net position and corresponding with them to match up transaction information. Next, it updates the recipient's and user's real-time account balances to reflect changes. Finally, the system confirms the successful fund transfer settlement by sending alerts to both parties.

- **Scenario 4**
  The commercial bank logs into the CBDC system, navigates to the "Fund Transfer" section, and selects the customer account. After verifying the customer's details, the bank initiates a fund transfer, specifying the recipient's CBDC account and amount.

10 Project Plan

From Proposal to SDD.

Task	Start date	End date	Duration	Role
Information Collection and researches	20/10/2023	13/11/2023	24 days	All team members
Survey and proposal preparation	20/10/2023	13/11/2023	24 days	All team members
Proposal presentation 10%	13/11/2023	15/11/2023	3 days	All team members
SRS Documentation	30/11/2023	01/01/2024	32 days	All team members
SRS presentation 35%	15/01/2024	18/01/2024	3 days	Habiba and Mennah
SDD preparation	01/02/2024	20/02/2024	20 days	All team members
Working on ethereum tool	20/02/2024	27/02/2024	7 days	All team members
Web application development	03/03/2024	08/04/2024	35 days	Karim and Haidy
Working on smart contracts	22/02/2024	15/04/2024	53 days	All team members
SSD Documentation	8/03/2024	30/03/2024	23 days	All team members
SSD presentation 35%	15/3/2024	01/04/2024	3 days	All team members
Working on API provider	02/04/2024	19/04/2024	3 days	All team members

Table 6: Time plan

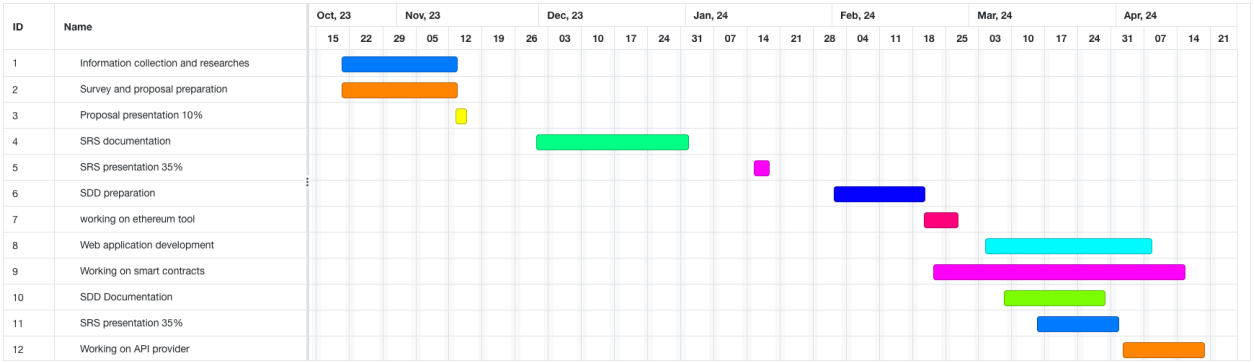

Figure 10: Gantt chart

11 Appendices

11.1 Definitions, Acronyms, Abbreviations

Abbreviation	Definition
CBDC	Central bank digital currency
Block chain	A distributed ledger with growing lists of records (blocks) that are securely linked together via cryptographic hashes.
AML	Anti-money laundering
CFT	Countering the financing of terrorism
KYC	Knowing your customer
UTXO	Unspent transaction output
CBE	Central bank of Egypt
DLT	Distributed ledger technology
FMI	Financial Market Infrastructures
eKYC	Electronic Customer Identification System
eNaira	Nigeria CBDC project
CBUAE	Central bank of the United Arab Emirates
SAMA	Saudi Central Bank digital currency
CBUAE	Central Bank Digital Currency - the Digital Dirham
RingCT	Ring Confidential Transaction
ZKP	Zero-Knowledge Proof
MPC	Multi-Party Computations

