International Journal of Grid and Distributed Computing
Vol. 10, No. 12 (2017), pp.81-92
http://dx.doi.org/10.14257/ijgdc.2017.10.12.08

Design and Implementation of System for Reliable Application using Blockchain: A Case Study in P2P Crowdfunding

Kyoung-Jin Kim and Seng-Phil Hong*

Department of Convergence Security Engineering, Sungshin Women's University
{kyongjin, philhong}@sungshin.ac.kr

Abstract

P2P financial transactions are available to any lenders and borrowers, who can access the internet, without any intervention of financial companies or trusted third parties. To address the foregoing challenge, this study simplifies the application process for P2P crowdfunding to the maximum extent possible, and proposes a secure system with reinforced security authentication for transparent borrowers to transact with others. This paper proposes a method of safe transactions in blockchain by means of smart contracts.

Keywords: *P2P crowdfunding, Lending system, Blockchain, Smart contract*

1. Introduction

P2P crowdfunding is a financial service that directly connects borrowers with investors who intend to lend and invest money via an online marketplace [1, 2], and refers to lending and collecting funds between individuals through an online platform without any intervention of financial institutions like banks. The word 'crowd' implies that lenders are allowed to diversify investment opportunities.

P2P crowdfunding has emerged as an alternative for those who are denied loans by major banks and other lenders because of unfavorable credit ratings. At the same time, money lenders have launched P2P businesses adopting Fintech. P2P crowdfunding service providers rely on online platforms only and offer marketplaces to connect loan applicants with individual and institutional lenders [2-4].

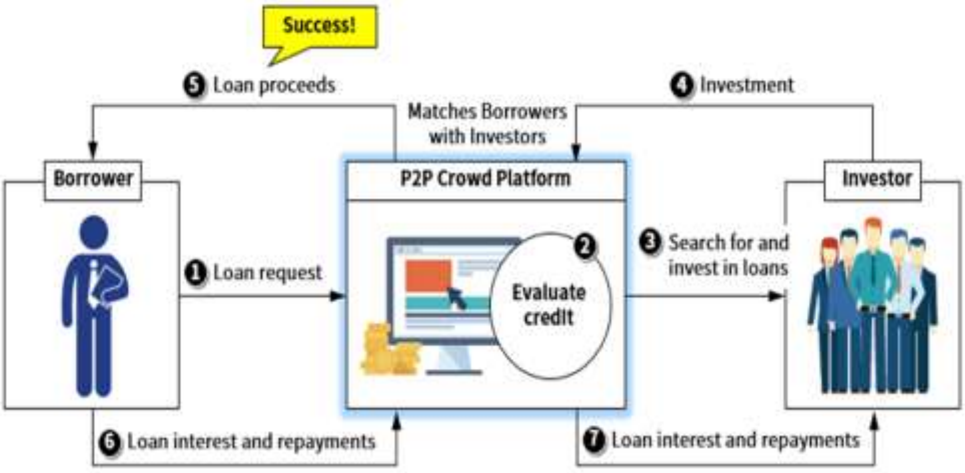

Success!
5 Loan proceeds
4 Investment
Matches Borrowers with Investors
Borrower
P2P Crowd Platform
Investor
1 Loan request
2 Evaluate credit
3 Search for and invest in loans
6 Loan interest and repayments
7 Loan interest and repayments

Figure 1. P2P Crowdfunding Service

Received (October 20, 2017), Review Result (December 2, 2017), Accepted (December 7, 2017)

[*] Corresponding author

ISSN: 2005-4262 IJGDC

This paper concerns applying blockchain technology to P2P crowdfunding to provide a service for investing or lending funds to individuals [5, 6]. Many researchers, however, are raising concerns about using the blockchain technology as a payment gateway system in that P2P financial transactions are available to any lenders and borrowers, who can access the internet, without any intervention of financial companies or trusted third parties. That is, the safety and security of platforms are overarching components in P2P financial transactions as they deal with virtual currencies.

To address the foregoing challenge, this paper simplifies the application process for P2P crowdfunding to the maximum extent possible, and proposes a secure system with reinforced security authentication for transparent borrowers to transact with others. Also, the proposed system ensures safe and transparent management of transaction information with the blockchain technology, and stores confidential information in a reservoir fitted with a robust internal encryption scheme. For funding, the system uses smart contracts and runs a program to assess the terms and conditions of loans. That is, the system eliminates the need for a manual assessment of a borrower's capacity to afford a loan by offering the self-executing smart contracts for funding.

