Final Report

An E-Wallet Solution for Financial Inclusion

Gu Yining  3035638064

April 18, 2023
Abstract

The term “financial inclusion” has gained importance since the early 2000s and has made substantial strides forward over the past ten years in expanding access to financial services [1]. However, many remain excluded from the formal financial system due to unequal regional development and the lack of a coordinated framework for the development of the financial system. Financial technology (FinTech) innovations represent an opportunity to promote financial inclusion. But conventional online financial services solutions based on an internet connection may not work for those who don’t always have stable internet access. This project aims to design an e-wallet solution for financial inclusion which provides fundamental savings, loan, and payment services that work both online and offline. The project employs innovative financial technologies, including but not limited to blockchain, cryptocurrencies, cryptographic methods, and network communication technologies. The team has finished the basic design and literature evaluation. Currently, the team is analyzing the key technical points of the e-wallet platform and has proposed preliminary suggestions for innovative solutions based on the evaluation of existing relevant solutions. The next step is developing a self-designed solution with code demos.
Acknowledgements

We would like to express our deepest gratituation to our final year project supervisor, Prof. S. M. Yiu, for his unwavering guidance and support. We are also grateful to the Department of Computer Science, the University of Hong Kong, for providing us with the opportunity.
List of Figures

Figure 1. Workflow of the proposed e-wallet. 15
Figure 2. Pure Wallet implementation architecture. 17
Figure 3. Allpay online-to-offline (O2O) transaction. 18
Figure 4. QR code payment model. 19
Figure 5. Client setup process. 23
Figure 6. Offline P2P payment process. 25
Figure 7. Smartphone ownership rate in sub-Saharan Africa countries 27
Figure 8. The increasing percentage of smartphone ownership rate in sub-Saharan Africa countries 27
Figure 9. The usage rate of electronic payments, from 2009 to 2011 29
List of Tables

Table 1. Millestones
<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AML</td>
<td>Anti-Money Laundering</td>
</tr>
<tr>
<td>DLT</td>
<td>Distributed Ledger Technology</td>
</tr>
<tr>
<td>ECDSA</td>
<td>Elliptic Curve Digital Signature Algorithm</td>
</tr>
<tr>
<td>G2P</td>
<td>Government-to-Person</td>
</tr>
<tr>
<td>KYC</td>
<td>Know Your Customer</td>
</tr>
<tr>
<td>NFC</td>
<td>Near-Field Communication</td>
</tr>
<tr>
<td>P2P</td>
<td>Peer-to-Peer</td>
</tr>
<tr>
<td>SE</td>
<td>Secure Element</td>
</tr>
<tr>
<td>SSL</td>
<td>Secure Sockets Layer</td>
</tr>
<tr>
<td>TEE</td>
<td>Trusted Execution Environment</td>
</tr>
<tr>
<td>TLS</td>
<td>Transport Layer Security</td>
</tr>
</tbody>
</table>
# Table of Contents

Abstract 1

Acknowledgements 2

List of Figures 3

List of Tables 4

Abbreviations 5

1 Introduction 8
   1.1 Background 8
   1.2 Problem Statements 9
   1.3 Motivation 9
   1.4 Deliverables 10
   1.5 Outline of the Report 10

2 Literature Review 11

3 Methodology 12
   3.1 Financial Technologies 12
      3.1.1 Blockchain 12
      3.1.2 Cryptocurrency 12
      3.1.3 Cryptographic Method 12
      3.1.4 Network Communication Technology 13
   3.2 Literature Evaluation 13
   3.3 E-Wallet Design 13

4 Findings 13
   4.1 Project Milestones 13
   4.2 Functions of the e-wallet 14
   4.3 Key Technical Problems 16
   4.4 Literature Evaluation 17

5 The proposed e-wallet platform 20
   5.1 Proposed decisions to the four key technical problems 20
5.1.1 Overall structure  
5.1.2 Client side data storage and manipulation  
5.1.3 Offline P2P transaction  
5.1.4 Data synchronization  
5.2 Protocol  
5.2.1 Key distribution  
5.2.2 Client setup  
5.2.3 Deposit and withdrawal money  
5.2.4 Interest calculation and accumulation  
5.2.5 Offline P2P payment  

6 Discussion  
6.1 Our proposed e-wallet solution  
6.2 Offline e-wallet to financial inclusion  
6.2.1 Necessities of achieving inclusive finance through offline e-wallet  
6.2.2 Rationalities of achieving inclusive finance through offline e-wallet  
6.2.2.1 User position  
6.2.2.2 Provider position  

7 Conclusion  
References
1 Introduction

1.1 Background

Financial inclusion is defined as the availability and equality of opportunities to access financial services [2]. It refers to a process by which individuals and businesses can access appropriate, affordable, and timely financial products and services, including banking, loan, equity, and insurance products [3]. Financial inclusion typically directs sustainable financial services to those who are unbanked and underbanked. It empowers the poorest and most vulnerable in society with the ability to manage money and even step out of poverty. From a broader perspective, it may ultimately be able to help develop entire communities and lead to more robust and sustainable economic growth.

