

Design and Implementation of Blockchain Based Central Bank Digital Currency

- Master Thesis Defense -

Sajan Maharjan

Supervisor: Prof. James Won-Ki Hong

**Dept. of CSE, DPNM Lab., POSTECH, Korea
thesajan@postech.ac.kr**

2020. 06. 30

Table of Contents

- **Introduction**
- **Background & Related Work**
- **Requirements & Design**
- **Implementation**
- **Evaluation**
- **Conclusion**

Introduction

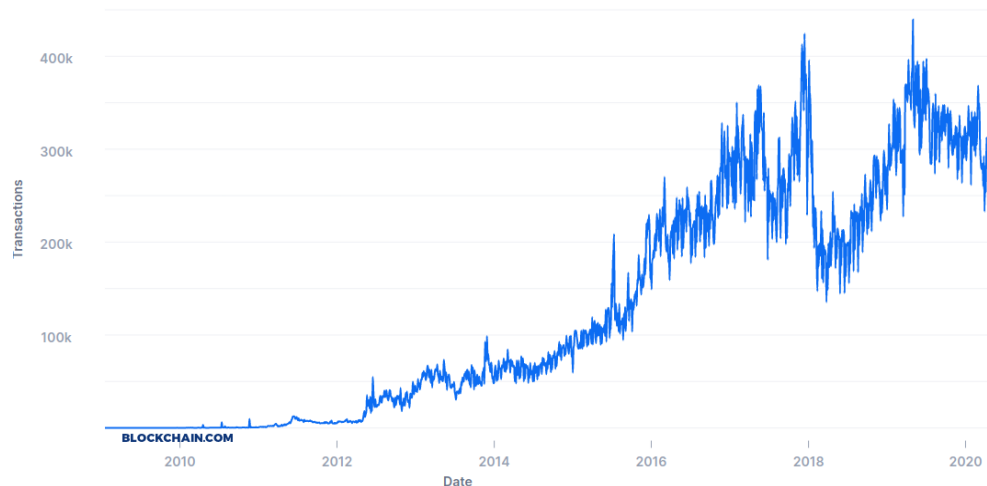
Introduction

■ Rise of Blockchain and Cryptocurrencies

- Gradual increase in the price of Bitcoin, Ethereum and other cryptocurrencies
- Increasing number of transactions using cryptocurrencies
- Concern of banks & governments over regulation & valuation of cryptocurrencies

Confirmed Transactions Per Day

The total number of confirmed transactions per day.



<https://www.blockchain.com/charts/n-transactions>

Ethereum Daily Transactions Chart

Source: Etherscan.io
Click and drag in the plot area to zoom in



<https://etherscan.io/chart/tx>

Introduction

■ Inherent Problems of Fiat Cash

- Expensive to produce and circulate
 - Bank of Korea reports it costs 20KRW to produce coins worth 10KRW^[1]
 - 20M KRW worth of bills is subject to damage and 60B KRW is invested in re-issuance annually^[1]
 - The US Federal Reserve spends \$827M for printing bills and engraving coins^[2]
- Difficulty in Cash Movement
- Lack of Transparency
- Storage and Safety Requirements

■ Domination of private PSPs and e-money

[1] <https://www.blockmedia.co.kr/archives/114942>

[2] <https://www.federalreserve.gov/foia/files/2020currency.pdf>

Introduction

■ Motivation

- Banks and governments desire control and authority over the payments market
- Maintain monetary sovereignty & discourage use of non-regulated cryptocurrencies
- Curb and limit illegal activities on cryptocurrencies
- Devise an effective alternative to fiat cash

■ Research Goals

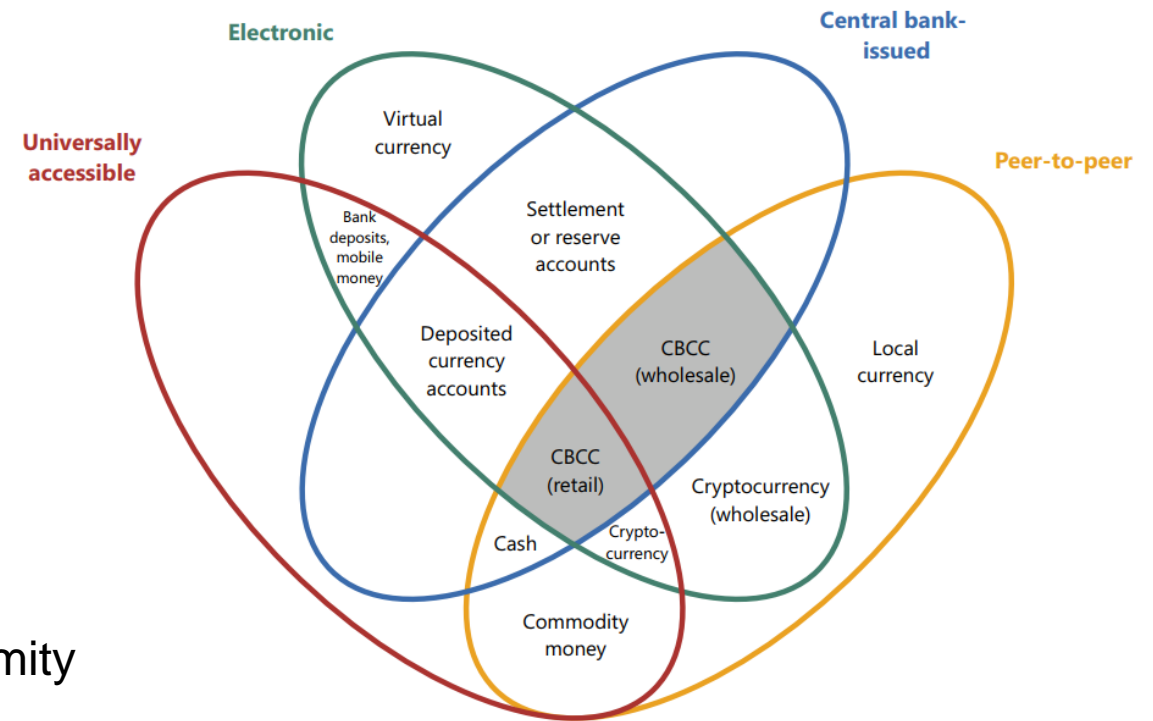
- Study and explore different CBDC initiatives taken by banks around the world
- Design and implement effective blockchain based CBDC models
- Compare different blockchain platforms for CBDC implementation

Background & Related Work

Background

■ Central Bank Digital Currency (CBDC)

- Digital currency issued by a central bank
- Money flower^[3] visually depicts major forms of money and defines CBDC
 - Central bank issued electronic form of money
 - Peer-to-peer transfer
 - Accessibility
- Classification of CBDC
 - Retail vs Wholesale CBDC
 - Direct vs Indirect CBDC vs Hybrid CBDC
 - Cross-border CBDC vs Domestic CBDC
 - Account-based CBDC vs Token-based CBDC
- CBDC Design Considerations
 - Geographical, Political & Technological factors
 - Availability; Custody; Transaction Limits; Anonymity



[3] https://www.bis.org/publ/qtrpdf/r_qt1709.pdf

Background

■ Central Bank Digital Currency (CBDC)

- Retail vs Wholesale CBDC

Features	Retail CBDC	Wholesale CBDC
Accessibility	General Public	Banks and Financial Institutions
Use Case	Daily payments	Interbank settlements
Value of transactions	Small	Large

