A

PROJECT PROPOSAL REPORT

ON

CENTRAL BANK DIGITAL CURRENCY(CBDC) SIMULATION USING ETHEREUM NETWORK

BY

Prashant Soni

Bikesh Maharjan

January, 2023

ABSTRACT

Central Bank Digital Currency (CBDC) is a digital form of currency notes issued by a central bank. While most central banks across the globe are exploring the issuance of CBDC, the key motivations for its issuance are specific to each country's unique requirements. CBDC must support public policy objectives without impeding central banks' ability to fulfill their objectives [1]. It is recommended that a prototype of CBDC should be developed and simulated in a closely controlled environment before developing and launching any real CBDC[1]. Thus with the leverage of public distributed Ledger technology and collection of web3 libraries, a CBDC simulations system can be designed to meet the specific requirements for developing a CBDC proof of concept for Nepal Rastriya bank. There are some architectural designs and ledger infrastructure combinations for system design of CBDC for Nepal. The suitable design choice for Nepal recommended in [1] is referred to develop this project. In this proof of concept, the demonstrative environment for multi-level CBDC is build on Ethereum network and Node.js server. The CBDC simulation system is divided into two loosely coupled sub-system namely retail CBDC system and wholesale CBDC system. In this project, we will be demonstrating the core feature of CBDC like election of controlling party/member, creation, distribution of token to financial institute, pausing the entire token circulation and destroying excessive circulating wholesale CBDC. Also broader features like buy, sell, transfer, withdraw, lock and unlock mechanism for retail CBDC which is used by financial institute and end-user can be demonstrated.

Keywords: CBDC, technical aspect of developing a CBDC, CBDC using Ethereum network, CBDC for Nepal, distributed ledger technology.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

CBDC	Central Bank Digital Currency
CPMI-MC	Committee on Payments and Market Infrastructures and the Markets Committee
CSS	Cascading Style Sheets
DLT	Distributed Ledger Technology

CHAPTER 1

INTRODUCTION

1.1 Background

The report by the CPMI-MC published in 2018 defines CBDCs as new variants of central bank money different from physical cash or central bank reserve/settlement accounts. That is, a central bank liability, denominated in an existing unit of account, which serves both as a medium of exchange and a store of value. The four different properties of CBDC are:

- Issuer (central bank or not)
- Form (digital or physical);
- Accessibility (wide or narrow);
- Technology (peer-to-peer tokens, or accounts) (Bech and Garratt (2017))

There are mainly three conceptual CBDC operating model.

- Unilateral CBDC
  Central bank issues money and performs all functions, including direct interaction with end users
- Intermediated CBDC
  Central bank issues money, but delegates functions to non-central bank intermediaries who interact with end users
- Synthetic CBDC
  Non-central bank actors issue money that is backed by central bank assets that they acquire from the central bank.

The goal of a digital currency system is to track the balance of its users, allowing each to transact only their coins(tokens) (Allen et al., 2020). This requires maintaining a ledger to record transactions and balances of end users. The ledger could be a

conventional centrally controlled database, or a novel distributed ledger (Auer and Bohme, 2020). Allen et al. (2020) state that in a fully-centralized design, the choice of nodes and their operation are all under the direct control of the central bank, and thus the central bank itself or a malicious insider at their will, can potentially change, roll back, rewrite or delay transactions. But in a semi-centralized design, the central bank chooses entities to run the nodes instead of having sole control over all the nodes and their operations. Hence, no single party or group of parties below a certain size can tamper with the transactions. However, the central bank can facilitate an agreement of all parties to perform arbitrary changes (Allen et al., 2020).