11.2 Supportive Documents

- Survey responses

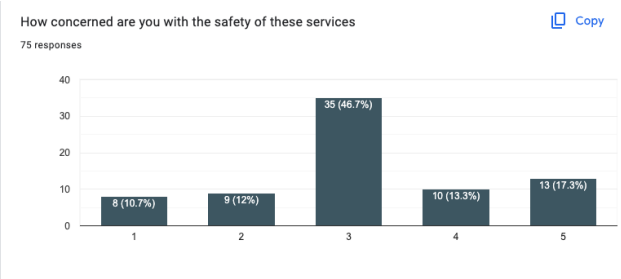

Figure 11: Concern about safety

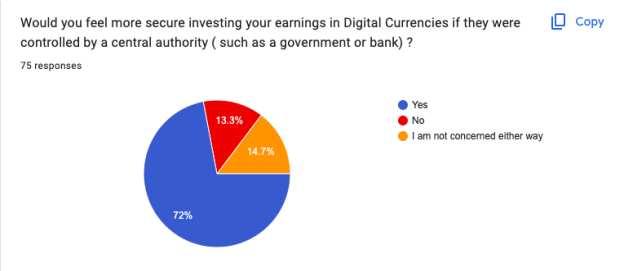

Figure 12: Central bank controlling digital currency

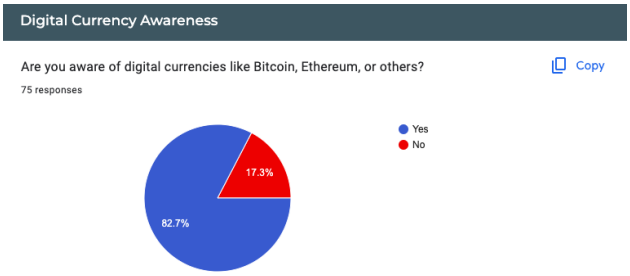

Figure 13: Awareness of digital currencies

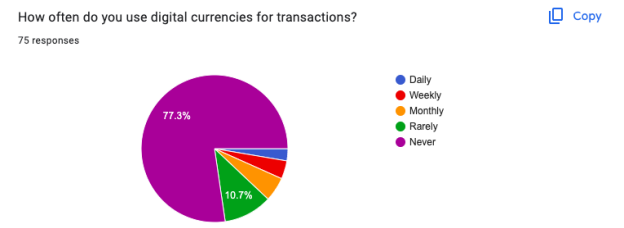

Figure 14: Use of digital currencies

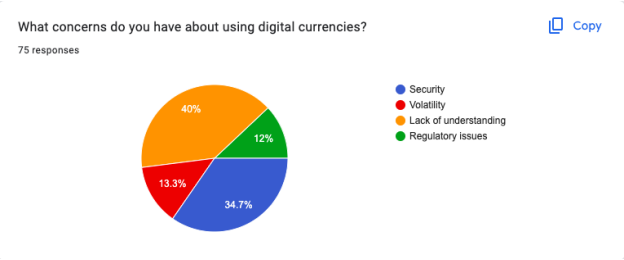

Figure 15: Concerns about using digital currencies

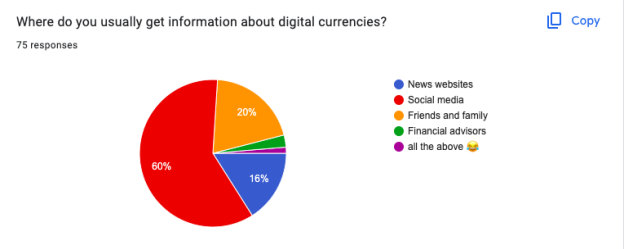

Figure 16: Information about digital currencies

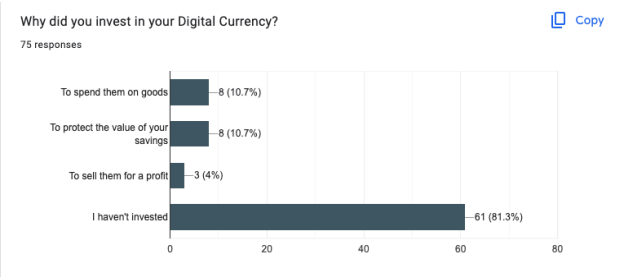

Figure 17: Investment in digital currency

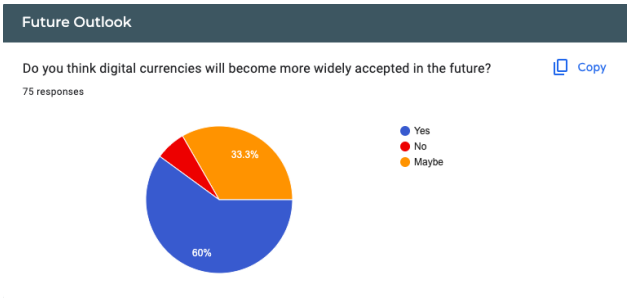

Figure 18: Future of digital currencies

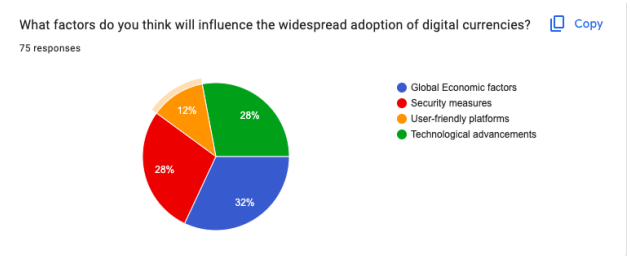

Figure 19: Future of digital currencies

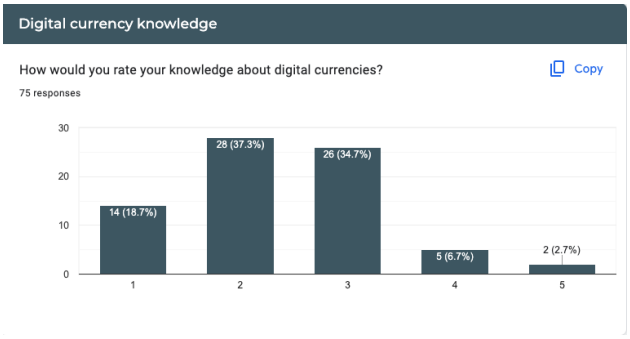

Figure 20: Rate Knowledge about digital currencies

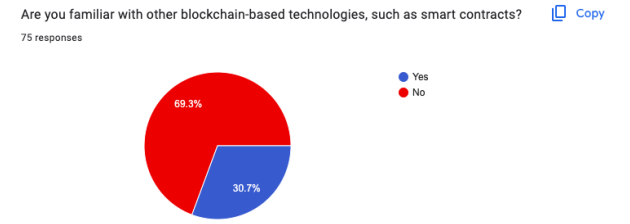

Figure 21: Blockchain-based technologies

References

[1] Eseose Oseghale. *Egypt's journey towards digital pound implementation*. en. https://www.mariblock.com/egypts-journey-towards-digital-pound-implementation/. Accessed: 2024-1-14. Dec. 2023.

[2] *Central Bank Digital Currency (CBDC) Tracker — cbdctracker.org*. https://cbdctracker.org/. [Accessed 06-01-2024].