- Direct CBDC vs Indirect CBDC vs Hybrid CBDC

Features	Direct CBDC	Indirect CBDC	Hybrid CBDC
Presence of intermediary	No	Yes	Yes
Claim on Central Bank	Yes	No	Yes
Division of Responsibilities	No	Yes	Yes
Deferred Settlements	No	Yes	Yes

Related Work

■ Discussion Papers

- *Central Bank Digital Currencies* by Bank for International Settlement
- *The Rise of Digital Money* by International Monetary Fund → Hybrid CBDC
- *Central Bank Digital Currency Policy Maker Toolkit* by World Economic Forum

■ Technical Papers

- *Centrally Banked Cryptocurrencies* → RSCoin
 - Central authority mints digital currency and verified entities (commercial banks) validates transactions
 - Use of sharding
 - Overcomes the issues with Bitcoin
- *PRCash: Fast, Private and Regulated Transactions for Digital Currencies*
 - Extension of RSCoin
 - Use of Homomorphic Encryption and Zero-Knowledge Proofs to hide transaction details
 - Focuses on user anonymity and privacy

Related Work

■ Banking Initiatives

- *Project Jasper* by Bank of Canada
- *Project Ubin* by Monetary Authority of Singapore
- *Project Khokha* by South African Reserve Bank
- *Project Bakong* by National Bank of Cambodia

■ Industrial Initiatives

- *Digital Fiat Currency* by VISA
 - Patent registered at USPTO
 - Replace existing fiat currency for digital cash
 - Incorporates private transaction processing networks, central banks, commercial banks & end-users
- *Libra* by Libra Association
 - Promote financial inclusion
 - Provide a global, open, instant and low-cost payments network
 - Permissioned network with strong regulations and compliance

Main Contribution

- **Blockchain-based Retail CBDC Implementation**
 - Most initiatives taken by central banks have been focused at wholesale level
 - Prototype implementation for CBDC offering at retail level
- **Proposed indirect model mimics general banking environment**
 - Offering of banking services via smart contracts executed on top of blockchain
 - Mapping of real-world user identities with account addresses
 - Regulation over services (blacklisting and whitelisting)
- **Comparison between popular blockchain platforms for CBDC**
 - Direct Model has been implemented using Hyperledger Iroha
 - Indirect Model has been implemented using Quorum

Requirements & Design

Requirements

- **General Non-Functional Requirements of a CBDC System**
 - Payment system should be simple and easy to use
 - Near-immediate transaction finality
 - High-availability
 - API access to third-party applications
 - Stable, non-volatile digital currency pegged at a specific rate to fiat cash
- **Functional & Non-Functional Requirements**
 - Central Banks
 - Initialize or setup blockchain
 - Issue digital currency
 - Create wallet addresses for commercial banks (in indirect model) and for users (in direct model)
 - Distribute digital currency to commercial banks (in indirect model) and to users (in direct model)
 - View transactions
 - Burn digital currency when required
 - Deploy multiple nodes if needed

Requirements

▪ **Functional & Non-Functional Requirements**

- Commercial Banks and Intermediaries
 - Create wallet addresses for users
 - Distribute digital currency to users
 - View transactions
 - Offer additional financial services on top of CBDC platform
 - Maintain a local node of the blockchain
- End-Users
 - Access individual wallet to view transactions and balance
 - Conduct P2P transfers
 - Burn digital currency owned by it
 - Ensure the safety of private keys of corresponding wallet addresses
 - Provide necessary information or documents to banks