Auer and Bohme (2020) state that once the architecture and infrastructure for CBDC have been chosen, the question arises of how and to whom one should give access. This design choice is concerned with either tying access to the CBDC to an identity system adopting an account-based technology, or securing via cryptographic schemes. Blockchain is a type of distributed ledger technology (DLT) which is a rapidly evolving approach to recording and storing data across multiple participants in multiple locations. Unlike traditional databases, transactions and data are replicated, stored, and synchronized over a distributed network consisting of several nodes. In a blockchain, each transaction (block) is linked together in a list (chain) with a cryptographic hash. DLTs have some key characteristics: they can be public or private, permissioned or permissionless. A public DLT can be accessed by anyone, whereas a private DLT is access restricted. In a permissionless DLT, any participant can make changes to the ledger provided they are able to achieve consensus, while in a permissioned DLT, only specific entities can authorize or commit updates to the ledger. Due to the absence of a central authority to ascertain the veracity of data and to commit new transactions, DLTs rely on consensus algorithms that ensure the validity of such data. Once a consensus is reached among the participating nodes, a new transaction is added to the ledger. Reaching a consensus is appropriately difficult, and this establishes overall reliability of the system. Source: Bansal and Singh (2021).

Depending on the forms of issuance either as account or token based CBDCs, they shall carry different legal significance. The account based CBDCs which is like

the existing account forms of money shall not be considered to be a new form of money, instead as the digital form of 'book money', which are credit balances on accounts. In contrast, token-based CBDCs are a new form of money where the central banks' liability is incorporated in the token[2].

Considering the three highly desirable policy goal and a moderately desirable policy goal of Nepal Rastriya Bank, the literature [1] suggests that a permissioned, intermediated, and semi-centralized infrastructure-based CBDC with both account-based and token-based access is suitable for Nepal[1]. Also according to section 7 of Nepal Rastriya Bank act 2058 B.S prohibits Nepal Rastriya Bank in participating in commercial activities of bank which reject other operational architecture and insist in choosing two-tier(intermediated) model for developing CBDC in Nepal.

1.1.1 Feature of CBDC

The core features of CBDC implemented in our simulation are:

- CBDC is sovereign currency issued by Central Banks in alignment with their monetary policy.
- Must be accepted as a medium of payment, legal tender, and a safe store of value by all citizens, enterprises, and government agencies.
- Freely convertible against commercial bank money and cash.
- Fungible legal tender for which holders need not have a bank account.
- Expected to lower the cost of issuance of money and transactions.

1.2 Objectives

The objectives of this project are:

- To develop a full-stack web3 applications for simulating the concept and working mechanism of CBDC.
- To provide a explanatory interface for CBDC issuer like Nepal Rastriya Bank, intermediaries like commercial banks/Financial institutes and end-users like

private organization/citizens.

1.3 Technical Features

The features of our project are as follows:

- Distributed ledger technology.
- Token based CBDC
- Two-tier Model(Intermediary Model)
- Semi-centralised
- Smart contract based data and transaction

1.4 System Requirements

The system requirements of our project are:

1.4.1 Software Requirements

The software requirements for our project are as follows:

(a) Ethereum test network like Goerli

(b) Web3 development kit like Ganache, Remix IDE, Metamask.

(c) Web3 libraries like web3.js, Chai, openzeppelin-solidity

(d) Web3 framework like Truffle

(e) Node.js for backend server

(f) React and Tailwind CSS for developing user interface.

CHAPTER 2

LITERATURE REVIEW

The specific research goal of this literature is to demonstrate that it is technically viable to equip smart contract technology which is already a game-changer in many sector - with the ability to use retail CBDCs and the benefits of doing so for industrial use cases[3].

The intermediate model can take different forms depending on how functions are distributed between the central bank and private intermediaries. When discussing the distribution of functions between actors, it is useful to distinguish between the owner of the technical system necessary to carry out a specific function and the executor of the function itself. These are not always the same; indeed the system might be owned by the central bank while the function is carried out by a private company[4].

Figure 2.1: Functions to be carried out in a CBDC system

Patterns set by major cryptocurrencies, pseudonymous CBDC ledgers, which maintain balances spendable by the owners of private cryptographic keys, promise to be a viable and robust technical approach, able to accomodate ”account-based” as well as ”token-based” CBDC approaches[3]

The Norges Bank, Norway’s central bank, has announced that Norway’s central bank digital currency (CBDC) prototype infrastructure is based on Ethereum technology. The Norges Bank has been testing various designed for their anticipated CBDC for two years, noting that ‘interoperability’ was their highest priority while assessing the different solutions available today[5].

