UNIVERSITY OF NATURAL SCIENCES

FACULTY OF INFORMATION TECHNOLOGY

HIGH QUALITY PROGRAM

NGUYEN HOANG THIEN – NGUYEN CHAU THANH THIEN

BLOCKCHAIN APPLICATION FOR PEER-PEER LENDING SYSTEM

BACHELOR OF IT GRADUATION THESIS COURSE

City. HCM, 2018

CLC

BLOCKCHAIN APPLICATION FOR PEER-PEER LENDING SYSTEM

2018

UNIVERSITY OF NATURAL SCIENCES

FACULTY OF INFORMATION TECHNOLOGY

HIGH QUALITY PROGRAM

NGUYEN HOANG THIEN - 1453044

NGUYEN CHAU THANH THIEN - 1453045

BLOCKCHAIN APPLICATION FOR PEER-PEER LENDING SYSTEM

BACHELOR OF IT GRADUATION THESIS COURSE

INSTRUCTORS

Dr. DINH BA TIEN

City. HCM, 2018

THANK YOU

After more than seven months of research and implementation, the thesis "Application of blockchain for peer-to-peer lending system" has basically been completed. To achieve results Today we tried very hard and received great help from our brothers, sisters, teachers and friends.

First of all, we would like to sincerely thank the Board of Directors of the University of Natural Sciences, Vietnam National University, Ho Chi Minh City for creating the most favorable conditions for We can study at school during the past four years of University.

We would like to thank the members of Viet Community Online Services Joint Stock Company (VietUnion) for creating a convenient, comfortable and enjoyable working space. Your concern and enthusiastic help throughout the implementation process.

We would like to sincerely thank Mr. Dinh Ba Tien because he enthusiastically guided, helped, cared for and encouraged us every time we encountered difficulties, and always created the most favorable conditions possible. so we can Complete the project on time.

We would like to sincerely thank Mr. Nguyen Thanh Son - Head of PayooX, who researched, commented and solved problems in the project with us throughout the process of working on the project.

Finally, I would like to thank my family and friends for always caring and sharing Share and encourage us during the times we encountered difficulties while implementing the project during the past period of time. Special thanks to Cao Y Ly for advising the team on the application's interface.

The thesis was completed with certain results, but still not avoid errors. We look forward to the comments and opinions of our teachers and friends.

Implementation group

Nguyen Hoang Thien and **Nguyen Chau Thanh Thien**

TABLE OF CONTENTS

LIST OF IMAGES

LIST OF TABLES

LIST OF TERMS AND ABBREVIATIONS

STT	English terms/ abbreviations	Meaning
1	P2P lending	Peer-to-peer lending model, abbreviated from peer-to-peer lending
2	Blockchain	Form of shared, distributed data storage According to the data structure, blocks are connected one after another to form a chain. Data Once stored, data cannot be changed
3	Crowd-funding	Form of raising capital from many people
4	Peer/Nodes/ledger	Terms used to refer to storage places data in the blockchain network
5	Smart Contract/SC	Online electronic contracts, basic application of blockchain network
6	Chaincode	The term is equivalent to Smart Contract
7	Transaction	A term referring to online transactions
8	Layer	The term refers to the separation of architecture into different layers
9	API / Restful API	Application Programming Interface - application programming interface
10	JSON	Javascript Object Notaion - common data structure of information transmitted on the network
11	Client	Clients, in this project, are mobile phones
12	Server	Client
13	Request	Request to retrieve data from the client
14	Response	The set of data that the client returns to the corresponding client
15	Database	Database

SUMMARY

1. Research topics and issues

Learn about the peer-to-peer lending model. Applying blockchain data storage technology to an online peer-to-peer lending platform. Develop mobile applications to realize the peer-to-peer lending model. From there, identify the advantages and disadvantages and evaluate the technological feasibility of this financial model.

2. Approaches - novelty of the topic

Applying blockchain data storage technology, especially applying Smart Contract (Chaincode) as evidence and representation for transactions and traditional contract documents.

Automate most lending processes, allowing parties to link and conduct direct transactions with each other through the peer-to-peer lending model with the support technology aid.

Transaction data cannot be changed once recorded and distributed on the blockchain system, helping to reduce the risk of fraud and increase transparency.
transparency for financial modeling.

Apply the flexibility of mobile platforms and the ubiquity of smartphones to increase the user experience in loan origination, investing
loans and loan management.

3. Research results and application development

Solve the problem of transparency and anti-fraud for the peer-to-peer lending model. Highlights of blockchain technology are applied to the model
Peer-to-peer lending has contributed to solving the above problem effectively.

Successfully build a mobile application on both Android and iOS platforms capable of allowing both investors and borrowers to perform other streams
each other independently.

4. Contribution and expansion of the topic

Academically, the project applies blockchain technology to the peer-to-peer lending system to solve problems of transparency, fraud, and investment risks of financial model. At the same time, evaluate the feasibility and suitability of this technology when combined with the peer-to-peer lending model.

In terms of socio-economic aspects, the project aims to contribute to the units in the fields of technology and finance to expand the business model. At the same time, it helps the group of users who own idle money to invest profitably and the group of users who urgently need money to spend can take out consumer loans without having to go through complicated, time-consuming processes. . Thereby, contributing to stimulating financial market demand Lending is currently thriving in the domestic market as well as in some other countries.

The project is researched and implemented in the spirit of being scalable and ready to easily integrate third-party services into the system, towards the goal Build an application capable of operating experimentally on the market.

PREAMBLE

Currently, all humanity is starting to implement the 4.0 digital revolution in which information technology is considered the core field and is the focus of this historical period. We can easily name some of the technologies that are leading the trend such as: artificial intelligence, augmented or mixed reality.
(Augmented/Virtual Reality) or Internet of Things (IoT). From the end of 2017, emerging among these trends is blockchain data storage technology, which is considered the key to solving current user data storage problems. Cryptocurrencies, notably Bitcoin and Ethereum, were born as a product of blockchain as a demonstration of the applicability of this technology. They are even identified as the future of the world financial system once approved by law. Besides,

Blockchain also has great applications across many different fields due to its settlement
The issues of transparency, anti-fraud, and automation are suitable for many
type of business model: financial, service, industrial.

At the same time, the consumer lending industry is currently in a prosperous phase. According to estimates by VnExpress [1] - the scale of this market in Vietnam reached 26 billion USD in 2016. A series of lending financial institutions were established such as FE
Credit, Home Credit, HD Saigon... Most of these companies operate under the model of mortgage loans or unsecured loans via credit cards. In other countries around the world
In the world, users often favor the peer-to-peer lending model because lending procedures are significantly shortened and loan interest rates are moderate in accordance with loan needs, although this model has weaknesses in transparency and ease of use. fraud, high risk of default.

Applying blockchain to the peer-to-peer lending model will be a great combination because this technology solves existing problems in the above model.
The authors find this an interesting problem that can both explore and learn from one of the current technology trends, and can also be applied to a specific financial model to turn it into a product. promises to be implemented in practice.

Therefore, the authors decided to choose the topic **"BLOCKCHAIN APPLICATION FOR A PEER-PEER LENDING SYSTEM".**

Within the framework of the topic, the author group focuses on understanding and applying technology blockchain into the processes of the peer-to-peer lending model. At the same time, the group also develop mobile applications on both Android and iOS platforms to serve the goal of realizing this model. From there, it serves as a basis for the team to evaluate the advantages, disadvantages, and feasibility of combining blockchain in the financial model.

CHAPTER 1: OVERVIEW

ÿ *The first chapter will include three parts focusing on economic and technological information related to this project. The first is to introduce the peer-to-peer lending financial model by clarifying how it works, what is different from other models, and the advantages and disadvantages of this model. Along with that will be a basic introduction to the blockchain system: properties, characteristics and practical applications that make this technology a trend in the current technology world. From there, the group will present the reasons why blockchain is incorporated into the peer-to-peer lending model. Finally, there is the goal and approach to solving the problems*
through this project.

1.1 Peer-to-peer lending financial model

1.1.1 Introduction

Peer-to-peer lending, peer-to-peer or person-to-person (P2P lending) is a form of lending and capital mobilization for an individual or an organization to carry out the borrowing process by direct connection. with other individuals and organizations that own free money and need to invest and lend for profit without direct approval or intervention from domestic banks. This business model is commonly used
Using online services as an intermediary platform (loan platform) connecting investors with individuals or business units who want to borrow [2]. In terms of finance, the main form of loan of this model is an unsecured loan, which means the loan interest rate is assessed based on the individual's credit score. However, some other companies also expand in the form of mortgage loans, which means the loan interest rate and loan amount are evaluated according to the collateral like the traditional loan process at a bank.

According to Guardian [3], Zoopa was the first financial company to widely introduce this model to users in the UK in 2005 with many loan packages with corresponding interest rate brackets suitable for different loan purposes. The goal here is not simply to call for the community's help to complete projects as a form of capital mobilization, but also to borrow to solve consumer needs, buy a house or

Pay off other consumer debt. Peer-to-peer lending platforms often involve two sets of end users who interact directly with the system:

- Borrowers: individuals and organizations who are in need of a loan
  Money serves a certain purpose.
- Investors: individuals and organizations that own free money and have needs
  Invest and lend to make a profit.

Normally, a loan application is made with a relationship between one borrower and many investors, meaning a group of investors will share investment in the same loan application with benefits depending on the capital contribution ratio for that loan application. . This relationship is considered a general regulation for the above model with the purpose of sharing the risks that investors must bear in each loan application.

1.1.2 How it works

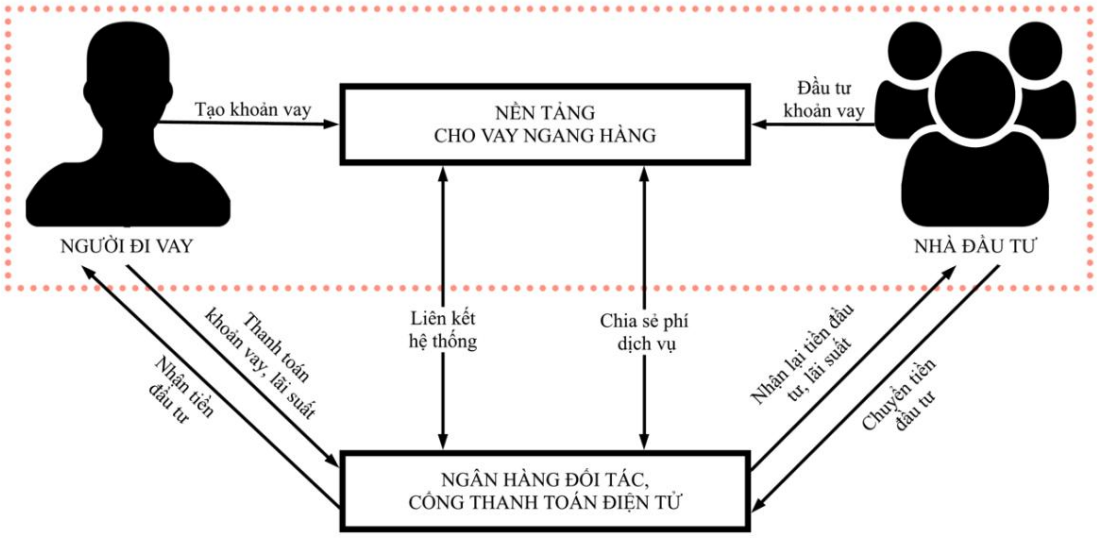

Figure 1-1. Peer-to-peer lending financial model

Over time, the peer-to-peer lending model has many ways
Operate differently to suit each user group in each country. In general, online peer-to-peer lending systems carry out certain processes [4]:

- Before a loan is created, the borrower must submit a loan application that includes personal information, certified legal information, and necessary information about the loan.

- The system will base on the above information from different data sources to evaluate the risk level of the loan application and classify the loan application according to a specific interest rate. Loan applications may be rejected if the risk of default is too high.
- If the loan application is approved, investors can view basic information of the loan and decide to invest depending on their wishes and different interest rate preferences. The investment decision here will be recorded by the system as a loan capital contribution commitment.

- If enough groups of investors are gathered to contribute capital to the loan application, the system will transfer to the domestic bank to review the loan application again (sub depends on the laws and financial protection rights in each country).
- Domestic banks are responsible for receiving money from investors and transferring it to the borrower who owns that loan application.
- The system will collect fees on each loan application as well as calculate the initial participation fee investment on each investment capital commitment.

1.1.3 Comparison with other lending models

Characteristics of Traditional Loans Consumer Loans			**Peer-to-peer lending**
Representative	Agribank, Citibank	FE Credit, Home Credit	Prosper, Lending Club
Purpose get a loan	Develop enterprise, buy houses	Serving consumer and shopping needs	Diverse, mostly consumer and shopping needs
Procedure get a loan	Done entirely by hand, certified by documents and current assets	Reviewed by child people, time shortened, application review process improved	Performed automatically yes technology applications, Savings loan implementation time

	things cost a lot time	Shorten through basic documents such as ID card…	significant, verified by credit information use
Capital	From lending banks. The loan amount is relatively large and affected by the assets Mortgage	From financial organizations related main. Number Relatively small loan amount determined by information of borrower	From the user set Another is called the investor group through the work The loan is broken down into parts
Loan interest rate	Small 8.5% - 25% [5]	High 15% - 70% [5]	Medium 5.99% - 36% [6]
Risk of default	Short	Short	Pretty high
Calculate intelligence White	Managed and controlled by the bank	Due to banks and groups financial position control	Not yet clear and controlled by the platform loan
Legality Protection law		Protection law	Most of them do not have specific regulations law

Table 1-1. Compare peer-to-peer lending with other models

1.1.4 Advantages

P2P lending platforms have become widely popular in foreign markets because this model possesses many properties that bring benefits not only to end users: borrowers, investors, but also show positive aspects. negative for the economy and society association in that market.

1.1.4.1 For borrowers

The average interest rate of the loan is more attractive when compared to traditional bank lending models or other financial models.

Loan processes and procedures are optimized and automated using an online technology platform to help borrowers shorten implementation time.

Borrowers can make choices - decisions that suit their desired loan purpose. You can refuse or not create a loan without penalty
influenced by human factors.

1.1.4.2 For investors

Take advantage of free money to invest for profit. The benefits received are more attractive when compared to bank savings interest rates.

The profitable investment process is also automated, creating convenience for investors when making investment decisions and commitments.

Investors can track and check the disbursement progress of the loan
make a decision to divest capital in case of necessity.

1.1.4.3 For economics and society

Diversify lending financial models, compete directly with other models
Traditional bank loans or consumer loans by financial institutions.

Meeting people's increasing consumer demand, contributing to stimulating the currently thriving lending market.

Peer-to-peer loans can completely replace black credit and hot loans with interest rates high, helping society reduce illegal acts.

1.1.5 Disadvantages

Peer-to-peer lending is not a comprehensive financial model. Although there are many strengths, this model also has many weaknesses and negative effects:

- The possibility of default and risk for each loan is relatively high. Because the banking function is reduced in the process, the credit score risk is borne entirely by the loan investor pool.

- The possibility of fraud and fraud increases because the loan - investment process takes place out completely online.
- Transparency of the model operating system is also an issue large, does not rule out the case of the platform taking over its own interests each loan.
- In some countries, this model is not specifically regulated by law.
- The model needs a user base: borrowers and investors large enough to operate and maintain the model.
- The model depends on an online credit scoring system. This is a new model that is still being developed to be able to calculate and make more appropriate decisions.

1.1.6 Development potential

Launched in 2005, the first platform was Zoopa in the UK, followed by other famous platforms appearing in the US such as Prosper, Lending Club. Currently, around the world there are hundreds of thousands of financial institutions operating in this field, predicting an extremely large and potential market. According to Transpanrency Market Research [7], the global P2P lending market will be worth $897.85 billion by 2024, an annual global growth rate of 48.2%/year. The potential of the market is also shown through the amount of loan application and the successful disbursement rate of the loan application. Total value of all global loan applications expected to reach $1 trillion by 2025 [8], default rate The estimated improvement is 4.8% per year, according to Zoopa's 2017 statistics [9].

Figure 1-2. Overviewof loan volume in the US market in 2016 [10]

In the Vietnamese market, although the consumer loan finance sector is thriving, the p2p lending model is still very new and only flourished starting in mid-2017.

Some financial companies are in the testing phase of this model such as: Tima.vn, lendbiz.vn or mofin.us with the hope of dominating the peer-to-peer lending market in a time when consumer loans are increasingly popular. in people's lives.

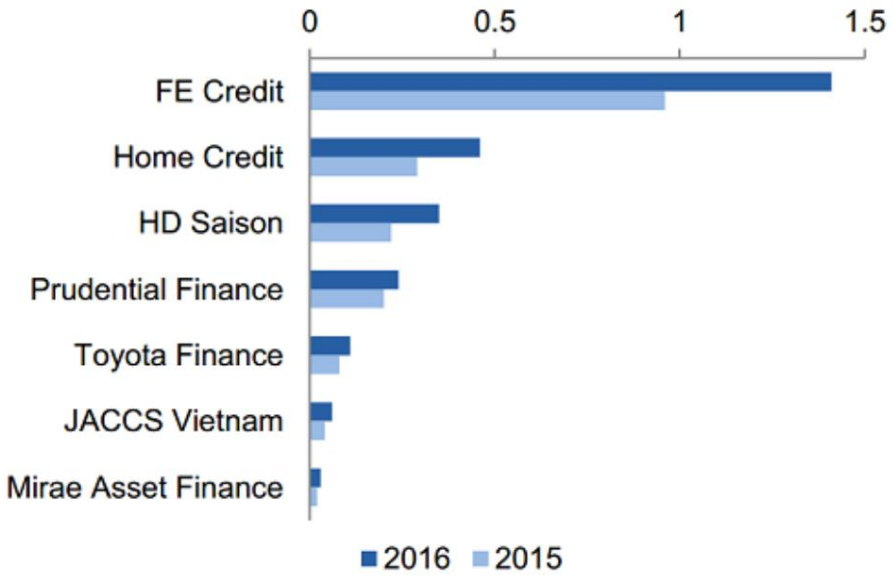

Figure 1-3. Outstanding debt of consumer loan companies in Vietnam [1]

1.2 Blockchain – shared, distributed data storage technology

1.2.1 Introduction

[11] In 2009, the Bitcoin network was first introduced by Satoshi Nakamoto through a 9-page report. The purpose of this electronic currency is to replace the current world financial system, which depends entirely on centralized banks and is falling into an economic crisis at that time. By 2014, when the value of Bitcoin was increasing and attracting the attention of many people, scientific researchers began to study the technology behind this electronic currency. blockchain. In addition, a series of cryptocurrencies associated with other blockchain networks were born. At the end of 2015, the Ethereum network and Ether coin were born, popularizing the concept of Smart Contract. In July 2017, the Hyperledger Fabric network was born, focusing on building a closed blockchain system that does not depend on cryptocurrency.

By definition, blockchain is a type of shared, distributed database used for Store data through a secure form of encryption, distribution, synchronization and unification of a single copy of data between information storage locations, also known as ledgers - ledger [12]. When the system generates transactions, the ledger will encrypt this data

and pack them into a block of data (block) using a specific algorithm.
A data block also contains link information of the previous data block (if any) and from there Data blocks are linked together to form a chain. Entire tissue system
described above will be called the blockchain data storage network.

Smart Contract (SC) in fact, this concept has appeared since 1997 by Nick Szabo [13] with the idea of creating an electronic method (protocol) to
Store the agreement and commitment of both parties during online transactions without the intervention of a third party to perform the authentication task. However, this concept only began to gain popularity in early 2017 when the Ethereum network emerged to play a leading role in the blockchain era. According to IBM [14], Chaincode (another term equivalent to Smart Contract) can be defined through two perspectives: technology and business. In terms of technology, chaincode can be viewed as a piece of computer program stored on the blockchain next to the main transactions to support users in interacting with stored data in a manner prescribed by developers. . In terms of business, chaincode can be considered an agreement between two parties when an online transaction occurs on the blockchain network.

1.2.2 Characteristics and how it works

Some typical features of the blockchain system:

- Encryption security: means that transaction information is encrypted according to a pre-specified algorithm to ensure the nature and integrity of transactions. security of each transaction. The Bitcoin network uses algorithms hash SHA-256, while Ethereum uses the ETHASH algorithm (improved from the Dagger-Hashimoto hash algorithm).
- Distribute, synchronize, and unify a single data copy: this process is operated and maintained by consensus algorithm. In more detail, the ledgers in the network must be consistent when participating in recording data together, which transactions are in the block, and their order

This transaction, the addresses related to those transactions are valid and together solve the difficulty problem of the consensus algorithm. The Bitcoin network uses Proof-of-Work (PoW), Ethereum is gradually transitioning from PoW to Proof-of-Stake (PoS) to achieve higher efficiency.

Each blockchain system has different operating principles, described below are the basic steps for the Bitcoin blockchain to record data when a money transfer transaction occurs on this network:

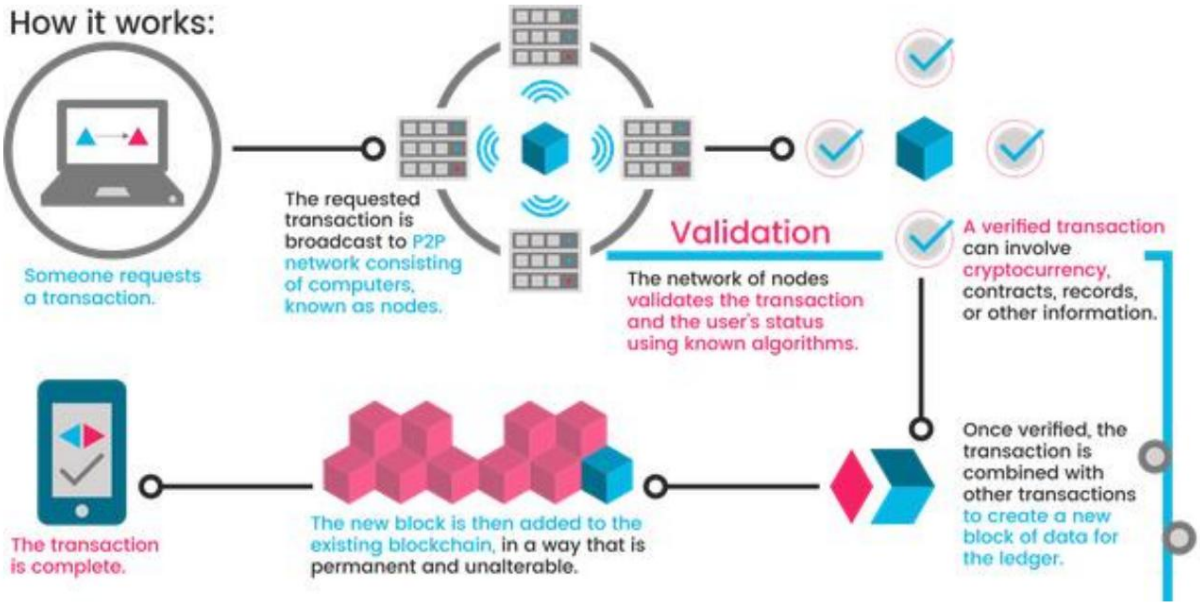

Figure 1-4. How the bitcoin network actually works [15]

- Someone makes a request to transfer money.
- This request is widely distributed as an incoming packet all ledgers in the network.
- The ledger is responsible for validating whether the transaction request is valid or not by checking the account of the remitter as well as the address of the recipient.
- Once authenticated, this transaction information will be combined Other transaction information is packaged into a block of data. The

ledger together solve the consensus problem to find the nonce code and the appropriate hash code.

- This data block is then appended to the previously existing data string. This process is repeated steadily and steadily change as previously prescribed.
- The process of a transaction is completed.

Normally, a data block in the Bitcoin blockchain network stores 1 MB of data and takes 10 minutes to execute [16]. For Ethereum, this number is 0.02 MB, it takes an average of about 15 seconds to create a new block and the number This is adjusted depending on the number of ledgers in the system.

1.2.3 Properties

Currently, there are many different blockchain methods and networks being born one after another, each different network possesses its own strengths and tries to improve the weaknesses of previous systems. However, these systems all achieve some common properties to show that this is a blockchain network actually:

- Stored data cannot be changed: No third party or individual ledger in the network can delete data that has been agreed upon by the entire network and has been distributed throughout the system. Reserved data Can only insert new, or expand (insert/append) but cannot delete (delete) in any form.
- Eliminate the role of intermediaries: trust, dependence Third parties when making transactions are completely eliminated. Instead, the entire blockchain network, specifically the ledgers, will perform this task together in a unified way.
- Publicity and transparency: Data recording takes place publicly to promote consensus among ledgers in the network.

Fraud and falsification of data will be limited to the lowest possible level. Therefore, complete transparency is enhanced.

- Security and stability: this property causes some controversy among those pursuing blockchain technology today. In principle, no supercomputer in the world can easily solve the consensus problem and control 51% of the ledgers in the network. Even if a large number of legers collapse or become inoperable, the rest of the system still functions normally. However, in reality some cases of the blockchain network being attacked are completely possible such as "The DAO Attack" [17] on the Ethereum network.

1.2.4 Applications of blockchain

Besides Smart Contract as a typical application, blockchain also has many other practical applications in all different fields such as [18]:

- Finance - technology: is the field most exploited to apply blockchain from payment systems, electronic money, cross-border money transfer methods. Many people believe that blockchain will play a central role in the financial system

the future itself. There is also the financial field of peer-to-peer lending as the authors will do in this project. This combination will work
Described more clearly in section 1.3 and chapter 2 of this report.

- Cloud computing: users rent out their leftover hard drive capacity to those who need this capacity to store data. The "thanks" stored data will be encrypted to help ensure security as well as increase transmission speed. • Supply chain: applying the immutable nature of blockchain will help shipping and manufacturing companies record and track the origin and origin of items. Check the safety and trust of goods when they reach consumers.

- Health and medical services (Healthcare): blockchain is used as a basis for storing data about patients' health. This data is stored synchronously and uniformly between hospitals as an internal ledger net.

1.3 Applying blockchain to the peer-to-peer loan model

1.3.1 Reason for combination

After learning an overview of the peer-to-peer lending model (presented in section 1.1), the group realized that this model possesses enormous development potential. However, compared to current bank-centric lending models, this model also possesses a significant amount of risk. In addition, blockchain data storage technology is developing strongly because of the features that this technology brings to solve long-standing problems, including problems that exist in the lending model. current peer. The authors see this as a huge opportunity when developing a peer-to-peer lending model that combines application with blockchain to optimize this model, turning it into a promising product that can be deployed in practice. If the blockchain application is successful, the new peer-to-peer lending system product will have the following outstanding features:

- Transparency: lending and investment processes all take place openly and transparently. Every process is recorded on the blockchain not by a single data recording unit but by the entire blockchain network system authenticating in the most effective and synchronous way.
- Fraud during the loan and investment process will be significantly reduced. Because of investment commitments and commitments to fulfill payment obligations Loan applications are controlled by the entire blockchain system and cannot editable (due to the nature of blockchain) once recorded. Beside Besides, the fraud that occurs at third parties is almost completely eliminated because this model is applied with

blockchain, the dominant role of third parties in transactions will no longer exist. This will result in significantly reduced costs.