■ Design of Direct CBDC Model

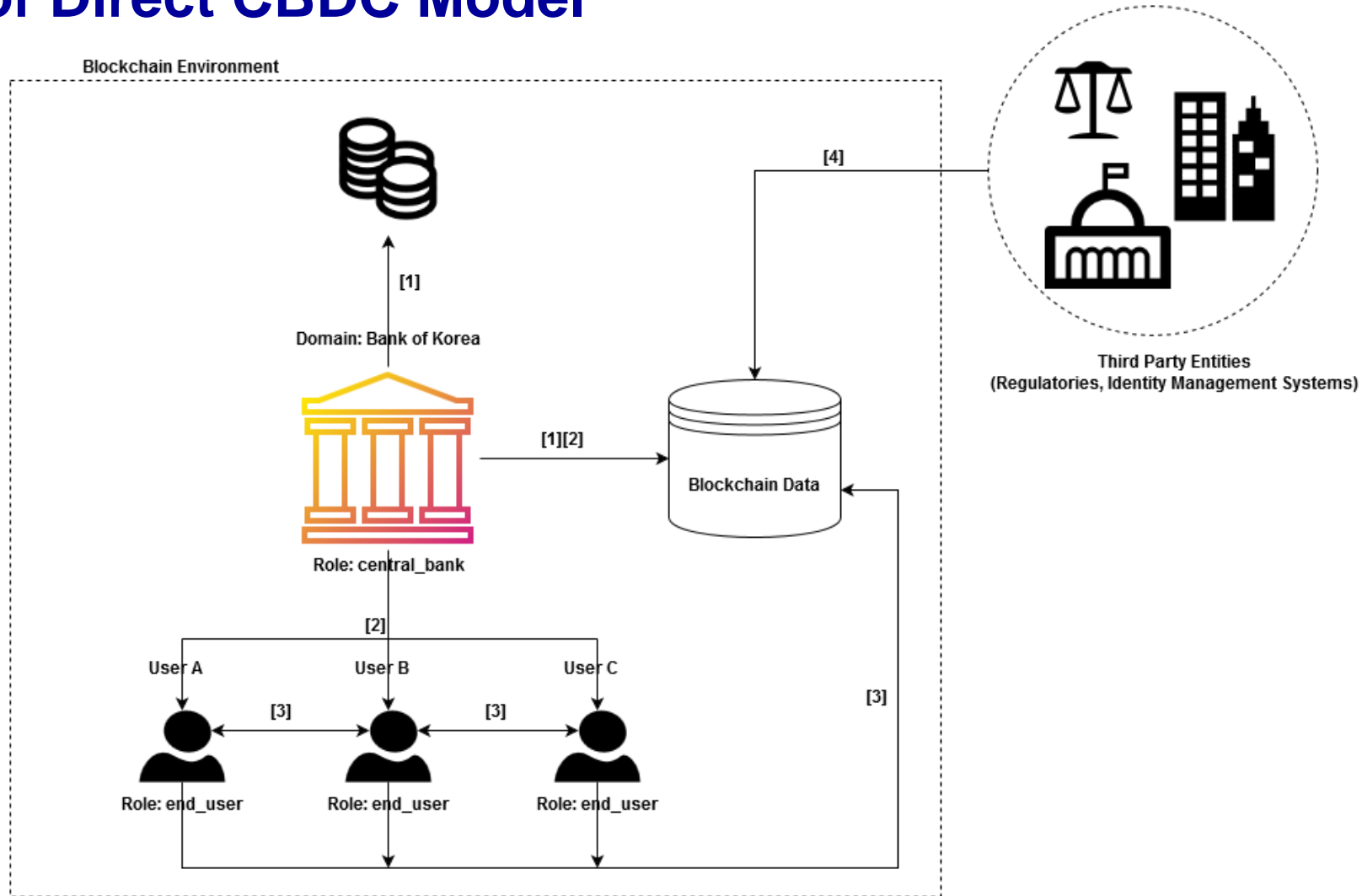


Fig. Proposed design for blockchain-based direct CBDC model

■ Design of Direct CBDC Model

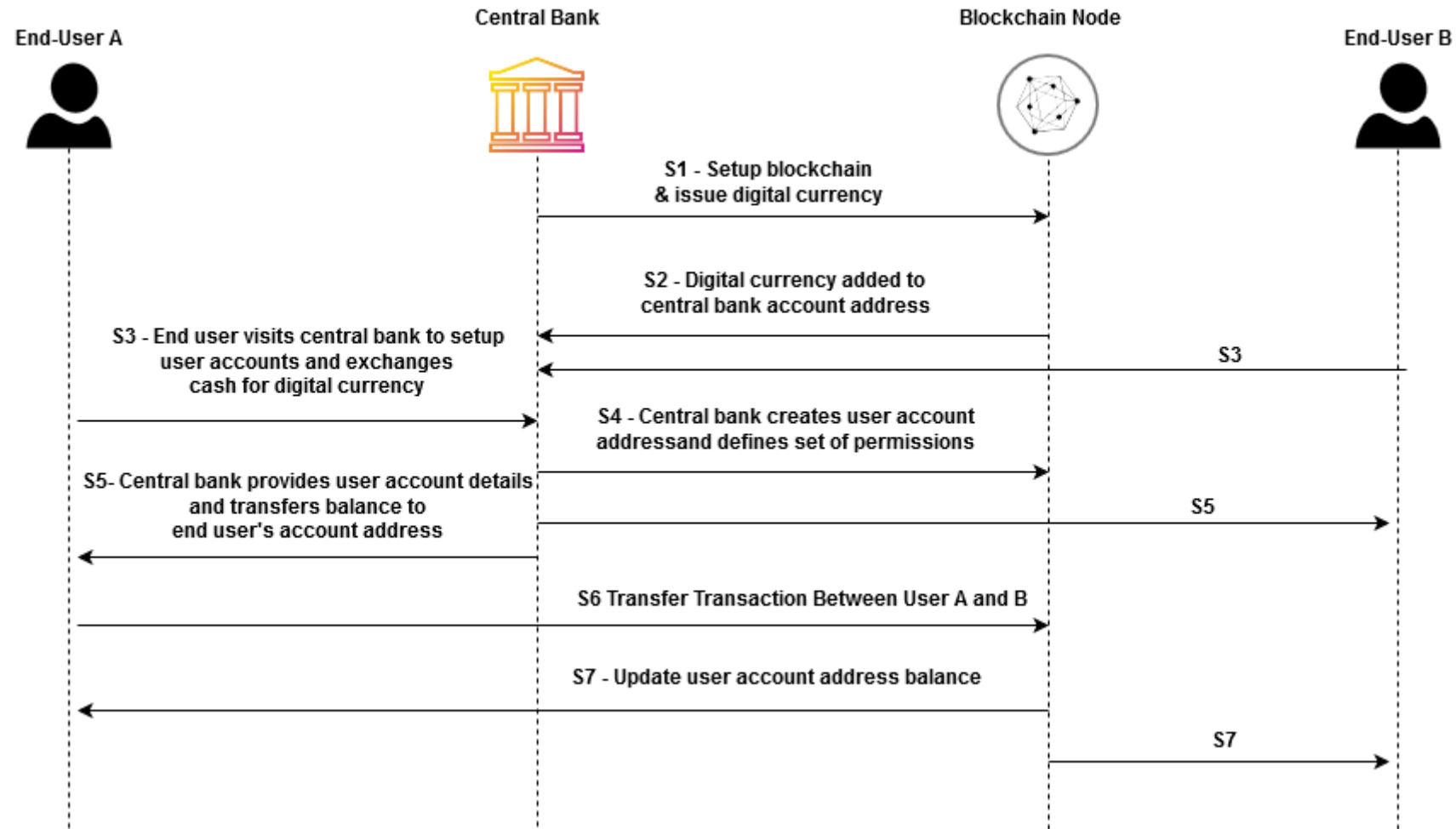


Fig. Sequence diagram depicting process flow in the proposed direct CBDC model

Design

■ Design of Indirect CBDC Model

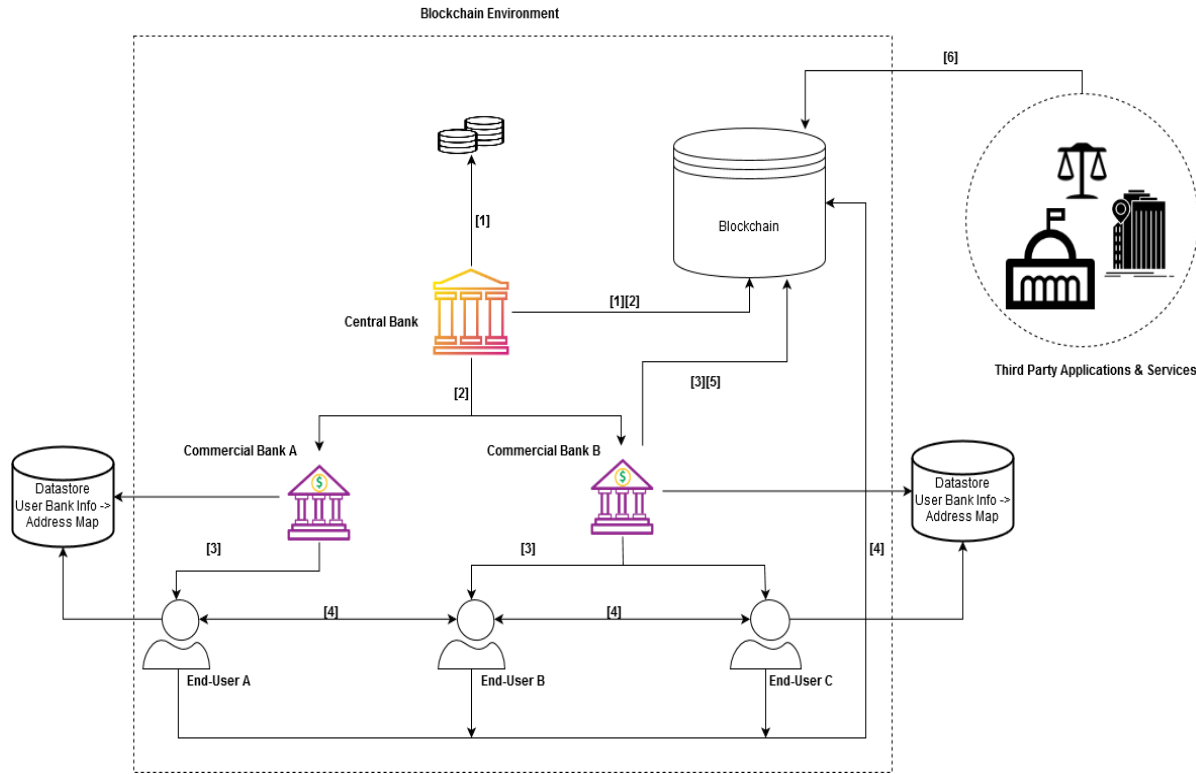


Fig. Proposed design for blockchain-based indirect CBDC model

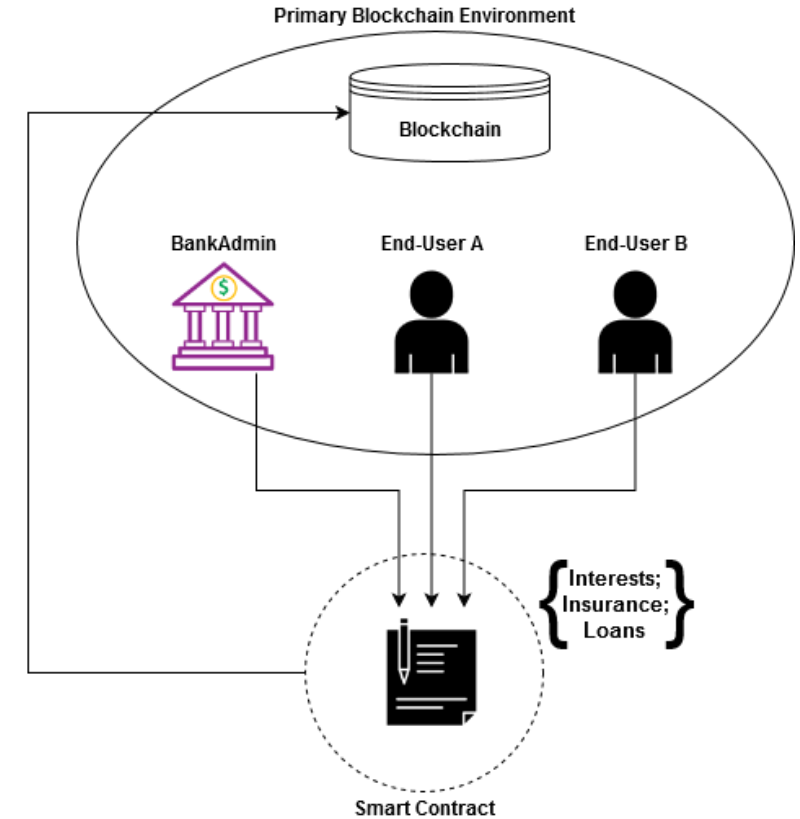


Fig. Offering of financial services via smart contracts

■ Design of Indirect CBDC Model

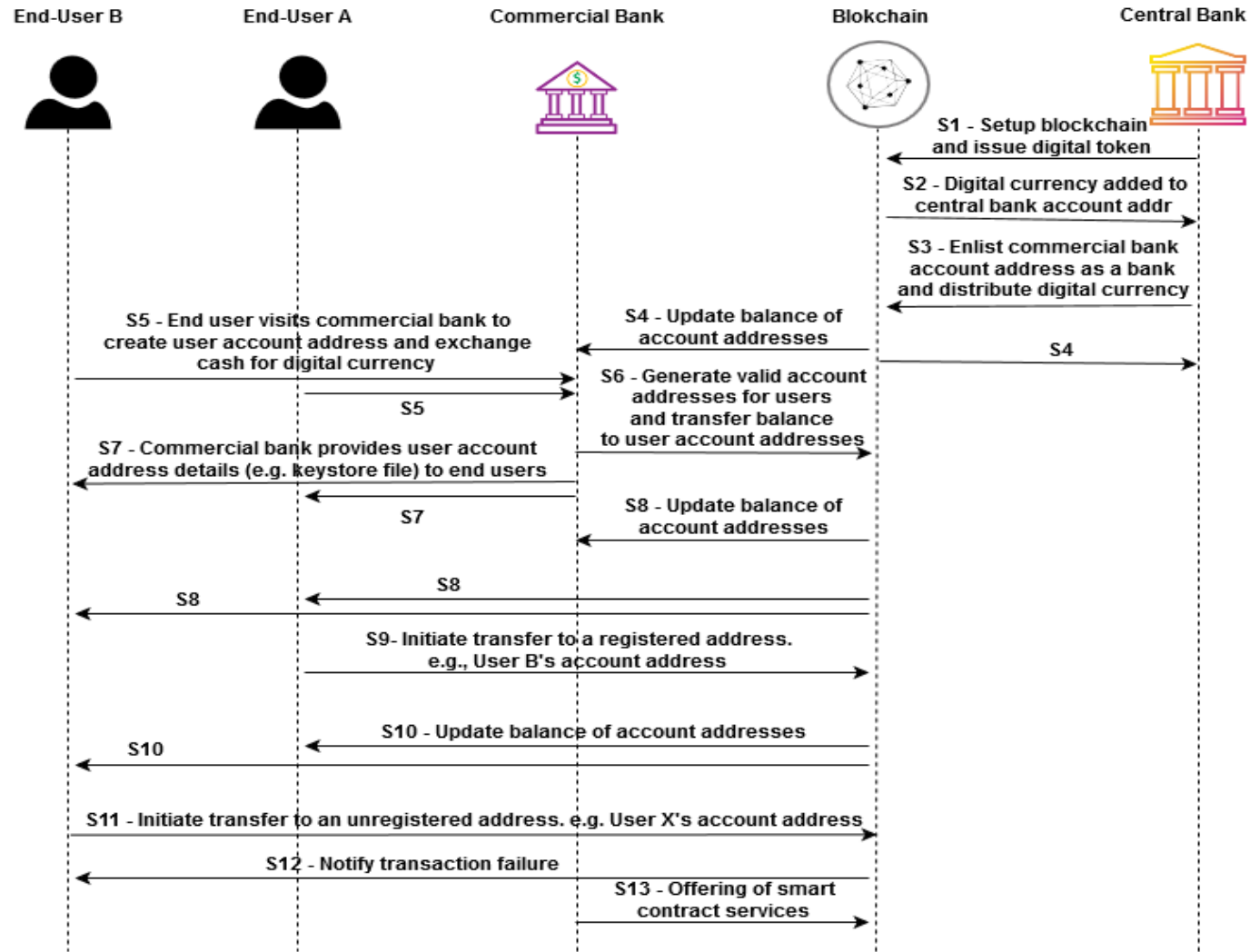


