Interim Report

An E-Wallet Solution for Financial Inclusion

Chen Jiakai (chenjk01@hku.hk) 3035639446
Gu Yining (eiragu7@hku.hk) 3035638064

Project Supervisor
Professor Yiu, Siu Ming

January 22, 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 appreciation 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

<table>
<thead>
<tr>
<th>Figure</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Figure 1</td>
<td>Workflow of the proposed e-wallet</td>
<td>15</td>
</tr>
<tr>
<td>Figure 2</td>
<td>Pure Wallet implementation architecture</td>
<td>18</td>
</tr>
<tr>
<td>Figure 3</td>
<td>Allpay online-to-offline (O2O) transaction</td>
<td>20</td>
</tr>
<tr>
<td>Figure 4</td>
<td>QR code payment model</td>
<td>21</td>
</tr>
</tbody>
</table>
List of Tables

Table 1. Schedule 14
## Abbreviations

<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>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>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*  
7  

1.1 Background  
7  

1.2 Problem Statements  
8  

1.3 Motivation  
8  

1.4 Deliverables  
9  

1.5 Outline of the Report  
9  

2 *Literature Review*  
9  

3 *Methodology*  
11  

3.1 Identifying Functional Design, Workflow, and Key Problems  
11  

3.2 Literature Evaluation  
12  

3.3 Problem-Solving with Innovation  
12  

3.4 Performance Analysis  
12  

4 *Findings*  
12  

4.1 Project Plan and Milestones  
13  

4.2 Functional Design, Workflow  
14  

4.3 Key Technical Problems  
16  

4.4 Literature Evaluation  
17  

4.4.1 Evaluation of the overall structure  
17  

4.4.2 Evaluation of offline P2P payment  
19  

4.4.3 Evaluation of data storage at client applications  
21  

4.5 Primitive Ideas on Innovative Problem-Solving  
22  

5 *Conclusion*  
23  

References  
24
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.

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].

Financial technology has been another popular topic in the past five years, referring to the implementation of new technologies in delivering financial services. The technologies include but are not limited to artificial intelligence, big data, and blockchain technology. With the development of fintech, various inclusive financial products are provided to render readily accessible financial services to the broad public, enhancing the coverage of those financial services. E-wallets, like Apple Pay, Google Pay, and Alipay, are among the most significant paragons of all fintech products. They aggregate traditional payment methods, like debit cards, credit cards, and smart cards, into one application with the technologies mentioned above, modern cryptography, and telecommunication technologies to provide secure and convenient financial services with a low threshold. With the scalability thanks to the minimal client-side terminal as
small as a mobile application, the e-wallets gained and will be gaining rapid development in coverage.

**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 [8]. 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 functional and technical design (Section 3.1), literature evaluation (Section 3.2), innovative solution (Section 3.3) and performance analysis (Section 3.4). In Section 4, our findings will be presented and analyzed. The schedule 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 and Section 4.5, respectively. The paper closes with a conclusion in Section 5.

2 Literature Review

There are a substantial amount of literature and real-life examples of online e-wallet implementations. Usually, a traditional centralized database is used to store account information and transaction data. Cryptographic encryption methods and digital signatures are utilized to keep the confidentiality and integrity of data transfer, with communicational technologies and protocols, like Secure Sockets Layer and Transport
Layer Security (SSL/TLS), securing the communicational channels between entities involved. For the transaction process, the initiator always needs to correspond with the financial institution to check the account balance, credit limits, and other related information to obtain authorization. Moreover, the transaction may involve multiple financial institutions, and specific procedures are designed for fund clearance and settlement. In this project, the e-wallet is designed to be backed by a single financial institution, and major attention will be given to offline functionalities and online-offline synchronization methods. Therefore, the online e-wallet models are informative but not fully applicable. Previous research has explored the offline implementation of payment methods on different subjects, including direct money transfers, bank cards, and cryptocurrencies. Several implementation models and the technologies and concepts used have practical implications for this project.

Godfrey-Welch et al. [9] proposed the implementation of blockchain in the card payment system. Blockchain is a distributed ledger technology (DLT) formed by a growing list of transaction record blocks linked to each other, forming a shared, decentralized database with non-repudiation. Blockchain in payment systems bypasses traditional financial institutions, reducing transaction costs and raising the level of cybersecurity to some extent. The study provided possibilities for applying blockchain with its decentralized features to card payment systems and suggested better data integrity.

Bamert et al. [10] proposed “Blue Wallet”, using hardware tokens as physical Bitcoin wallets. They implemented Elliptic Curve Digital Signature Algorithm (ECDSA) for identity verification and transaction signing to achieve adequate data transfer and storage security. In their design, the hardware token can authorize transactions offline, while the counterparty must be connected to the Bitcoin network so that the transaction can be validated and recorded in the blockchain. Though the model does not fully support offline transactions, it brings up the idea of using secured hardware tokens and an approach for online-offline data transfer.