Since the early 2000s, the term "financial inclusion" has obtained significance as the result of identifying financial exclusion and relevance to poverty according to the World Bank [1]. The reality that most poor people in the world still lack access to sustainable financial services has been widely aware. Building inclusive financial sectors has been promoted by United Nations to help improving people’s lives. Over the last ten years financial inclusion has made strong strides forward. International organizations such as the United Nations Secretary-General’s Special Advocate for Inclusive Finance for Development (UNSGSA), the United Nations Development Programme (UNDP), International Monetary Fund (IMF) and the Standard-Setting Bodies (SSBs) are committed to ensuring financial inclusion’s strong presence through international exchanges and cooperation, negotiates multilateral agreements, donations, and supervision.

Some countries have also made valuable attempts in the field of financial inclusion and achieved results. In the Philippines, Credit Information Bureau, Inc. (CIBI) benefit more than 4 million unbanked Filipinos by introducing a new set of credit scores for loans with lower requirement [4]. In India, the Reserve Bank of India (RBI) relaxed previous requirement policies about opening new bank branches to increase branches in underserved areas and achieve a more even spread of banking facilities [5]. The self-help group (SHG) linkage model has also been proposed to improve financial inclusion by linking relatively vulnerable community groups to the formal banking system [6]. MFI (Microfinance) ideals have been adopted in the United States to reach marginalized communities to support and promote upward mobility [7].
The development of FinTech provides opportunities to promote financial inclusion. Inclusive digital financial services such as mobile wallet, e-payment, digital currency can reach the formerly excluded groups of people. For example, banks develop mobile bank apps to provide financial services the same as physical banks. The financial service is now available in more than 80 countries, some of which are in a quite large scale [8].

1.2 Problem Statements

Existing solutions have promoted financial inclusion to a large extent, but there are still some deficiencies. First, the current services are still within the region of the traditional financial and banking system. Many excluded groups are located in economically underdeveloped areas with inaccessible transportation. It is more difficult for them to reach traditional banks directly. It is more difficult for them to have direct access to conventional banks. Broadening the reach of traditional banks and lowering barriers to entry does help, but it is not realistic for the wider marginalized group. Second, current inclusive digital financial services highly rely on a stable Internet connection. However, the targeted marginalized groups may not have a consistent and stable internet connection due to a lack of infrastructure.

1.3 Motivation

Given the exploration of financial inclusion and the development of financial technology, we believe that the research on the financial technology solution to financial inclusion is rewardable, necessary as well as feasible.

There is significant value and necessity in promoting financial inclusion, with consistent positive effects on economic growth and social development. Besides, it contributes to reducing poverty and inequality. According to the survey [8], around 90 percent of small businesses are not connected to formal financial sectors, and around 60 percent of the population even have no bank account. The development of financial inclusion benefits vulnerable and marginalized groups such as the poor, disabled, and rural populations with access to a full suite of quality financial services.

McKinsey & Company rightly points out that developing innovative products is essential to further expanding financial inclusion [9]. Examples are blockchain, cryptocurrency, and cryptography. To fill the current research gap, digital solutions to provide online and offline financial services are significant. Our team conceived of an
e-wallet solution that mitigates the limitations of traditional banks and the high dependence of today’s electronic solutions on the Internet.

1.4 Deliverables

Upon completion, the project will deliver a detailed discussion on the topic together with some code demos. The discussion will be on the proposed e-wallet system, analyzing the feasibility of approaches learned from existing solutions, and describing and evaluating the newly proposed innovative solution. The code demos are expected to demonstrate the innovative protocols of the core solutions to the key problems. Notably, they will not be completed and readily available products but technical samples to showcase the ideas of the solutions. The project will provide a prototype for an e-wallet solution for financial inclusion, which works under both online and offline circumstances. Though it cannot be directly deployed for commercial use, it renders a new perspective to connect the unbanked population to a relatively accessible financial service system. Hopefully, realistic financial products can be developed based on this prototype to enhance financial inclusion in underdeveloped areas and bring welfare to people suffering from the lack of banking services.