Fig. Sequence diagram depicting process flow in the proposed indirect CBDC model

Implementation

Implementation

■ Implementation of Direct CBDC Model

- Use of Hyperledger Iroha blockchain platform
 - Permissioned blockchain environment
 - Use Cases: digital asset and identities management, payment systems, logistics, etc.
 - Built-in commands and queries. e.g., create asset, create user, create role, view asset, etc.
- Custom definition of roles are attached to users

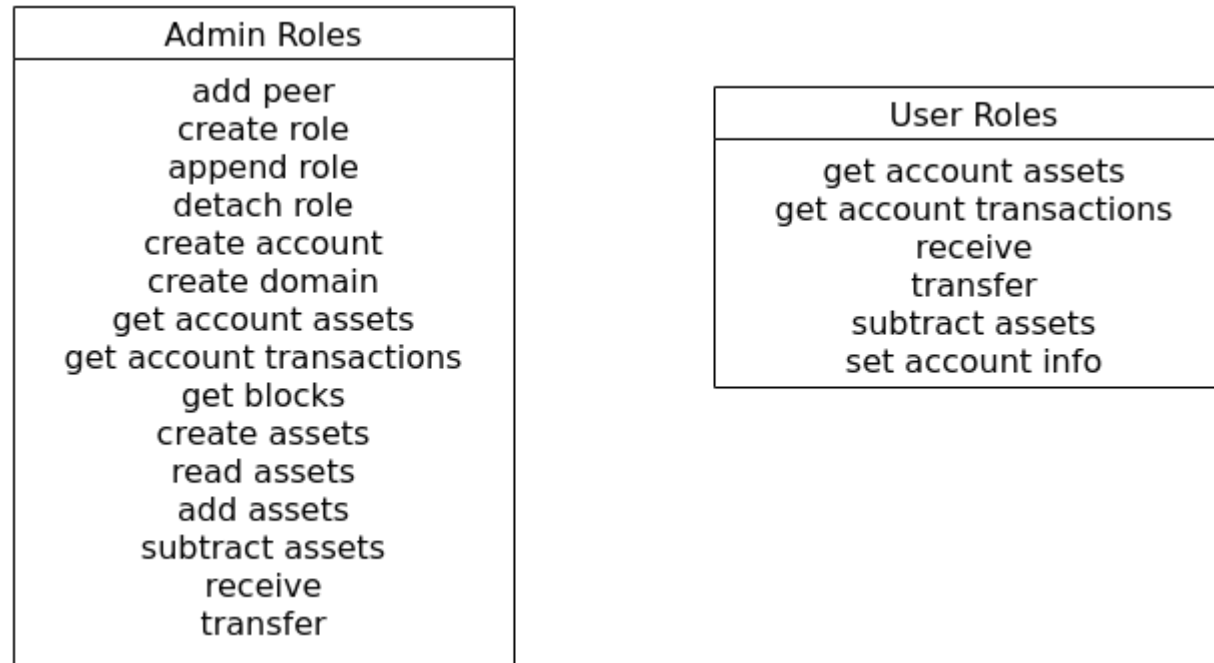


Fig. Custom defined set of roles created for end-user and central bank administrator