CHAPTER 3

METHODOLOGY

float

3.1 CBDC simulation system overview

The block diagram of our system is as follows:

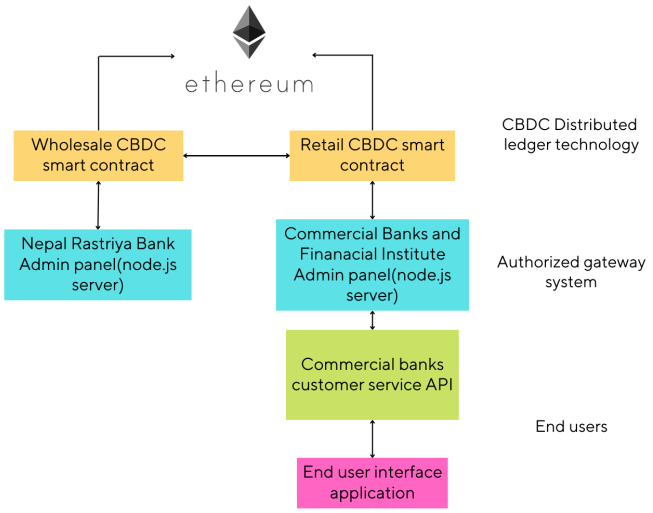

Figure 3.1: System Block diagram

Wholesale CBDC smart contract comprises of token definition and its behaviour i.e. the functionality required for creation(mint), distribution and destruction of CBDC token. It also defines the central bank duties and power. The functions of this smart contract can be accessed by Nepal Rastriya Bank through Wholesale-CBDC admin panel. Retail CBDC will be pegged to wholesale CBDC, that will be circulated by commercial banks and financial institutes. The issuance of retail CBDC will be controlled by Nepal Rastriya Bank however, the distribution and circulation will be controlled by financial institutes. Commercial banks can access their function through their admin panel provided by Nepal Rastriya bank. End-user can use

retail CBDC to transfer between persons or organization via commercial banks. End-user can access their token and perform transfer via end user application like CBDC wallet.

3.2 Wholesale CBDC

The major functions of Nepal Rastriya bank to operate a CBDC system are implemented in this simulation. The details of functions are explained below.

- Election for choosing a controlling party.
- Mint CBDC token(Creating new tokens)
- Transferring token to other banks
- Burn CBDC token(destroying excessive tokens)