This paper is organized as follows: First, it analyzes and clarifies the concept, background and typology of blockchain. Also, it analyzes the status of blockchain-based P2P crowdfunding, and examines the challenges or issues relevant to security to be addressed for adopting the blockchain technology in practice. Based on the issues derived, this paper proposes a trust-based P2P crowdfunding system, implements its applicable prototype, and tests its performance ultimately to discuss a desirable future direction for the application of blockchain.

2. Background and Related Work

2.1. Background and Typology of Blockchain

The established financial transactions are prone to go awry and lose institutional and individual customers' trust if their central systems are compromised or infiltrated by hackers. Without doubt, businesses or organizations take preventive measures by building robust security systems, which however incurs administrative costs and expenses.

To address the challenges related to central systems, blockchain distributes a ledger on a P2P network, not a central server of a certain entity, so that participants can jointly keep and manage it. Blockchain calls for no third-party intervention, which helps save fees and administrative expenses, and allow a relatively safe cross-ownership of information, precluding any deliberate manipulation of data. Also, as blockchain is distributed, P2P transactions are enabled without any authorized third party. Moreover, as all users (nodes) share a ledger, any network glitches have negligible effects on the entire blockchain.

The typology of blockchain varies across researchers. Different types of blockchain exist depending on their network attributes and scopes and are applicable for intended purposes. As a rule, there are three types of blockchain, *i.e.* public, consortium and private blockchain [7, 8, 10].

- **Public blockchain** provides anonymity, are open to anyone and best reflect the attributes of P2P. As any unverified users are allowed to access public blockchain and engage in transactions, highly sophisticated encryption and authentication are needed, which decreases the network scalability and speed.
- **Private blockchain**, unlike the anonymous public blockchain, allows the identification of principals, accelerate transactions, are customized as needed, and thus draw attention from businesses and banks.

- **Consortium blockchain** is somewhere in between public and private blockchain. Unlike private blockchain whose owners have all rights, pre-selected nodes have priority rights over consortium blockchain.

Therefore, consortium blockchain maintain a distributed structure, strengthen security with limitations on participation, cope with the slow transaction speed and the network scalability issues found in public blockchain and are applicable to such purposes as inter-bank transactions. This paper draws on a consortium-based permissioned blockchain network infra to propose a safe P2P crowdfunding system.

2.2. Related work on P2P Crowdfunding

The essence of P2P crowdfunding is to provide a low-cost, fast and efficient settlement and payment system. There are different types of crowdfunding as shown in the figure below [2, 3]. Particularly, this paper is focused on the loan-based or lending-type crowdfunding.

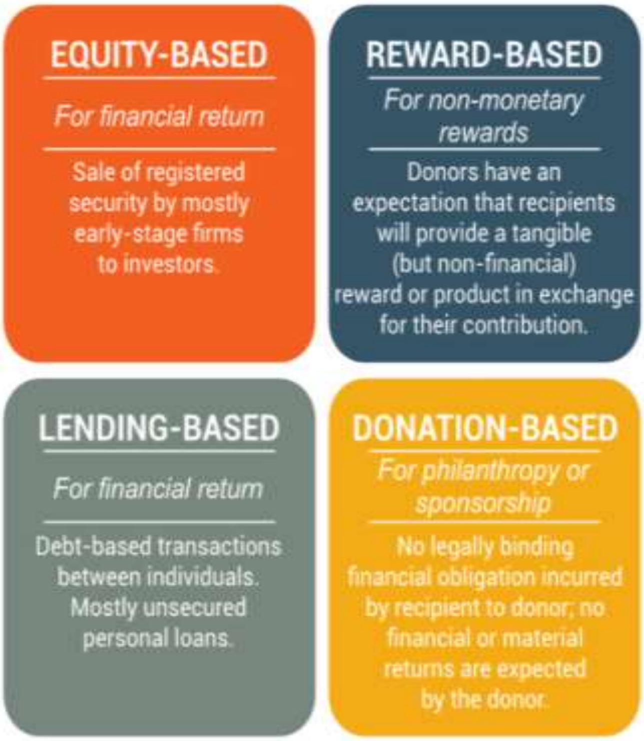

EQUITY-BASED
For financial return
Sale of registered security by mostly early-stage firms to investors.
REWARD-BASED
For non-monetary rewards
Donors have an expectation that recipients will provide a tangible (but non-financial) reward or product in exchange for their contribution.
LENDING-BASED
For financial return
Debt-based transactions between individuals. Mostly unsecured personal loans.
DONATION-BASED
For philanthropy or sponsorship
No legally binding financial obligation incurred by recipient to donor; no financial or material returns are expected by the donor.