1.5 Outline of the Report

The remaining of this report will first discuss the literature review in Section 2. It then proposed the project’s methodology in Section 3, including financial technology (Section 3.1), literature review (Section 3.2), and e-wallet design (Section 3.3). The milestone of our project is illustrated (Section 4.1). The functional design and workflow are described (Section 4.2), and key technical problems are identified (Section 4.3). Literature evaluation and preliminary ideas on the key technical problems are in Section 4.4. Section 5 explained the proposed e-wallet platform in detail, with decisions to the four key technical problems (Section 5.1) and designed protocols (Section 5.2). Section 6 is the discussion, including evaluate out proposed e-wallet solution (Section 6.1) and explain the reason and benefit to solve financial inclusion using a offline e-wallet (Section 6.2). The paper closes with a conclusion in Section 7.
2 Literature Review

There have been many related works on digital solutions for financial inclusion. The review is based on a problem-by-problem basis, helping to analyze the advantages and disadvantages of the solutions.

[10] proposed implementation of blockchain in the card payment system. The utilization of blockchain in payment systems bypasses traditional financial institutions, and therefore reduces transaction costs and raises the level of cybersecurity to some extent. The study provided possibilities of applying blockchain with its decentralized features to card payment systems and suggested better data integrity credited to blockchain.

Bamert et al. [11] proposed "BlueWallet", using hardware tokens as physical Bitcoin wallets. Elliptic Curve Digital Signature Algorithm (ECDSA) was designed to be used for verification and transaction signing to achieve an adequate level of security in data transfer and storage. Though the hardware token can authorize transactions offline, the counterparty must be connected to the Bitcoin network so that the transaction can be validated and recorded in the blockchain. Thus, it still does not support offline peer-to-peer (P2P) transactions.

A blockchain cryptocurrency system, DelegaCoin, for offline coin delegation is proposed by Li et al. in [12]. Remarkably, they suggested the utilization of trusted execution environments (TEEs) for the reliable execution of certain protocols. With some cryptographic procedures inside TEE, a coin owner can delegate the right of using the coin to a delegate without connecting to the blockchain network. Although DelegaCoin is only a model for coin delegation instead of offline transactions, it provides some hints for offline data transfer for token transactions.

In [13], the authors introduced an implementation of offline cryptocurrency transactions called Pure Wallet (PW) in the context of blockchain. It uses Ethereum smart contract and a new token to manage offline transactions and validation securely. PW successfully managed an offline transaction of 10 tokens, proving the architecture to be feasible for blockchain offline transactions. However, the authors claimed limitations such as token divisibility, falsified token detection, and different environment adoption.

This project will be built on all related studies, including but not limited to the four mentioned above, and further investigations and evaluations will be taken.
3 Methodology

3.1 Financial Technologies

To achieve deliverables, these financial technologies will be evaluated: blockchain, cryptocurrencies, cryptographic methods, and network communication technologies.

3.1.1 Blockchain

Blockchain is distributed ledger technology (DLT) with a linked list of “blocks”, that store data such as transaction records [14]. There is no centralized copy. The data are stored in its peer-to-peer (P2P) network which eliminates risks of vulnerable central points of failure [15]. Besides, Blockchain is non-deniable. Once the transaction data be recorded blocks cannot be edited without changing all the linked blocks.

In this project, the idea of Blockchain is applied in storing data to achieve offline e-wallet. Without instant Internet connection, data will not be transmitted to the server immediately. Thus, storing data in each client’s “block” securely is the key.

3.1.2 Cryptocurrency

Cryptocurrency provides an alternative way of payment using the format of a digital currency with encryption algorithms. It serves as an intermediary for transactions. It belongs to a decentralized system without reliance on central authority, such as traditional banks or government institutions.

To achieve offline payment in the project, cryptocurrency is applied in the combination of distributed ledger technology, Blockchain, to equip payment and verify the claimed money of transaction parties.

3.1.3 Cryptographic Method

Cryptography refers to methods of making data unreadable or undecipherable to ensure secrecy and integrity. Two key problems, the method to guarantee the security and integrity of the transaction records, and the approach to enable offline transactions, are crucial to the design and implementation of the proposed e-wallet.
The former is an inevitable problem for all kinds of transaction tools, and the latter is a specific requirement for the proposed e-wallet for financial inclusion as one of the features. This project will use cryptographic methods to encrypt user information and transaction records to achieve security in the e-wallet.