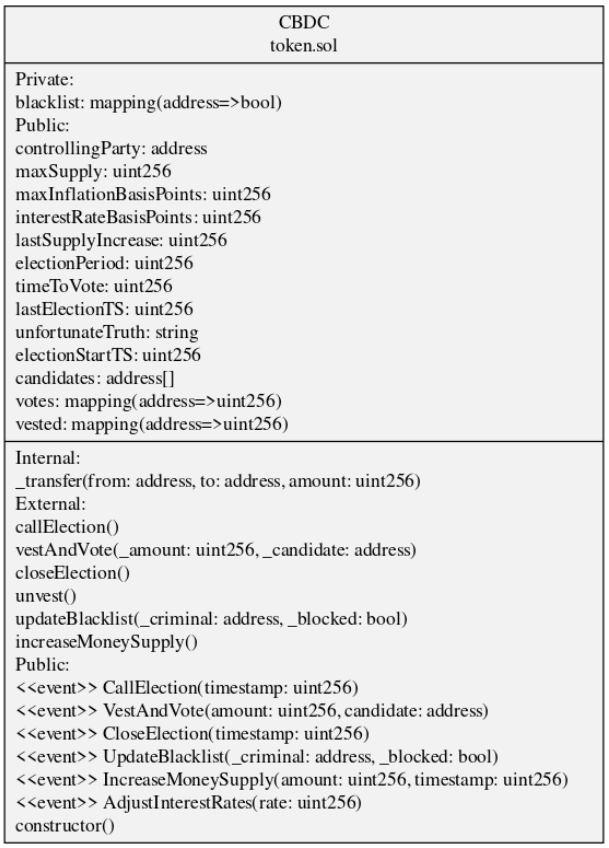

Figure 3.2: Class diagram of wholesale CBDC smart contract

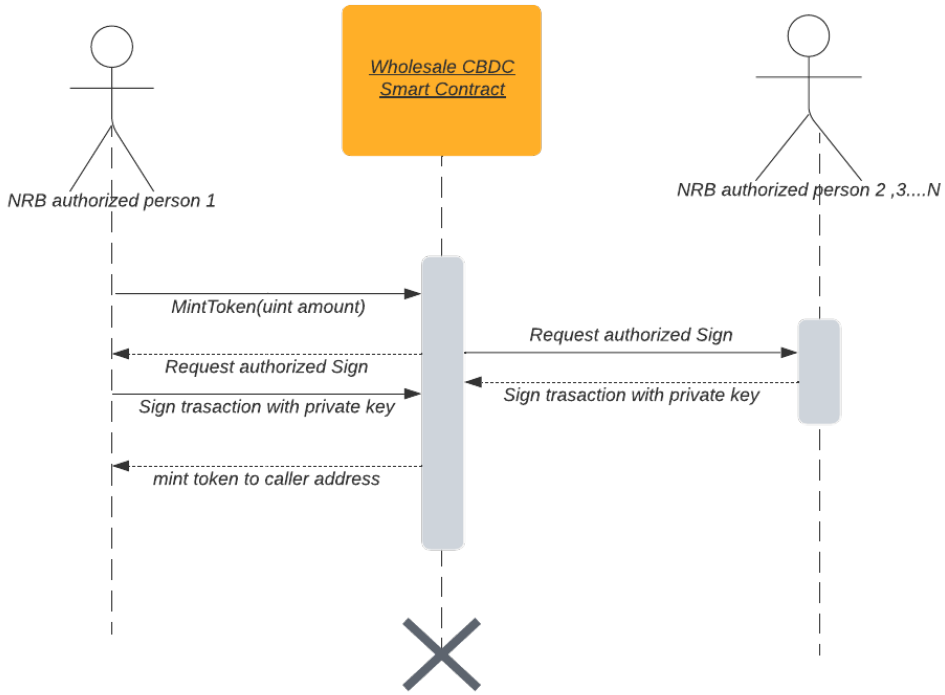

Figure 3.3: Sequence flow diagram for creating CBDC token by Central bank

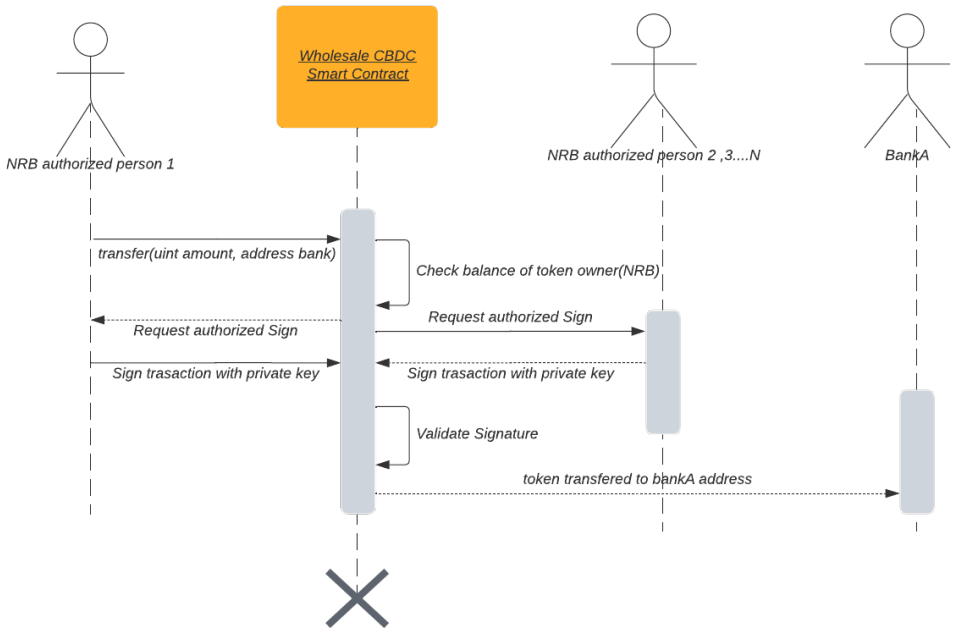

Figure 3.4: Sequence flow diagram for transferring CBDC token from central bank to financial institute

3.3 Retail CBDC

The major functions of commercial banks and financial institutes to meet their objectives in a CBDC system are explained below.

- Mint the amount of retail CBDC limited by wholesale CBDC contract.
- Buy(cash to CBDC conversion)
- Sell(CBDC to cash conversion)
- Transferring token to private sectors and individual.
- Deposit of CBDC in bank internal system
- Withdrawal of CBDC from bank internal system
- Staking/locking of CBDC in bank internal system for interest.
- Unstaking/unlocking of CBDC from bank internal system.
- End-user can also transfer retail token to any other end-user via banks.