Figure 2. P2P Crowdfunding Types [15]

Lending-type crowdfunding refers to money transactions, where multiple people pool their money together, lend it to those who need funding, and collect interest. Lending-type crowdfunding takes note of for what a prospective borrower needs a fund and how the person will repay the loan.

The lending service involves individual credit loans, SME loans and housing loans and many others. Yet, this paper proposes a blockchain-based P2P crowdfunding for university student loans. As the blockchain-based P2P crowdfunding deals with financial information, it should be a semi-open type that proves transactions within the information, and allow real-time transactions. That is, blockchain is used to keep a shareable and replicable ledger in a distributed manner, to eliminate the legacy central database in favor of efficient loans and investments, and ultimately to enable a safe inexpensive real-time financial transaction.

3. Technical Issues of Blockchains

Bitcoin was not only the first and the most widely used digital currency but also the first case of applying a blockchain[7,9,10]. As a typical digital currency on a distributed network, Bitcoin is a decentralized currency free from the influence of central banks or official issuers. Bitcoin's owner-less P2P system does not limit any right to alter its ledger to a particular being. The digital currency is bought and sold through Bitcoin exchanges whose infrastructure has been established and operated in most advanced countries, where relevant legislation is underway.

Due to its advantages, Bitcoin has attracted worldwide attention as an alternative to the existing centralized transaction system. Still, concerns have been raised over its technical issues despite its exponential growth. First, Bitcoin is ① irrevocable. That is, the blockchain is irreversible once a transaction is confirmed and stored in a block. Unless the receiver is willing to send it back, there is no way to cancel or undo the transaction. ② The blockchain per se has the integrity and provides security but not confidentiality. Although Bitcoin does not require personal information, its transaction details are open to all. Therefore, it is possible to trace the Bitcoin transaction by combining the available information associated with the owner of a Bitcoin address. Also, despite the robust security of the blockchain, ③ should its infra be hacked, the digital currency transactions are irremediable. For example, in case the private key containing Bitcoin information was lost or stolen, the exchange could be hacked. In that case, there is no remedy as of now on the grounds that the digital currency has no agency or authority responsible for issuing and managing it. In addition to the security-related technical issues, the need for constant development and scalability has caused challenges hampering the implementation of a range of services.

To address the foregoing challenges, Ethereum has been developed with a new blockchain network[11]. Lots of consortia have paid attention to Ethereum's improved blockchain, which is academically more approachable in comparison to that of Bitcoin. Ethereum supports Turing-complete languages and allows Javascript or Python coding, which has resulted in the development of diverse application programs. In addition, the PoS method, which is a reinforcement of the PoW method, enables the design of a verification algorithm capable of creating a block in 12 seconds or so. That is, it used to take 10 minutes to authorize a transaction, whereas Ethereum has rectified the blockchain's speed issue. Given Ethereum is a digital currency using blockchains without a central server, it saves server and security costs and basically defends against DDoS attacks. Also, it enables distributed applications based on a shared agreement among blockchain participants. In comparison to existing web applications, distributed applications are open sources and easier to develop using HTML and Javascript. Moreover, as data is stored in blockchain, the blockchains' security scheme protects the data, whilst the network facilitates cross-border services. Furthermore, the salient feature of Ethereum blockchain is smart contracts. With almost every Turing-complete code supported, it is possible to define states and functions. With state transition and data storage enabled, it is possible to define the contracts in a manner similar to coding on computer. A limited number of parties are involved in a transaction based on a smart contract between individuals and blockchains (P2O: Parties to Organization) or between individuals (P2P). Once a contract is concluded, the transaction is automatically run through events without any intervention. Therefore, smart contracts ensure real-time services. Smart contracts also address the foregoing Bitcoin-related irrevocability issue with a safe use of blockchain by implementing an escrow service for the transaction process, where Ethereum is transferred to a receiver once the cash remittance is completed and the contract terms and conditions are met. This paper proposes a method of safe transactions in blockchain by means of smart contracts.