Implementation

■ Implementation of Direct CBDC Model

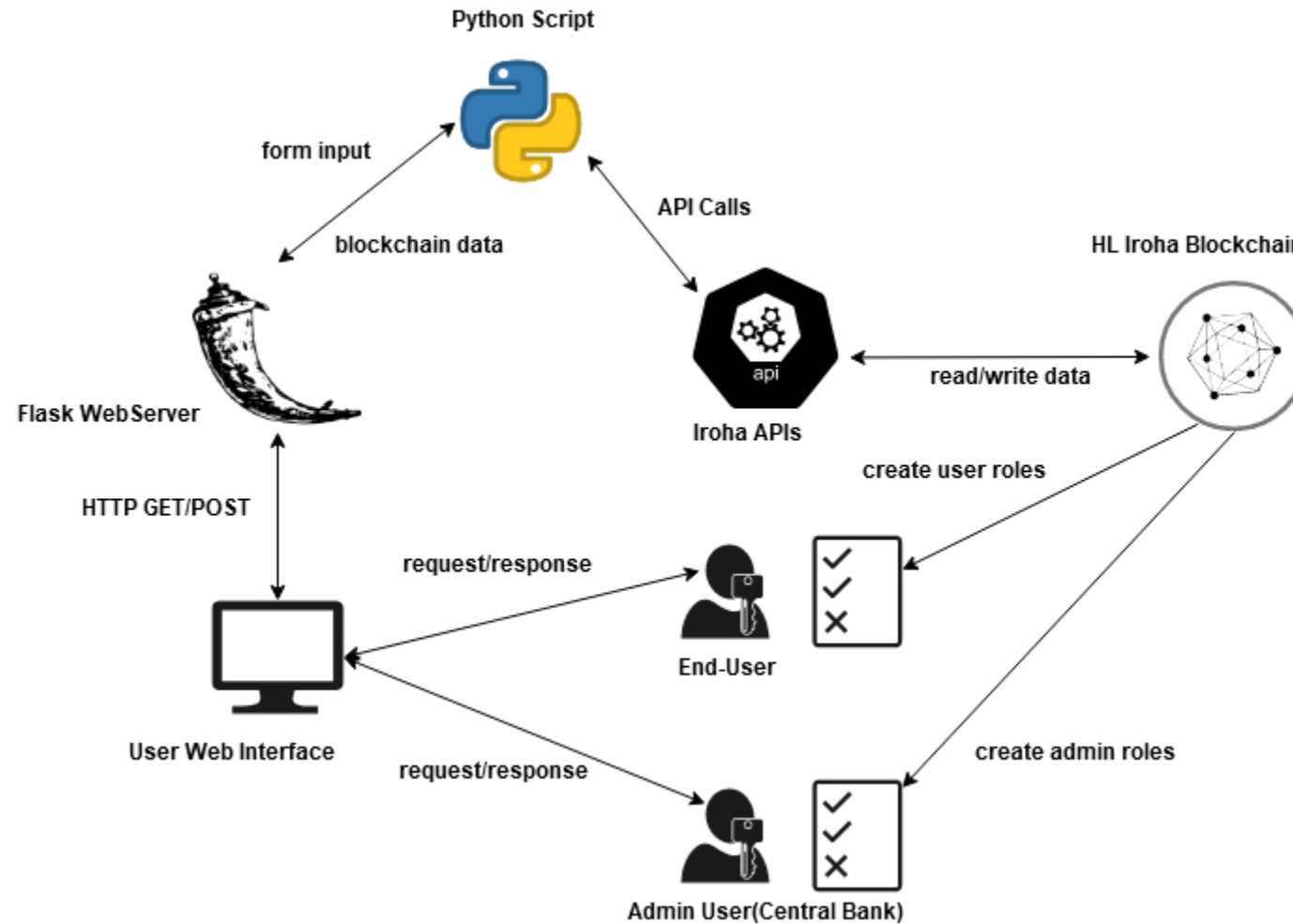


Fig. Implementation details of direct CBDC model using Hyperledger Iroha

Implementation

■ Implementation of Indirect CBDC Model

- Use of Quorum Blockchain Platform
 - Permissioned blockchain network
 - Support for “private” transactions
 - Smart contract execution functionality
- Deployed a token smart contract containing additional financial services e.g., deposit service, mapping of address to real-world identity, controllable actions, etc.

```
1 struct Deposit {
2     uint256 id;
3     address payable depositor;
4     address payable provider;
5     uint256 rate;
6     uint256 timeperiod;
7     uint256 principal;
8     uint256 maxDepositAmt;
9     uint256 endtime;
10    uint256 starttime;
11    uint256 interest;
12    uint256 amt;
13    bool isAvailable;
14    bool notWithdrawn;
15 }
16 mapping(uint256=>Deposit) public deposits;
```

```
17 struct AccountInfo {
18     address userAddress;
19     address creatorAddress;
20     string name;
21     string identification;
22     uint256 idnum;
23 }
24
25 mapping(uint256=>AccountInfo) public accountDetailsById;
26 mapping(address=>AccountInfo) public accountDetailsByAddr;
```

```
1 mapping(address=>bool) public validAddresses;
2 mapping(address=>bool) public validBankAddresses;
3
4 function addUserAddressInfo(...) public bool (returns success) {
5     require(validBankAddresses[msg.sender] == true);
6     ...
7 }
8
9 function transfer(address _to, uint256 _val) public bool (returns
10 success) {
11     require(validAddresses[_to] == true);
12     ...
13 }
14 function makeDeposit(...) public bool (returns success) {
15     require(validAddresses[msg.sender] == true);
16     ...
17 }
```

Fig. Smart contract code snippet for deposit object, account address mapping and control of token transfers