3.1.4 Network Communication Technology

Network Communication Technology defines a set of protocols that allow application programs to transfer information among each other without regard to the hardware and operating systems where they are run [16]. In the project, a protocol should be generated to transfer data between the two parties.

3.2 Literature Evaluation

The project is going to evaluate related literatures on the topic. The evaluation will be based on security, efficiency and scalability. The part that inspires our project’s e-wallet development will be justified.

3.3 E-Wallet Design

Based on the evaluation of related literatures, our team will propose our own design. We first raise key technical problems for the e-wallet platform. The evaluation of those problems will be applied to literatures. The findings and solutions will be shown in our design. A code demo in Python will be provided to address the main idea of our proposed solution.

4 Findings

4.1 Project Milestones

The Project Milestones are shown in table 1. We have completed the final report and code demo. Next, we will be prepared for the project exhibition and possible project competition.
<table>
<thead>
<tr>
<th>No.</th>
<th>Date</th>
<th>Task</th>
<th>Remarks</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>October 2, 2022</td>
<td>Completion of a detailed project plan. Initialized project webpage</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>November 30, 2022</td>
<td>Completion of functional design and key technical problems</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>January 15, 2023</td>
<td>Completion of the review and analysis of related literature</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>January 18, 2023</td>
<td>First presentation</td>
<td>Content of the presentation may include literature evaluation and preliminary ideas on key technical problems solutions.</td>
</tr>
<tr>
<td>5</td>
<td>January 22, 2023</td>
<td>Completion of detailed Interim report</td>
<td>Same as 4.</td>
</tr>
<tr>
<td>6</td>
<td>February 28, 2023</td>
<td>All self-designed solutions to all key problems with code demos</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>March 20, 2023</td>
<td>Evaluation of proposed methods</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>April 18, 2023</td>
<td>Final report and all code demos</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>April 17–21, 2023</td>
<td>Final presentation</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>May 3, 2023</td>
<td>Project exhibition</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>May 30, 2023</td>
<td>Project competition</td>
<td>Selected projects only.</td>
</tr>
</tbody>
</table>

Table 1. Milestones.

### 4.2 Functions of the e-wallet

Our design of the e-wallet have these functions.

- Online or in-person money deposit and withdrawal
- Online transaction
- Offline interest calculation and accumulation
• Offline P2P transactions

Figure 1 illustrates the workflow of our proposed e-wallet platform. The red arrow represents the control flow. The blue arrow is the money flow. Application A is for the registration. To enable the e-wallet, the client needs to open an account online or in-person at a physical financial institution. The e-wallet will approve and store the client’s information if the registration is successful. At this time, the backend server will record the account information and the balance. Then the client can do money deposit and withdrawal (shown in Application B). This also require Internet connection to validate the account balance and transfer the money. With the account set up, the client can perform transactions as long as there is enough balance (shown in Application C and Application D). For online transaction, the platform will send the latest ledger to the backend server. And the server will immediately check the balance. Data synchronization is critical in this part. For Offline P2P transaction (shown in Application E), both parties are supposed to validate the payment and check the balance. Protocol and physical media are needed. There remains a loan
function workflow demonstration, but the solution will not be included in our final proposed project due to the time limitation. The further study of the loan part integrated with offline scenarios could be conducted. We hope the platform will manage it offline automatically and apply a penalty whenever the contract is violated.

4.3 Key Technical Problems

- Overall structure
- Client side data storage and manipulation
- Offline P2P transactions
- Data synchronization

To implement those functions of our e-wallet mentioned in Section 4.2, four key technical problems are identified.

For the overall structure, the way to storage the clients’ and the transaction data, and the balance form have to be figured out. For the form of data storage, basically there are two main ways. One is centralized, which means one single database at the central party, the other is decentralized, use distributed ledger such as blockchain. For the form of balance, there are token-based and account-based. In token-based platform, balance is transacted in the unit of tokens. Each token has a unique identifier and only the owner can spend it. In account-based platform, balances are deducted and added for the two parties in each transaction.

The second problem is data storage and manipulation on client application. Which is the key to realize the proposed offline functions and data security and integrity. For Data storage, it is important to ensure the modification of the data by malicious user to gain improper benefit. For Data manipulation, the e-wallet platform have to ensure the pre-defined protocols and programs be correctly executed.

The third is offline P2P payment. The offline payment media that facilitate the message exchange between the two parties, such as NFC, QR code or others should be decided. The payment protocol which conveys necessary information for the transaction should be carefully designed. The efficiency, integrity, and security is crucial.