- Currently, the peer-to-peer lending model is not officially recognized by law in some countries because of the above issues. However, the recognition ability of this new model will increase due to the solution of transparency and anti-fraud. At the same time, the control and auditing process, normally carried out by State agencies, will be supported

  maximum support due to the characteristics of blockchain technology.

1.3.2 Objectives

The goal of this project is to realize the peer-to-peer lending model and evaluate the feasibility of combining with blockchain technology. From a technological perspective, the proposed system must achieve the following main functions:

- Loan creation: the borrower has the ability to create a loan, requesting no Loan amount and disbursement date according to the user's desired purpose. The system will evaluate the loan with previous user information to inform the risk of the loan, through the loan interest rate, so that the borrower can clearly understand. When the borrower accepts the loan interest rate
  In addition, all loan information will be stored on the blockchain as an actual contract.
- Loan investment: investors through the system can review existing loans in the system to make decisions about which loan to invest in that suits each person's goals. The investment commitment will be recorded on the blockchain as an actual contract.
- Loan term payment: the borrower is responsible for paying the term when notified by the system that the term has come. Information about
  Forward payments will be stored on the blockchain as an actual contract.

- Processing loans: the system acts as an intermediary platform connecting borrowers and investors. Under the authority of the controller, the system will check the validity of loan applications at the same time. has the right to publicly change loan application status information in accordance with the peer-to-peer lending model. For example, check the loan application is in progress
  What is the process, whether the investment process of the loan application has ended or not, whether the loan application is due for disbursement or not. In addition, the system also publicly records investment service fee contracts according to each term of the loan application for each group of investors, helping to support the comparison and audit process later. The team's goal is to automate all of the above processes to minimize objective human factors in the lending or investment process.

1.3.3 Approach

To solve the problem "Application of blockchain for peer-to-peer lending system" and to meet the set goals as presented in chapter 1.3.2,
The author group intends to carry out the following tasks:

- Surveying the lending model for goods on a number of popular platforms today.
  From there, we can summarize the advantages and disadvantages of these platforms.
- From the survey platforms, the team applied business analysis techniques on the software model to propose the system that the authors plan to build in this project.
- After proposing the system, the team will start designing the system. List in detail the components, architecture, and basic functions of the system. At the same time, during this phase the author team will decide which technology to apply to build the system.
- Most of the time spent on this project is to install and build the system system. The team will make a priority list of needed functions

built to avoid shortcomings in main streams or focusing too much time on unimportant streams.

- After building the system, the team will focus on testing system to minimize application errors. At the same time, the team also edited the user interface to make it intuitive and easy easier to operate.
- After completing the installation and debugging of the application, the team will focus on summarizing the work done to evaluate the feasibility and consider the advantages and disadvantages of the system. Also the author group also points out unfulfilled goals and sets out directions for expansion and development of the peer-to-peer lending system in the future.
- Document the work performed and completed.

To perform the above tasks, in terms of technology, the authors apply the software development process according to the Scrum process and Agile method. Specifically, this is a flexible software development process, adapting to changes in software requirements with each Sprint. In the Scrum model that the team applies, the team collaborates

The audience is divided into the following main roles:

- Product Owner: Mr. Dr. Dinh Ba Tien
- Scrum Master: Mr. Nguyen Thanh Son - Head of PayooX
- Development team: students Nguyen Hoang Thien, Nguyen Chau Thanh Thien.

A Sprint in this process is calculated on a weekly basis. Every week the group will Hold a meeting to determine the work done in the past week, the tasks for next week, how to achieve the goal in this sprint. With a duration of 7 months, the team plans to divide it into 28 Sprints to complete the set goals. This process has been described specifically in the topic outline.

CHAPTER 2: SURVEY AND PROPOSAL SYSTEM

ÿ *The main content of the chapter revolves around a survey of currently available software systems in the world and Vietnam, and comments on the advantages and limitations of each platform. From there, propose a system with appropriate criteria with the initially stated goals of the project. In the proposed system, chapter 2 will focus on describing the operations, features, and basic functions of the system along with the combination with the blockchain system that the authors plan to implement.*

2.1 Survey of actual systems and software

The business processes of the platforms surveyed below are summarized processes, provided by the platforms themselves, to ensure the specificity of each individual system.

2.1.1 Prosper system

Home page: https://www.prosper.com/

[19] Prosper is the first online peer-to-peer lending platform in the US that was first launched in 2005. The platform has provided a total of over $12 billion in personal loans to over 770,000 people. to the present time.

Borrowers (individuals): the system requires individual users to satisfy

The following 3 factors must be met to be able to make a loan:

- From 18 years old or older.
- Be a US citizen (except the states of Iowa, North Dakota and West Virginia).
- Are in good standing (have a credit score of 640 or higher).

Making a loan in the Prosper system is somewhat similar to other online lending systems, borrowers can borrow between $2,000 and $40,000 with an annual interest rate (APR) that ranges from $2,000 to $40,000. about 6.95% - 35.99% and loan term from 3 years to 5 years.

Loan implementation process:

1) Check personal interest rates: users need to provide the necessary information personal and loan information.

2) Select loan recommended by the system: user selects recommended loan appropriate from the system based on different criteria.

3) Receive money: after choosing the loan and being invested, the loan amount will be Transfer directly to bank account.

Investors: Prosper allows individual investors to look through the list of loans available in the system and invest in those that fit their criteria. Investors can also build their own criteria and authorize the system to automatically invest.

Investment process:

1) View loan list.

2) Investment decision.

3) Earn profit

Advantage:

- Business processes are clear and intuitive, attracting numbers large user base.
- Has an automatic investment function, helping to make loans and investments faster and more convenient.

Limit:

- Prosper Daily mobile application has stopped service since August 31, 2017.
- [20] Web platforms are often complained about being difficult to navigate and difficult to find information.

2.1.2 Lendbiz system

Home page: https://lendbiz.vn/

Lendbiz is a Vietnamese financial company in the field of peer-to-peer lending investment that directly connects small and medium-sized businesses to the investor community, helping businesses borrow capital as desired and investors. Investors get income from idle money.

Borrowers (businesses): [21] the system requires businesses to meet the following conditions to be able to borrow capital:

- Is a joint stock company, limited liability company, private enterprise or cooperative.
- Operating in major cities of Vietnam.
- Operating time from 1 year or more.
- Have positive profits in the most recent year

Lendbiz supports mobilized loans ranging from 100 million to 1 billion contract with a payment term ranging from 3 to 12 months. Loans need to be approved within 48 hours. Especially for large loans, assets may be required guaranteed.

Procedure for calling for loan capital:

1) Business owner registers to raise capital
2) Lendbiz staff conducts appraisal procedures.
3) Loan approval is communicated to investors.
4) The enterprise is notified to accept the deposit.
5) Lendbiz prepares legal procedures.
6) Money is transferred directly to the designated bank account.

Investors: [22] Lendbiz allows individual investors to access and invest in businesses with a minimum of 500,000 VND. In addition, the system allows investors to withdraw investment capital or resell the investment to other investors if certain conditions are met.

Investment process:

1) Open an account online.

2) Choose an investment portfolio.

3) Transfer investment money.

4) Receive monthly principal and interest via account.

5) Reinvest.

Advantage:

- Business processes are changed to suit the market
  Vietnamese market but still ensures the typical characteristics of the tissue peer-to-peer lending.
- Has the function of allowing investors to withdraw capital or resell investments to other investors.

Limit:

- The system has not completely automated all stages because there are still factors legal and impact appraisal staff.
- Ability to require collateral for mobilized loans
  large capital.
- There is no integrated mobile application platform.

2.2 Proposed process and system

With the above analysis, the team found that each system has its own features suitable for each user target and market share that each platform targets.

Besides, each system has its own strengths and some limitations and risks in each model. With the knowledge learned in the subject "Software design analysis" and "Information system analysis and construction", the group has researched and inherited ideas and features from those systems to propose a solution. peer-to-peer lending system by applying blockchain to achieve the goals set out in chapter 1.3.2 and to create a practical software suitable for the lending market share in this environment.

Vietnam.

2.2.1 Describe peer-to-peer lending operations

2.2.1.1 Financial operations process

Depending on the way of operation, market size, and national territory, each bank and financial institution has its own business processes to implement and manage the lending model in different ways. Based on a limited understanding of economics and finance combined with reference to a number of related operations [23], the authors agreed on some basic financial regulations to serve as a foundation for building Build the proposed system in the next part, chapter 2.2.2. The regulations for peer-to-peer lending combined with blockchain that the group proposed include the following main parts:

1) The main task of the model is to connect borrowers and investors, automating most processes to minimize intervention.
of people, contributing to reducing costs incurred during the borrowing process.

2) The platform is linked to the user information authentication system.
The group's system will provide user information for this party to calculate and return the credit score results of the corresponding information. This is an important process in the model because it directly affects the credit risk of loan applications in subsequent processes.

3) Besides, the platform also links with electronic payment gateways
Determined to be Payoo payment gateway or linked with other banks.
The goal of this cooperation is to authorize the above system to transfer and receive money arising during the loan process. Peer-to-peer lending platforms cannot arbitrarily transfer or receive money for financial and legal information security reasons.

4) Regarding loan applications, borrowers can only own one loan application at a time. If the borrower owns a loan application that is in the investment process or is in the process of making term payments, the borrower cannot perform the new creation function.

5) Base amount is the amount that the system self-regulates as a basis
Break loans into small parts. The regulation of money

Facility is a prerequisite for the peer-to-peer lending model because it limits the case of investors monopolizing loan applications as well as sharing credit risks for the group of investors. System default number

Base amount is 500,000 VND.

6) The loan application amount must be between 1,000,000 VND and 50,000,000 VND, the loan amount must be divided by the base amount (500,000 VND). The number of loan months must be between 1 and 18 months. Loan purpose cannot be left blank and no loan purpose is accepted

for actions contrary to Vietnamese law.

7) Loan disbursement date is the date the borrower wishes to receive money from the electronic payment gateway. The disbursement date must be selected to begin 10 days after the loan origination date. The forward base date is the date disbursement but within the term, that month. For example, disbursement date loan is March 12, 2018. The base date of the term is April 12, 2018, May 12, 2018...

8) The loan interest rate is calculated and rounded according to Decree 174/2016/ND-CP [24] of Vietnam's accounting law. Formula [25]:

= a ÿ b. + .

In there:

r: interest rate of loan application.

ÿ: economic impact index, default ÿ = 36.

ÿ: credit score impact index, default ÿ = $\frac{3}{100}$

ÿ: impact index of loan amount, default ÿ = $\frac{3}{107}$

ÿ: impact index of loan months, default ÿ = $\frac{1}{3}$

s, c, m: are the variables credit score, loan amount and number of months of loan, respectively.

9) The loan is paid each term. In each term, the borrower must pay term principal, term interest, and previous term debt (if any). The cycle of each term is 1 month. The time limit for payment is 5 days. The end date of the term is the base date

of that month according to the provisions in section 7). The payment term is successful when the borrower pays the entire amount of the loan in full.

10) Term principal and term interest are calculated and rounded according to Decree Decree 174/2016/ND-CP of Vietnam accounting law. Recipe:

= ; — ' =

In there:

P, P': are the principal and term interest to be calculated, respectively.

c, m, r: are the variables respectively the total loan amount, number of months of loan and interest rate of that loan application.

11) The time to invest in a loan application is 10 days from the date of creating the loan application. A day is calculated from the time frame from 0:00 to 23:59 minutes 59 seconds same day. After this time the status of the loan will be automatically processed by the system according to the provisions in section 12).

12) A loan is considered a successful investment when it collects enough investment money from a group of investors. On the contrary, a loan is considered a failed investment when not enough contributions are collected. The loan is considered to end when the borrower has paid all terms.

13) With an investment application, the investor can only contribute money once per loan. And this time, investors can only invest in one denomination of money, which is the base currency (500,000 VND). This process is called the matching process, supporting the connection between investors and borrowers to suit each investor's loan purpose.

14) When committing to invest, investors will be clearly informed about the term principal amount, term interest, and monthly service fee. These numbers are calculated and rounded according to Decree 174/2016/ND-CP of the Accounting Law.
Vietnamese math. Recipe:

= —— = ; — ' = ; =

In there:

I, I': are the investor's principal and term interest related to a loan, respectively.

F: is the investment service fee when investing in a loan application through the platform.

P: is the term principal that the borrower needs to pay.

b: is the default base currency denomination of 500,000 VND.

c, m, r: are variables that are the total loan amount, number of months of loan, and interest rate of that loan application, respectively.

ÿ: is the default investment service fee percentage of 5%.

15) When the investor agrees to commit to invest, the investor is obliged to transfer the corresponding contribution to the electronic payment gateway within 3 days after receiving notification of a successful investment loan application. If investors do not comply with the above rules, they will be banned by the system
The penalty means not being allowed to make an investment within 1 month from now on After 3 days of receiving notification of successful loan.

16) The term amount that the investor receives from the electronic payment portal are automatically deducted from additional fees including money transfer fees and investment fees through the platform. In the case of personal income tax or value added tax, the platform does not bear any responsibility
in these cases.

17) Information about the loan process including: loan contract, loan contract, term payment contract, investment service fee contract must all be stored on the blockchain to ensure transparency, Minimize fraud and eliminate third-party risks to the system. Users will be allowed to view information about loan or investment applications related to that individual on the blockchain network. As for information about service fee contracts, only relevant parties who carry out cross-checking and verification from State agencies are allowed to access.

Scope: The system model the authors proposed above and intended to build is intended to illustrate the flow of a basic peer-to-peer lending system.
However, the proposed author group system is still within the scope of an undergraduate thesis, so there are some limitations in terms of legality and connection with service parties.

Tuesday:

- In section 2) linking with a third party providing user information authentication services, the authors intend to only build a model for declaring borrower information when the borrower registers a user account. use the system. After that, the information is saved to serve different purposes. Specifically about the rating score of the borrower, the authors propose that the default rating score of each borrower in the system is 580/980.
- In section 3) linking with payment gateways, the authors only intend to make a sample model describing the linking process when creating a loan, investing in a loan, and paying off a term loan. Legal limitations as well as some quite complicated regulations when having to link with a bank, such as the system does not intervene and record any financial transaction information of the user but completely The bank and payment gateway take care of it.

2.2.1.2 Diagram - operating principle

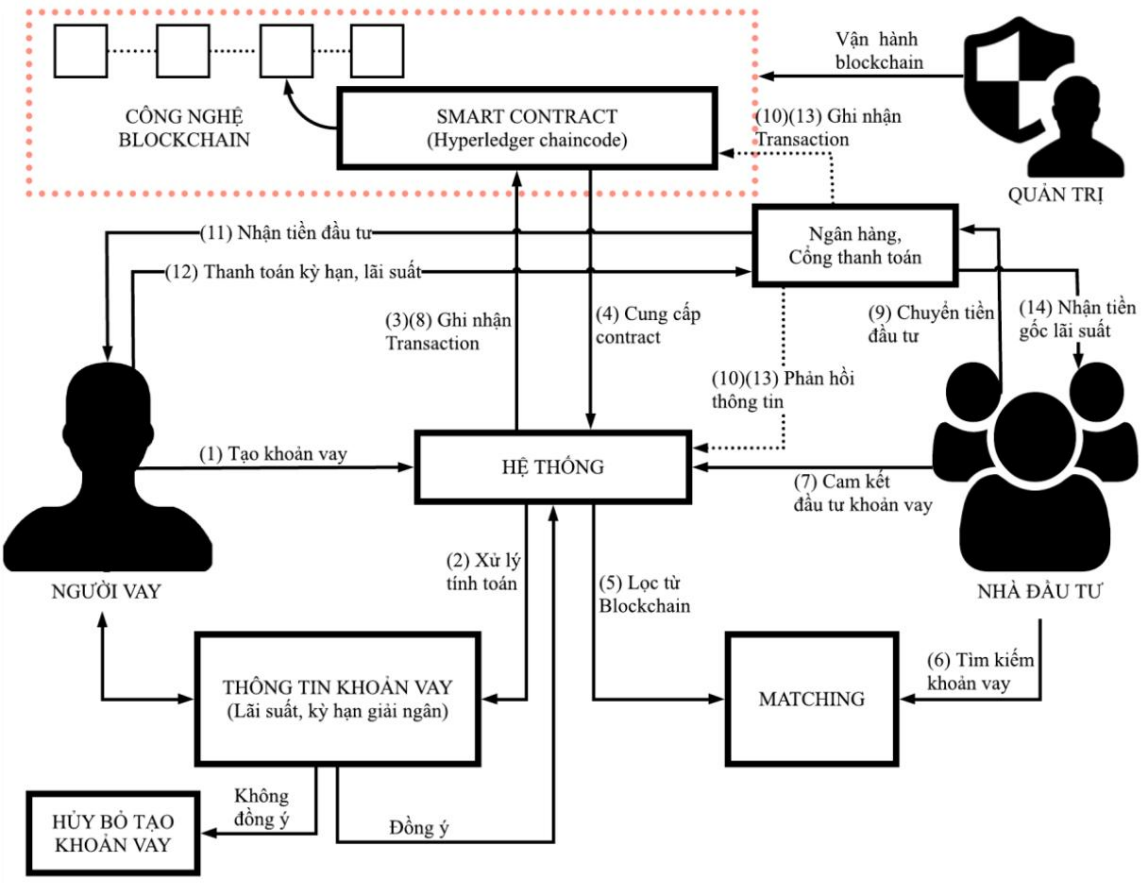

Figure 2-1. Peer-to-peer lending model combining blockchain

2.2.2 Description of the blockchain system

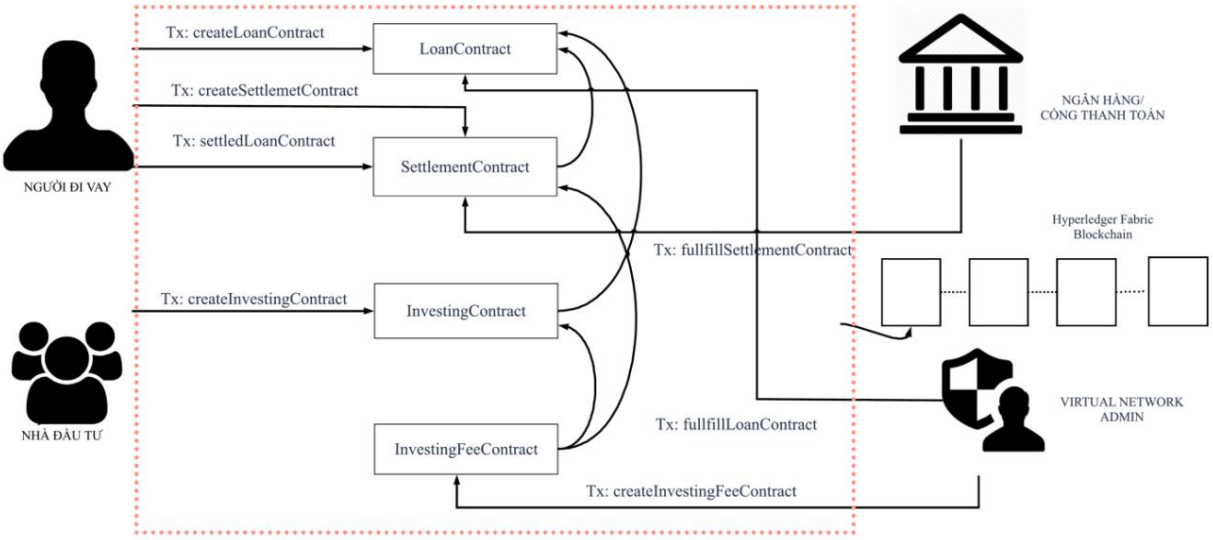

Figure 2-2. Smart Contract operating model

2.2.2.1 Overview

Applying the properties of the blockchain network, the authors propose a separate blockchain network for application in storing electronic contracts arising during the borrowing and investment process:

- The group proposes a blockchain data storage network according to a closed model (private blockchain). Regarding this system, all ledgers must have authentication certificates and network consent to participate in the system's data storage process. Compared to the blockchain system
  open (Bitcoin, Ethereum) this model is more suitable for the peer-to-peer lending model because of the fast recording speed, the user's credit information is kept confidential, and the dependence on cryptocurrencies is not yet legal. Recognition laws are completely eliminated.
- The blockchain system only stores electronic contracts that represent users' credit commitments. These electronic contracts include: loan contract (LoanContract), lending contract (InvestContract), term payment contract (SettlementContract), fee collection contract
  service (InvestingFeeContract). Except for the above types, other data types

such as user information, account information, credit scores, connection information with related parties... are all stored in the platform's own system.

- The blockchain network will interact with four main types of users: borrowers, investors, peer-to-peer loan system control, and electronic payment gateway control. Each type of user only has the right to access and manipulate a certain portion of data on the network through the functions provided by the system.

- The createLoanContract transaction helps the borrower create a loan.
- The createSettlementContract transaction helps the borrower create a forward payment contract and this will be done automatically when the loan application is successfully invested due to the borrower's authorization to the system when
  create loan application. The settledLoanContract transaction helps the borrower to pay the term that has been created on the blockchain. Additionally, the borrower can
  Access to review these transactions and contracts.
- The createInvestingContract transaction helps investors create an investment commitment for a loan application. In addition, investors have the right to view information about loan contracts in progress and view information about investment applications created by themselves.
- Control of the peer-to-peer loan system is a component of the software system (not human) that supports the automation process in the network
  Blockchain network in peer-to-peer lending business process. This component has the authority to access and view information of all contracts
  Loans are stored on the blockchain. Through the fullFillLoanContract transaction, this component will have its single state updated
  loan in accordance with the business process in section 12) chapter 2.2.1.1. Through the createInvestingFeeContract transaction, this component will automatically create service fee contracts in accordance with the business process in section 1.
  17) chapter 2.2.1.1 regulations.

- Payment gateway system control is a component linked and authorized by the system to carry out the flow of events of transferring and receiving money arising during the loan process. This system has the ability to update status of the term through the fullFillSettlementContract transaction upon response comply with the regulations of sections 3), 9) in chapter 2.2.1.1.

2.2.2.2 Smart Contract

Loan Contract contains information about the borrower and information about the loan loan amount.

Investment Contract (InvestingContract) contains investor information, information Loan application investment information, investment service fees, link to loan application.

SettlementContract contains information of the borrower, payment term information, and link to the loan application.

The investment service fee contract (InvestingFeeContract) contains service fee information for each term of the loan application, links to a group of investment contracts and a term payment contract.

2.2.3 Description of centralized system

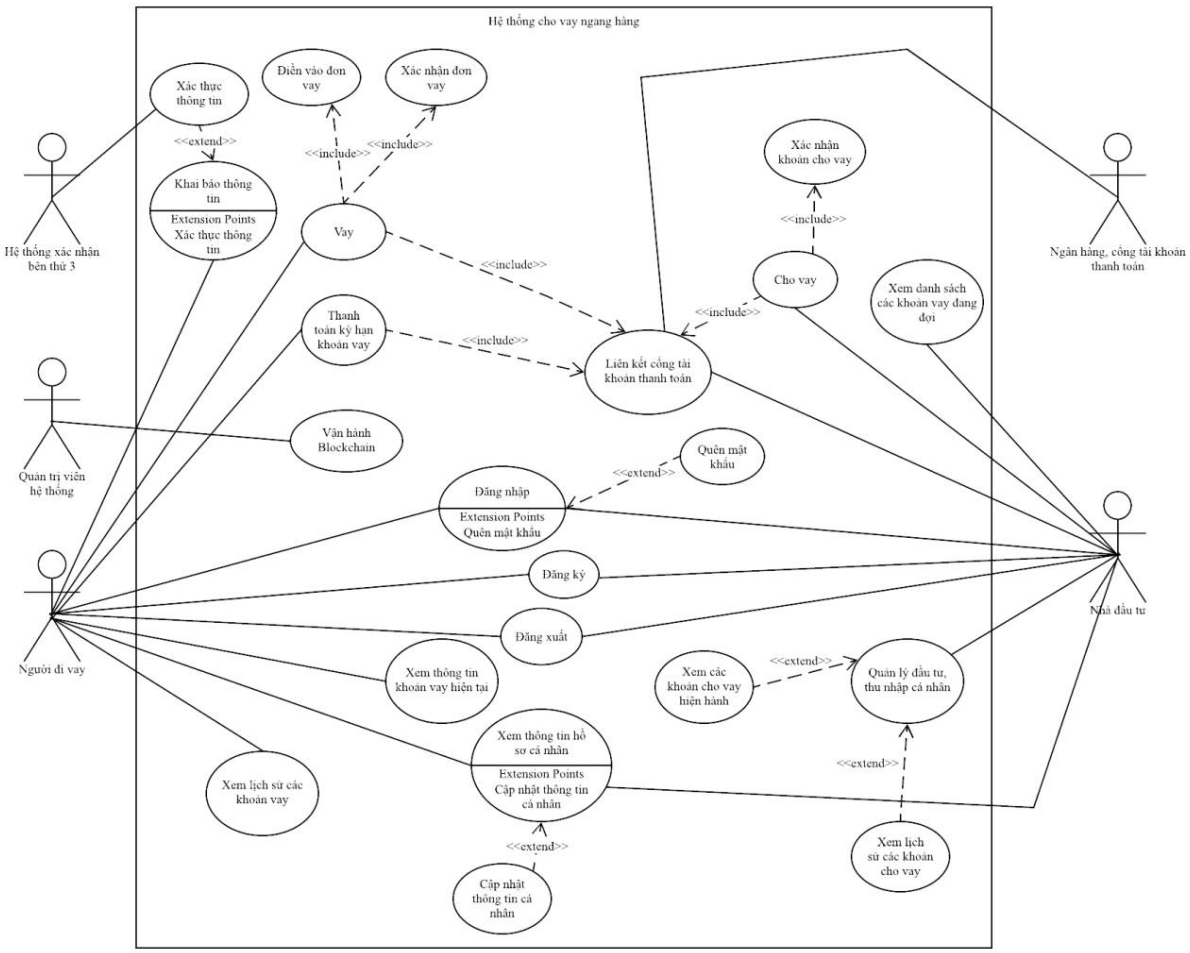

Figure 2-3. Use case diagram of centralized system

2.2.3.1 General features In

general, two main types of users: borrowers and investors will be able to perform some basic functions of a technology application:

• Register a new account in the system. •

Log in, log out of the system, change password when necessary. • Link the payment gateway to an electronic payment platform or to

Some banks link directly to the system. • Manage and

update personal profiles.