A blockchain cryptocurrency system, DelegaCoin, for offline coin delegation is proposed by Li et al. in [11]. Remarkably, they suggested the utilization of trusted execution environments (TEEs) for the reliable execution of specific protocols. With some cryptographic procedures inside TEE, a coin owner can delegate the right to use 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 [12], the authors introduced an implementation of offline cryptocurrency transactions called Pure Wallet in the context of blockchain. It uses the Ethereum smart contract and a new token to securely manage offline validation and transactions. Pure Wallet successfully managed an offline transaction of 10 tokens, proving the architecture feasible for blockchain offline transactions. However, the authors claimed limitations such as token divisibility, falsified token detection, and different environment adoption. All these insightful literacies demonstrate some practical hints on the design of the proposed e-wallet. Blockchain can be of paramount importance as a means of data storage to prevent data from being tampered with. Cryptographic methods should also be deployed to secure data transactions. Further, TEE can be a reliable environment to place core operational codes and execute the pre-designated procedures in offline circumstances. Though any single previous study cannot fulfill complete offline transactions, their implications lay a solid basis for the discussions in this project.

3 Methodology

3.1 Identifying Functional Design, Workflow, and Key Problems

The project’s general objective is to design a mobile e-wallet platform to facilitate payment in both online and offline conditions. The first step is to identify the functional design and workflow of the e-wallet system. Most financial service systems, including traditional banks, virtual banks, and existing e-wallets, require customers to apply for an account with identification documents. The e-wallet in this project should also start with opening an account in the backend financial institution in online or face-to-face conditions to validate the customers’ identity and manage the risk. Building on the account, the e-wallet should at least support short-term to middle-term offline usage that enables offline P2P transactions. Other functions like loan making and offline loan maintenance are desirable but not mandatory. The functional design and workflow should be concise and efficient with minimal reliance on the Internet connection and on-branch face-to-face operations. The key problem in this project, as mentioned in the introduction, can be refined and presented more clearly after defining functional designs.
3.2 Literature Evaluation

Given the considerable amount of related works on the topic, the literature will be reviewed to analyze the advantages and disadvantages of the solutions to corresponding problems in implementing our e-wallet. They will probably be examined on a problem-by-problem basis. For each key problem in our design, relevant solutions will be evaluated from different aspects, including feasibility and compatibility with this project.

3.3 Problem-Solving with Innovation

Based on the analysis of the previous literature, we will attempt to address the critical design problems with our knowledge. The building blocks of innovation include but are not limited to blockchain technology for data storing, zero-knowledge proof for validation, cryptography methods for data encryption and decryption, and network communication technologies for data transfer. Self-designed protocols and operating procedures will be created. Furthermore, to deliver the results, some code demos will be used to showcase the functional essence of the protocols briefly.

3.4 Performance Analysis

After coming up with the solutions, we will analyze the performance of the proposed methods. Measurements will be taken from security, efficiency, scalability, and all other reasonable aspects. Comparisons will be made between our proposed solutions and existing approaches. And limitations and future research directions will also be discussed.

4 Findings

Currently, we finished project planning, designing the e-wallet’s functions and workflow, identifying key technical problems, and evaluating existing solutions. This section will illustrate the detailed results in the three areas above. An additional fifth part will discuss the primitive ideas for the proposed problems.
4.1 Project Plan and Milestones

Basic information and directional ideas that shape the general idea of the project were formed in August and September 2022, including the social and academic background, project objectives, and methodologies. The project plan presented all the planning, and most information is also included in previous parts of this report.

The timeline and milestones (see table 1) were also set for completing the project step-by-step. The planning stage terminates at the beginning of October 2022 with the output of a detailed project plan. The interim report and presentation will come in the middle of the project timeline in January 2023. Finally, the project will end with the final project report and presentation in April 2023, with an alternative project exhibition and competition in May.

<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.</td>
<td>Initialized project webpage</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>November 30, 2022</td>
<td>Completion of functional design and</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>key technical problems</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>January 15, 2023</td>
<td>Completion of the review and analysis of</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>literature evaluation and preliminary ideas</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>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</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>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>----</td>
<td>-----------------</td>
<td>-------------------</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. Schedule.