The last one is Data synchronization. As multiple clients may have to connect to the central ledger at different time, data synchronization is important to ensure the integrity of the entire e-wallet financial platform.
4.4 Literature Evaluation

[17] proposes an electronic payment architecture named Pure Wallet (PW), which applies Blockchain cryptocurrency technology in offline transactions. Figure 2 illustrates the complete workflow of PW. Before the transaction, the token manager converts cryptocurrency into digital cash in the form of a trusted secret token and leaves the transaction information to be completed in the token with an Internet connection. Then the sender encrypts the transaction value in the form of a token and sends it to the receiver through Near Field Communication (NFC). Last, the receiver converts the received token into cryptocurrency during an Internet connection by sending the information required to complete the transaction to the token manager.

![Figure 1. Pure Wallet implementation architecture [17].](image)

Pure Wallet successfully managed an offline transaction of 10 tokens, proving the architecture feasibility of blockchain offline transactions. PW performs real-time transactions that can be quickly done at any time. An NFC phone operating at 13.56 MHz frequency delivers a data rate of 424 kbit/s. A token of 64 characters encoded with UTF-8, UTF-16, or UTF-24 32 is delivered in 0.0012 s, 0.0023 s, and 0.0047 s, respectively. Moreover, as the decentralized feature of Blockchain, PW is independent of the immediate transaction fee. The token manager is able to complete the transaction when the fee is relatively low.

Considering security, PW uses NFC to perform closed communication between the sender and the receiver, which prevents cyber-attacks. Based on legacy NFC devices, higher-layer cryptographic protocols such as secure socket layer (SSL) are used. The token is generated by the cloud-based Trusted Certified Authority (TCA) and stored in a tamper-resistant Secure Element (SE) and Trusted Platform Module (TPM)-based attestation modules on the devices. In the token exchange process, the receiver will
remove the used tokens from the sender’s device after retrieving the value of the transfer. The removal of the used token is the first preventive measure against double-spending. The authors also claimed limitations such as token divisibility and falsified token detection, which are common concerns for a token-based system.

[18] Proposes a mobile e-wallet application, “Allpay,” which offers online-to-offline (O2O) payment. The Application and server have updated the user’s balance when connecting to the Internet. At the time of the offline transaction, Allpay will first check the required amount of payment is within the balance. If not, the payment request will be rejected directly, and the user will receive a notification message. In the case that the payment requirement is valid and there is no Internet connection, Allpay generates an RSA encrypted SMS containing the token, which uses the homomorphic properties of the RSA encryption, and then sends encrypted SMS with transaction information, such as sender and receiver IDs, the amount of payment, time and date to the server. The server decrypts the token using the latest online token and the account phone number. If the token is confirmed, the server will send a Time-based One-Time Password (TOTP) to the user to validate the transaction. Otherwise, a warning message will be sent, and the account will be blocked for half an hour. Figure 3 demonstrates the process of an payment.

![Figure 2. Allpay online-to-offline (O2O) transaction [18].](image)

The payment is secured using the homomorphic features of the RSA cryptosystem so that the data is fully encrypted to users and potentially malicious access during an offline transaction. The encrypted tokens with the user’s phone number sent by the server expire in thirty seconds, which contributes to preventing fraud and keeping the application.
Allpay designed components in secure authentication to ensure only authorized users can log in to the application and conduct financial activities. Offline device-based biometric authentication is suggested, including fingerprint readers, facial recognition, and speech recognition. It is also convenient for users as only one verification at the login stage is required. After successful login, the user can conduct transactions plenty of times without further identification. However, the significant problem is that the system uses SMS to communicate with the central server when there is no Internet connection. As “offline” refers to the completion of the transaction without the involvement of the backend server or the central party, Allpay actually provides a fake offline system for payments.

[19] introduces a mobile-to-mobile offline payment approach by scanning the QR codes generated by the applications. The account registration process, contacting the bank and downloading the cash, should be accomplished with Internet connection before paying or transferring offline. In the P2P payment process, the receiver generates a QR code with personal and payment information (receiver’s ID, receiver’s public key, the timestamp at the starting time of the payment process, and the reference number of the payment). The sender scans the code and then retrieves the receiver’s information. A series of encryption on the amount of money to be transferred, the password, and transaction information will be done in the designed key exchange algorithm. A receiver-only QR code will be generated with the encrypted values. In the end, the receiver scans the QR code. After decrypting and verifying the transaction, the receiver saves the money, and the P2P transaction is completed.