2.2.3.2 Specific features corresponding to user type

Each type of user can interact with the system through functions

Characteristic for each type of user:

- Borrower: Declare and authenticate personal information, create account confirmation loan, pay the loan payment term. In addition, borrowers can also track the progress (investment, repayment) of the current loan and calendar
  History of previous loans.
- Investor: review existing loans in the system, commit to investing in the loan, track the progress of the investment, the payment term of the loan application, and previous investment history. In addition, investors can also manage personal income through investment.
- Bank, payment account gateway: responsible for recording the payment accounts of borrowers and investors during the account linking process. The operation of receiving investment money from investors and transferring money to borrowers (cash flow) is undertaken by this third party.
- System confirms user information: receives user data from
  system to authenticate and evaluate the borrower's credit score and return the corresponding results to the system. Evaluating credit through user information is extremely important because it directly affects the default risk of each loan application.

2.2.4 Description of basic functions

2.2.4.1 Account registration function

1) Description: the user creates an account by providing a new phone number that is not yet recorded in the system. There are two types of accounts corresponding to two types of users: borrowers and investors.

2) Pre-conditions: (none)

3) Following condition: the system recognizes the newly created user account. At the same time, depending on the type of user, the application returns a corresponding interface corresponds to that type of user.

4) Secondary event stream: (none)

5) Main event flow:

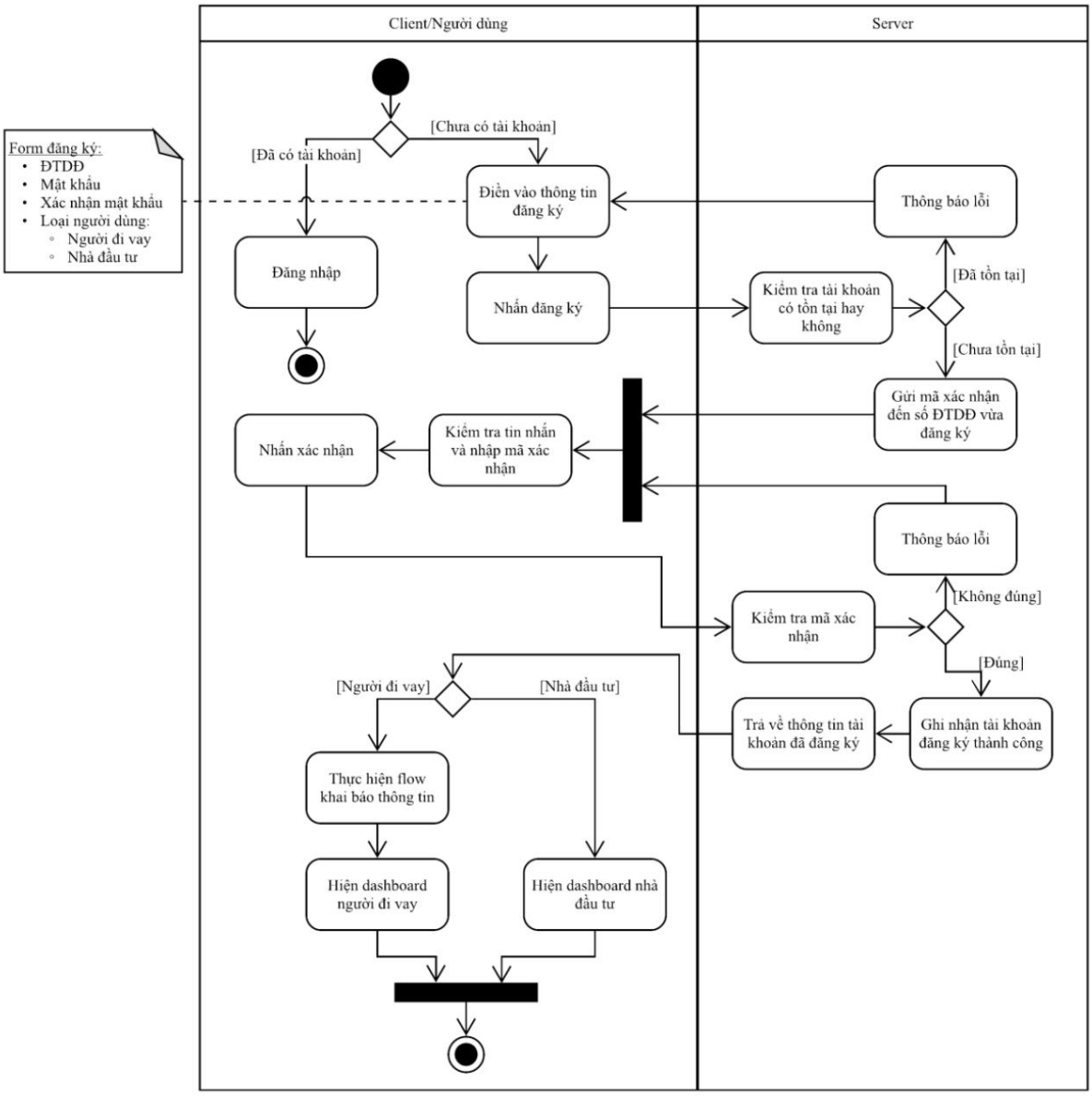

Figure 2-4. Account registration event flow

2.2.4.2 System login function

1) Description: user logs into the system with the phone number provided Registered before. 2)

Pre-conditions: (none)

3) Following conditions: Depending on the type of user, the application returns the interface corresponding to that user type.

4) Secondary event stream: (none)

5) Main event flow:

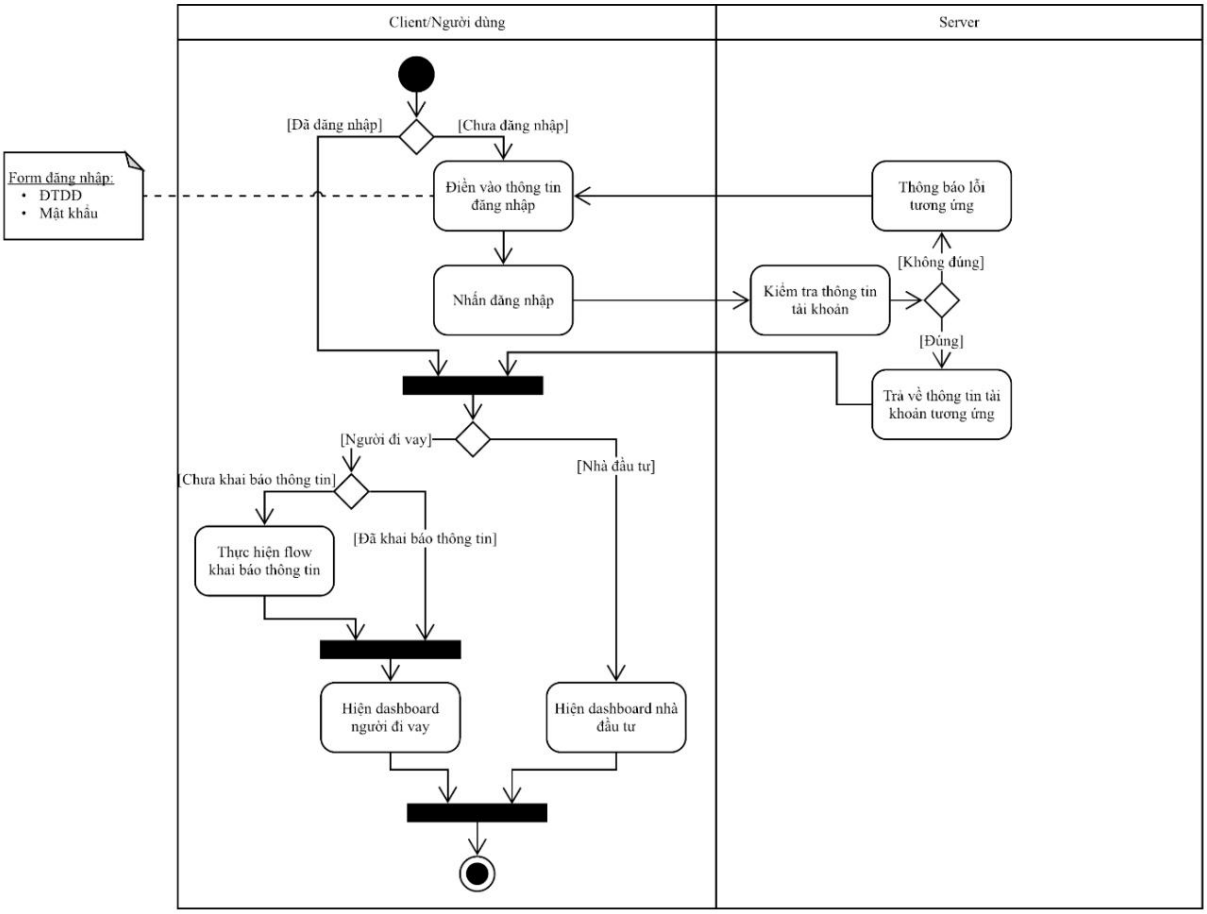

Figure 2-5. System login event stream

2.2.4.3 Information authentication declaration function

1) Description: the borrower provides personal information for the platform to authenticate and calculate credit scores for future loan creation.

2) Precondition: User has logged into the system. Account
The user belongs to the category of borrower. The user has never declared previous information.

3) Following conditions: The system records personal information and credit scores have been calculated from a third party. Returns the user to the main interface application.

4) Secondary event stream: (none)

5) Main event flow: Follow the professional regulations described above section 2) chapter 2.2.1.1.

6) Exception: When the 3rd party verifying information cannot authenticate user information, the system will not allow the borrower to make any loans. In other words, loan origination only
takes place once the borrower's information has been verified and an assessment score is returned from the 3rd party service.

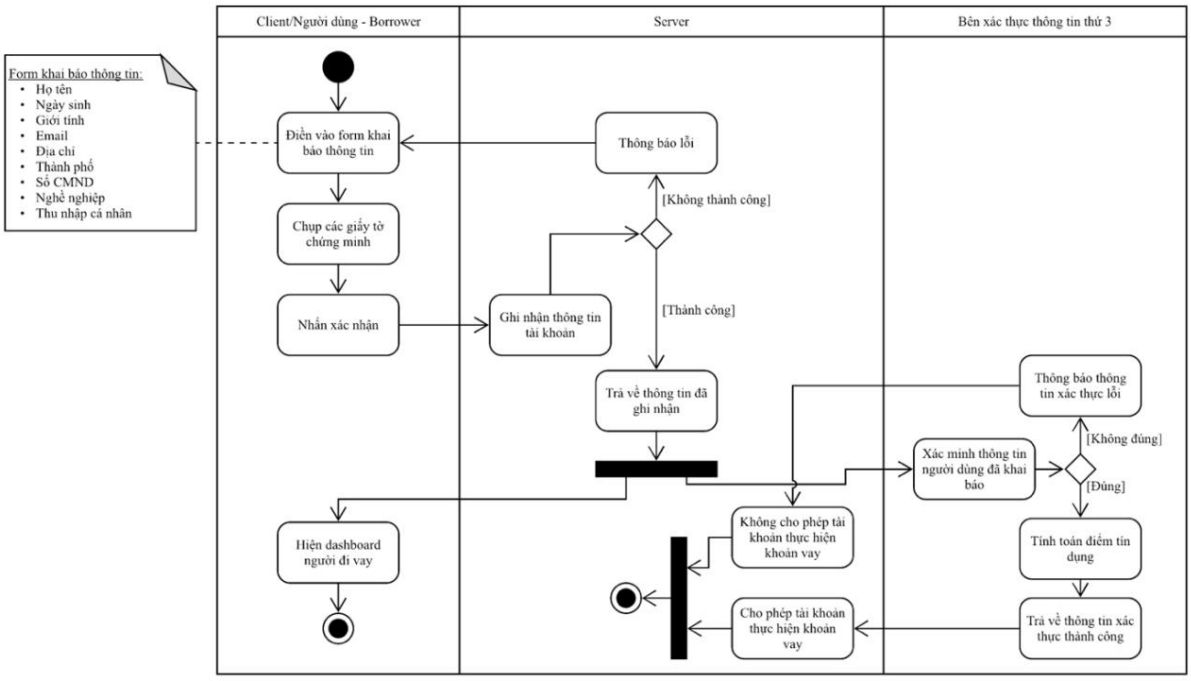

Figure 2-6. Event stream validates information

2.2.4.4 Payment gateway linking function

1) Description: the borrower links the electronic payment gateway to serve the stream of money transfer and receipt events generated through the system of electronic payment gateways. This linkage only takes place when performing loan creation flows (section 2.2.4.7), loan investment (section 2.2.4.9) and pay off the term loan (section 2.2.4.8).
2) Precondition: user has logged into the system. If the user is a borrower, they need to declare and authenticate the previous information.
3) Following conditions: the system is authorized to record linked account information. Show notification about link results.
4) Secondary event stream: (none).
5) Main event flow: Follow the regulations on tissue operations described in section 3) chapter 2.2.1.1.

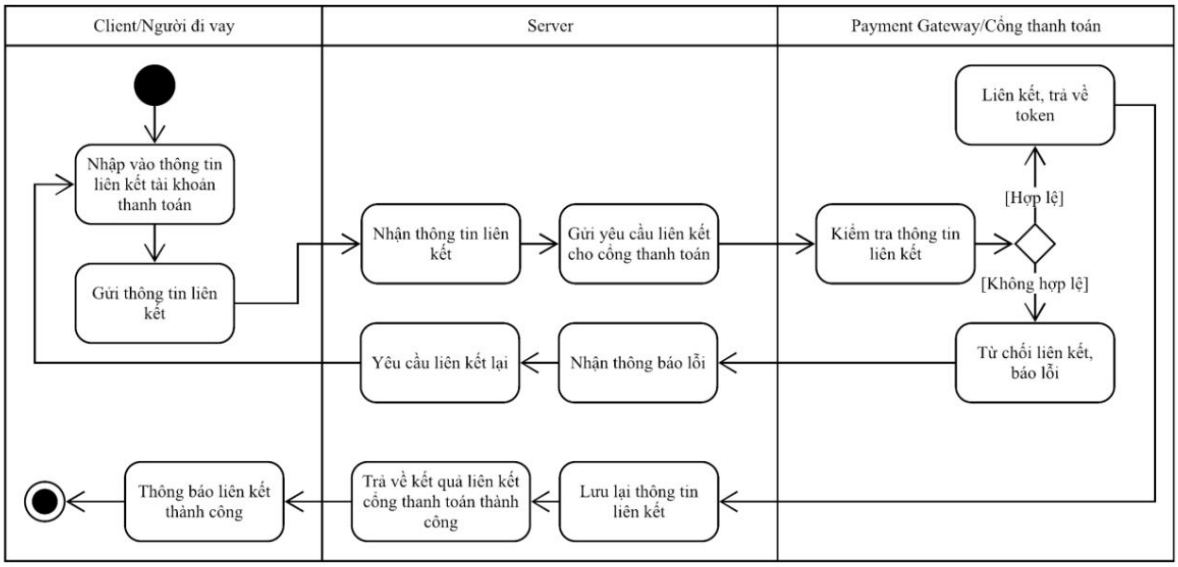

Figure 2-7. Stream of events linked to electronic payment gateway

2.2.4.5 Function to view current loans

1) Description: users can view progress, status, detailed information of current loan.

2) Precondition: user has logged into the system.

3) Following conditions: (none)

4) Secondary event stream: (none)

5) Main event flow: The application displays detailed information about the loan, loan status and other corresponding information (investment progress/disbursement progress) based on simulated business regulations. described in section 11), 12), 17) chapter 2.2.1.1.

2.2.4.6 Function to view loan history

1) Description: users view loan history by each jurisdiction different (borrower/investor).

2) Precondition: user has logged into the system.

3) Following conditions: (none)

4) Secondary event stream: (none)

5) Main event stream: The application displays detailed information about the loan, loan status and other corresponding information (investment progress/disbursement progress) that has occurred in the past and is actually happening. appear correctly Professional regulations described in sections 11), 12), 17) chapter 2.2.1.1.

2.2.4.7 Loan creation function

1) Description: the borrower creates a loan by providing information about the loan: loan amount, loan period, disbursement period, purpose get a loan.

2) Precondition: user has logged into the system. Account the user belongs to the borrower type who has declared authentication information.

3) Following conditions: loan application recording system on blockchain. Notice of successful loan application creation and return to the main interface.

4) Secondary event stream: event stream linking the electronic payment gateway.

5) Main event flow: comply with the business regulations described above sections 4), 6), 7), 8), 9), 10), 11), 17) chapter 2.2.1.1.

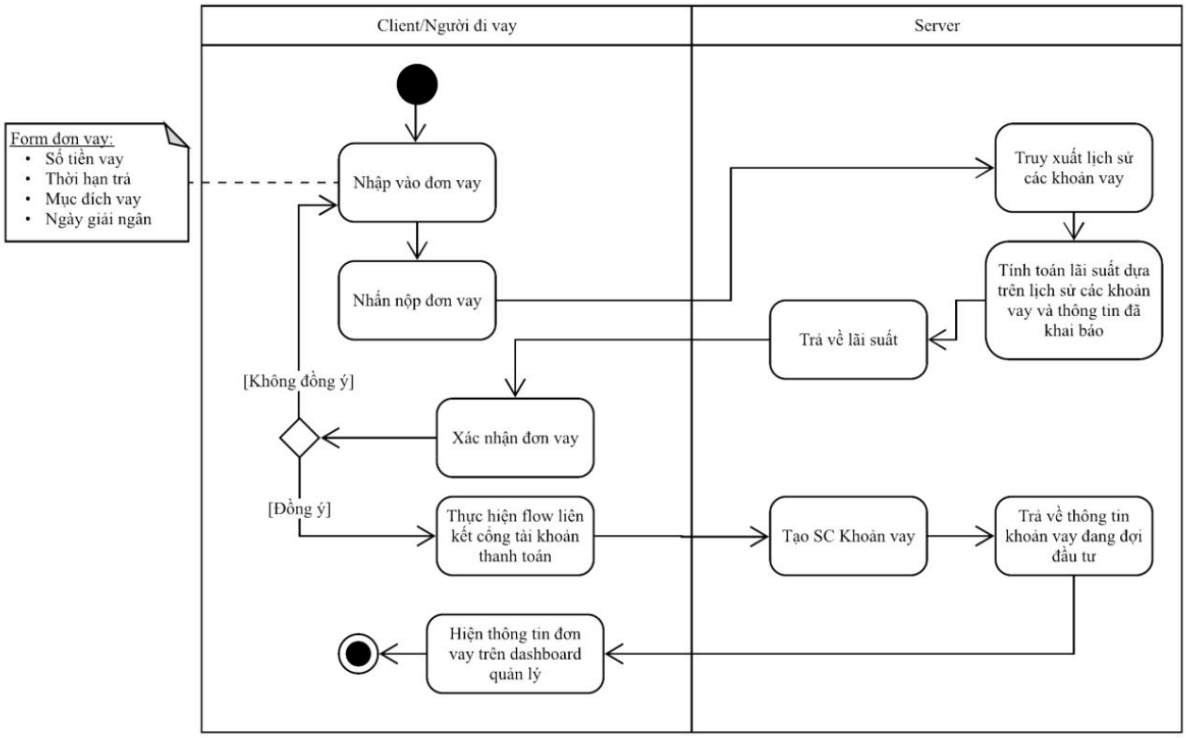

Figure 2-8. Loan creation event flow

2.2.4.8 Loan term payment function

1) Description: the borrower pays the term of the current loan.

2) Precondition: user has logged into the system. Account
The user belongs to the category of borrower. The borrower has a loan
are in the loan repayment period.

3) Following conditions: the system records term payment information
Borrow on blockchain. Notify successful term payment and take the user to the
current loan management section.

4) Secondary event stream: event stream linking the electronic payment gateway.

5) Main event flow: comply with the business regulations described above
Sections 3), 7), 9), 10), 17) chapter 2.2.1.1.

6) Exception: When the available amount in the user account is not enough to make
the term payment, the payment gateway will
returns the corresponding error to the system, from which the system requests the user

Load enough money into the payment gateway and try again later, and the term loan payment flow will now return to its original status of unpaid.

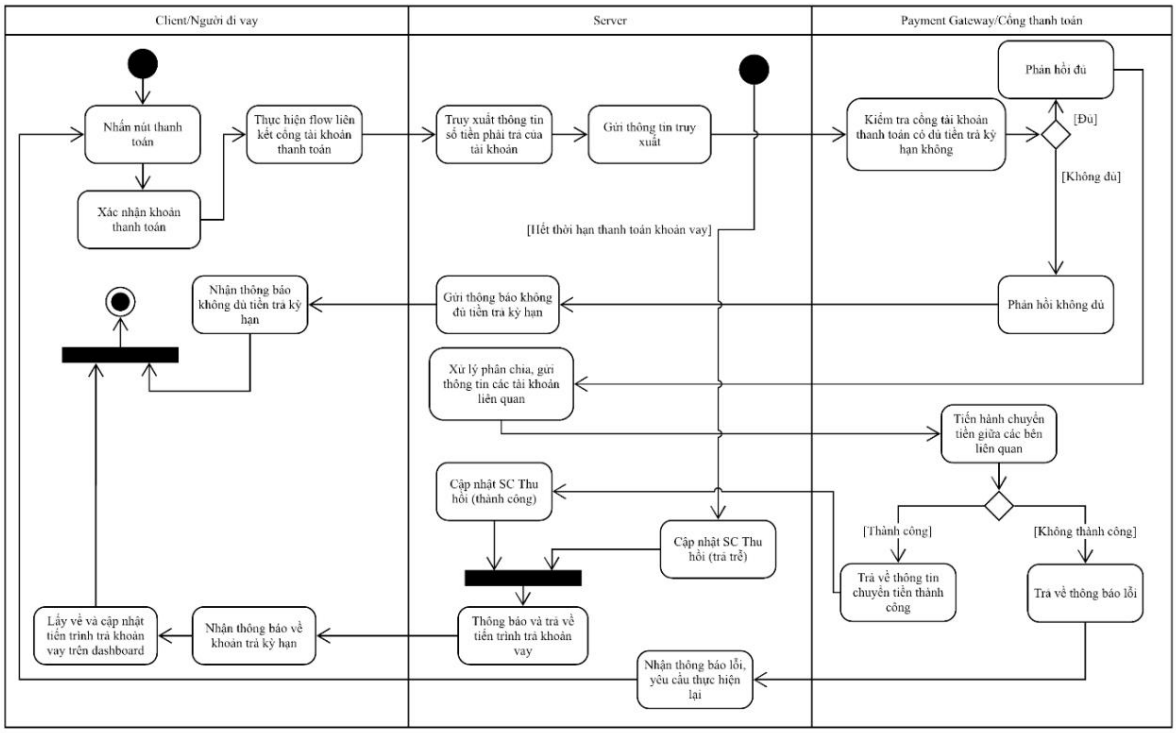

Figure 2-9. Term payment event stream

2.2.4.9 Loan investment function

1) Description: investor creates loan investment commitment.

2) Precondition: investor logs into the system.

3) Following conditions: investment application recording system on blockchain. Notify the results of the investment application and return the user to the main interface application.

4) Secondary event stream: event stream linking the electronic payment gateway.

5) Main event flow: comply with the business regulations described above Sections 11), 12), 13), 14), 15), 17) chapter 2.2.1.1.

6) Exception: When the loan has been invested successfully (enough amount committed to investment), and at the time of transferring money to the borrower (disbursement date), the investor must ensure there is enough money in

previously linked payment gateway account. If there isn't enough specified amount, the system will report an error and notify the investor to ensure the amount committed in the payment portal within a certain period of time. After the above period of time, if you still do not have enough money transferred to the borrower, the investor's account will be temporarily locked and no longer able to make investments. The loan will be recorded as failed and notified to other investors.

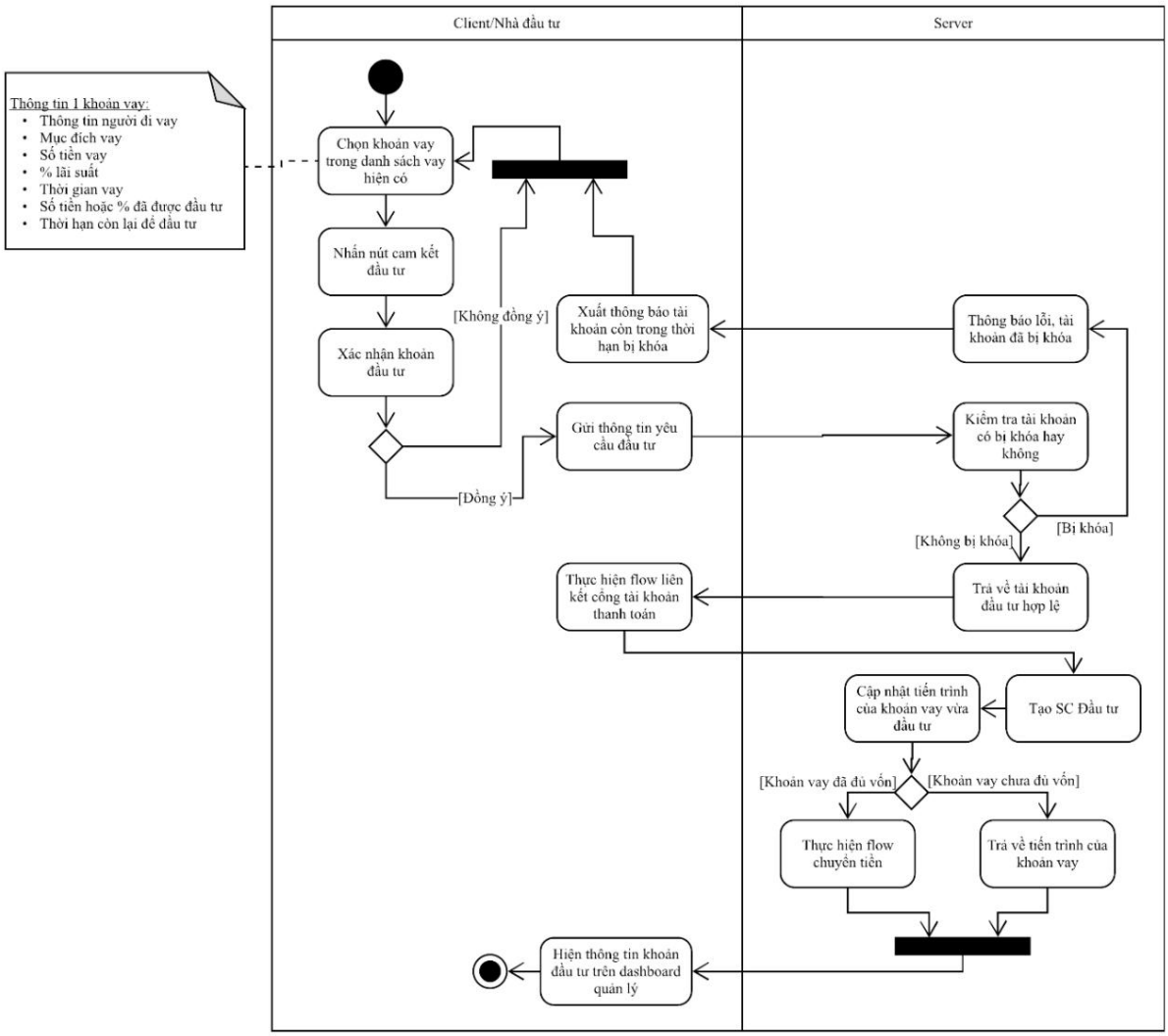

Figure 2-10. Loan investment event stream

2.2.4.10Functions of investment and personal income management 1)

Description: investors manage total investment and expected income. 2) Precondition: investor has logged into the system. 3) Following conditions: (none)

4) Secondary event stream: (none)

5) Main event flow: The application displays information about the amount of money invested, classification of principal, interest, and investment service fees for this individual investor.