4. Proposed TLS (Trusted Lending System)

4.1. Structural schema

Basically, a blockchain network verifies data with a system-based consensus formation structure, where trusted nodes verify data based on an agreement among the participants in a permissioned blockchain. Thus, this paper sets an issuer node pre-verified(licensed) in a permissioned blockchain for a trusted verifier node to verify the block(data) arising in the blockchain. Existing financial transactions require the authentication certificates, which need be verified via CA institutions. To provide such a trust assurance on blockchain networks, the nodes on a blockchain network use the distributed public key encryption and have the issuer and verifier nodes verify the important blocks.

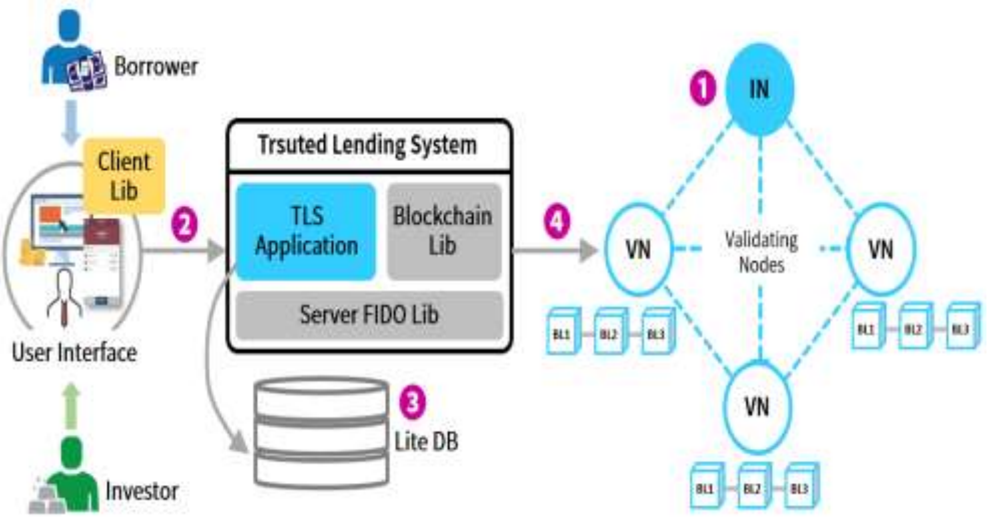


Figure 3. Overall Structure of the Trusted Lending System

① With the issuer node serving as a trusted third party in a small chain, and the verifier node chosen as an intermediate, the verifier node verifies the block when a transaction occurs. For future research, a node should be trusted by a majority of voters to become a verifier node before it verifies other nodes and transactions. As participants, or nodes have tokens based on the distributed public key encryption to identify users, they ensure the safety of data and transactions by selecting a trusted verifier node in the blockchain.

Based on the permissioned blockchain network, ② users (participants) access TLS on their mobile phones or through web browsers and are registered with transactions encrypted using the distributed public keys and identified through blockchain. Among the users, borrowers (more critical parties) must receive a second FIDO-based authorization to use the service.

③ For every block(data), each blockchain and event incurs fees. To reduce fees, general information is kept in the Lite DB, whilst critical information is subject to a one-way encryption for a separate storage of confidential data. Also, the results from the implementation of a smart contract are stored.

④ The events arising in TLS are recorded in the blockchain. This is a permissioned blockchain in itself, gaining the data integrity of every process and task with transactions recorded like logs. Tasks defined in the smart contract are performed by transactions as well as log records. For example, a smart contract enables a P2P lending without the intervention of an agent. A smart contract implied within a contract is used for business rules and logic and executed when transactions are performed. Different smart contracts are defined for different purposes in TLS. A smart contract is performed when its terms and conditions match up with a transaction.

This paper uses Ethereum's block structure for storage and adds authentication values.