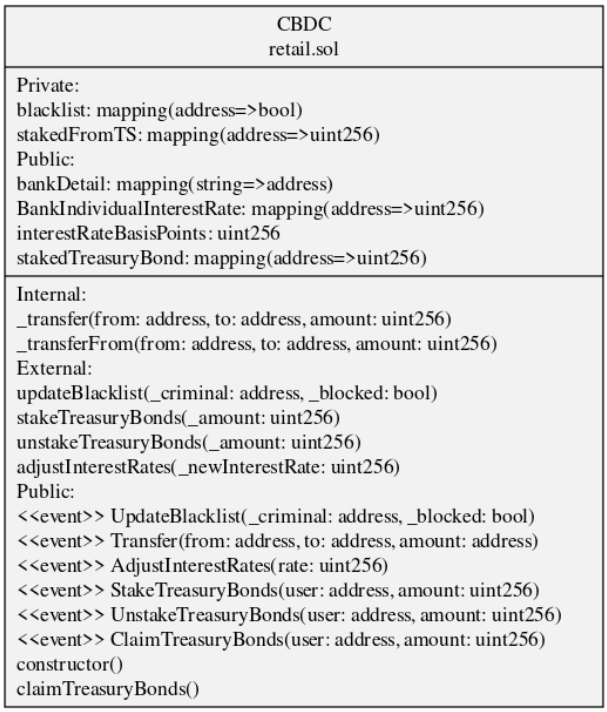

Figure 3.5: Class diagram of retail CBDC smart contract

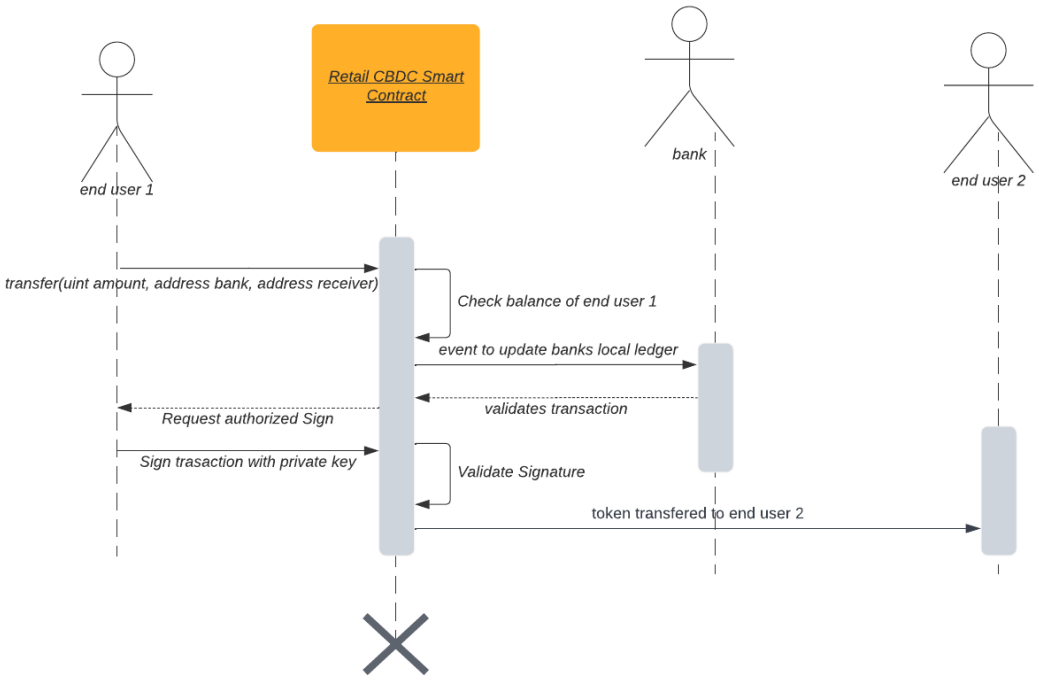

Figure 3.6: Sequence flow diagram for transferring CBDC token from end user 1 to end user2 through retail CBDC smart contract and commercial bank

CHAPTER 4

EXPECTED OUTPUT

This project is a approach to simulate a national level CBDC using distributed ledger technology and smart contract. The result of this project will be demonstration of CBDC system mechanism in a simulation environment. Neapl Rastriya bank will be able to conduct election to choose CBDC controlling party, create new tokens, transfer token to banks and destroy excessive CBDC tokens through their node.js based application communicating to wholesale CBDC smart contract. Commercial banks will be able to create retail CBDC issued by Nepal Rastriya bank, provide platform for end-users to buy, sell, transfer, stake, unstake their CBDC token through their node.js based application communicating with retail CBDC smart contract. The end users can check balance, transfer, stake token for earning interest and withdraw token as cash from their node.js based wallet like application communicating with banks system API. This project is expected to provide insights on how CBDC system will look like in operation and what leverage can it provide over physical cash system. Since this simulation will be deployed on live Ethereum network, we can expect to perform further analysis on the reliability, security, efficiency and scalability of CBDC run environment.

CHAPTER 5

LIMITATION OF THIS PROJECT