2.2.4.11Personal information management function 1)

Description: users manage personal information entered into the system. 2) Precondition: user has logged into the system. 3) Following conditions: (none)

4) Secondary event stream: event stream that authenticates user information.

5) Main event flow: The application displays personal information that the user has entered into the system such as: full name, phone number, address, occupation, gender... Users can change the information This is real

Re-show the function of declaring and authenticating user information.

CHAPTER 3: SYSTEM DESIGN AND BUILDING

ÿ *Based on the surveys and recommendations in chapter 2, the main content of chapter 3 revolves around presenting technological solutions that will be applied to implement actual projects. The main components include analysis of the overall model design, detailed architecture, database of the entire system as well as related components.*

3.1 System architecture design

From the advantages and disadvantages of the systems surveyed above, the system architecture The following system is built to meet the necessary requirements.

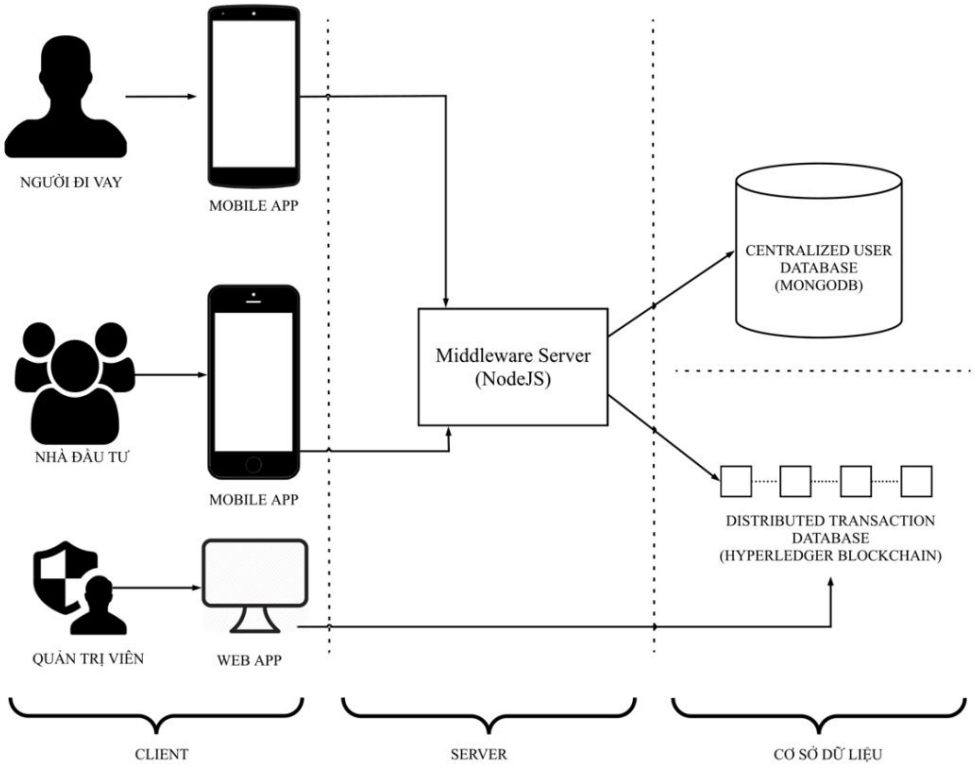

Figure 3-1. Proposed system architecture diagram

Based on the knowledge learned from the subject "Software Analysis and Design", the proposed system architecture is designed according to a 3-tier model, including 3 main components, each with its own organization. individual:

Client:

- Mobile application runs on both Android and iOS operating systems.
- Application for both borrowers and investors to manage and perform basic functions.

Server:

- Built on the NodeJs platform.
- Provides RESTful APIs for the real mobile client side perform the functions mentioned in section 2.2.3.
- Connect to the database (mongoDB) to perform read, write, Delete and update user data.
- Connect to the blockchain system used to store electronic contracts related to the loan process.

Database:

- Consists of 2 parts: centralized and decentralized database.
- Centralized database (mongoDB) serves the purpose of storing data data related to user information.
- Blockchain database is deployed on the Hyperledger Fabric private blockchain network system, with the purpose of storing electronic contracts of related loan processes.

3.2 Client design - mobile application

3.2.1 Technology used

Programming language: Javascript according to ECMAScript standard version 2015 (ES6).

Support tools: npm support libraries installation manager (Node Package Manager).

Platform: React Native version 0.55.3.

Development browser: Visual Code version 1.24.1.

Supported mobile operating systems: at least Android 4.1 (API 16) and iOS 8.0.

3.2.2 Reasons to choose React Native

Save time and effort: Native mobile app development requires an understanding of separate programming languages (Objective - C or Swift for iOS, Java or Kotlin for Android) which can be time-consuming and development effort. While with React Native, you only need to use the Javascript programming language, you only have to build the application once and the platform will display pure native interface (UI) components suitable for both Android and iOS.

Large support community: React Native is a new technology today but promises to grow into the future of mobile application development. Therefore, the support community is quite large and can solve common problems fast.

Unified user experience: React Native has a great advantage by displaying purely native interface (UI) components, not browsers or web views such as Web App, Hybrid App. Thanks to that, the platform helps users have a good and unified experience.

In terms of ideology: the author group has experience developing native Android applications, so they want to expand their learning and application of new technologies, while also serving the purpose of comparing and evaluating current mobile development platforms. in.

3.2.3 Architecture

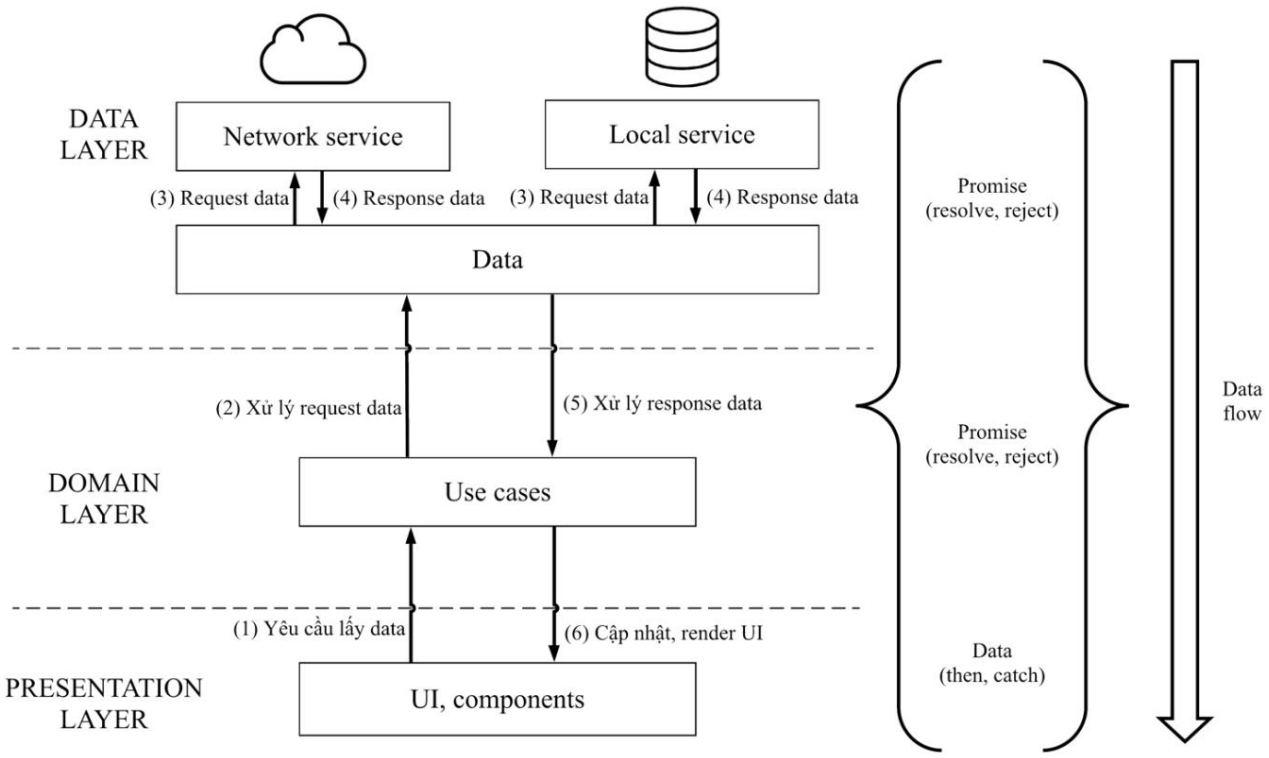

Figure 3-2. Client - Mobile app architecture diagram

Client side architecture diagram - Mobile app is designed based on Clean Architecture [26], divided into 3 main parts:

- Data Layer: This layer is responsible for the functions required to create, read, write and update data of the entire system. In the current application, there are two types of data: data returned from the server and data stored directly on the computer (local database). When receiving a request from the domain, this layer will execute related functions and return data raw material as required. Functions are only executed when the domain layer has a request, however, when the domain has a structural change, the data layer does not need to change because it is independent and independent. depends on how it is handled at the domain layer.

- Domain Layer: this is the intermediate layer between the data layer and the interface layer. When there is a request from the interface, this layer will execute logical processing functions to make decisions that affect the data layer. Once raw data is received from the data layer, decisions will be made to return the data as requested at the interface layer.

- Presentation Layer: This layer is responsible for displaying interface elements (UI) on the screen for users to interact with. When there is interaction with a certain component from the user, this layer will ask the domain layer to return the necessary data to update the interface accordingly. This layer does not know whether the returned data comes from the server or from the machine (local database), but only cares about it

  displays the appropriate interface depending on the returned data.

Reasons to choose Clean Architecture:

- Easy to maintain and manage: in Clean Architecture, floors and layers are clearly separated, each layer takes on separate functions and does not depend too much on each other, ensuring easy maintenance. and code management. In addition, the independence of the layers makes it possible
  The ability to expand and change when required is more convenient, avoiding the need to completely change due to the connection between components.
  too tight.
- Independence between the interface (UI) and the database: in the above architecture, data flow is poured from the data layer to the processing domain layer and finally to the interface layer to represent the functions. on-screen interface elements. Therefore, if there is a change or redesign of the interface without changing the system structure, it is only necessary to update the interface layer and keep the same way of handling data from related sources.

  mandarin.

- Easy to write unit tests: According to the above design rules, at the data layer and domain layer, the functions written are guaranteed to be pure Javascript functions. This helps when writing unit tests because these two layers do not contain components that depend on the React Native platform. Writing unit tests helps the ability to detect and identify errors quickly and accurately

more precise.

3.3 Design and deploy server - back-end

3.3.1 Technology used

Programming language: Javascript according to ECMAScript standard version 2015 (ES6).

Platform: Node.js, version 8.10.0, open source developed and managed Managed by The Linux Foundation. (https://nodejs.org/en/)

Deployment environment: Heroku, company service Salesforce.com, supported Deploying back-end systems and databases to cloud computing (cloud platform). (https://www.heroku.com/)

Development tools: Visual Studio Code, version 1.24.1 developed by the Microsoft community. (https://code.visualstudio.com/)

3.3.2 Reasons to choose Node.js

Javascript language: Node.js supports server system development in the language Javascript language, a language with simple, clear syntax, suitable for groups who already have knowledge of this language, just need to learn more about the platform to install and develop the system. system.

Easy to install and expand: the server is built using the compliant Node.js platform Single-threaded input and output event handling principles supported by the Express.js library help the team optimize installation time and be suitable for future development. This.

Fast processing speed: Node.js operates on the Google V8 Engine platform developed by Google and is the main component of the Google Chrome browser, supporting source code compilation and Javascript execution at remarkably fast speeds. Comparing between Node.js and other platforms [27], node.js only lags behind Go in request/second and is on par with Java:

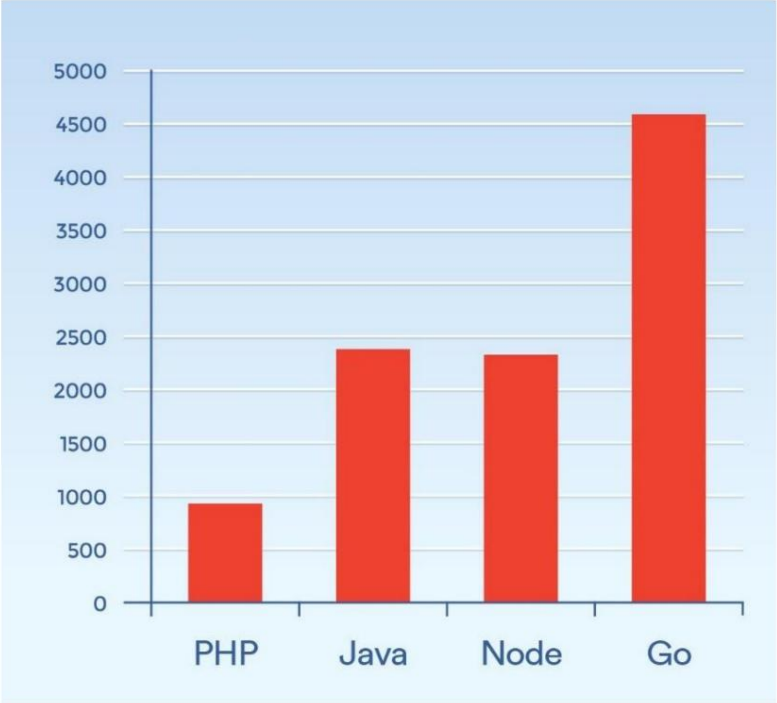

Figure 3-3. Request/ second of back-end platforms

Strong development community: Node.js is one of the most popular platforms for building back-end systems today. Communities from Github have developed free rm modules that help the authors a lot in integrating into the system.

system through Node Package Manager (npmjs).

3.3.3 Reasons to choose Heroku

Easy to deploy and expand: with the support of the Heroku Command Line Interface (CLI) tool, deploying the back-end system to cloud computing is easy.

with a simple Git command. This takes less than 5 minutes. Developers only need to understand how basic CI/CD (Continuous Integration/Deployment) works without worrying too much about Apache or Nginx.

In addition, Heroku also provides support services for bringing the MongoDB database to the cloud.

Cost-effective: Heroku allows developers to deploy private systems on the platform's containers at a nominal cost. With the goal set before, the team is using the platform for free and is considering using a $7 per month plan to expand the system with better functions.

System security support: By separating independent Dynos on different clusters at different times, Heroku has created a basic security layer for the systems operating on this. In addition, the platform also clearly distinguishes between data
Temporary data storage and permanent data storage (Ephemeral filesystem) supported in Securing and backing up user databases.

3.3.4 Server architecture

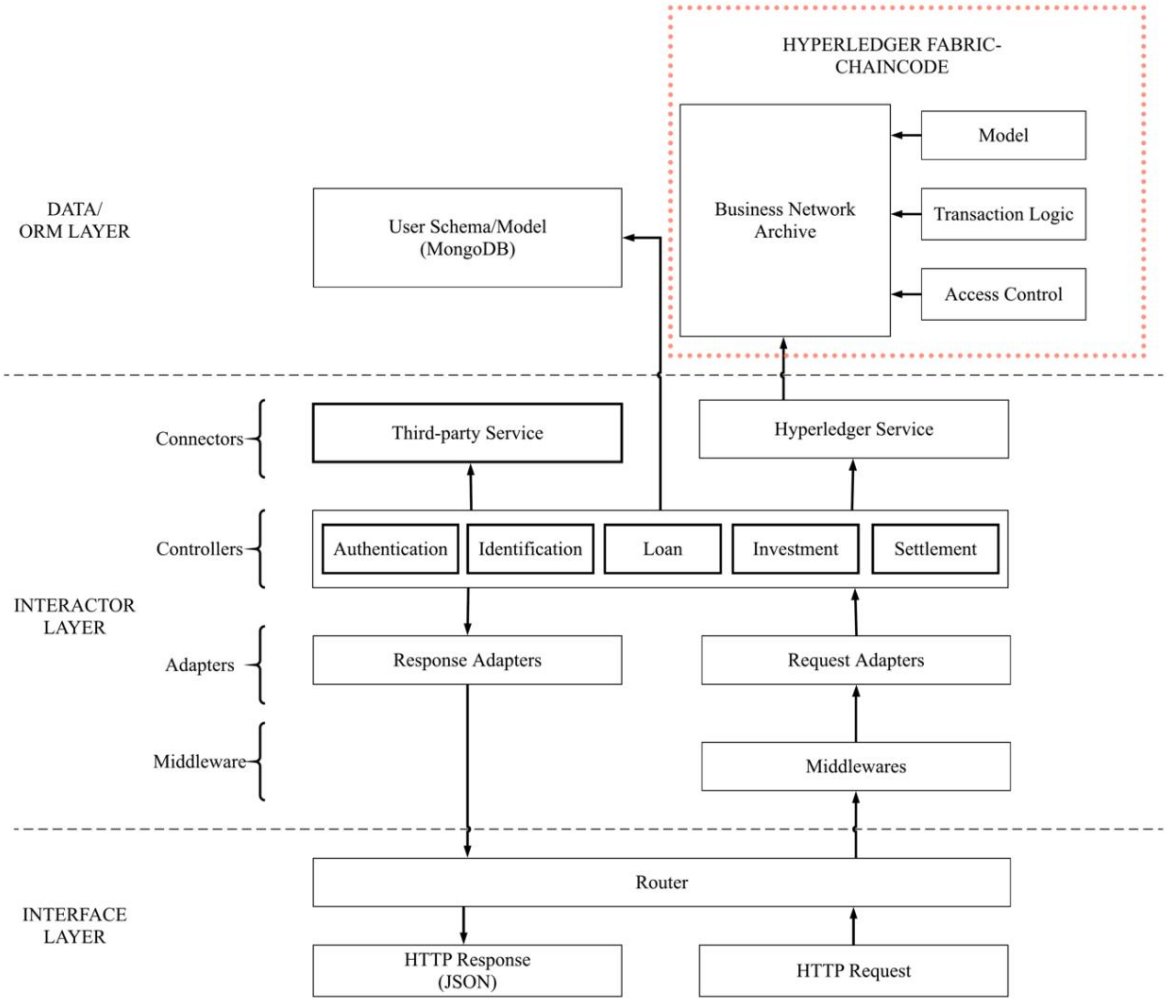

Figure 3-4. Node.js back-end system architecture

The authors propose a back-end system based on a layer-by-layer architecture. The goal of this separation is to help the author team easily manage source code components, save installation time, and easily expand the system.
system in the future. In each layer, each part is installed in separate layers
based on different roles:

- Interface Layer: plays the role of receiving requests from the client side. Then coordinate other components of the system for retrieval and return response about the data corresponding to that request.
- Interactor Layer: plays the central role of the system. Business processes, financial regulations, and peer-to-peer lending processes are specifically shown in this layer. Middleware and Adapters play the role of receiving requests, decentralizing permissions, and authenticating users from the Interface layer. Controllers are divided into small parts, each part handles
  Manage different operations such as: loan application management, investment application management, term payment management. Connectors assist in linking queries to third-party services and connecting directly to the network blockchain.
- Data/ORM layer: plays the role of mapping database layers from the system MongoDB serves the CRUD (Create Read Update Delete) task for the Interactor layer. The Hyperledger Fabric – Chaincode part will be described in more detail in chapter 3.5.

3.3.5 Main processing issues

3.3.5.1 User authentication method

To authenticate users, the authors propose a method to authenticate people
used using JSON Web Token (JWT):

- Scenario: When a user logs into the system, the system provides a token so that subsequent requests from the user must add this token. Specifically, this token must be attached to the part

header of each request. Based on the token, the middleware department will Classify the user, accept or reject this request and transfer assign the controller to perform the corresponding business process.

- Description: JWT is a secure way of transmitting information according to the standard (RFC 7519) [28]. JWT is essentially a string encrypted according to a specified hash algorithm consisting of three main parts: Header, Payload, Signature. Header contains hash algorithm information (group uses HCMA SHA-256). The payload will contain the information to be transmitted (the group transmits the user's id combined with the salt string to enhance security), the signature part contains the private key code specified by the group to distinguish it from other users. Other platforms use JSON Web Token.

3.3.5.2 Organize and deploy RESTful API

Endpoint URL address: https://p2p-lending-14clc.herokuapp.com/

Support library: Express.js (https://expressjs.com/)

Testing support tool: Postman, version 6.1.3.

The protocol used is HTTPS. The main methods used are POST, GET, DELETE, PATCH.

API requests are clearly specified in terms of transmitted arguments and information needed to retrieve data for each different lending process and are agreed upon in advance between client and server. Specifically, arguments are classified according to the type of business process: account-related (endpoint/auth), loan (endpoint/loan), investment process (endpoint/invest)... for the same business. differentiated by position functions: create loan (endpoint/loan/create), evaluate loan (endpoint/loan/rate)

··· The query part (for POST) is placed in the request body in JSON form. The This API is coordinated and managed by the Router component in the interface layer.

For each request, the server returns the corresponding response. All responses have a code that indicates the status of the request. Code 200: query successful,

code 400: invalid query, code 401: no permission to query... Returned data
placed in the body of the response and formatted according to JSON standard to meet the financial business process in the Adapters section of the Interactor layer.

3.3.5.3 Authenticate user information

Authenticating user information involves two separate processes: digital authentication phone and verify personal credit information.

Phone number validation occurs when a user registers a phone number. System through Twilio library (https://www.twilio.com) will generate a random string of 6 digits and send a message to the phone number just registered. Users must enter this authentication code to complete the account registration steps for the system.

Verifying personal credit information is a mandatory requirement for borrowers to be able to carry out the loan process. Users must provide complete information
Full name, address, gender, occupation, personal income, email... The system will provide this information to a third platform to evaluate the user's credit score.
As for Identification, the interactor layer will take on this role.

3.3.5.4 Decentralization of user functions

Determining the user type is done in the middleware part of the layer
Interactor by decoding the JWT attached to the request header.

Users through the client only have the authority to perform a certain group of functions through corresponding requests. The borrower can only manipulate the account
Loans through API POST endpoint/loan or POST endpoint/settlement... Investors can only invest through APIs POST endpoint/invest or view
loan via GET endpoint/loan/current…

Decentralizing user rights helps the system ensure the functionality of each type users, increase security, and minimize access errors from the client side.

3.3.5.5 Direct connection to the blockchain network

Support library: Hyperledger Composer

Description: The server system acts as an intermediary providing API for users to perform functions related to the blockchain network. This function uses

Use implementation functions in the Hyperledger Service class that inherits from the Composer and instance superclasses

appears in the interactor layer. These functions are mainly related to issues: connecting to the blockchain network, authenticating users, creating new transactions, querying transaction data.

pandemic.

Scenario: To ensure the independent operation of both systems, users access the blockchain network through the identity certificate including publicKey, privateKey, certificate that the blockchain network provides. According to the business process, the back-end system will be authorized to create and keep this authentication information as part of the user account to synchronize the system account with the blockchain identity. This means that when logging into the system, the user will be able to

The ability to interact directly with the blockchain network according to the horizontal lending process

goods ordered by the group.

3.4 Database design and implementation

3.4.1 Technology used

Database: MongoDB, version 4.0, (https://www.mongodb.com/).

Support library: Mongoose, version 5.1.7, (http://mongoosejs.com/).

Database management system (HQTCSDL): MongoDB Compass, version 1.14.5,

(https://www.mongodb.com/products/compass).

3.4.2 Reasons to choose MongoDB

MongoDB is a non-relational (NoSQL) database

Store information in documents to form a collection

Because relational databases store rows of data to form a data table

data (table). Storing data in JSON will make it easier for the back-end system

Easily map back and forth between data types in the Javascript programming language.

The process of reading and writing data achieves high performance thanks to the Embedding document form without having to go through the operation of joining table data like CDQL.

relationship.

Thanks to the support of the document-oriented mapping library (Object Document

Mapping) Moongose, building databases through Schema/Model helps teams save installation and management time.

Future expansion of CSQL is also made easy because of the structure

Flexible databases do not need to consider binding relationships such as table structures.