4.2. Key Algorithms

Using the existing blockchain like Ethereum, the proposed method provides the interface for businesses to easily manage the throughput and speed of transactions and to control the access to transactions in a way that is applicable to P2P crowdfunding.

(1) Authority-based block creation, using FIDO

The authentication in this paper involves building a trusted authentication system to identify users and determine their authenticity. Also, the system provides encryption/decryption and digital signatures for the P2P network communication with intent to prevent any forgery, using FIDO. FIDO, or Fast IDentity Online, is a convenient and safe personal authentication technology using biometric information, *e.g.* fingerprints and irises, online. By applying FIDO to TLS to separate the authentication protocol from the means of authentication, the proposed method ensures security and convenience. The biometric information used to identify users is stored and registered in personal devices. The authentication process is run on personal terminals. As the biometric information is securely stored on smartphones(TrustZone), it is hardly leaked.

Hence, authenticated users are identified and allowed to share a group token and to engage in the blockchain network as a verified participant (node).

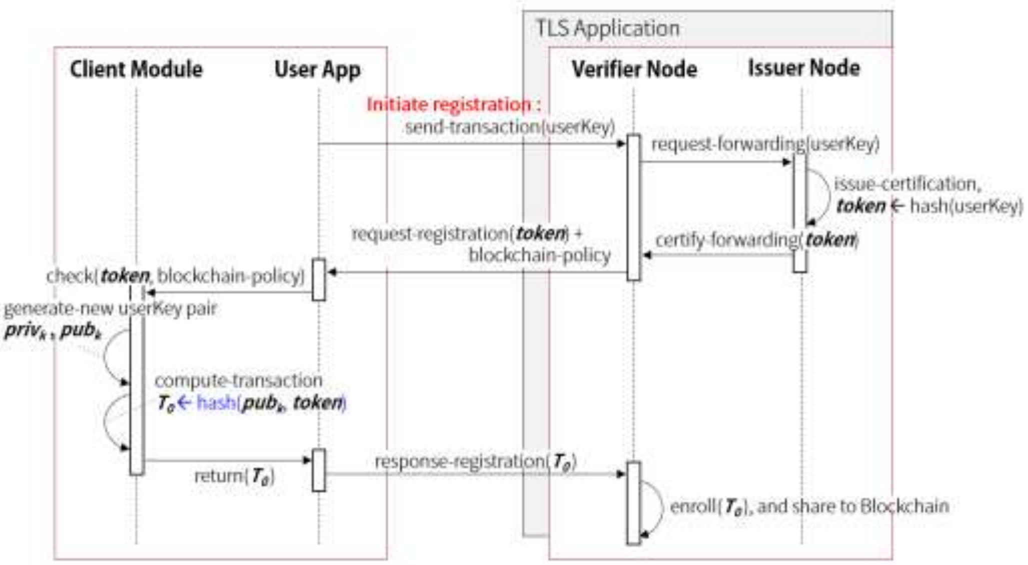

TLS Application
Client Module
User App
Verifier Node
Issuer Node
Initiate registration :
send-transaction(userKey)
request-forwarding(userKey)
issue-certification,
token ← hash(userKey)
request-registration(token) +
blockchain-policy
certify-forwarding(token)
check(token, blockchain-policy)
generate-new userKey pair
$priv_k$, pub_k
compute-transaction
T_0 ← hash(pub_k, token)
return(T_0)
response-registration(T_0)
enroll(T_0), and share to Blockchain

Figure 4. Strengthening Security with User Authentication Using FIDO

Upon completion of authentication, users can access TLS and request transactions, whose block(data) is verified by the Verifier Node, serving as a verifier. Then, every event occurring, every authentication of those who request information and the attempts to access are recorded as transactions on blockchain.

(2) A smart contract is created when a borrower applies for a loan

In the P2P crowd TLS supporting Ethereum, a borrower can apply for a loan, whilst investors can invest certain amounts of money in a borrower of their own choice. Once a borrower applies for a loan, the internal credit rating system assesses whether to accept the application. If accepted, the loan amount, interest, repayment plan and other terms and conditions are uploaded to the Smart Contract.

The specific scenario of the foregoing lending process flows as follows:

1) A borrower applies for a loan by entering the required information, *e.g.* education, income and existing loans from other institutions.

2) TLS internally assesses whether to accept the loan application, and estimates the interest and maximum loan amount.