This project focuses on simulating the necessary function of a CBDC system, however a sufficient system may need different approach. The technology used in this project are well suited for simulating a CBDC, but more research on the security, efficiency, cost and scalability of a technology or a network is required. Our system is a proof of concept which excludes the optimization of transaction cost and operational cost during actual operation. Although, this project is done with reference from valid literature and documentations, the major objective was to develop a CBDC from technical aspect. So, the legal validation and real world financial function may need to be discussed with legal and financial experts. We have discussed about tying account to user identity using online KYC, which required further research and study on decentralised storing of files and form data, thus it is expected to be included in next version of this project.

REFERENCES

[1] Central Bank Digital Currency (CBDC) - NRB kernel description. https://www.nrb.org.np/contents/uploads/2022/10/CBDC-for-Nepal.pdf. Accessed: 2010-09-30.

[2] Concept note on CBDC - Reserve Bank of India kernel description. https://rbidocs.rbi.org.in/rdocs/PublicationReport/Pdfs/CONCEPTNOTEACB531172E0B4
Accessed: 2010-09-30.

[3] Imre Kocsis, László Gönczy, Attila Klenik, Pál Varga, Attila Frankó, and Bence Oláh. Research report cbdc-based smart contract ecosystems. 2021.

[4] Wouter Bossu, Natasha Che, John Kiff, Inutu Lukonga, Tommaso Mancini-Griffoli, Tao Sun, and Akihiro Yoshinaga. Behind the scenes of central bank digital currency. 2022.

[5] Runar Alvseike and Geir Arne Gjersvoll Iversen. Blockchain and the future of money and finance: a qualitative exploratory study of blockchain technology and implications for the monetary and financial system. Master's thesis, 2017.