3.4.3 Description of data classes

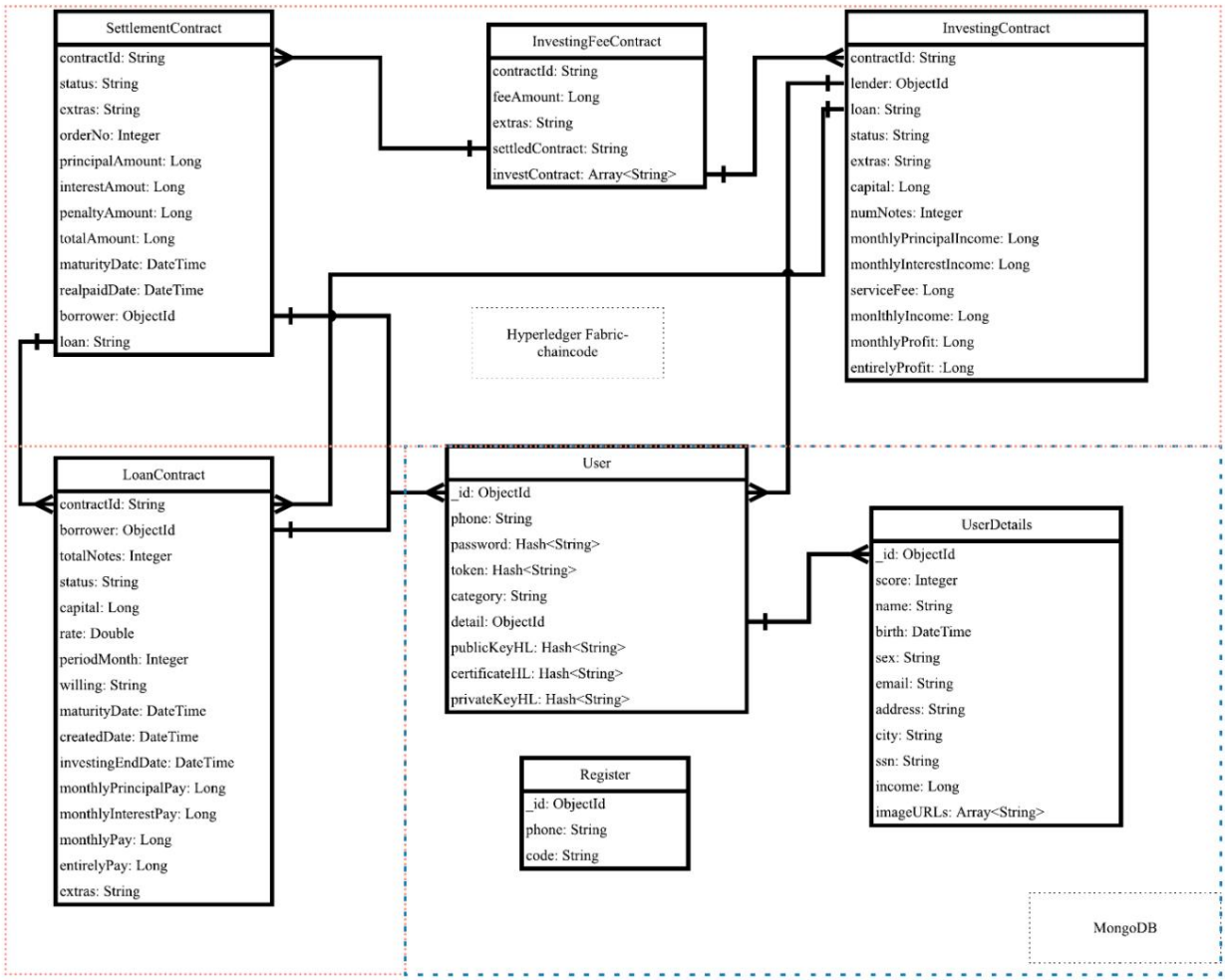

Figure 3-5. Database architecture diagram

MongoDB database is a centralized database deployed to the heroku cloud environment along with a back-end system provided by the service (addons) that heroku provides. This database only stores information about the user's login account and detailed information that the user provides during the information declaration process. Information about electronic contracts will be stored in the blockchain network described above

Chapter 3.5 to ensure transparency and prevent fraud during the implementation process

loan submission. In addition, personal financial information will not be stored but will authorize a link with the electronic payment gateway to perform related operations.

3.4.3.1 Registration information

Stt	School	Datatypes	Meaning
1	_id	ObjectId	Main courses
2	phone	String	Registered user phone number
3	code	String	Verification code sent to phone number

Table 3-1. Schema Register

3.4.3.2 User accounts

Stt	School	Datatypes	Meaning
1	_id	ObjectId	User account ID, primary key
2	phone	String	User phone number
3	password	Hash<String>	The account password has been encrypted according to SHA256 algorithm
4	token	Hash<String>	Json Web Token
5	category	String	User type
6	detail	ObjectId	Link to detailed information
7	publicKeyHL	Hash<String>	Public key of blockchain network account
8	certificateHL	Hash<String>	Blockchain network access certificate
9	privateKeyHL	Hash<String>	Private Key of blockchain account

Table 3-2. Schema User

3.4.3.3 User details

Stt	School	Datatypes	Meaning
1	_id	ObjectId	Primary key ID
2	score	Integer	User credit score
3	name	String	User name
4	birth	DateTime	Date of birth
5	sex	String	Sex
6	email	String	Email address
7	address	String	Address
8	city	String	City
9	ssn	String	Identity card number
10	income	Long	Personal income
11	imageURLs	Array<String>	Path of authenticated images

Table 3-3. Schema UserDetails

3.5 Design and deploy blockchain networks

3.5.1 Technology used

Programming language: Javascript, Go.

Blockchain network: Hyperledger Fabric, version 1.0, (https://hyperledger-fabric.readthedocs.io/en/release-1.0)

Deployment platform: IBM Kubernetes Container Service, version 1.9.8, (https://www.ibm.com/cloud/container-service)

Support tools: Hyperledger Composer, version 0.16.7, (https://hyperledger.github.io/composer/)

Blockchain tracking system: Hyperledger Explorer, version 3.2, (https://github.com/hyperledger/blockchain-explorer)

3.5.2 Reasons to choose Hyperledger Fabric

Hyperledger Fabric is an open source platform developed by the Linux Foundation community since July 2017. The goal is to build a closed blockchain network with a modular architecture that creates opportunities to build private networks as technology services serving various economic business processes.

A closed blockchain means that ledgers must go through a process of authentication and approval Only after agreeing with the entire network can you join and record data. Modular architecture is an architecture that helps developers build and manage their own network with that model instead of everyone having to use the same common network.

The authors evaluate Hyperledger Fabric as a blockchain network that is extremely suitable for the peer-to-peer lending model for many reasons. The closed network ensures that user information, especially financial information, is kept confidential and controlled by authorized organizations, avoiding disclosure of user credit information. Write speed

Fabric's data reception is faster than public blockchain networks. The network does not depend on cryptocurrencies, which play a central role in the network

public blockchain.

The Hyperledger Fabric community is extremely popular. The birth of Hyperledger Composer helps the team build, deploy, and manage blockchain network ledgers effectively. Hyperledger Composer supports chaincode building

in Javascript, the programming language of this project, instead of the team having to learn and learn the GoLang programming language to install this part.

Some differences between Hyperledger Fabric and Ethereum [29]:

	Ethereum	**Fabric**
Type	Public blockchain	Private blockchain
Architecture	Generic platform	Module platform
Main algorithm	Proof of Work (PoW)	Practical Byzantine Fault Tolerance (PBFT)

Establishment language submit	Solidity, Javascript	GoLang, Javascript
Cryptocurrency	Ether	Do not have
Object recognition	~15s / block	~1s / block
speed	Community applications need popularity	Calculating application commerce: finance, health

Table 3-4. Compare Ethereum and Fabric networks

3.5.3 Description of electronic contracts - Smart Contract

3.5.3.1 Loan contract

Stt	School	Datatypes	Meaning
1	contractId	String	Loan ID
2	borrower	ObjectId	Borrower ID
3	totalNotes	String	Total number of splits
4	status	String	Loan status
5	capital	Long	Amount to borrow
6	rate	Double	Loan interest rate
7	periodMonth	Integer	Number of loan months
8	willing	String	Loan purpose
9	maturityDate	DateTime	Disbursement date
10	createdDate	DateTime	Date created
11	investingEndDate	DateTime	Investment end date
12	monthlyPrincipalPay	Long	Principal paid each term
13	monthlyInterestPay	Long	Interest paid each term
14	monthlyPay	Long	Total payment per term
15	entirelyPay	Long	Total payment
16	extras	String	Additional

Table 3-5. LoanContract

3.5.3.2 Investment contract

Stt	School	Datatypes	Meaning
1	contractId	String	ID of the investment
2	lender	ObjectID	Investor ID
3	loan	String	Loan application link - contractId
4	status	String	Investment status
5	capital	Long	Investment amount
7	numNotes	Integer	Investment part number
7	monthlyPrincipalIncome	Long	Principal received back each term
8	monthlyInterestIncome	Long	Interest received each term
9	serviceFee	Long	Term service fee
10	monthlyIncome	Long	Total amount received per term
11	monthlyProfit	Long	Real receipt every term
12	entirelyProfit	Long	Total amount received for the entire loan
13	extras	String	Additional

Table 3-6. InvestingContract

3.5.3.3 Forward payment contract

Stt	School	Datatypes	Meaning
1	contractId	String	Loan ID
2	borrower	ObjectId	Borrower ID
3	orderNo	Integer	Term number
4	principalAmount	Long	Term principal
5	interestAmount	Long	Term interest
6	penaltyAmout	Long	Previous term debt
7	totalAmount	Long	Total amount payable
8	maturityDate	DateTime	Payment deadline
9	realpaidDate	DateTime	Actual payment date
10	loan	String	Loan application link - contractId

11	extras	String	Additional

Table 3-7. SettlementContract

3.5.3.4 Service fee contract

Stt	School	Datatypes	Meaning
1	contractId	ObjectId	Loan ID
2	feeAmount	Long	Term service fee
3	settledContract	String	Link to loan term - contractId
4	investContract	Array<String>	Link to associated investment applications related to this term - contractId
5	extras	String	Additional

Table 3-8. InvestingFeeContract

3.5.4 Network design

[30] Hyperledger Fabric is a closed blockchain network that brings together many storage units (nodes) that play different roles and communicate with each other. This network is set up to execute chaincode (a term equivalent to smart contracts), store and execute transactions when appropriate conditions are met. As stated before, Fabric is a modular platform that allows different projects to build their own networks for each business model. These systems, including the group's systems, must comply with the architecture proposed by Fabric to ensure the properties of the blockchain network.
closed.

3.5.4.1 Ingredients

Hyperledger Fabric architecture includes the following main components:

- Client/submitting-client is the component that sends requests to execute transactions to endoresers and distributes these transactions after authentication to orderers.

- Peer is the place to manage and record blocks from orderer. Some special peers also perform transaction policy functions called endorsers.

Peers only perform a storage function called committing peers. Transactions stored on peer include two main parts: transaction log and world state. state. Transaction log is where blocks are stored and expanded as a chain into a blockchain storage architecture. World state is a mapping of The transaction log is considered a regular database (in This is the CouchDB database) that supports viewing and managing data.

- Orderer is a particularly important component in the blockchain network. This component plays a central role in ordering transactions to prevent double-spending, deciding the time and number of transactions contained in a block.

3.5.4.2 Transaction scenario

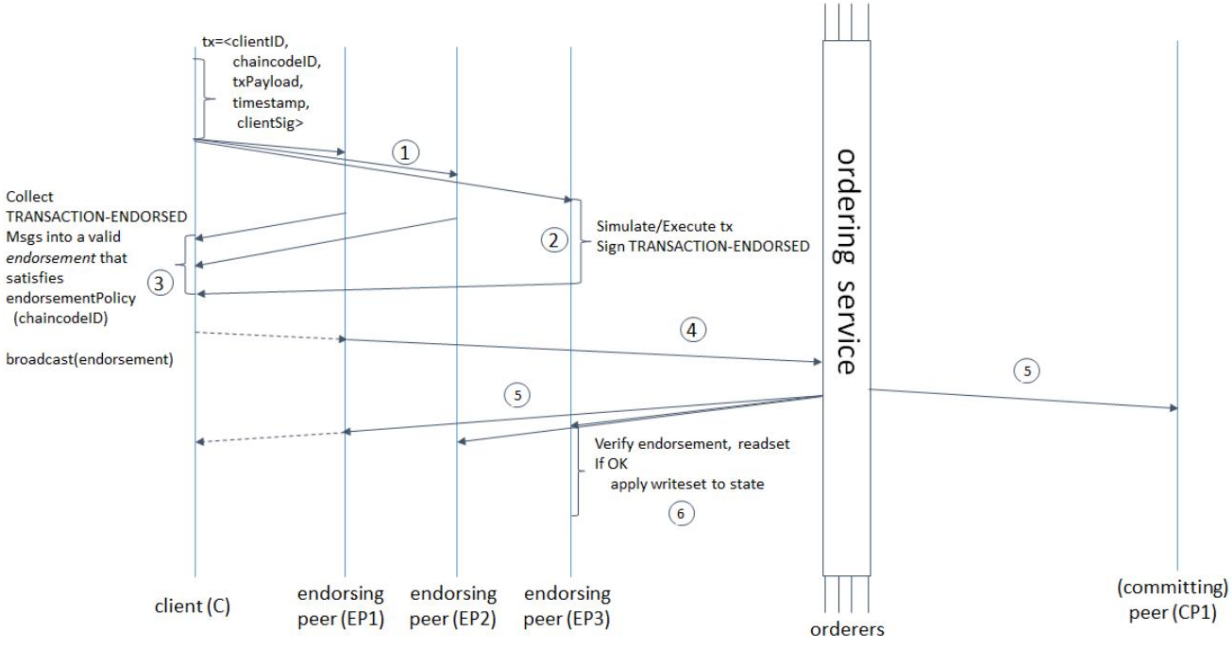

Figure 3-6. Architecture - transaction lifecycle on Fabric 1.0 network

The transaction life cycle on the Fabric network is the settlement of the consensus algorithm that nodes are forced to follow when joining the network. In general, the life cycle of a transaction consists of 6 steps:

1) Transaction initiation: client sends transaction request to endorers. This request includes the identity of the user initiating the transaction, the id of the chaincode to be executed, and the data information of the transaction.

2) Authentication and trial execution of transactions: Endorsers verify that transactions are organized in the correct structure and whether any similar requirements arise in the transaction. Whether or not the identity information is valid, whether the identity has the right to access the chaincode or not. Endorers try to execute chaindoce on the current data source to generate read set and write set (data has not been updated on the block at this time). Then, this component will respond this result back to the client with authentication of that endorer.

3) Check response: the client verifies the response from the endorer. If it is a request to read data, the transaction ends here.

4) Transaction dissemination: if it is a request to expand data, the client will broadcast the transaction, along with read set, write set to orderers in the system.

5) Arrange transactions and distribute blocks: orderers will receive transactions and distribute this set into one or more blocks based on system configuration. Orderers will then distribute the ordered blocks all peers in the network.

6) Check and record: blocks after being distributed must meet the authentication policy conditions and ensure the read-set and write-set have not changed since phase 2). If the above conditions are met, the peers will perform the task of adding new blocks to the current blockchain chain. At the same time, a signal will be transmitted back to the client notifying the transaction success or failure.

3.5.4.3 Authentication policy

A validation policy is a set of conditions that must be met when executing a transaction or block request. Normally, to ensure network security, transaction information must be encrypted before being transmitted and must be encrypted.

is initialized by the identity of the user who has the authority to perform that transaction. Identity is generated by a separate component that acts as a client in the network mesh is called Fabric certificate authority (FAC). This process of creating a certificate is also considered a transaction recorded in data blocks. An identity includes three main parts: public Key, private Key, certificate signature.

3.5.4.4 Architecture of blocks and transactions

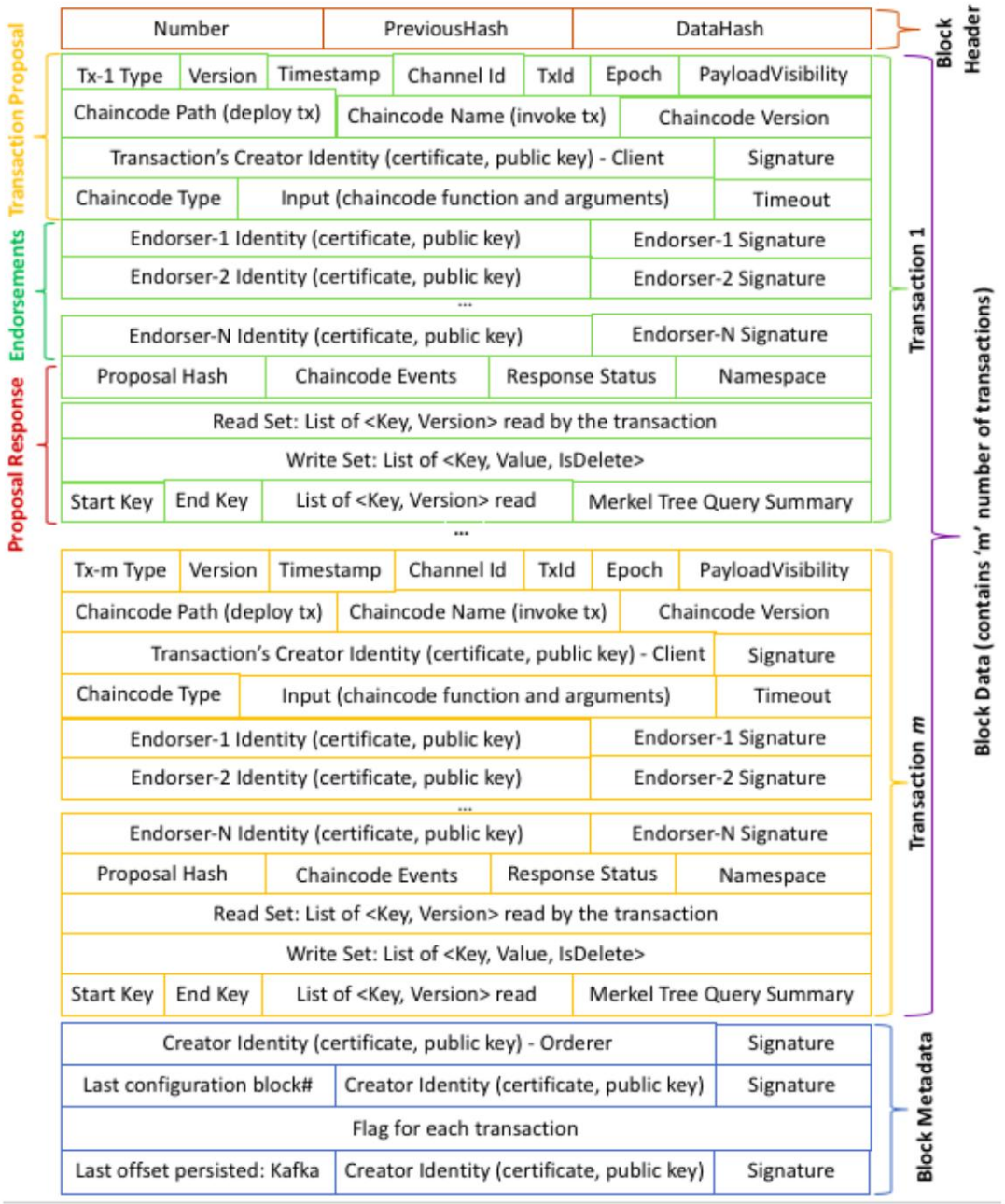

Figure 3-7. Architecture of blocks and transactions

A block of data in the network consists of three main components: Block Header, Block Data and Block Metadata [31]

- Block Header includes three other small components. Number is the sequence number that distinguishes that block from the remaining blocks. The number starts from 0, called the genesis block, then increases by one unit after each chain extension. Previous Hash is the SHA256 hash code of the previous Block Header. If If it's a genies block, this part is "nil" by default. Data Hash is the code SHA256 of Block Data in the current block.
- BlockData is an array of transactions in which each word part is a transaction that has been encoded into a byte array. The number of transactions is equal to the number of elements in the parent array of BlockData. Each byte array is transaction data consisting of 3 main components: Transaction Proposal, Endorsement, Proposal Response. Transaction Proposal contains transaction request information, user identity, and related chaincode ID. Endorsements contains the identity of the endorer. Proposal Response contains the query information of this transaction (read-set) and contains extended information (write-set).
- Block Metadata is an array of 4 elements, each word part is an array byte type contains different information. Signature contains evidence only authenticated by the orderer that created it. Last config contains the certificate of the last peer to change it. Transaction filter contains key value pairs corresponding to the number of transactions in the block to indicate which transactions are valid or invalid. Last offset contains the orderers' Kafka certificates.

3.5.5 Network deployment

3.5.5.1 Hyperledger Composer – IBM Cloud Platform

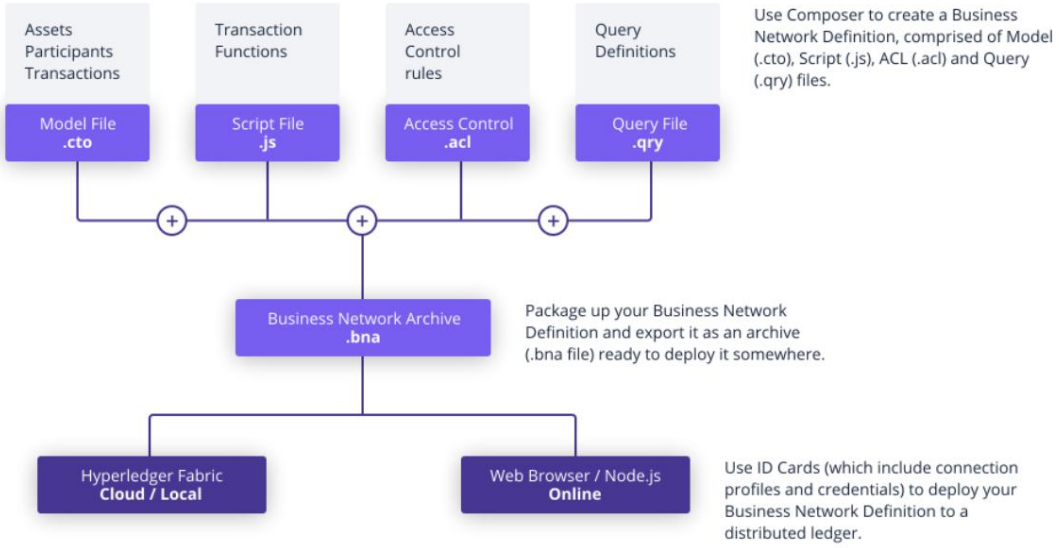

Figure 3-8. Architecture of Hyperledger Composer

The team uses Hyperledger Composer and IBM Kubernetes Container Service to deploy the blockchain system as the architecture designed in chapter 3.5.4.

The deployment group network includes the following components:

- Submitting Client is the team's back-end system. Already hosted heroku and described in chapter 3.3.5, the URL is: https://p2p-lending-14clc.herokuapp.com/.
- Hyperledger Composer chaincode development assistant, address URL: http://173.193.120.168:31080 .
- Component that performs the Fabric Certificate Authority (FCA) function, URL address is: http://173.193.120.168:30054
- Endoserer component 1: http://173.193.120.168:30110
- Endoserer 2 component: http://173.193.120.168:30210
- Orderer component: http://173.193.120.168:31010
- Committing peer component 1: http://173.193.120.168:300111

• Committing peer component 2: http://173.193.120.168:30211

Regarding Hyperledger Composer, the team uses this tool to create the chaincode through compiling business network archive (bna) files into GoLang language - the main language of chaincode. A bna file consists of four components Main: model file, transaction logic, access control, query helper. The model file contains data structures that will be stored in the blockchain: assets - Assets are electronic contracts (LoanContract, InvetingContract, InvestingFeeContract, SettlementContract), network participant – participant: is a user of the system systems (borrowers and investors) and definitions of transactions involving the above structures. Transaction logic contains the transaction's implementation defined in the model file. Access Control contains user permissions for each type of data structure in the model file such as: view, edit, delete, create new. Query Helper assists in helping back-end systems query data into the blockchain network.

3.5.5.2 Hyperledger Explorer – Blockchain Explorer

To make the system transparent, the team also installed the Hyperledger Explorer website to support system controllers in monitoring transactions and blocks that have occurred on the blockchain network.

URL address: https://aqueous-hollows-61580.herokuapp.com .

CHAPTER 4: INTRODUCTION TO THE APPLICATION INTERFACE

ÿ *The main content of this chapter focuses on describing and introducing the system application, including two main components: a mobile phone application and a web application to track transactions taking place on the blockchain.*

4.1 Introducing mobile phone applications

The authors designed a mobile application for both borrowers and investors, with different accounts having different interfaces depending on the user's role. However, there is also sharing between borrowers and investors

Common interfaces perform basic functions such as login, registration, authentication, etc. In addition, the system also supports pull to refresh function on certain screens to Update the latest data for users.

4.1.1 General interface

4.1.1.1 Login/ Register

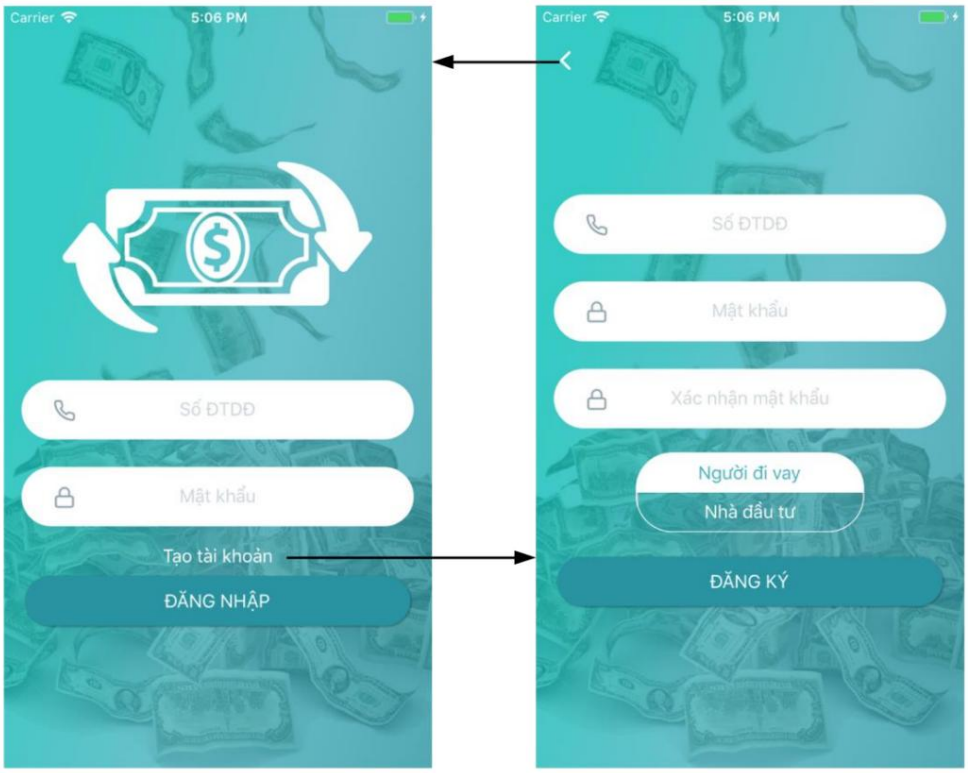

Figure 4-1. Login/ registration screen

After installing and opening the application, the login screen will appear as the screen default. The authors use the JSON Web Token technique (in section 3.3.5.1), which means that every time the user opens the application, the login screen is always the first screen, regardless of whether the user is logged in. in the past or not.

The user enters **his email** and **password** if he has registered an account, presses the **Login button,** then the application will request to the server to identify whether the account is a borrower or an investor, thereby moving to the management screens. corresponding reason (section 4.1.2, section 4.1.3)

If you do not have an account, the user clicks on **Create account** to move to the account registration screen, declaring basic information such as **mobile phone number, password, password confirmation** and **user** role. **borrow** or **investors** to
Register a new account.