Implementation

■ Implementation of Indirect CBDC Model

- Deposit service implemented using smart contract

Algorithm 1 offerDeposit

Parameters: $rate, timeperiod, maxDepositAmt, msg.sender$

Require: $SenderBalance \geq maxDepositAmt$

Stage 1: Initialize Deposit

$depositCount \leftarrow depositCount + 1$

$deposits[depositCount].id \leftarrow depositCount$

$deposits[depositCount].provider \leftarrow msg.sender$

$deposits[depositCount].rate \leftarrow rate$

$deposits[depositCount].timeperiod \leftarrow timeperiod$

$deposits[depositCount].maxDepositAmt \leftarrow maxDepositAmt$

$deposits[depositCount].isAvailable \leftarrow true$

Algorithm 3 withdrawDeposit

Parameters: $id, msg.sender$

Require: $now() \geq deposits[id].endtime$

$msg.sender = deposits[id].depositor$

$deposits[id].notWithdrawn = true$

Stage 1: Update balance

$balanceOf[depositor]+ = amt$

$balanceOf[provider]- = amt$

Stage 2: Update notWithdrawn flag

$deposits[id].notWithdrawn = false$

Algorithm 2 makeDeposit

Parameters: $id, principal, msg.sender$

Require: $SenderBalance \geq principal$

$deposits[id].maxDepositAmt \geq principal$

$deposits[id].isAvailable = true$

$validAddresses[msg.sender] == true$

Stage 1: Update deposit

$deposits[id].depositor \leftarrow msg.sender$

$deposits[id].principal \leftarrow principal$

$deposits[id].starttime \leftarrow now()$

$deposits[id].endtime \leftarrow now() + timeperiod$

$deposits[id].notWithdrawn \leftarrow true$

$deposits[id].isAvailable \leftarrow false$

Stage 2: Transfer balance

$balanceOf[depositor]- = principal$

$balanceOf[provider]+ = principal$

Stage 3: Calculate interest and amount

$deposits[id].interest \leftarrow principal * timeperiod * rate / 100$

$deposits[id].amt \leftarrow principal + deposits[id].interest$

Fig. Algorithm for implementing deposit service between commercial bank and end-user using CBDC token

Implementation

■ Implementation of Indirect CBDC Model

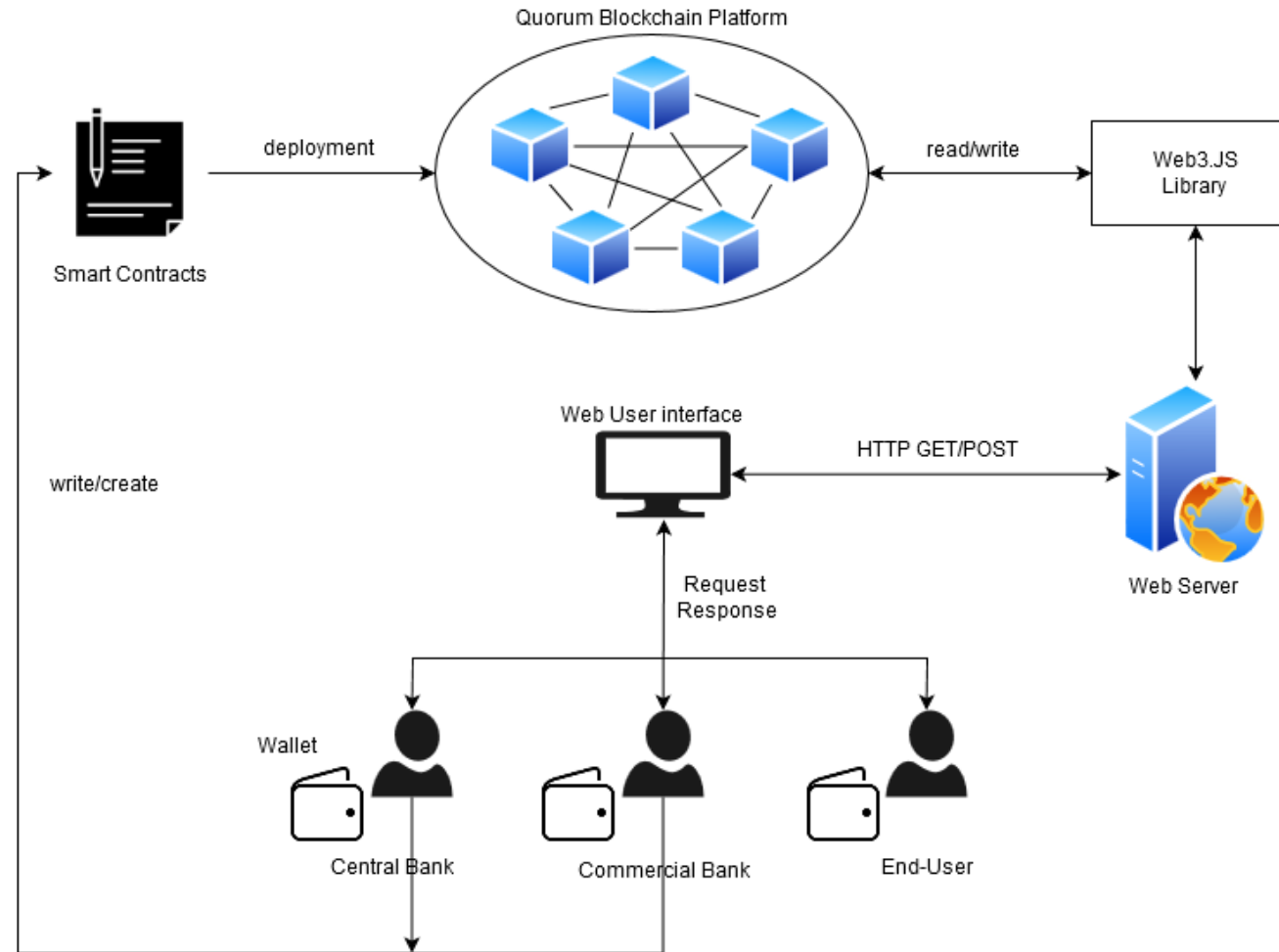


Fig. Implementation details of indirect CBDC model using Quorum blockchain

Evaluation

Evaluation

- **Quorum and Hyperledger Iroha Use Cases**
 - Project Ubin (Retail CBDC)
 - Project Khokha (Wholesale CBDC)
 - Project Bakong (Wholesale CBDC)
- **Quorum vs Hyperledger Iroha**

Features	Hyperledger Iroha	Quorum
Consensus Mechanism	YAC	I-BFT and RAFT
Support for Private Transactions	No	Yes
Smart Contract Execution	No	Yes
Built-In Commands and Queries	Yes	No
Native Cryptocurrency	No	Yes (Ether)
Decimal Precision Support	Yes	No
Metamask Compatibility	No	Yes

Evaluation

■ Pros

- Retail CBDC implementation that fits well with current banking environment
- Offering of financial services by commercial banks
- Mapping of account addresses to real-world identities + control of actions
- No use of external datastore

■ Cons

- Not absolutely relevant to any central bank initiative
- “BOKCoin” bears no relation with Bank of Korea CBDC initiative
- Improvements in UI possible
- Throughput analysis not performed

Conclusion

Conclusion

■ Summary

- Explained the concepts of CBDC
- Designed and implemented blockchain-based retail CBDC models
 - Direct model implemented using Hyperledger Iroha blockchain
 - Indirect model implemented using Quorum blockchain
- Offering of financial services via smart contracts on top of CBDC platform

■ Future Work

- Mobile application development to encourage ubiquitous use
- Scalability measure
- Use of enhanced “privacy” features of Quorum to hide transaction details
- Testing against known smart contract vulnerabilities

감사합니다

Appendix

▪ User Interfaces for Direct CBDC implementation

Central Bank Digital Currency Web Application

Home Sign Up Login

UserName

Desired username without space Eg. 'thesajan'