### 4.2 Functional Design, Workflow

The e-wallet proposed in this project will feature the following functions:

- Online or in-person money deposit and withdrawal
- Online transactions
- Offline interest calculation and accumulation
- Offline P2P transactions
- Online or in-person loan making and offline loan maintenance (optional)

To enable the e-wallet, a customer needs to open an account online or at a physical financial institution branch. Same for money deposit and withdrawal, an Internet connection or in-person show-up is required to validate the account balance and transfer the funds. Online transaction refers to P2P transactions and payments to merchants when shopping online, which is a common practice for e-wallets and is widely enabled in existing payment methods. Therefore, there are a variety of materials to refer to, which will not be specifically studied. As a critical way to earn money from the capital, interest accumulation is one of the essential functions of banking services. The e-wallet will support interest calculation in offline conditions to accommodate this requirement, automatically calculating and adding interest to users’ balances. Moreover, offline P2P transactions, also serving as a key feature to enhance financial inclusion, allows both parties of a transaction to be offline and pay with the e-wallet balance. An optional function is to enable loan-making in the e-wallet. Since the loan issuer needs to assess the risk, the borrowers should submit applications to the issuer, and the assessment and issuing process should be completed online or in person. Then the e-wallet will record the contract terms and conditions and maintain them even under offline circumstances. Borrowers must return the fund to the issuer before the due date, or the e-wallet will automatically implement penalties like an account freeze.
The workflow starts with opening an e-wallet account online or on a branch with a balance either immediately deposited by the account owner or received from later transactions. The backend server will record the account information and balance at the time. With the e-wallet application and the account, the owner can perform online or offline P2P transactions as long as there is enough balance. For each online payment, the e-wallet application will send the latest transaction ledger of the account to the backend server, which immediately validates and synchronizes the data. Offline P2P payments will be validated by both parties’ e-wallet applications, with several information exchanges via physical media like near-field communication (NFC) or QR code. The account owner can also deposit money to or withdraw from the e-wallet balance online or at a branch. For online deposit and withdrawal, another bank account will be required to extract funds from or send funds to. And both cash and bank transfers will be accepted for an on-branch deposit or withdrawal. Furthermore, the customer can apply for loans anytime and use the money borrowed for a designated period. The e-wallet will manage the loan offline automatically and apply a penalty whenever the loan contract is violated. Finally, the account owner can apply to cancel the account before repaying all loans or withdrawing the remaining balance. Figure 1 visualizes the workflow with a flow chart showcasing the money, information, and control flow.

Figure 1. Workflow of the proposed e-wallet.
Red lines indicate control flows, and blue lines show money flow. Client application A shows the process for account registration, which should be completed before all other functional processes. Client application shows the money transfer for depositing and withdrawing money to or from the e-wallet account. Client application C and D indicate the online transaction process, and client application E and F explain the offline P2P transaction process. Client application G demonstrates the loan-making and offline maintenance process. All client applications in the figure are the same, and different names are assigned only to illustrate different processes.

4.3 Key Technical Problems

To support the functionalities mentioned above and workflow, several key technical problems are identified, including the system’s overall structure, data storage and manipulation on the client application, offline P2P data transfer and mutual verification, and server-client data transfer and synchronization. These four problems form the basic framework of the research and discussion of this project, and further investigations will be implemented into the issues as the project progresses.

The overall structure issue can be divided into two sub-problems, including the form of data storage and the form of balance. Abundant client information and transaction data will be stored on the backend server. Therefore, an efficient structure to organize and utilize data on the server is needed to accelerate the system’s processing speed. Structural design, including centralized and decentralized databases and additional measures, should be considered to find the balance between efficiency and security. For the balance form, the two options are token-based and account-based, migrated from the concepts of cryptocurrencies. For a token-based system, each token has its own identifier, and only the owner of the token can spend it legally. In an account-based system, the balance of each user is demonstrated simply by a number in the e-wallet. Each transaction is the process of deducting the balance of one wallet and increasing the other one. The form of balance defines how the remaining values in each wallet are represented, thus is critical for the realization of functions.

To facilitate short-term or middle-term offline usage, it is paramount to find a secure and efficient way to store and manipulate data on the client applications so that the stored data can only be modified according to the pre-defined protocols. Tamper-proof is the top requirement for data storage in the client application, as malicious users may attempt to modify the offline data to gain improper benefits. Protocols and operational components should also be securely stored to ensure the proper implementation of the protocols and the functioning of the application. And data manipulation should strictly follow the pre-installed protocols and prevent external interventions.
To enable offline P2P transactions, a protocol must be found or created together with some physical media to transfer data between the two parties and check the transaction’s validity. In an offline P2P transaction, the e-wallets of both parties should be able to check the validity of the counterparty account and confirm the transaction result on both e-wallets’ balances. The selected physical media should probably support multiple data transfers between the two e-wallets carrying transaction and verification messages in pre-defined formats.

The proposed e-wallet will be an online-offline hybrid system. Client-server data transfers and synchronization issues are crucial to the consistency of the entire system, which requires the proper timing and formatting of data transfer. At the same time, data transfer protocols should consider the probable different data storage forms in client applications and the back server, making the transfer message package compatible with both sides. Additionally, cryptographic or protocol-level protection should be applied to prevent malicious activities on the packages.