The design satisfies the requirement of the P2P payment in the situation of no Internet connection. For security, it implements Bouncy Castle, an Android API in cryptography, and elliptic curve key generation. Digital signatures with hash functions are also used in the key exchange for verification.

The efficiency of the system does not perfectly fall within the expectations. Double scanning on the QR code during each transaction is troublesome, jeopardizing the consumer experience. Besides, according to the performance test on two different
devices, the average time to process a payment is 12.76 seconds, which is relatively slow.

5 The proposed e-wallet platform

5.1 Proposed decisions to the four key technical problems

For the four key technical problems for the e-wallet development mentioned in Section 4.1, decisions of our team’s proposed e-wallet platform design will be raised in this part.

5.1.1 Overall structure

The trusted centralized system is chosen for data storage and the account based system will be chosen for the form of the balance. Though decentralized ledger technology, including blockchain technology, is popular nowadays, a traditional centralized database may be adequate for server-side data storage as the server storage does not need integrity preservation between multiple untrusted parties. Compared to DLT, a centralized database is more efficient in storing and fetching data, thus accelerating the whole system. Besides, an account-based design is chosen. Since the e-wallet will be registered in account format, it’s easier to implement the interest accumulation function in account based. Handling individual tokens is time consuming and storage space occupied.

5.1.2 Client side data storage and manipulation

For data storage and manipulation on the client side, existing approaches are usually smart cards or the special hardware token proposed in [19], but none can be implemented in an e-wallet system composed of servers and smartphone applications. Our platform store key pairs and execute the protocol in secure elements. Private key digital signature is used to ensure security and integrity of information such as transaction records in the secure element.
5.1.3 Offline P2P transaction

For offline P2P data transfer media, NFC may be a better option than QR code to facilitate mutual validation, as QR code only supports one-way communication. NFC can be more convenient in operation and more flexible for protocol design.

5.1.4 Data synchronization

A central database with all the transaction records will be applied to ensure data synchronization. Whenever a user connect to Internet, the platform will upload all the transaction details that have not been uploaded to the database. The central party checks the transaction entries in the central database. Three scenarios will be encountered, confirmed, inconsistent, or suspicious. If there is inconsistent records, the central party will lock the two user accounts immediately and report the issue to the back office. A balance program will be developed to check the details of the inconsistent transaction and fix the total balance in both the sender and the receiver sides. If the program failed to figure out the balance, it will report the issue for manually check. After the balance is correct, the account will be unlocked. However, in this case, a credit points deduction will be applied. For suspicious record, central party will monitor the account’s behavior. A suspicious mark will be applied on them.

5.2 Protocol

5.2.1 Key distribution

The central party stores the following elements in secure element.

- A pair of public key $pk_c$ and private key $sk_c$
- User’s public key $pk_u$
- User’s balance
- User’s information (User’s real name, contact number, .etc. )

In the user side, the following elements are stored in secure element.

- User public key $pk_u$ and private key $sk_u$
- User public key certificate $C_u$ (A signed user public key by the central party’s secret key)
- Central party public key \( p_k_c \)
- Active timer \( at \) (The active period of the account)
- User login password \( pw \)
- User balance \( b \)

### 5.2.2 Client setup

When it comes to a new customer, the e-wallet platform will set up the client account in the following process.

a. The client generates a key pair (private key \( sk_u \), public key \( p_k_u \))

b. Central party sends a request to active the account to the client: \( \text{clientstep()} \)

c. The client generates a random number nonce \( n \), and send it to the central party for a digital signature verification

d. The central party will sign on \( n \), \( \text{signature}(n) \) using private key \( sk_c \) and sent it back to the client

e. The client checks the received \( \text{signature}(n) \) using the central party’s public key \( p_k_c \). After validate it, a random number and a pair of key (private key \( sk_u \), public key \( p_k_u \)) are generated. The public key \( p_k_u \) should be sent to the central party.

f. The central party will sign \( p_k_u \) using \( sk_c \), \( \text{signature}(p_k_u) \). The activated period \( t \) of the client is set.

g. The client verifies \( \text{signature}(p_k_u) \) and sends a confirmation to the central party. The activated period \( t \) starts and the balance is set as 0.
5.2.3 Deposit and withdrawal money

For money deposit and withdrawal, central party verified by the client send the balance to the client, and the client will check if the payment is valid, in the case that the money out flow is lower than the money inflow. Detailed process:

a. The central party sends the request of balance modification, balanceChange()

b. The client verified the central party as in Sectioin 5.2.1

c. The client sends his public key certification and current balance information with digital signature of private key $sk_u$

d. The central party verifies the certification and signed the balance. Balance to be added and deducted is sent to the client.

e. The client checks the balance. If the payment is valid, the balance will be updated on the client. The transaction is recorded on the client side and submitted to the database when there is Internet connection. The client sends a termination signal to the server to finish the process.
5.2.4 Interest calculation and accumulation

To promote financial inclusion, the e-wallet is expected to calculate and accumulate interest even in offline condition. In our design, we are currently simply to accumulate daily interest rate at the set time stamp, 4:00 am HKT. A timer is set in secure element to ensure the correctness and consistence of time at all the accounts. A function `interestCalculation()` will be developed to calculate the interest accumulation.