Domain

Admin Private Key

User accounts must be authorized by administrator

Sign Up

Fig. User account sign-up requires central bank authorization

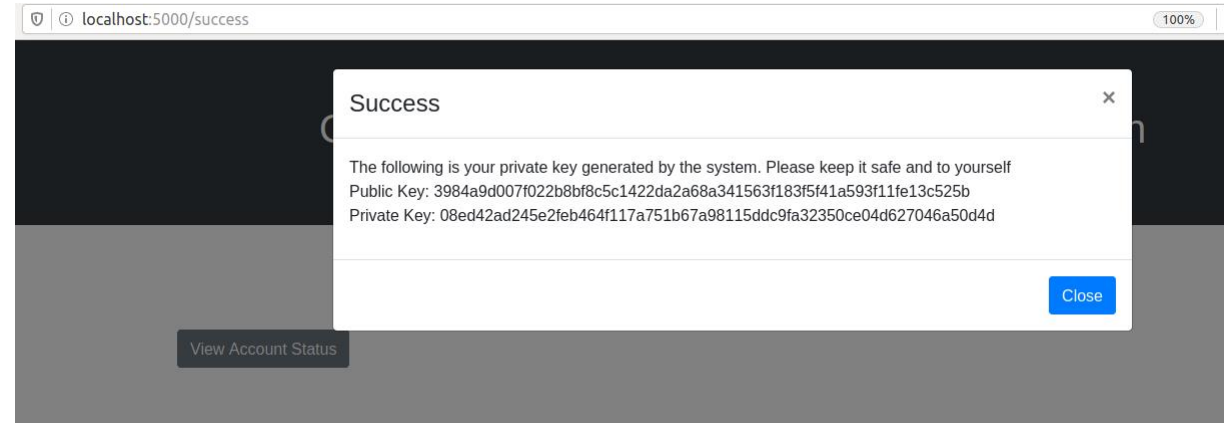


Fig. Private public key-pair generated for an end-user

Central Bank Digital Currency Web Application

Home Sign Up Login

Welcome rajan@bok

The following is your data on asset holdings

Asset ID	Balance
NULL	0.0

Add New Coins New Transaction View Transactions Burn Tokens

Fig. Newly created user has no initial balance

Appendix

■ User Interfaces for Direct CBDC implementation



Central Bank Digital Currency Web Application

Home Sign Up Login

From

sajan@bok
Sender's username with domain. Eg. 'thesajan@bok'

To

rajan@bok
Receiver's username with domain. Eg. 'thesajan@bok'

Amount

200.55
Upto 2 decimal precision. Eg. '12.34'

Message

init top-up for my brother
Message attached to transfer. Eg. Init TopUp

Private Key

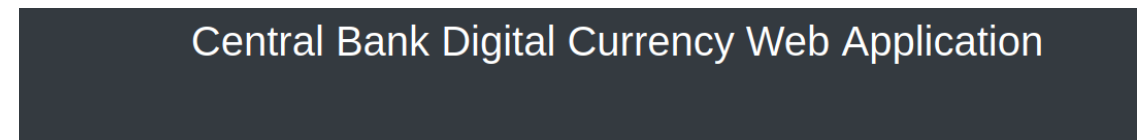
9c77cb435e64ceba6945ed82a8e1b884fe32d197ecd61062508af3c7cf811579
Sequence of private key digits and alphabets

Send Reset

Fig. P2P Transfer between two users in the system

```
File Edit View Search Terminal Tabs Help
sajan@sajan-X542UN: ~/cbdc
root@75660cd05d8f: /tmp/block_store
root@75660cd05d8f: /tmp/block_store# cat 0000000000000017
{"blockV1":{"payload":{"transactions":[{"payload":{"reducedPayload":{"commands":[{"transferAsset":{"srcAccountId":"sajan@bok","destAccountId":"ana@bok","assetId":"bokcoin#bok","description":"just for you","amount":"20.34"}]},"creatorAccountId":"sajan@bok","createdTime":"1590421384943","quorum":1},"signatures":[{"publicKey":"2d59468d4d0bebf98d41cce40b3810dfb887f95b6d134784da0e96eede645503","signature":"c6be4ffbaaf726f5d2db65d5cd2175df673be569d67aafe1fdb75418390770b45ab2380e693421f07b427ce4fe8a3f5f740beee843c707668da2368ab51b1303"}]}],"height":"17","prevBlockHash":"47f760fab01788309ba13a35256894c7ee1a960c9b617e607ccd908cc2f26edf","createdTime":"1590421386283"},"signatures":[{"publicKey":"bddd58404d1315e0eb27902c5d7c8eb0602c16238f005773df406bc191308929","signature":"becb6036ad380c05019f1142d371999ca7be0d97d0024fd3c7187cd5514f5a2173d7f121f74bc7a9a1f3900a2414cbc056c42774e64dfbe3ae0e14b82ce60b04"}]}]}root@75660cd05d8f: /tmp/block_store#
```

Fig. Transaction data stored in blockchain in JSON format



Central Bank Digital Currency Web Application

Home Sign Up Login

Welcome rajan@bok

The following is your data on asset holdings

Asset ID	Balance
bokcoin#bok	200.55

Add New Coins New Transaction View Transactions Burn Tokens

Fig. Update in balance after transaction execution

Central Bank Digital Currency Web Application

Home Sign Up Login

Welcome sajan@bok

The following are the list of transactions you have initiated:

Sender	Receiver	Amount
admin@bok	sajan@bok	777.77
sajan@bok	ana@bok	123.45
sajan@bok	chkang@bok	99.99
sajan@bok	ana@bok	20.34
admin@bok	sajan@bok	1000.5
sajan@bok	rajan@bok	200.55