4.1.1.2 Account confirmation

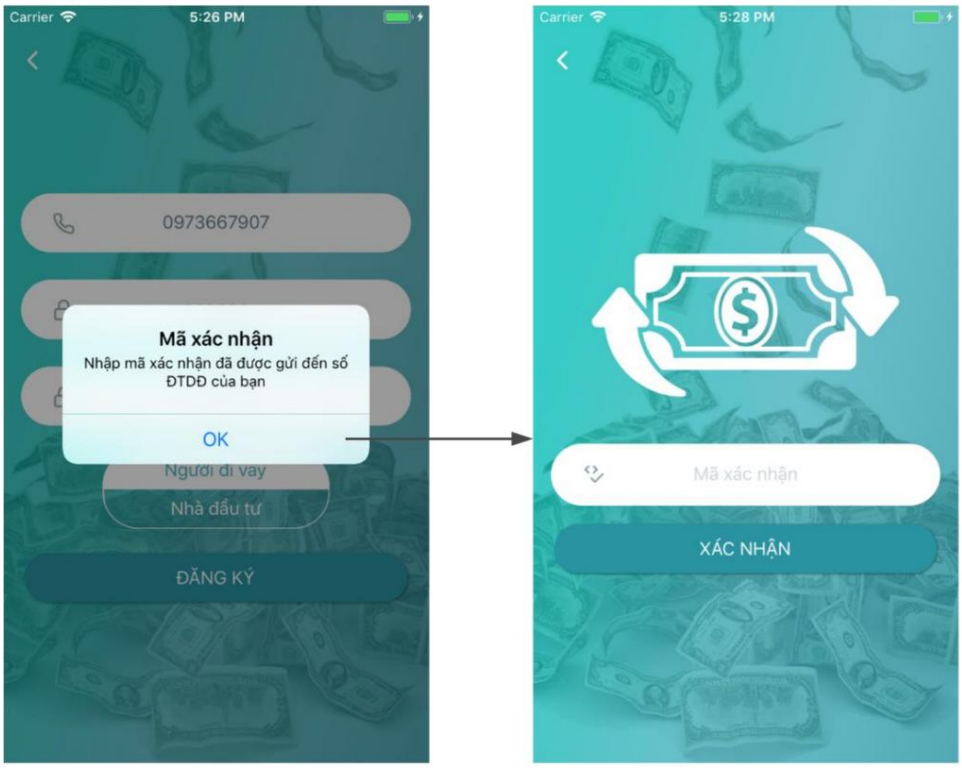

Figure 4-2. Account confirmation screen

On the account registration screen, after declaring the necessary basic information, the user presses the **Register button.** After that, the system will request to the server, record the account and send a 6-digit confirmation code to the registered phone number, and the mobile application will switch to the **Enter authentication code screen.** Here, the user enters the received authentication code to complete the account registration step.

If you are a borrower, after this step, the user needs to declare additional personal information for the personal credit score evaluation system and mobile application to transfer.
to the **Information Information** screen (section 4.1.2.1).

If you are an investor, the user does not need to declare additional information or application mobile phone to the Investor **Management Screen** (section 4.1.3).

4.1.1.3 View transactions

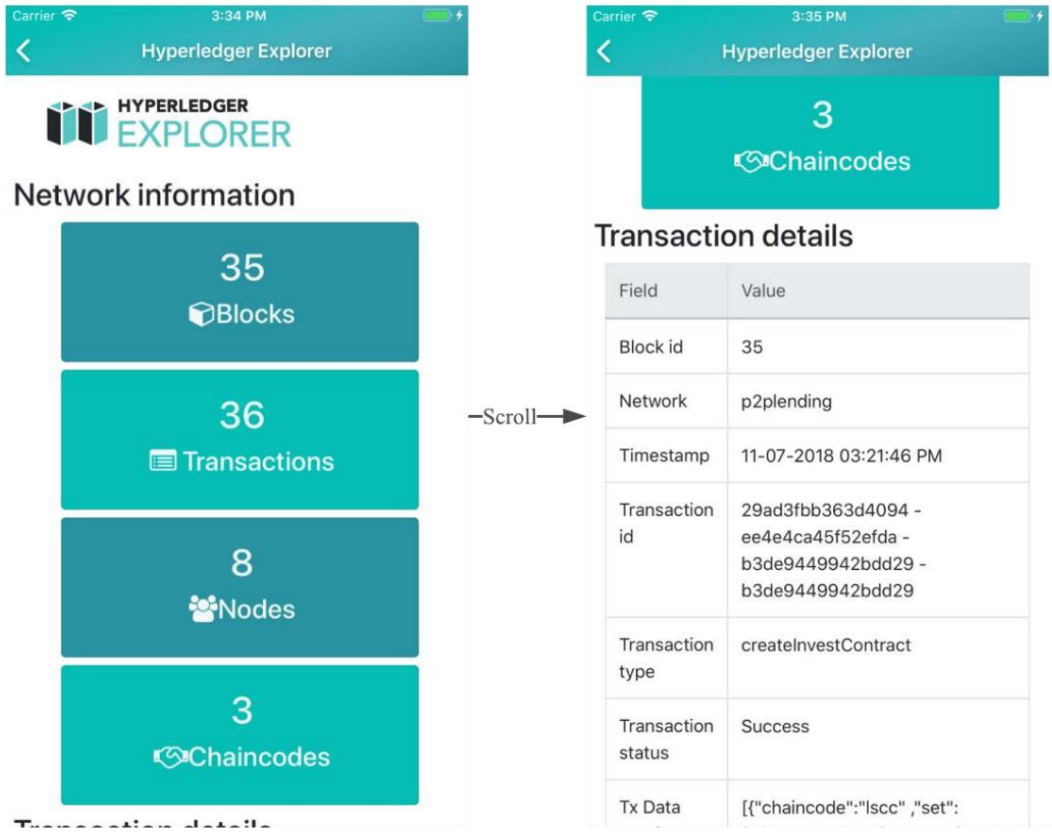

Figure 4-3. Screen to view transactions on the blockchain

This is a web view screen so users can check the transactions they have made. For the functions in sections 4.1.2.3, 4.1.2.4, 4.1.2.6, 4.1.3.2, 4.1.3.4, the detail screen has a **View transaction** button so users can view recorded transactions. receive on blockchain.

4.1.2 Interface for borrowers

4.1.2.1 Declare user information

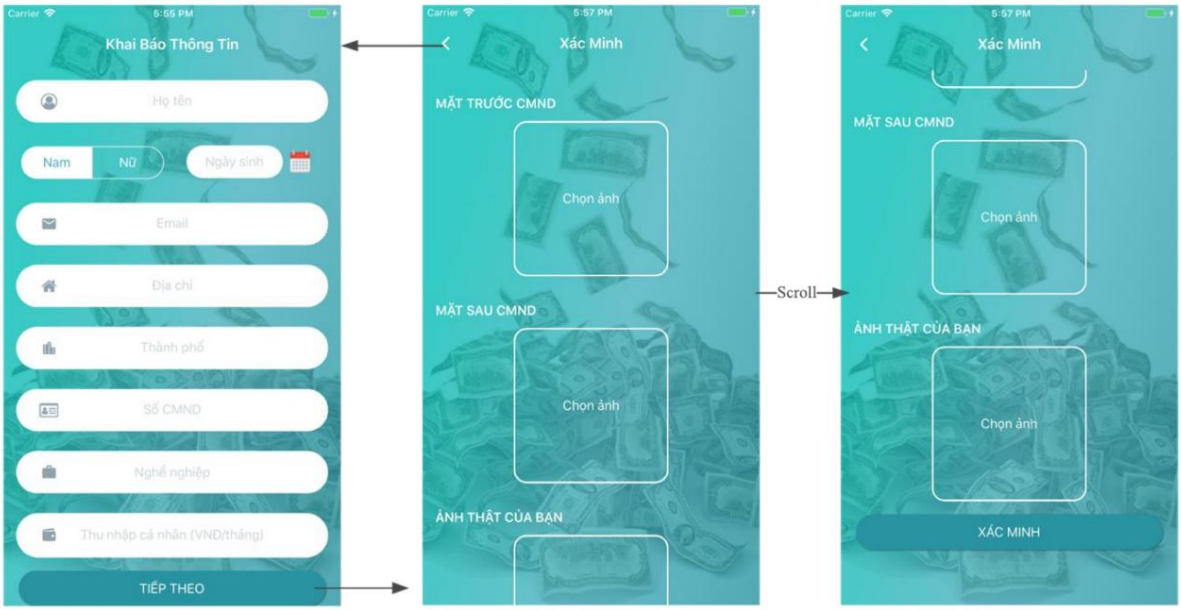

Figure 4-4. Information declaration screen - borrower

After authenticating account registration as a borrower in section 4.1.1.2, the user needs to declare detailed personal information so that the system can evaluate personal credit scores to serve customers. related functions. Information that needs to be declared includes: full name, gender, date of birth, email, address, city, identity card number, occupation, personal income per month. In addition, the borrower needs to provide 3 personal photos for the system to authenticate: front photo ID card, back side of ID card, real photo.

After this step, the application will switch to the main screen so users can create a loan. The main screen includes 3 tabs: **Loans, History** and **Personal.**

4.1.2.2 Loan creation

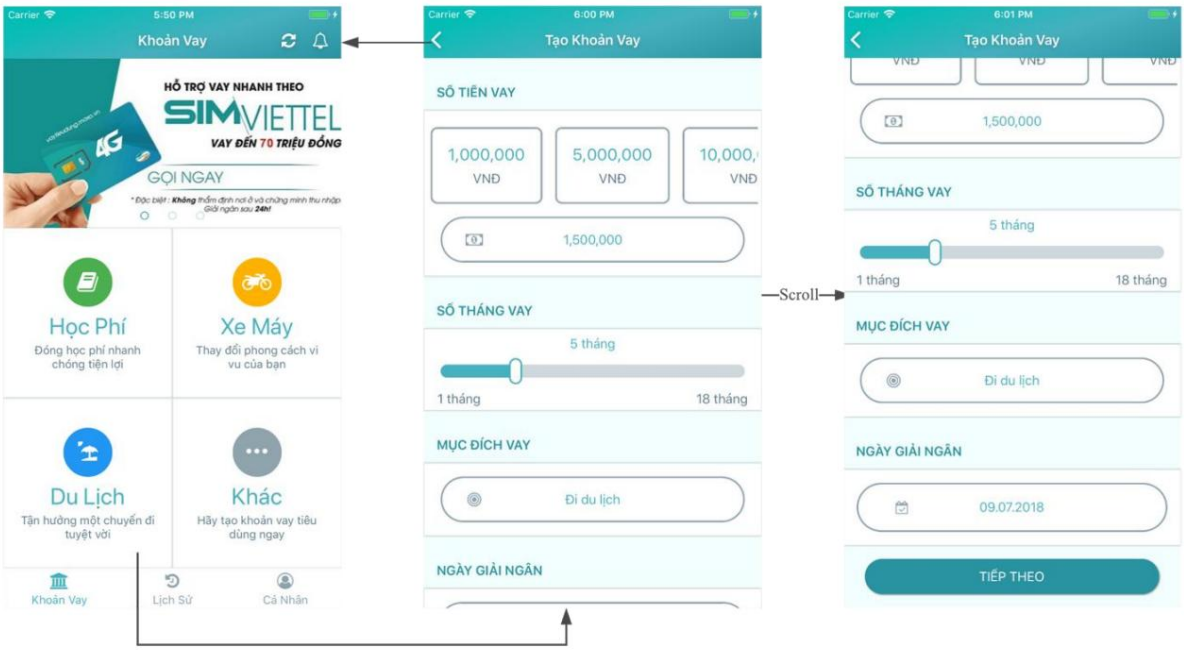

Figure 4-5. Loan creation screen - borrower

On **the Loans tab,** if the user does not currently have any loans, apply will display a loan creation suggestion screen.

When the user selects the suggestions, the application switches to the **Loan Creation screen,** the user proceeds to declare the necessary information of a loan: loan amount, number of loan months, loan purpose and disbursement date, Then press the **Next** button to let the application request to the server to perform calculations and then move to screen 4-6.

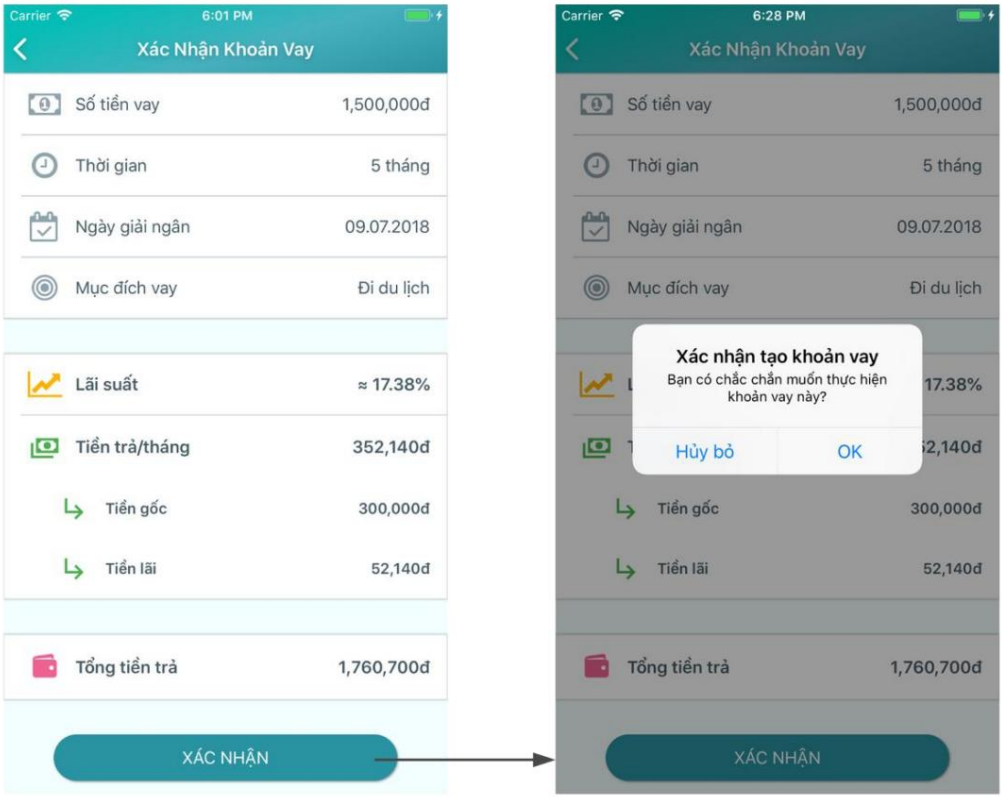

Figure 4-6. Loan creation confirmation screen - borrower

On this screen, the application displays necessary loan information

will create for the user **to Confirm** the creation of this loan. The information includes:

- Loan amount
- Loan period
- Disbursement date
- Loan purpose
- Interest rate
- Payment/month
    - Principal
    - Interest
- Total payment

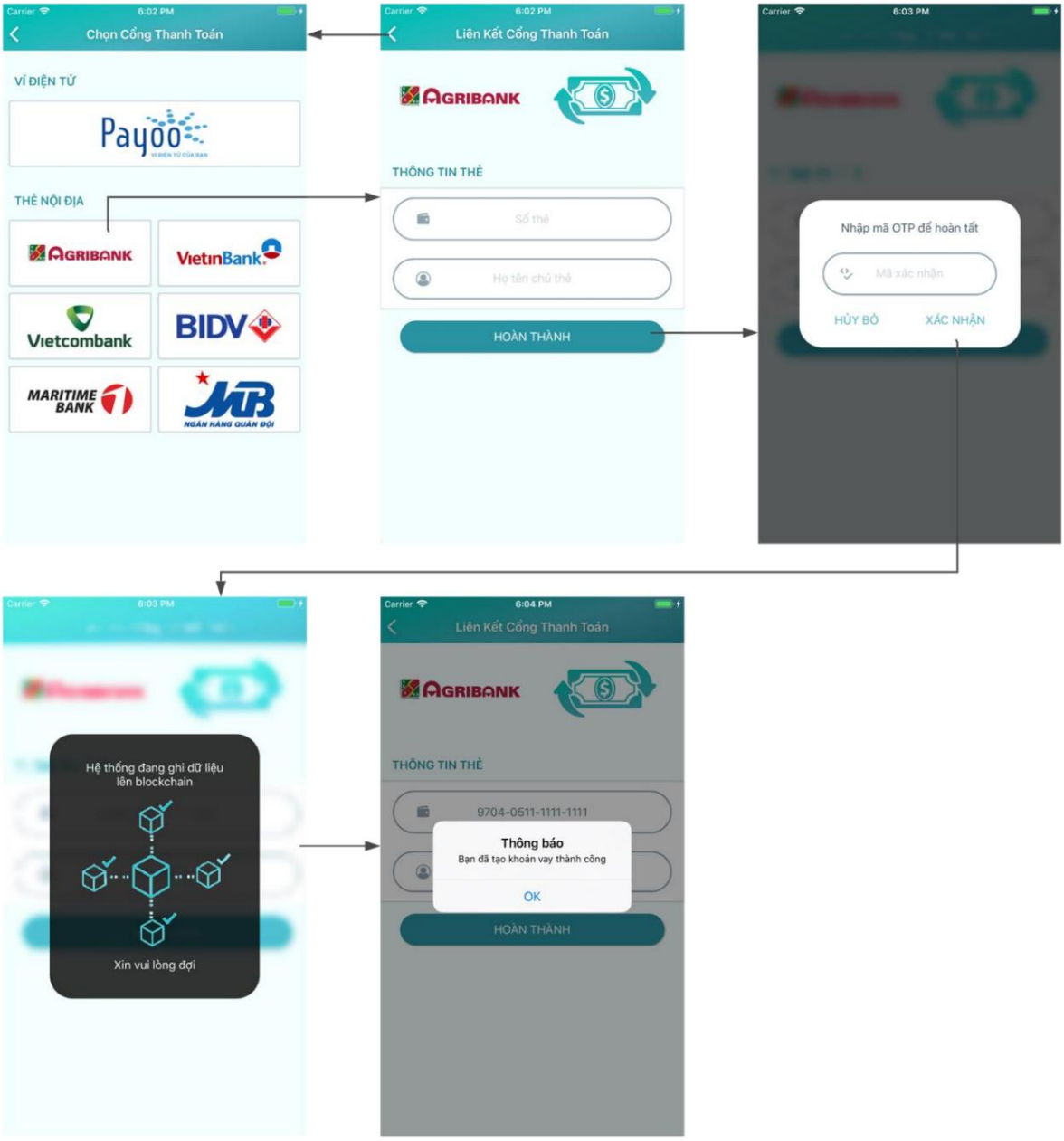

Figure 4-7. Payment gateway link screen when creating loan - borrower

After confirming the loan creation, the user proceeds to link the payment gateway so that the system stores the place to deposit money when the loan has been fully invested.

Finally, when the connection is successful, the loan will be created on the system and the screen will move to section 4.1.2.3.

4.1.2.3 Management of loans awaiting investment

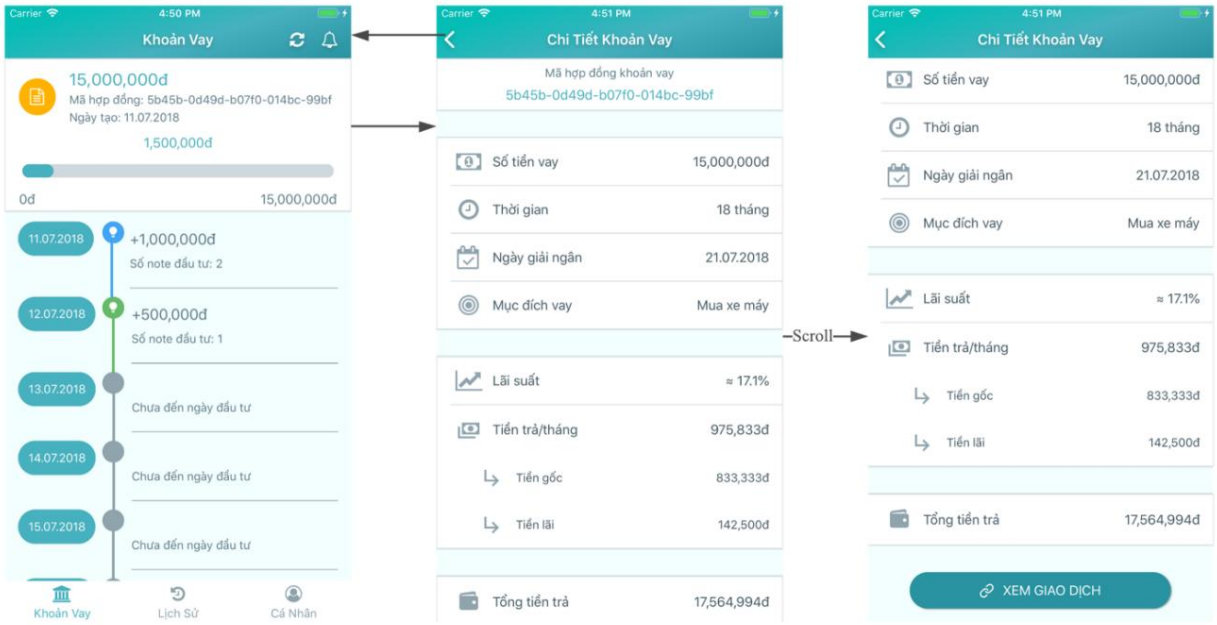

Figure 4-8. Loan management screen waiting for investment – borrower

After successfully creating a loan, the application will display the newly created loan information on the screen. Information includes: investment progress of the loan application over the days, general information of the loan application.

Invested progress includes the following statuses:

- Date of receiving investment money.
- Date of not receiving investment money.
- The date of receiving investment has not yet arrived.

In addition, users can check the transaction recorded on the blockchain system by clicking the **View transaction** button in the **Loan Details** screen , the application will switch to the web view display screen (section 4.1.1.3).

4.1.2.4 Successful investment loan management

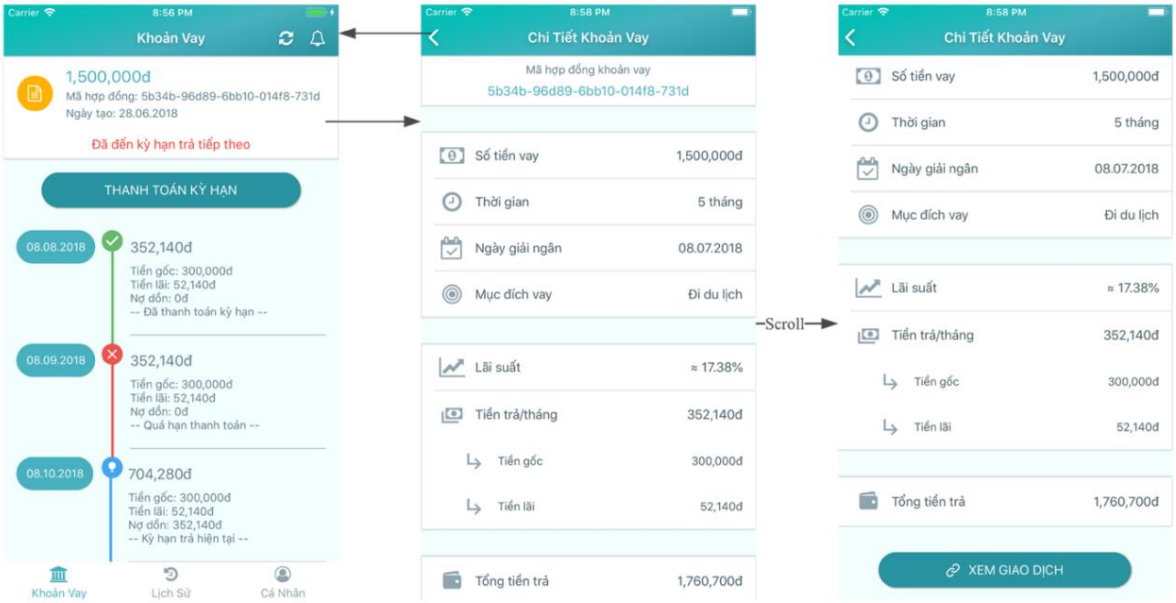

Figure 4-9. Loan management screen Successful investment - borrower

After the loan has been invested with enough money from the investor, the application will be displayed Successful loan information on the screen. Information includes: term payment progress, Term payment button and general information of the loan application.

Term payment progress has the following statuses:

- The term has been paid on time.
- Late payment period.
- Current payment term.
- The payment due date has not yet reached.

In addition, users can check the transaction recorded on the blockchain system by clicking the **View transaction** button in the **Loan Details** screen , the application will switch to the web view display screen (section 4.1.1.3).