5.2.5 Offline P2P payment

a. Generate and submit confirmation code, and set the timer: The receiver will received a confirmation code of 6 digits random number generated by the sender application. The submission of the correct code is needed on the receiver’s device. After checking the confirmation code, both sides set a timer. If time is out, an error message will be shown on both sides’ devices and the process is interrupted.

b. Identify users: The sender and the receiver exchange the certificate, which contains user public generated by the trusted central party. The signature is identified using the public key on both sides.

c. Validate the transaction: The sender sends the private key signed transaction information (confirmation code, amount of the transaction, balance of the sender) to the receiver. The receiver check the sender’s signature and confirmation code. Then he checks if the amount of transaction is within the sender’s balance. After these steps, the transaction request is validated. The receiver signed his amount of balance and send it to the sender.

The sender received the receiver’s balance information checks the signature. If valid, the sender-signed balance is transact to the receiver, and deduction of balance is applied on the sender. The receiver check the received balance from the sender. If correct, the balance is added on the receiver. Last, the sender checks the receiver’s balance. Then send a termination signal to the receiver.
6 Discussion

6.1 Our proposed e-wallet solution

For functionality, the proposed e-wallet platform meets the essential financial services that a client may require. Money deposit and withdrawal, interest calculation and accumulation and P2P payments well designed and explained in details in Section 5.2. Online transaction will not be discussed in detail in this report as there are already many mature solutions of this function. Overall, the target unbaked groups’ need in participating fundamental banking services. The interest accumulation suits their desirable in accumulating interests, so that they can have a higher chance to step out of poverty. However, functions in our e-wallet are limited. Other functions such as loan making, credit card payment and pad-off, insurance services may also be desired. Further research on these functions can be conducted.
For security, the e-wallet are integrated with plenty technologies. Cryptocurrency method of two-key encryption and communication is applied in the design. A pair of public key and secret key is generated among the central party, the sender and the receiver. Exchanging keys with digital signature in the financial activities following the designed protocol can ensure security to a larger degree. Sensitive data are stored in Secure Element. Moreover, the activation system will monitor the user behavior and block their accounts when necessary.

For scalability, the e-wallet platform may have a relatively fast transaction speed as the protocol designed are neat. The chosen centralized database may ensure a reasonable amount of data storage, comparing to decentralized database. The operation of the platform is clear and concise.

In general, we believe our proposed design is a good offline e-wallet model, which contributes to the electronic payment research.

### 6.2 Offline e-wallet to financial inclusion

Above all, we have proposed an e-wallet model that can be used offline feasibly. We believe the outcome would be an important contribution to solve financial inclusion.

Even in today's world, there are still a considerable number of people are unbanked. According to McKinney [20], 2.5 billion adults are estimated no connection to financial services, even save and borrow money services will not be accessed by them. The amount of 2.5 billion is over the half of the population of adult in the whole world. Most of them (2.2 billion) are in Africa, Middle East, Southeast Asia, and Latin America. These regions have more than 60% population are unbanked, whereas only 8% adult in high-level development countries.

Traditional physical banks cannot reach this group of people very well. The relatively high access mechanism, review standards and the cost of providing financial services make it difficult for economically underdeveloped unbanked regions to be accessed by traditional banks. Digital wallet is a significant solution to fill in the gap. While making payment more convenient for users, electronic payment is also considered to reduce the payment costs of financial institutions, regulators and governments. Bank accounts, on the other hand, are seen as a gateway into the wider world of formal financial services, such as savings, insurance and credit. Digitizing these services will increase the development benefits of economy and finance in the society.
Our team proposed an e-wallet solution to improve financial inclusion. Given the online e-wallet already been well developed and extensively used in some regions, our project has researched on extend the solution to offline circumstances. We believe our approaches to offline will contribute to financial inclusion to a relatively larger extend.