### 4.4 Literature Evaluation

#### 4.4.1 Evaluation of the overall structure

Chaum [13] introduced blind signature together with an untraceable payment system which is called DigiCash later. It is a centralized token-based system with a bank as the central party. And the blind signature scheme guarantees the anonymity of the payment procedures by allowing the signer to digitally sign a message without knowing the content. Considering the system’s workflow, the payer first submits the blinded digital coin containing information, such as denomination and serial number, to the bank with the corresponding amount of money. The bank verifies the information without directly seeing the content of the coin, digitally signs on the coin using blind signatures, and issues the coin to the payer. Receiving the signed coin, the payer can unblind the coin to get the digital signature. To spend the coin, the payer can simply send the coin with the signature to the payee in offline conditions. The payee must verify the signature using the bank’s public key to validate the coin. And to finally get paid, the payee returns the coin to the bank for payment.

Considering only the functions, the proposal of DigiCash fulfills the requirement of offline P2P payment by enabling the offline exchange of the coin and verification simply by the bank’s public key, which can be pre-installed in advance. However, the nature of the token-based system decides that offline interest accumulation is almost impossible since the issuance of a new coin requires the permission of the central party.
Also, a severe security concern for the system is the lack of protection against double spending. Since the mechanism guarantees the total anonymity of the payments, double spenders cannot be identified even if the bank discovers the double spending when the coins are returned. Otherwise, it requires the payee to immediately check with the bank for double spending upon receiving the coin, making it an online system. Therefore, the system has meaningful implications for our design that it’s challenging to implement a token-based approach for interest accumulation and that double spending prevention is critical.

[14] 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 2. Pure Wallet implementation architecture [14].](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.

4.4.2 Evaluation of offline P2P payment

[15] 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.
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.

[16] 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.

4.4.3 Evaluation of data storage at client applications

Two common and similar solutions are usually implemented to secure sensitive data on mobile devices, namely secure elements (SE) and trusted execution environments (TEE). According to [17], a secure element is usually a platform like a chip that is tamper-resistant and can store confidential data and host the execution of programs. Apple Pay [18], one of the most successful e-wallets in the world, stores the credentials, including account numbers, locally in an SE, which is isolated from the device’s operating system and the cloud. Without a doubt, SE is consistent with the tamper-resistant requirement of our design as it’s an isolated environment for secure storing and program execution. An additional concern can be the storage capacity of the SE since the long-term offline usage of the client application requires storing huge amounts of transaction data that may exceed the capacity.

TEE has roughly the same function as SE, except that it is usually a part of the main processor of the device. Apart from the applicability and concern similar to SE, TEE usually requires a higher level of permission as the main processor needs to care for the
operation of all the applications within the device. Much fewer resources for storage and program execution can be distributed to the e-wallet application.

4.5 Primitive Ideas on Innovative Problem-Solving

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. Several backup databases should be prepared to store the exact copy of the data to prevent unexpected data loss. At the same time, an account-based design will probably be chosen since it’s easier to implement the interest accumulation function while there’s no need to handle individual tokens, saving time and storage.

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. Secure elements (SE) will be considered due to their secure storage and program execution functions. To eliminate storage concerns, only sensitive data, including private keys, personal information, and other confidential information, will be stored within the SE. Other data, like transaction records, can be stored in shared storage but encrypted or digitally signed by the stored private keys.

As no existing protocol is fully applicable, specific protocols should be designed respectively for offline P2P and client-server data transfer. 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. And in client-server data transfer, we primarily want the client applications to update the latest balances and transactions to the backend server whenever they have connections. The SSL/TLS layer should also be added to the message packages to secure the communication channel. It is also worth considering enabling NFC data synchronization between the client and server to provide more access points to the backend server. The details need further investigation to make the protocols ensure the integrity of the entire system.
5 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. Functions of the e-wallet feature online and offline payments, interest accumulation, and loan making, while the workflow emphasizes simplicity and security. Four key technical problems were identified, and corresponding existing solutions were discussed and evaluated for their applicability to our project. Additionally, ideas and directions for further solving the problems are also presented. Hopefully, the proposed e-wallet in this project can provide a new perspective and prototype to enhance financial inclusion and ultimately brings improved welfare to the unbanked population.

The current works are mainly theoretical designs and literature evaluation. To present the ideas of our solution, code implementation should be completed in future work. Further work should be progressed according to the schedule, including innovatively creating new solutions, producing code demos for the proposed protocols, and analyzing the performance of the model. Attention should be given to not only realizing the functions efficiently but also security, scalability, and compliance issues. Noticeably, deploying a complete product with our solutions requires further research beyond this project. Moreover, our team acknowledges that innovative financial platform development requires sound legal supervision. While as engineering students without a law background, we have not covered this aspect of research.
References