4.1.2.5 Payment of term loan

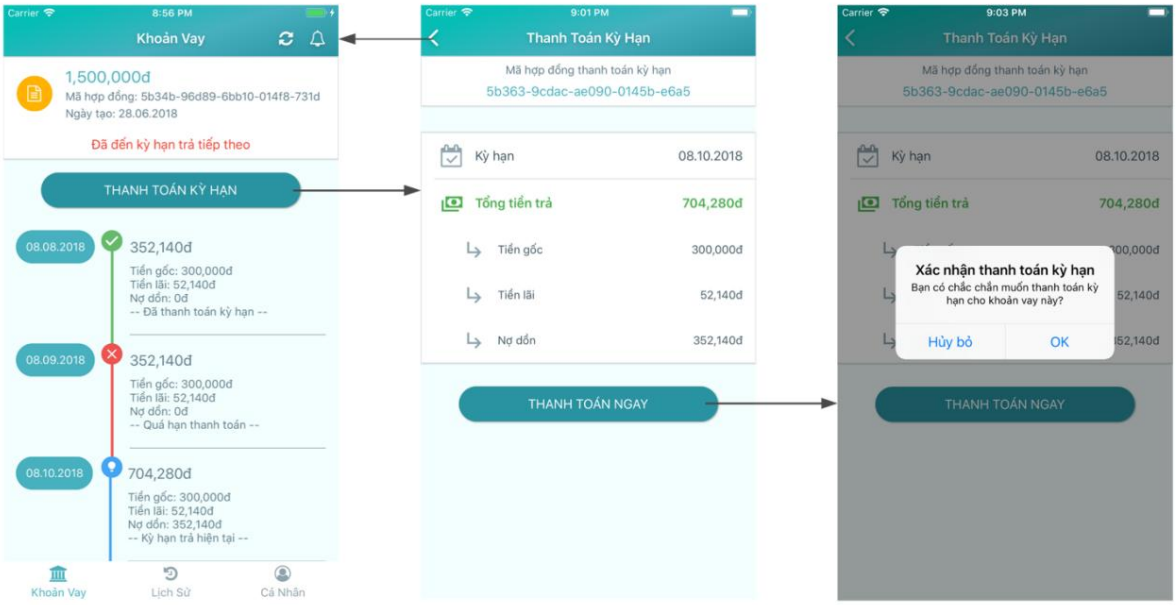

Figure 4-10. Term loan payment screen - borrower

Users can pay for the loan term by clicking the Pay term button, the application switches to the screen confirming the information to pay for the current term. The information includes:

- Forward payment contract code
- Term
- Total payment
    - Principal
    - Interest

o Accumulated debt

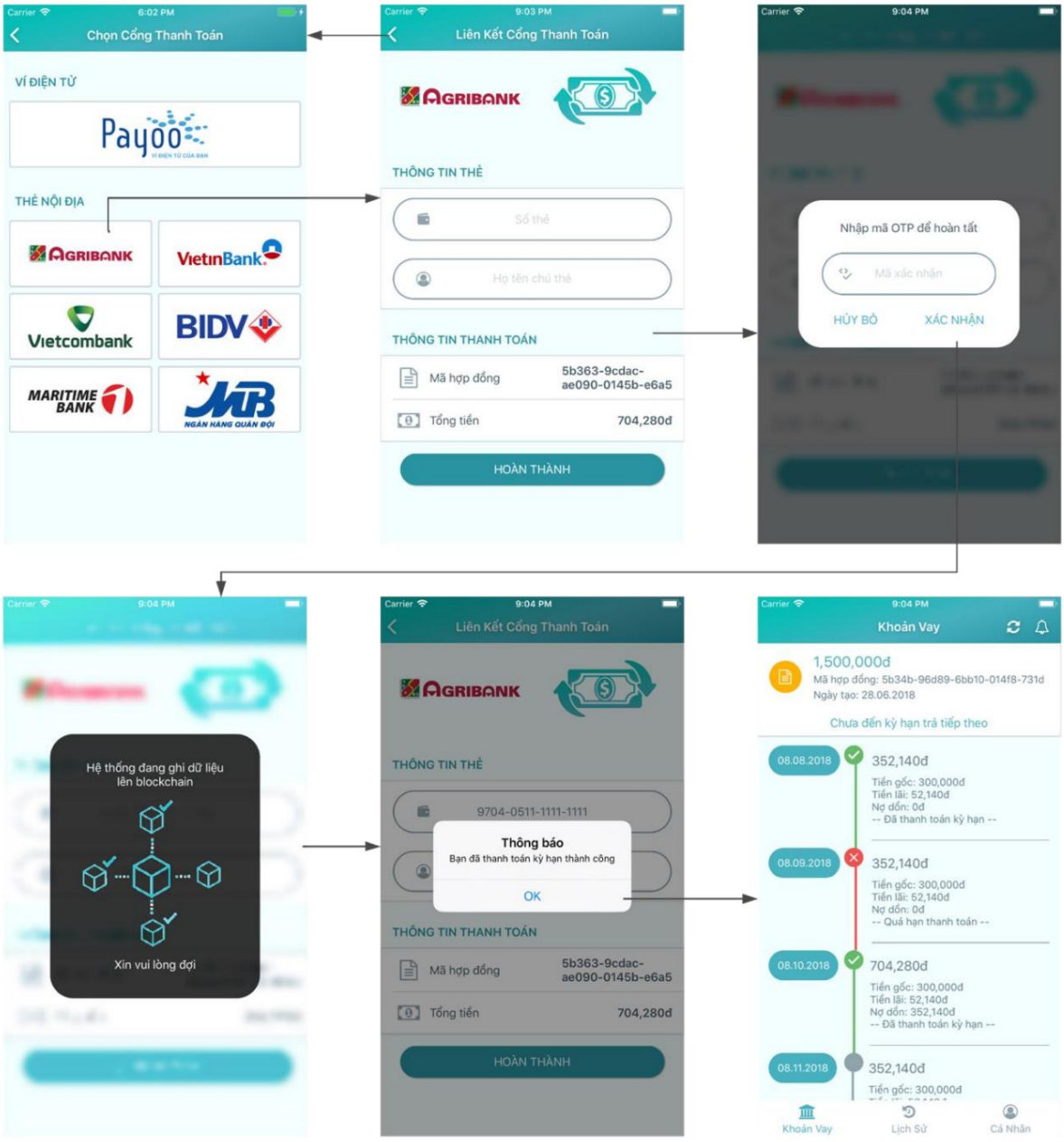

Figure 4-11. Payment link screen when paying term - borrower

After confirming the term payment, the user links the payment gateway so that the system records where the payment will be withdrawn. Finally, once linked payment, the current term will be paid successfully and the application reloads the account information loan after the term has been paid.

4.1.2.6 View loan history

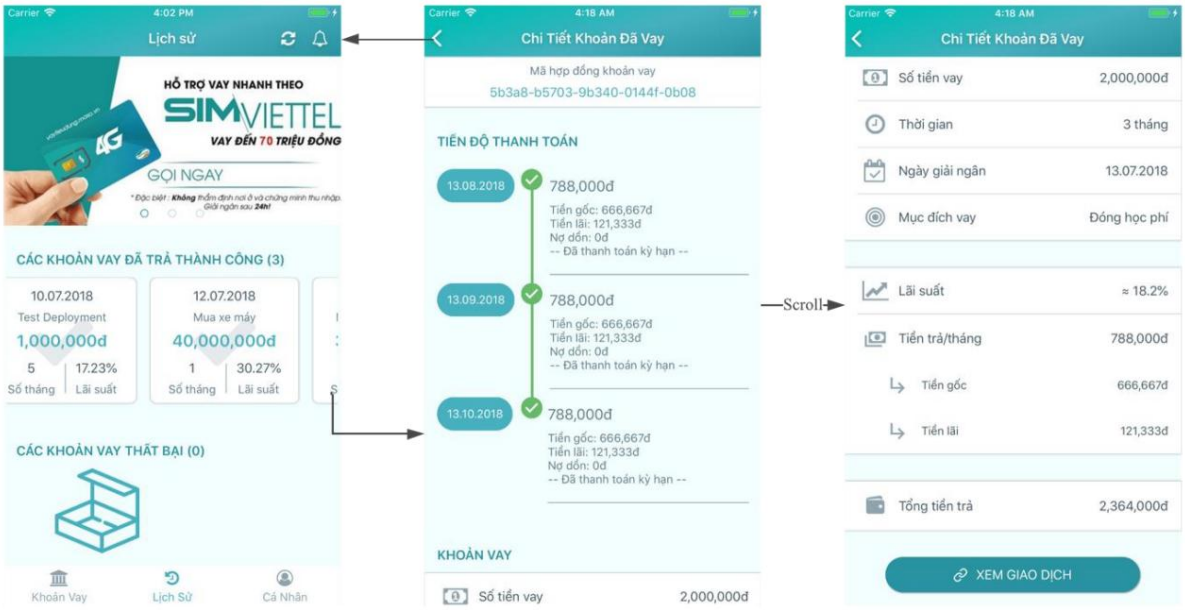

Figure 4-12. Screen to view loan history – borrower

In the **History** tab of the main screen, users can view loans that have completed their repayment period and loans that have failed - there is not enough money invested after when the waiting period is overdue (10 - 11 days).

In the list of corresponding loans, users can view information Detailed information about whether the loan has been paid successfully or failed by clicking on each specific loan.

With successfully repaid loans, users can check the most recent term payment transaction recorded on the blockchain system by clicking **View transaction** button in the **Loan details** screen , the application will switch to the web view display screen (section 4.1.1.3).

4.1.2.7 View/ log out account information

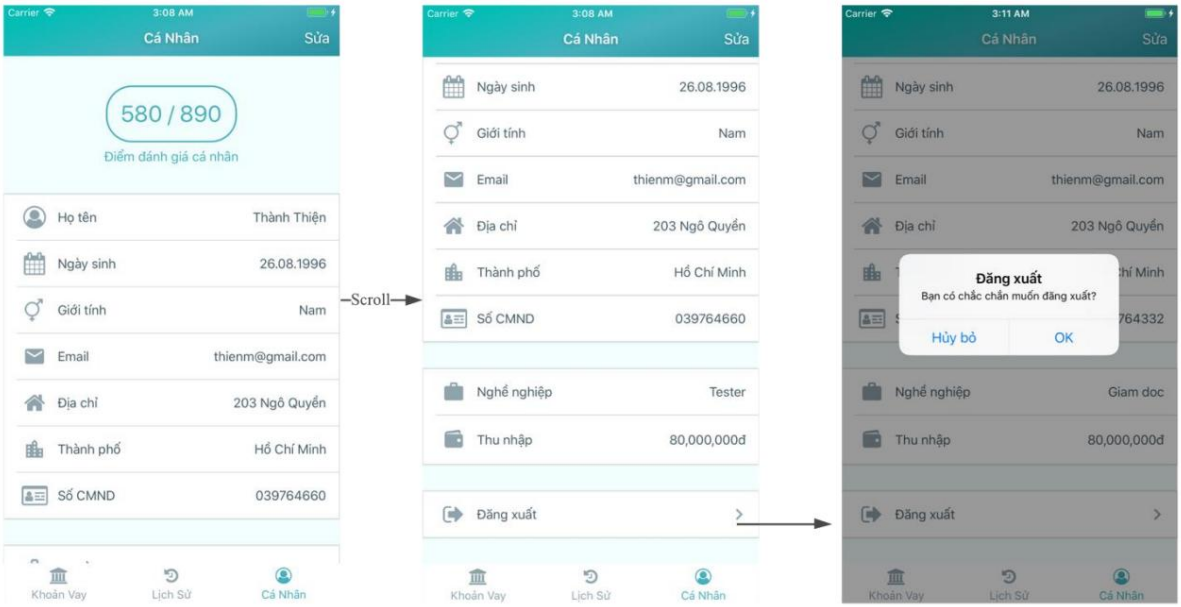

Figure 4-13. Screen to view/ log out account information - borrower

On the **Personal** tab of the main screen, users can view the personal information declared in section 4.1.2.1, and can edit that information and log out of their account.

If you select **Log out,** the system will display a confirmation dialog box. If the user selects **OK,** the application will request to the server and move to the **Login** screen (section 4.1.1.1).

4.1.2.8 Edit account information

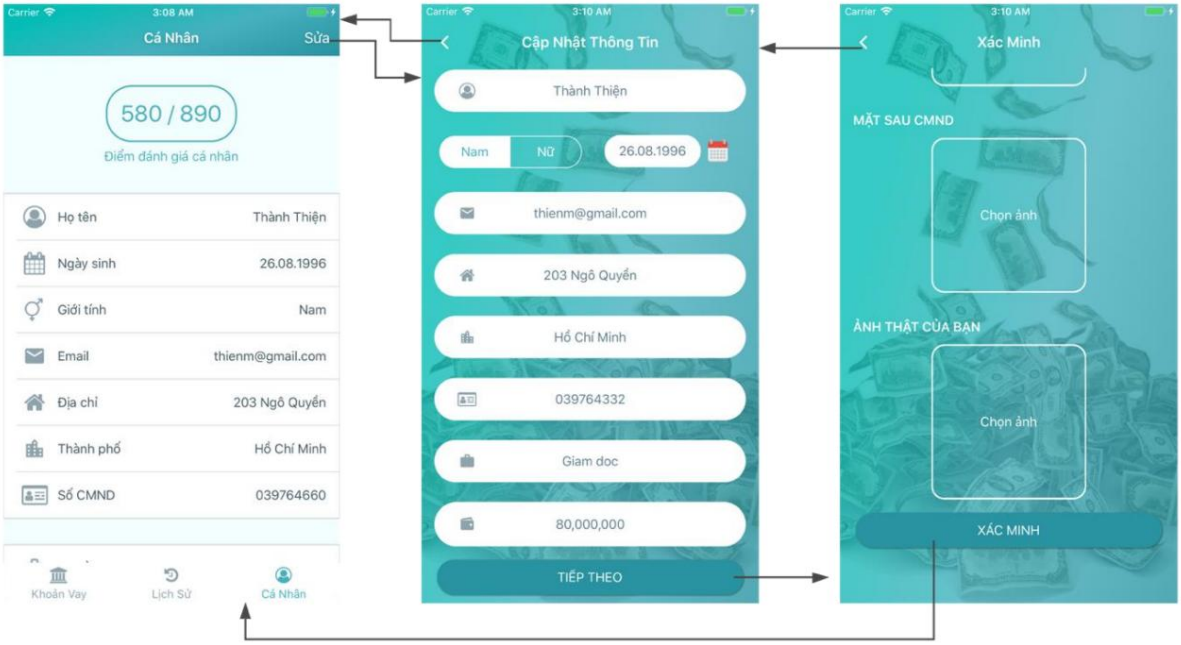

Figure 4-14. Screen for editing account information - borrower

On the **Personal** tab of the main screen, when the user selects the **Edit** button on the header, the application will switch to the information update screen with information boxes pre-filled with old data that has been declared by the user. The user updates the information again, and finally the system will reload the latest information that has just been updated updates from users.

4.1.2.9 View notifications

Figure 4-15. Notification view screen - borrower

The mobile application supports viewing notifications related to loan status to remind users.

Borrowers can view the notification screen by clicking on the image icon bell in the header bar, the application will switch to the notification screen.

4.1.3 Interface for investors

The investor interface includes three main tabs: **Management, Investment** and **Personal.** The **Management** tab includes three subtabs: **Overview, Success** and **Waiting**

4.1.3.1 Personal income management

Figure 4-16. Personal income management screen - investor

On the **Management** tab of the main screen, in the **Overview sub-tab,** investors can manage this month's income based on loans that have been successfully invested and are in the process of term payment. Management information includes:

- Total amount received.
  - Principal.
  - Interest.
- Total net received this month.
  - Service fees.
- The pie chart shows the percentage between:
  - Principal.
  - Interest.
  - Service fees.

4.1.3.2 Managing successful investments

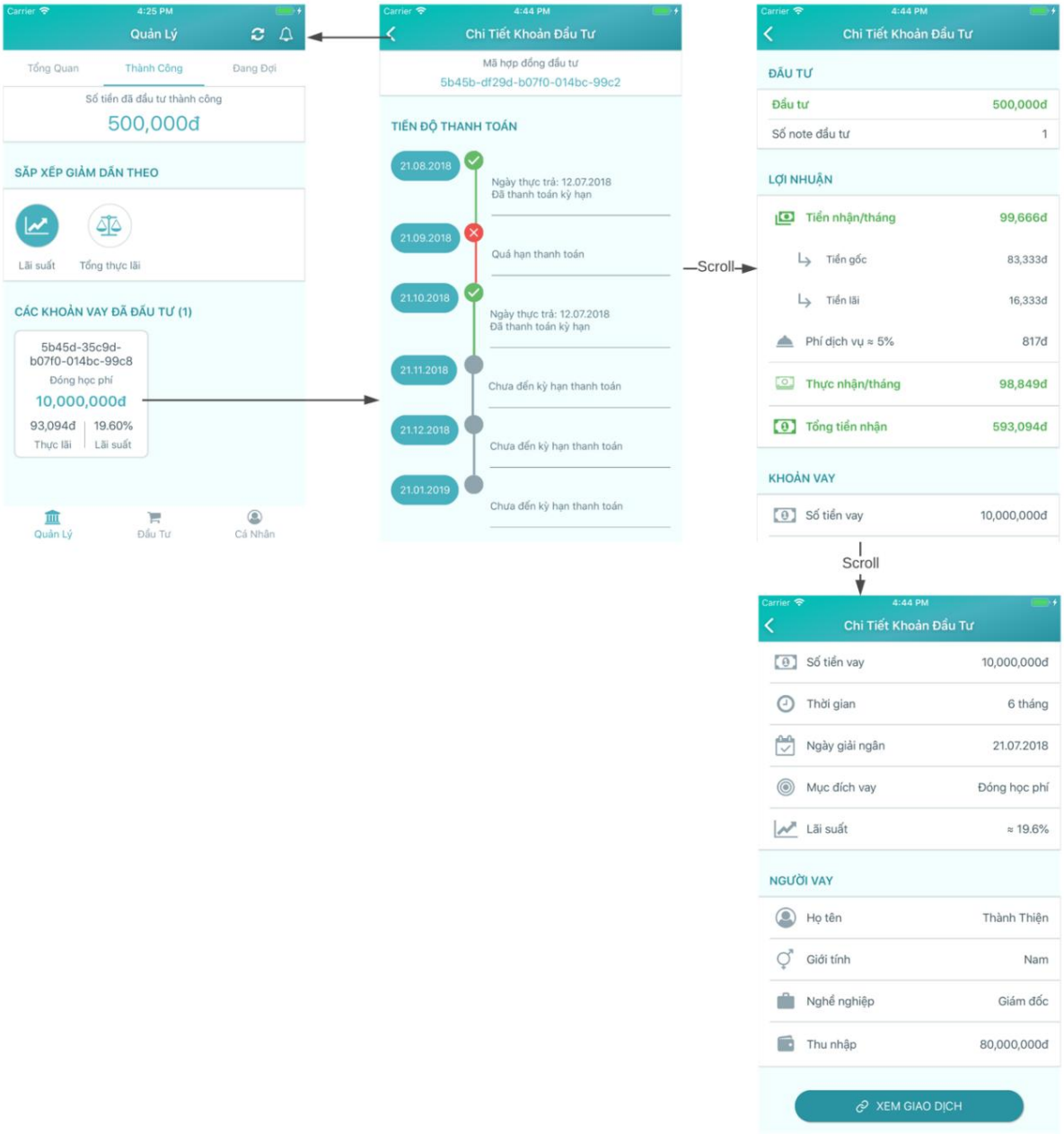

Figure 4-17. Screen for managing successful investments - investors

In the **Success** sub-tab of the **Management** tab on the main screen, users can see a list of their successful investments that are in the maturity stage. When clicking on each detailed loan on the **Investment Details screen,** users can check the investment transaction that has been recorded on the system.

blockchain by clicking the **View Transaction button,** the application will switch to the web view display screen (section 4.1.1.3).

Detailed information in the **Investment details screen:** investment contract code, payment schedule, profit, investment information, loan information and information. trust the borrower.

4.1.3.3 View notifications

Figure 4-18. Notice viewing screen - investors

The mobile application supports viewing notifications related to investment status to remind users.

Investors can view the notification screen by clicking on the image icon bell in the header bar, the application will switch to the notification screen.

4.1.3.4 Management of investments awaiting investment

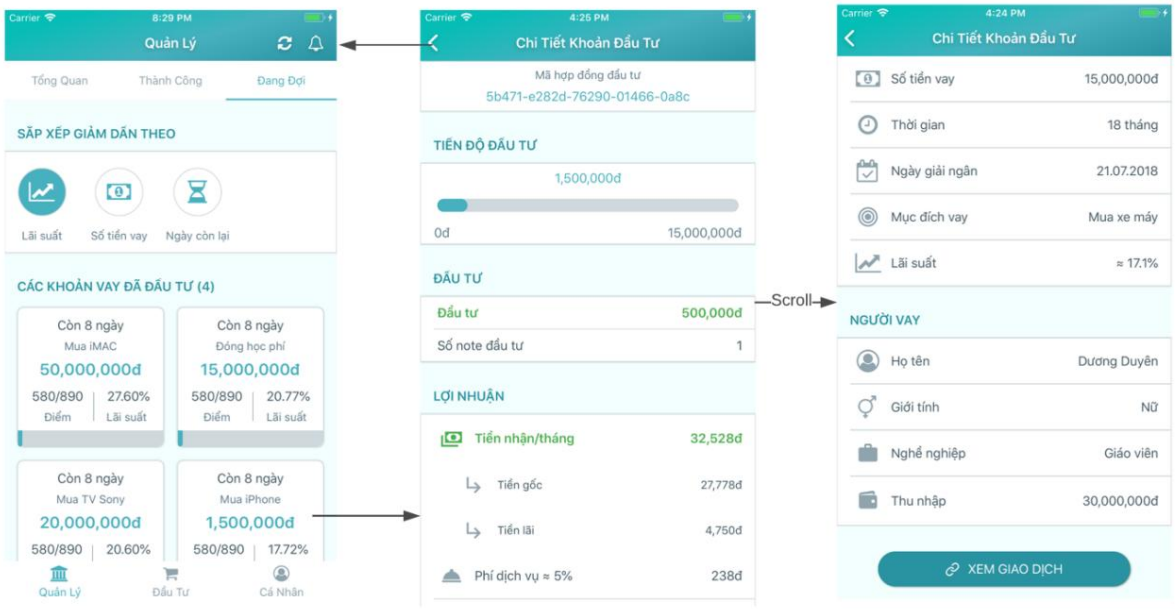

Figure 4-19. Loan management screen waiting for investment - investor

In the **Waiting** sub-tab of the **Management** tab on the main screen, users can view a list of their investments that are still waiting for another investment source. When clicking on each detailed loan in the **Investment Details screen,** users can check the investment transaction recorded on the blockchain system by clicking the **View transaction button,** the application will switch to the screen. display web view (section 4.1.1.3).

Detailed information in the **Investment details screen:** investment contract code, investment progress, profit, investment information, loan information and information borrower.

4.1.3.5 Loan investment

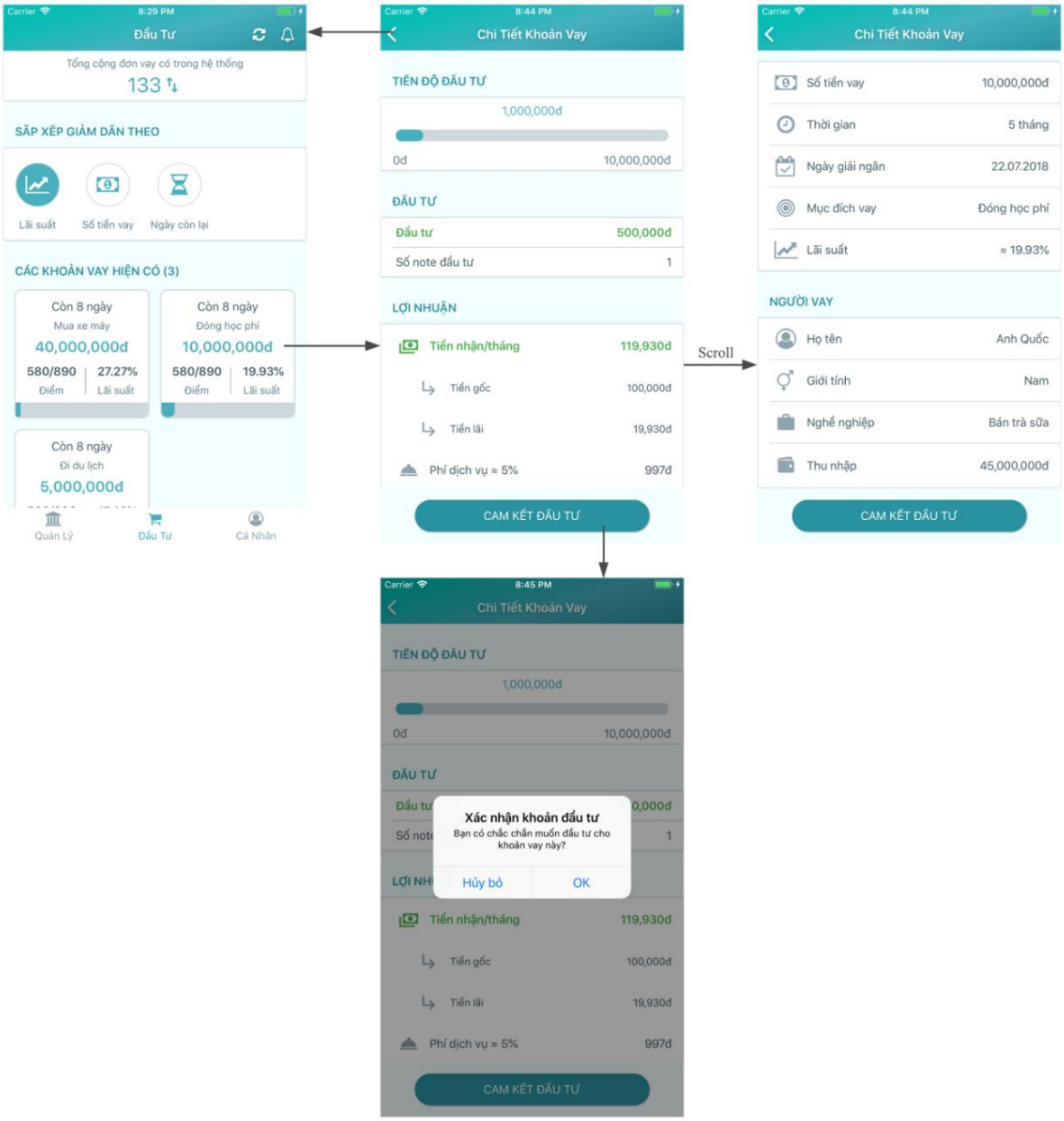

Figure 4-20. Loan investment screen - investor

On the **Investment** tab of the main screen, users can see all the loans waiting for investments in the system that the user has not yet invested in. From Users can then decide to invest in each specific loan by clicking on the loan details and pressing the **Commit to invest button.**

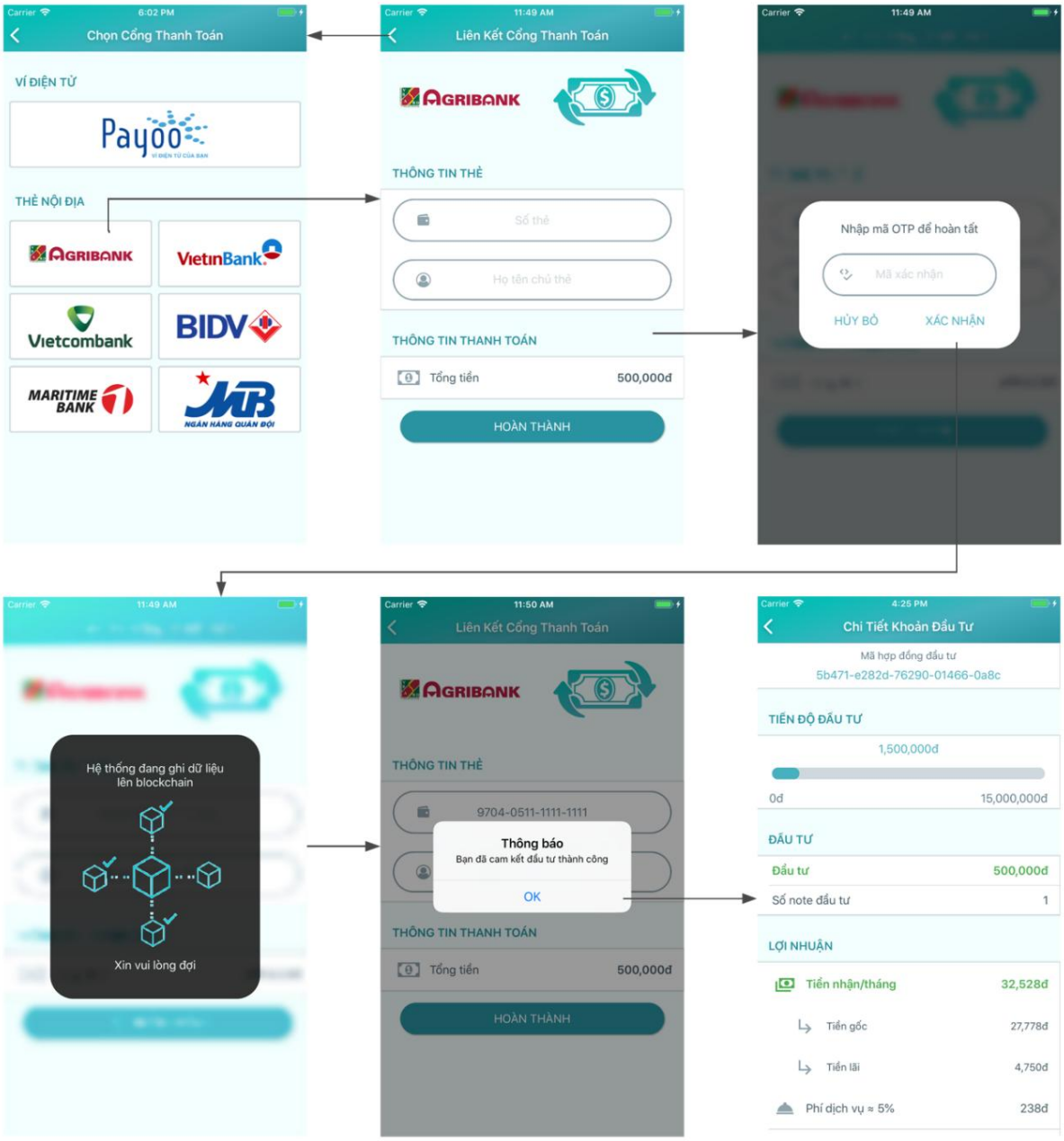

Figure 4-21. Payment link screen when investing - investor

After confirming the investment commitment for a certain loan, the user links the payment gateway so that the system records where the money will be withdrawn to transfer to the borrower of that loan when the loan has enough money. Invest within the time allowed. Finally, when the connection is successful, the investment will be recorded on the blockchain and the application will switch to the detail screen of the investment.