6.2.1 Necessities of achieving inclusive finance through offline e-wallet

Smartphones are widely used nowadays. According to Statista’s statistics in 2023 [21], 6.92 billion people are using smartphone in this world, which accounts for 86.29% of the whole population. Even in Africa, smart phone has been penetrated in people’s daily life. Many countries have at least one thirds population have their own smartphone. And the increasing trend of smartphone usage is upgoing at a decent speed. Though the rate is still relatively low among other more developed parts of the world, we estimated that the increasing trend will continue, and the increasing speed will accelerate. Besides, comparing establishing a complete physical financial service institution with the adoption to the world’s financial system and maintaining the whole branches, it is relatively more practical to distribute smartphones to poor areas in a reasonable proportion. According to Figure 1, majorities have accessed to basic phone, which makes it easier for them to accept and get used to using smartphones.

![Figure 7. Smartphone ownership rate in sub-Saharan Africa countries [22].](image1.png)

![Figure 8. The increasing percentage of smartphone ownership rate in sub-Saharan Africa countries [22].](image2.png)

The smartphone can be distributed once, the build of the internet network infrastructure in the whole area is expensive and almost impossible. The complex terrain and lack of transportation infrastructure in some remote areas have greatly
increased the difficulty of construction. The lack of skilled technical workers also makes construction and later maintenance difficult. The large amount of money spent will be difficult to cover. Since the distribution of the population is not concentrated in a considerable part of underdeveloped areas, the efficiency of investing in network facilities is very low. Therefore, offline payment is a problem worth solving, and its efficiency in promoting inclusive finance will be higher.

6.2.2 Rationalities of achieving inclusive finance through offline e-wallet

6.2.2.1 User position

For users, we believe offline e-wallet will be well-accepted by them. The justification is based on user preference and technology satisfaction.

As offline-payment have not been widely implemented, and the data of personal Internet financial product usage is limited in many parts of the world, we evaluate a government to person (G2P) payments case [23] to evaluate the users’ acceptance rate of our e-wallet product. The case selected Brazil, Colombia, Mexico and South Africa as examples. The electronic payment is able to satisfy the user’s need to a larger extent. In this case, it can store and deposit funds indefinitely, and access to mainstream financial infrastructure immediately. While physical cash is limited at a particular time and location. The benefits make the user more likely to prefer the electronic payment. In Figure 9, it can be seen the electronic payment is widely used in these countries. By 2012, only very few people still use physical cash payment way in Brazil and South Africa. Colombia’s quick change to electronic payment, from 76% to 9% physical cash using rate, shows a huge preference of the user. Though Mexico’s cash using rate is still over a half at the end of 2011, seeing Colombia’s implementation speed, we believe the situation of cash will be overcome once the electronic payment infrastructures are well settled.
It can be seen that the user value the benefit and convenience of electronic payment. The acceptance rate can be high when the system is well developed. For our e-wallet, we estimate it would be widely accepted as it truly solves the problems, access financial services without stable and constant Internet connection. The clear and efficient design of the e-wallet platform should not be ignored. For the real e-wallet mobile application, the function and user interface should be carefully designed to be not only easy for the less-technology accessed groups to use without confusion, but also well looking to attractive more users.

### 6.2.2.2 Provider position

For providers, the development of the e-wallet requires a certain amount of money, while as over time it could be cheaper as the platform is built and well maintained regularly. The cost of developing a e-wallet mobile application is around $15,000 to $40,000 for both Android and iOS platform. But after the development is done, the cost will be reduced at a large percentage. The maintenance service cost of an e-wallet app will be around 20% of the app’s development cost [24]. Besides, after development, multiple ways to raise income can be promoted. For example, posting advertisement on the mobile app to gain the fund.

Our platform requires more technology deployment in the offline part comparing to the usual mobile e-wallet. While based on our solution, the development and maintenance cost will be affordable. It would be an advantage for e-wallets to be promoted by governments or social institutions. In addition to obtaining financial support for research and development, it will also be of great help in promotion.
7 Conclusion

With the emphasis on financial inclusion and the development of financial technology nowadays, this project proposes an e-wallet solution for financial inclusion, implementing an online-offline hybrid mode to provide fundamental financial services to the unbanked population. Key technical problems, including overall structure, client side data storage and manipulation, offline P2P transactions and data synchronization were solved. Details of the designed functions, client account set up, money deposit and withdrawal, interest calculation and accumulation and P2P payment are explained. A code demo of the predefined protocols is developed. We hope this project will offer ideas to upgrade e-wallet in the offline circumstances and contributes to the solving of financial inclusion in the unbanked population.
References