Fig. List of transactions corresponding to a user

Appendix

▪ User Interfaces for Indirect CBDC implementation

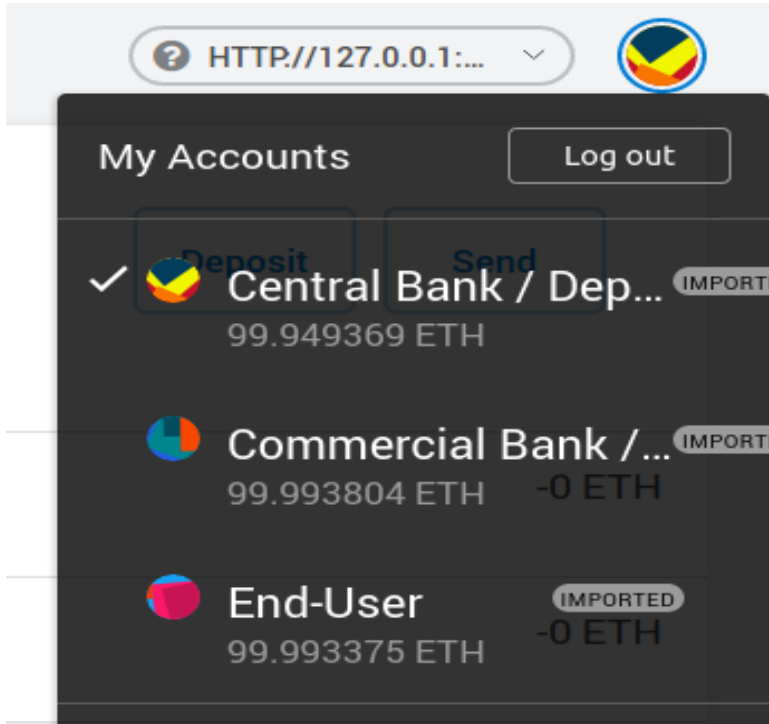


Fig. Example list of registered accounts

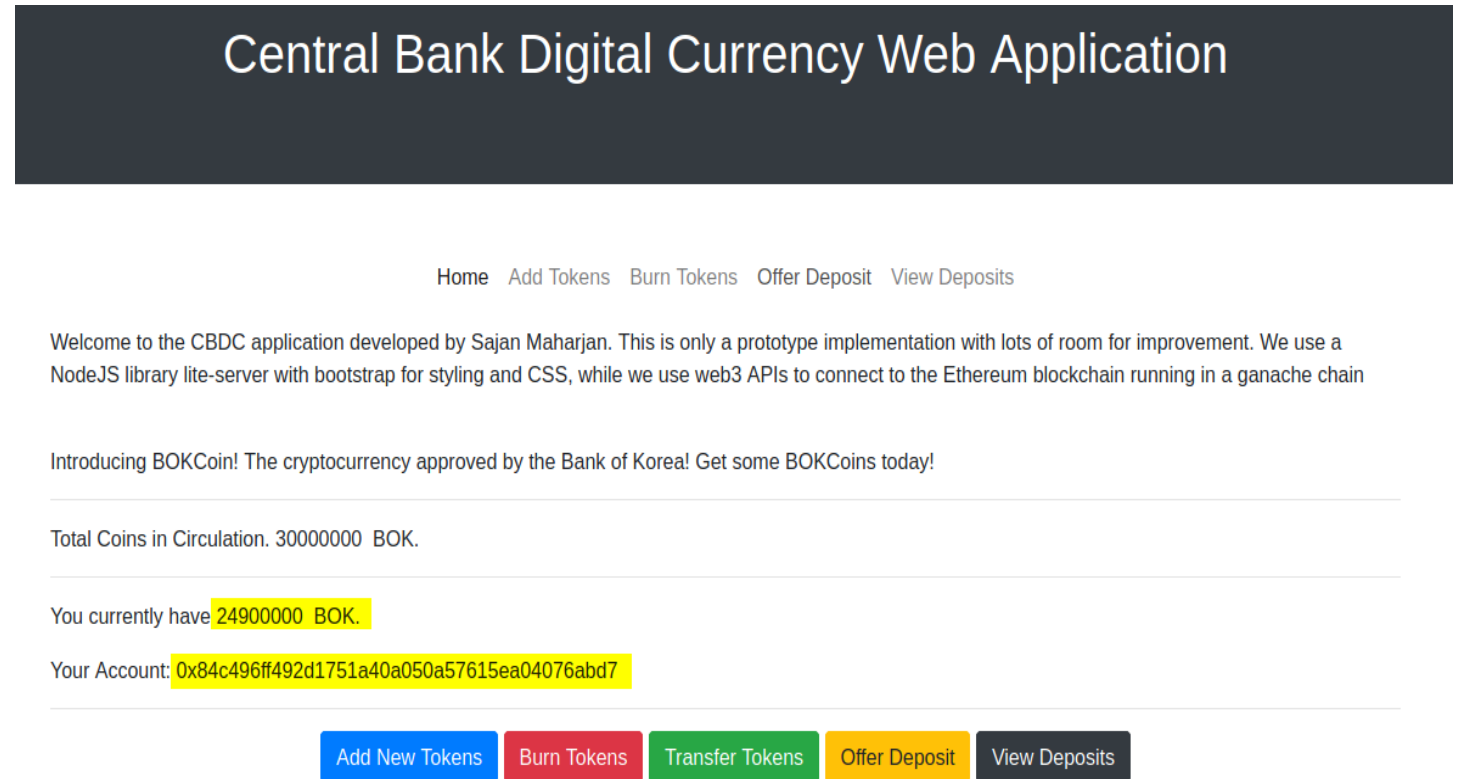


Fig. Landing page showing central bank's account balance

Appendix

■ User Interfaces for Indirect CBDC implementation

Central Bank Digital Currency Web Application

Home Add Tokens Burn Tokens Offer Deposit View Deposits

Welcome to the CBDC application developed by Sajan Maharjan. This is only a prototype implementation with lots of room for improvement. We use a NodeJS library lite-server with bootstrap for styling and CSS, while we use web3 APIs to connect to the Ethereum blockchain running in the ganache

Introducing BOKCoin! The cryptocurrency approved by the Bank of Korea! Get some BOKCoins today!

Total Coins in Circulation. 30000000 BOK.

You currently have 4999500 BOK.

Your Account: 0x1aa7d64a9fb75e4174dcfffd565851dd8dce461d

ID	Depositor	Provider	Rate	Timeperiod	Principal	Interest	Max Deposit Amount	Available	Not Redeemed
1	0x65d542e407470c4c49a96e5ee6545ac45647cf43	0x1aa7d64a9fb75e4174dcfffd565851dd8dce461d	5	1	10000	500	10000	false	false

Make Deposit Redeem Deposit

Fig. Initial List of Deposits

Central Bank Digital Currency Web Application

Home Add Tokens Burn Tokens Offer Deposit View Deposits

Introducing BOKCoin! The cryptocurrency approved by the Bank of Korea! Get some BOKCoins today!

Total Coins in Circulation. 30000000 BOK.

You currently have 4999500 BOK. Commercial Bank Address

Your Account: 0x1aa7d64a9fb75e4174dcfffd565851dd8dce461d

Rate
12
Rate of Interest you would offer to depositors. No decimals allowed.

TimePeriod
1
Number of TimePeriods before return. One Timeperiod equals 1 minutes.

Maximum Acceptable Deposit
1000
Number of TimePeriods before return. One Timeperiod equals 1 minutes.

Offer Deposit Services Reset

Fig. Offering of deposit by a commercial bank

Appendix

▪ User Interfaces for Indirect CBDC implementation

Home Add Tokens Burn Tokens Offer Deposit View Deposits

Introducing BOKCoin! The cryptocurrency approved by the Bank of Korea! Get some BOKCoins today!

Total Coins in Circulation. 30000000 BOK.

You currently have 99800 BOK. Deduction in End-User's Balance

Your Account: 0x65d542e407470c4c49a96e5ee6545ac45647cf43 End-User's Account Address

ID	Depositor	Provider	Rate	Timeperiod	Principal	Interest	Max Deposit Amount	Available	Not Redeemed
1	0x65d542e407470c4c49a96e5ee6545ac45647cf43	0x1aa7d64a9fb75e4174dcffd565851dd8dce461d	5	1	10000	500	10000	false	false
2	0x65d542e407470c4c49a96e5ee6545ac45647cf43	0x1aa7d64a9fb75e4174dcffd565851dd8dce461d	12	1	700	84	1000	false	true

Make Deposit Redeem Deposit

Fig. Deposit object's information is updated on making deposit

Home Add Tokens Burn Tokens Offer Deposit View Deposits

Introducing BOKCoin! The cryptocurrency approved by the Bank of Korea! Get some BOKCoins today!

Total Coins in Circulation. 30000000 BOK.

You currently have 99800 BOK.

Your Account: 0x65d542e407470c4c49a96e5ee6545ac45647cf43 End-User's Account Address

Deposit ID

Input the ID of which offered deposit and is available

Redeem Deposit Reset

Fig. Withdrawl of user's deposit with interest on maturity

Appendix

▪ User Interfaces for Indirect CBDC implementation

Home Add Tokens Burn Tokens Offer Deposit View Deposits

Introducing BOKCoin! The cryptocurrency approved by the Bank of Korea! Get some BOKCoins today!

Total Coins in Circulation. 30000000 BOK.

You currently have 100584 BOK. Increment in End-User's Balance

Your Account: 0x65d542e407470c4c49a96e5ee6545ac45647cf43 End-User's Account Address

ID	Depositor	Provider	Rate	Timeperiod	Principal	Interest	Max Deposit Amount	Available	Not Redeemed
1	0x65d542e407470c4c49a96e5ee6545ac45647cf43	0x1aa7d64a9fb75e4174dcfffd565851dd8dce461d	5	1	10000	500	10000	false	false
2	0x65d542e407470c4c49a96e5ee6545ac45647cf43	0x1aa7d64a9fb75e4174dcfffd565851dd8dce461d	12	1	700	84	1000	false	false

Redemption flag is updated

Make Deposit Redeem Deposit

Fig. Change in user's balance and deposit object's flag updated