4.1.3.6 Account Management/ Logout

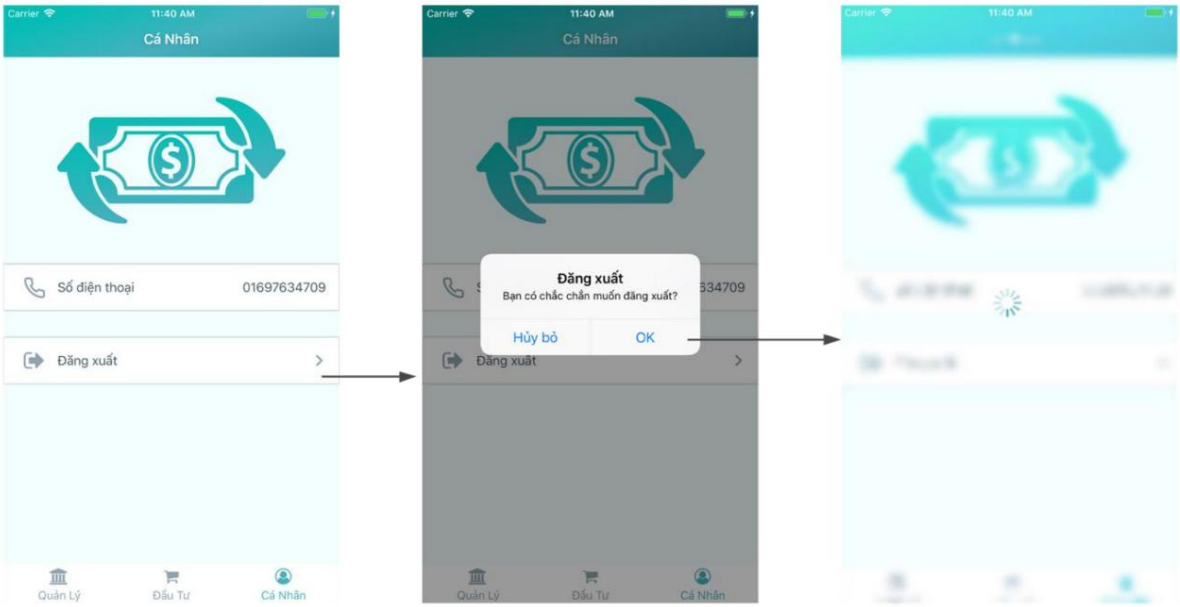

Figure 4-22. Account management/ logout screen - investor

On the **Personal** tab of the main screen, investors can see their account and perform the **Logout** function if desired.

If you select **Log out,** the system will display a confirmation dialog box. If the user selects **OK,** the application will request to the server and move to the **Login** screen (section 4.1.1.1).

4.2 Introducing the blockchain transaction management web application

The system has a web application built for admins (managers). to manage transactions that take place on the blockchain,

If you are an administrator, access the link https://aqueous-hollows-61580.herokuapp.com to view all ongoing transactions.

The web application interface includes 3 main tabs: **Dashboard, Blocks, Transactions** takes care of managing separate functions.

Blocks, transactions and detailed information on the system are encrypted and administrators can only view, but cannot edit the information due to the nature of the blockchain system.

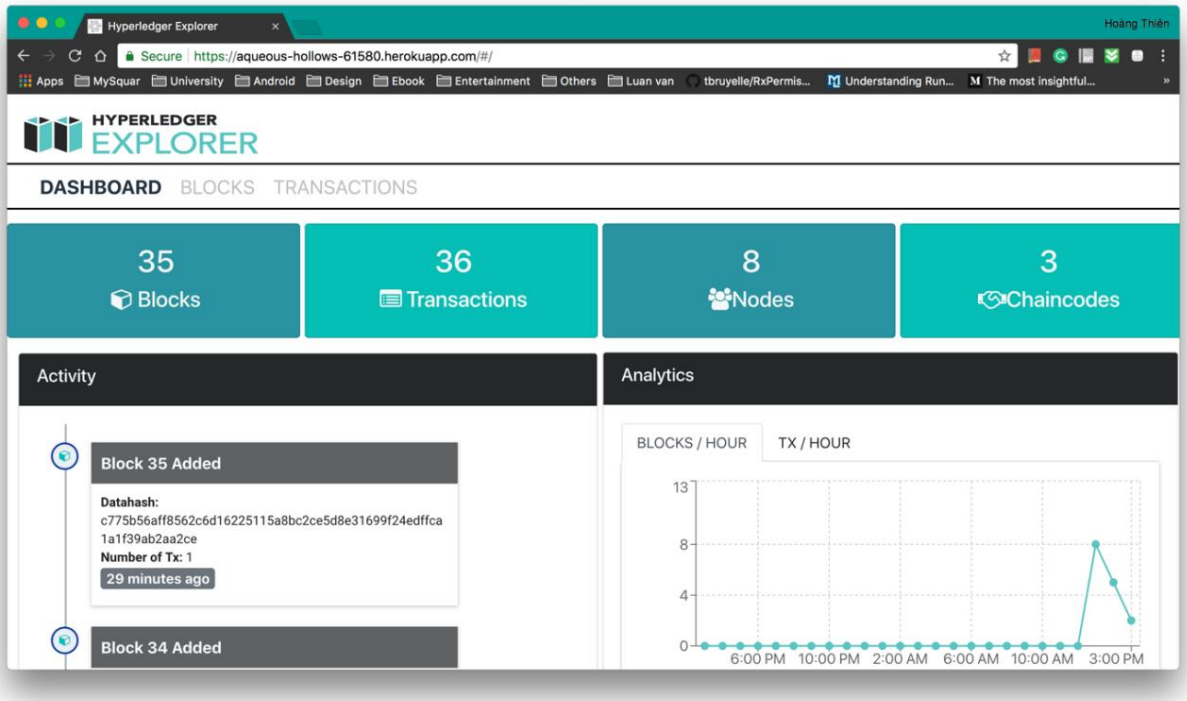

Figure 4-23. Overview management web screen - manager

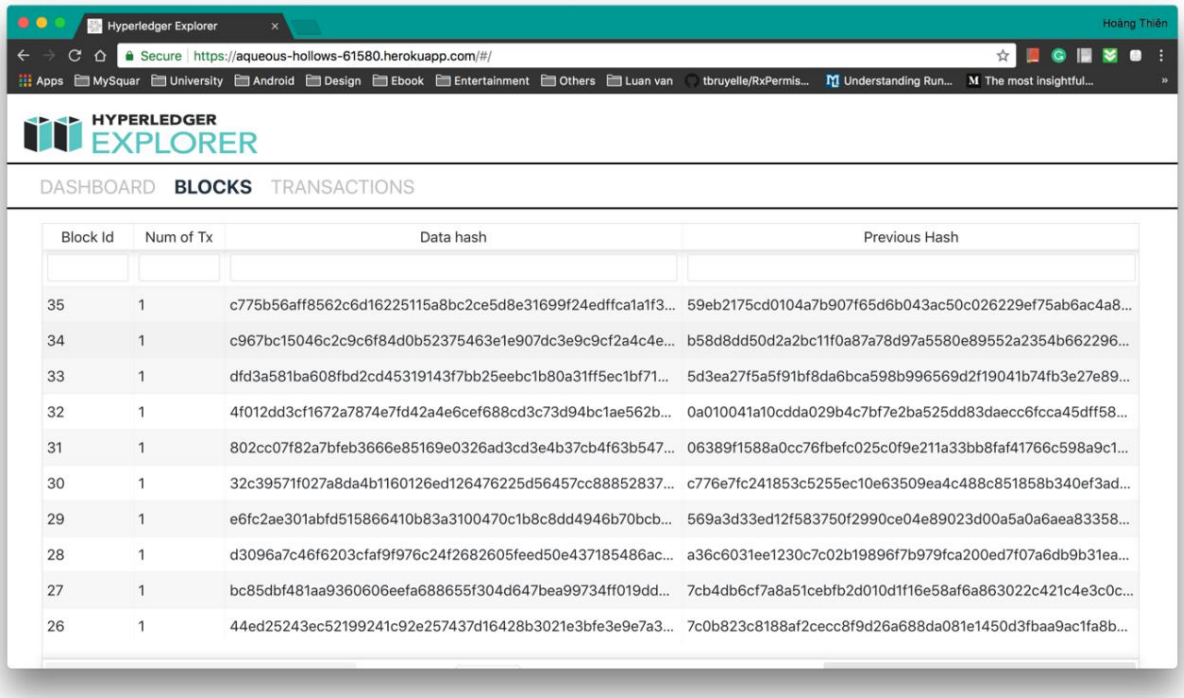

Figure 4-24. Web screen for data management on blocks - manager

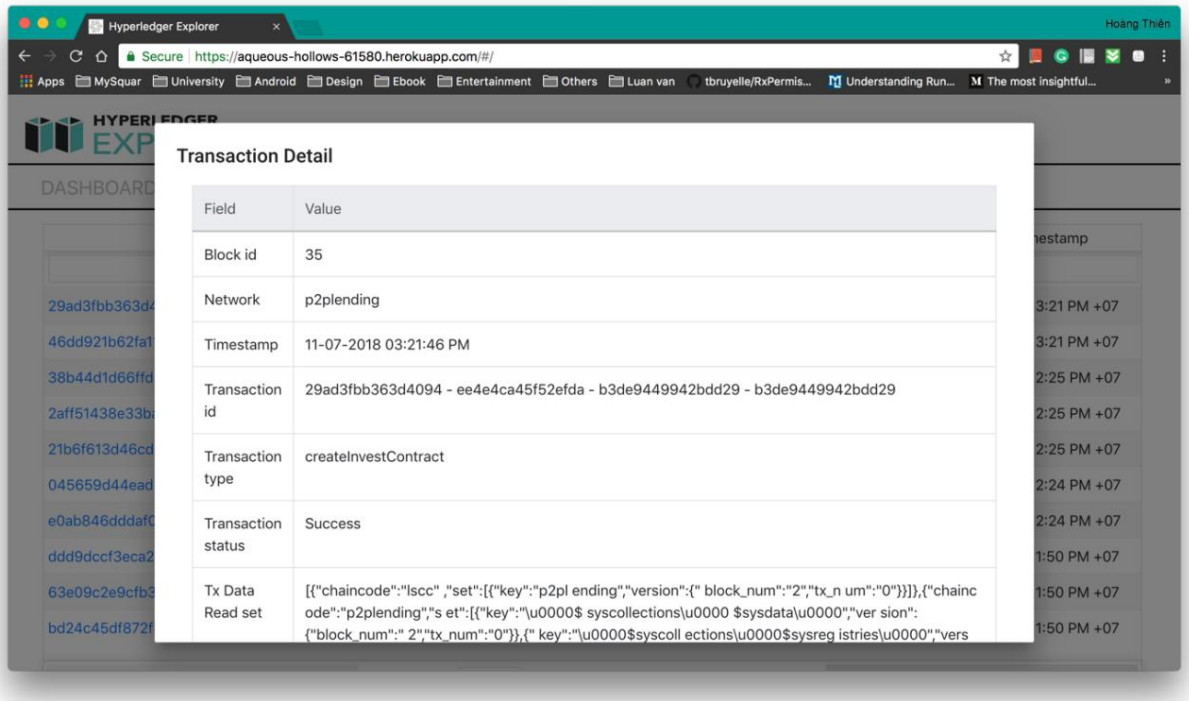

Figure 4-25. Web screen for managing transactions - manager

CHAPTER 5: CONCLUSION

ÿ *This chapter will summarize the parts that the author team has accomplished during the process of researching and developing the project. At the same time, from the perspective of a software developer, the team will evaluate the practicality as well as point out some remaining limitations in this project.*

5.1 Results achieved

5.1.1 About knowledge

After implementing the project, the group has improved some weak skills and learned some new knowledge in many fields of finance and technology including:

- Soft skills such as communication skills, self-study skills, teamwork skills, and time management skills are improved and progress clearly. • Knowledge of software requirements analysis and management, knowledge of information system analysis learned in the previous semester are applied to
  Optimize the software development process, helping the team save some money large amount of time for the project.
- Learn and grasp some basic processes in the financial sector, especially the fields of unsecured lending and peer-to-peer lending. At the same time, apply these processes to the system that the team builds.
- Improve mobile application programming skills on two platforms
  Android and iOS with React Native technology.
- Improve back-end system and database programming skills to build RESTful API for clients to access data through the technology.
  Node.js and MongoDB technology.
- Learn and apply blockchain network programming knowledge to store data of electronic contract transactions through technology
  Hyperledger Fabric và Composer.

5.1.2 About the system

The group's system has fulfilled almost all the requirements stated in the graduation thesis. The functions that the team has built into the application system
blockchain into the peer-to-peer lending model is:

- Mobile application for borrowers and investors.
- The back-end system is an intermediary connecting borrowers and investors to manage some centralized user data.
- The blockchain network stores electronic contracts arising during the lending process to minimize fraud risks and increase transparency for the peer-to-peer lending platform.
- Basic common functions for users: register, log in, log out of account.

- Borrowers have the following functions: create loans, view and manage loans borrow, authenticate user information, repay loans.
- Investors have the following functions: view, manage investments, invest accounts borrow and manage interest in the system.

5.2 System practicality

One of the important criteria when the authors evaluate the results in
This project is about the practicality and feasibility of the application for real needs:

- The topic's idea of applying blockchain to the peer-to-peer lending model is a quite new and interesting idea. There is almost no financial company in Vietnam that has officially developed software according to this model. However, there are also some companies that are testing products with a similar model as above, typically HVA company [23].
- The author team has succeeded in bringing the server system and blockchain network on cloud platforms, creating conditions for mobile applications to access data anywhere when there is a network connection.

Internet. However, the team has not yet deployed the mobile application to the Google Play Store or Apple Store platforms.

- Mobile applications on both Android and iOS platforms have interfaces consistent with UI and UX trends, improving user experience when using the product.
- The back-end system has average speed. Request execution time Normally (view, register, log in) is 2.5 seconds per operation. Requests related to the blockchain network take an average of about 20 seconds longer (these figures are measured and calculated using the Postman monitor tool).

5.3 System limitations

Due to time and human resource limitations, the application system will not Avoid errors:

- The peer-to-peer lending financial model proposed by the group has quite simple general business processes and has not been specifically verified by actual financial institutions. This is because team members do not have much financial expertise.
- The team has not yet implemented the flow linked to the electronic payment gateway and link with a third party to authenticate user information to complete a closed process like the actual product on the market.
- The mobile application has not been deployed in Google Play Store and Apple Store.
- The security of backing up user data was also omitted by the team.
- Speed when accessing the back-end system, especially in the blockchain network, is an issue that needs attention. Besides, there are also problems with actual notifications or user load problems is a major limitation of the current system.

CHAPTER 6: DEVELOPMENT EXPANDING DIRECTIONS

ÿ *This chapter focuses on briefly describing the future expansion of the system with the aim of developing additional features suitable to the needs of a peer-to-peer lending application. The description includes an extension of the system model system and technology expansion.*

6.1 About the system model

Besides the completed features currently in the build system, the authors also propose some other features that can be built in the future with the goal of improving the system:

- Link with a third party to build a credit rating system application based on the personal information the borrower has declared. This is an extremely important feature of a peer-to-peer lending system because it deeply impacts the interest rate calculation of borrowers, while also influencing the investment decisions of investors. However, determining the user's identity belongs to a different category of this thesis model, so the feature requires cooperation from a third-party.
- Applying reverse auction and matching algorithms to deploy the automatic authorization feature to link investments. This is a fairly common feature Variations of major systems in the world are being applied such as Lending Club and Prosper. In it, investors set their investment criteria for loans, then authorize the system to automatically search and link to loans that meet the above criteria, performing automatically. invest. This helps improve user experience, as well as stimulate the peer-to-peer lending market to come alive more dynamic.

- Deploy a feature that allows investors to withdraw capital or transfer investment rights of currently invested loans to another investor as the current lendbiz.vn system does (section 2.1.2)
- Regarding actual application deployment, typically release mobile application to Apple Store and Google Play Store, author team also thought about. However, peer-to-peer lending systems cannot Operates independently but requires close cooperation from third parties such as bank linkage or credit score assessment, so a company with a large enough scale is needed for practical implementation. Besides, as mentioned in section 4 of the **Summary chapter,** the goal of the system is built in the spirit of being able to help expand the business model. business of financial technology companies.

6.2 Regarding development technology

On the mobile application client side, the application is currently being deployed on the React Native platform with Javascript language due to the advantages of rapid product development of the platform. However, in the future, once the system is actually deployed and developed with many complex features, native Java or Kotlin development platforms for Android operating systems, Objective-C or Swift for iOS operating systems should be used. Considered by the stability of long-term application development as well as strong support strong from Google and Apple.

On the back-end system side, some additional technological techniques are applied Security to increase the information security of borrowers is also very important and affects users' trust in the system, determining the expansion of the system. system later.

As for the centralized database, the current system in use is a facility non-relational data (section 3.4). However, when applying the system there is a population For more widespread use, other relational databases such as MySQL, SQLite... should be considered for replacement to ensure the stability and scalability of the system.

As for blockchain, the team also considers testing open blockchains like Ethereum or EOS in the future. Although these platforms are still limited in speed and security of user information, the transparency is almost absolute and these blockchain models also help popularize products to a wide range of users.

In addition, the author team needs to research, develop, and use more advanced technological techniques in both mobile applications and server systems to perform these functions.
Real-time data update capabilities such as receiving notifications (sections 4.1.2.9 and 4.1.3.3), data synchronization between client and server in loan tracking, investment tracking functions...

LIST OF REFERENCES

[1] Minh Son, "Consumer lending boom", VnExpress, July 10, 2017, Last access: July 7, 2018 11:00, Link: https://lanhdoanh.vnexpress.net/ believe-tuc/ebank/bung-no-loan-use-use-3610238.html.

[2] Lendbiz, "How does the peer-to-peer lending model work", 2017, Last visit: July 7, 2018 12:00, Link: https://lendbiz.vn/mo-hinh-cho -get a loan-horizontal-hang-hoat-dong-nhu-nao.

[3] E. Miliband, "Banking will be transformed – by technology, not politics", The Guardian, January 19, 2014, Last access: July 7, 2018 14:00, Link: https://www.theguardian.com/commentisfree/2014/jan/19/online-banking-high-street-labour-reforms.

[4] Z.-e. Eiger và J. Mandell, "Practice Pointers on P2P Lending: How It Works, Current Regulations and Considerations", Morrison Foerster, 2015, pp. 01 - 02.

[5] Ha Vy, "Which bank loan interest rate is the lowest in January 2018", New Newspaper, January 12, 2018, Last access: July 7, 2018 15:00, Link: https://baomoi.com/lai-suat-cho-vay-ngan-hang-nao-thap-nhat-thang-1-2018/c/24600009.epi.

[6] D. Taylor, "Is peer-to-peer lending similar to a bank's personal loan?", Bankrate, March 1, 2018, Last access: July 7, 2018 16:00, Link: https://www.bankrate.com/finance/loans/peer-to-peer-lending-vs-bank-loan.aspx.

[7] Transparency Market Research, "Increasing Small Business Units to Act as Building Blocks for Peer-to-Peer Lending Market", Transparency Market Research, August 31, 2016, Last access: July 7, 2018 17:00, Link:

https://globenewswire.com/news-release/2016/08/31/868470/0/en/Increasing-Small-Business-Units-to-Act-as-Building-Blocks-for-Peer-to-Peer-Lending-Market.html.

[8] Statista, "Value of global peer to peer lending from 2012 to 2025 (in billion US dollars)", Statista, 2018, Last accessed: July 7, 2018 18:00, Link: https://www.statista.com/statistics/325902/global-p2p-lending/.

[9] J. Fitzsimons, "Peer-to-peer lending: should you worry about default rates?", YourMoney.com, August 24, 2017, Last accessed: July 8, 2018 11:00, Link : http://www.yourmoney.com/investing/peer-peer-lending-worry-default-rates/.

[10] C. Pastoll, "P2P Lending: A Regulatory Perspective", LendingLoop, 2017, pp. 12.

[11] Narayanan V, "A brief history in the evolution of blockchain technology platforms", Hacker Noon, February 15, 2018, Last access: July 8, 2018 12:00, Link: https://hackernoon.com/a-brief-history-in-the-evolution-of-blockchain-technology-platforms-1bb2bad8960a.

[12] P. Kasireddy, "How does Ethereum work, anyway?", Medium, September 27, 2017, Last access access last: 08/07/2018 13:00, Link: https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369.

[13] SJ Schillebeeckx, M. Soriano and EG Teo, "BLOCKCHAIN AND SMART CONTRACTS", Singapore Management University, 2016, pp. 03.

[14] M. Gupta, Blockchain For Dummies, New Jersey, Willey, 2017.

[15] J. Bagley, "What is Blockchain Technology? A Step-by-Step Guide For Beginners", Blockgeeks Inc, 2016, Last accessed: July 8, 2018 14:00, Link: https:// blockgeeks.com/guides/what-is-blockchain-technology/.

[16] Blockchain Luxembourg SA, "Average Block Size", Blockchain Luxembourg SA, 2018, Last visit: July 8, 2018 15:00, Link: https://www.blockchain.com/charts/avg-block-size.

[17] D. Siegel, "Understanding The DAO Attack", CoinDesk, June 25, 2016, Last Visited: access 08/07/2018 16:00, Road guide: https://www.coindesk.com/understanding-dao-hack-journalists/.

[18] Ngoc Do, "Blockchain/Bubble or technological revolution", Genk, November 20, 2017, Last access: July 8, 2018 17:00, Link: http://genk.vn/blockchain-bong-bong-hay-cach-mang-cong-nghe-20171120003549844.chn.

[19] A. Camp, "Prosper review", Finder, June 12, 2018, Last access: July 8, 2018 18:00, Link: https://www.finder.com/prosper.

[20] K. Herrick, "Peer-to-Peer Lending Sites: Lending Club vs Prosper vs Upstart", ASecureLife, March 5, 2018, Last access: July 9, 2018 11:00, Link: https://www.asecurelife.com/lending-club-vs-prosper-vs-upstart/.

[21] Lendbiz, "Investment needed", Lendbiz, 2017, Last visit: July 9, 2018 12:00, Link: https://lendbiz.vn/can-duoc-dau-tu/.

[22] Lendbiz, "Investment", Lendbiz, 2017, Last access: July 9, 2018 13:00, Link: https://lendbiz.vn/dau-tu/.

[23] fundgo.vn, "Project: "Peer-to-peer lending on blockchain technology"", fundgo.vn, January 2018, Last access: July 9, 2018 14:00, Link:

http://fundgo.vn/en/du-an/10/project-peer-to-peer-lending-on-blockchain-technology-.

[24] thuvienphapluat.vn, "Decree 174/2016/ND-CP guiding the Accounting Law", thuvienphapluat.vn, December 30, 2016, Last access: July 9, 2018 15:00, Link: https://thuvienphapluat.vn/van-ban/Ke-toan-Kiem-toan/Nghi-dinh-174-2016-ND-CP-huong-Luat-ke-toan-336391.aspx.

[25] A. Dietricha và R. Wernlib, "What Drives the Interest Rates in the P2P Consumer Lending Market? Empirical Evidence from Switzerland", EFMA, 2016, pp.13.

[26] F. Cejas, "Architecting Android...The clean way?", 03/09/2014, Lÿn truy cÿp last: 09/07/2018 16:00, Road guide: https://fernandocejas.com/2014/09/03/architecting-android-the-clean-way/.

[27] B. Peabody, "Server-side I/O Performance: Node vs. PHP vs. Java vs. Go", Toptal, 2017, Last visit: July 9, 2018 17:00, Link: https://www.toptal.com/back-end/server-side-io-performance-node-php-java-go.

[28] MJJB and NS . "JSON Web Token (JWT)", IETF, May 2015, Last access: July 9, 2018 18:00, Link: https://tools.ietf.org/html/rfc7519.

[29] M. Valenta và P. Sandner, "Comparison of Ethereum, Hyperledger Fabric and Corda", Frankfurt School Blockchain Center, 2017, pp.02.

[30] C. Ferris, G. Singh and N. Gaski, "Architecture Explained", October 12, 2017, Last accessed: July 10, 2018 11:00, Link: https://hyperledger-fabric.readthedocs.io/en/release-1.0/arch-deep-dive.html.

[31] P. Thakkar, S. N. N và B. Viswanathan, "Performance Benchmarking and Optimizing Hyperledger Fabric Blockchain Platform", IBM Research Lab, 2017, pp.02-03.