[3] *www2.deloitte.com*. https://www2.deloitte.com/content/dam/Deloitte/in/Documents/financial-services/in-fs-cbdc-noexp.pdf. [Accessed 13-01-2024].

[4] Jinnan Zhang, Rui Tian, Yanghua Cao, et al. "A hybrid model for central bank digital currency based on blockchain". In: *IEEE Access* 9 (2021), pp. 53589–53601.

[5] Tao Zhang and Zhigang Huang. "Blockchain and central bank digital currency". In: *ICT Express* 8.2 (2022), pp. 264–270.

[6] Edwin A Opare and Kwangjo Kim. "Design Practices for Wholesale Central Bank Digital Currencies from the World". In: *Symposium on Cryptography and Information Security (Kochi, Japan, 28-31 de enero de 2020)*. 2020.

[7] *CBUAE | Home — centralbank.ae*. https://www.centralbank.ae/en/. [Accessed 13-01-2024].

[8] *Central Bank Digital Currency Strategy - the Digital Dirham*. en. https://u.ae/en/about-the-uae/strategies-initiatives-and-awards/strategies-plans-and-visions/finance-and-economy/central-bank-digital-currency-strategy. Accessed: 2024-1-14.

[9] *eNaira &x2013; Same Naira, More Possibilities — enaira.gov.ng*. https://enaira.gov.ng/. [Accessed 13-01-2024].

[10] https://www.imf.org/en/News/Articles/2021/11/15/na111621-five-observations-on-nigerias-central-bank-digital-currency. Accessed: 2024-1-14.