3) Upon completion of the loan application, a smart contract is created based on the submitted information, and a transaction occurs to have the information recorded in a blockchain. The transaction is a (1) signed transaction that strengthens the security.

Then, the loan application information is registered in TLS.

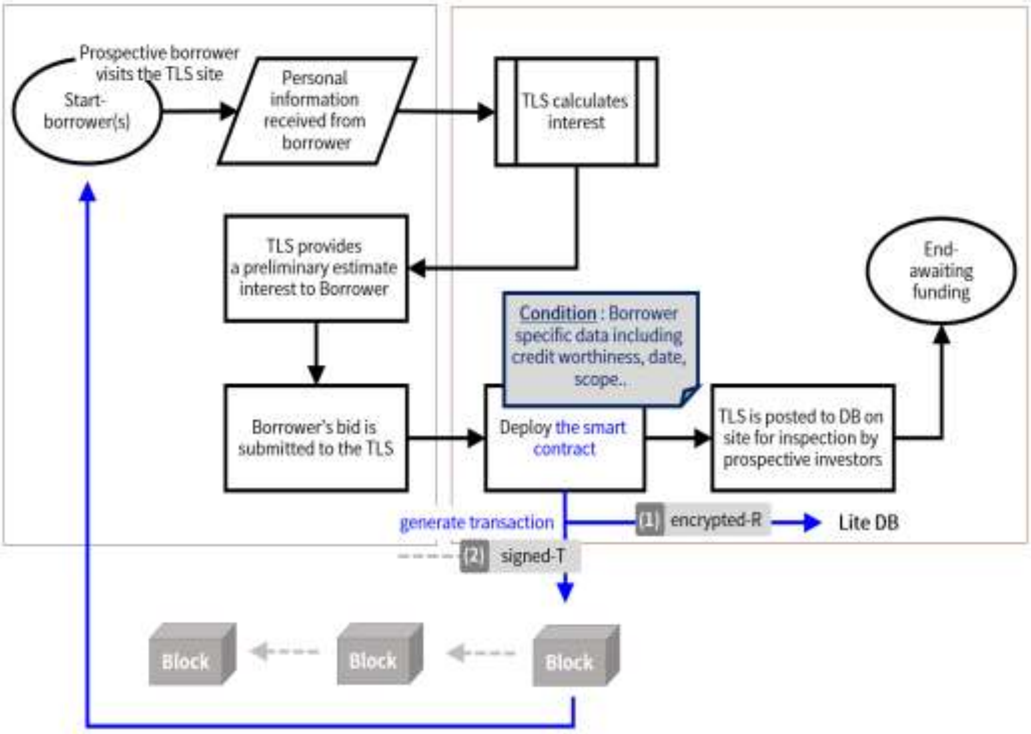

Prospective borrower visits the TLS site
Start-borrower(s)
Personal information received from borrower
TLS calculates interest
TLS provides a preliminary estimate interest to Borrower
End-awaiting funding
Condition : Borrower specific data including credit worthiness, date, scope..
Borrower's bid is submitted to the TLS
Deploy the smart contract
TLS is posted to DB on site for inspection by prospective investors
generate transaction
[1] encrypted-R
Lite DB
[2] signed-T
Block
Block
Block

Figure 5. Lending Process Flow When a Borrower Applies For a Loan

The borrower is authenticated to prevent any fraudulent registration and allowed to doublecheck the data. Transactions taking place are encrypted and securely recorded on the blockchain network.

(3) A smart contract is called when an investor applies for an investment

Upon completion of the foregoing scenario, an investor can retrieve the loan information registered in the system to invest a small amount of money. The investor may search investment terms and conditions as needed or view applicants meeting the given conditions in the order of credit ratings. Also, the registered loan information is uploaded on the blockchain network, which ensures the integrity and reliability of the information from lending to repayment.

The specific scenario of the foregoing investment process flows as follows.

1) An investor views the borrower information through TLS.

2) The investor chooses to invest in a borrower.

3) TLS calls the smart contract program to match the condition of the borrower with that of the investor before making an investment decision.

4) The investor receives the result and requests the investment.

5) When the investment is approved, the smart contract program is called to remit the amount of money to invest. The smart contract automatically manages the process, while the information in the blockchain is updated accordingly.

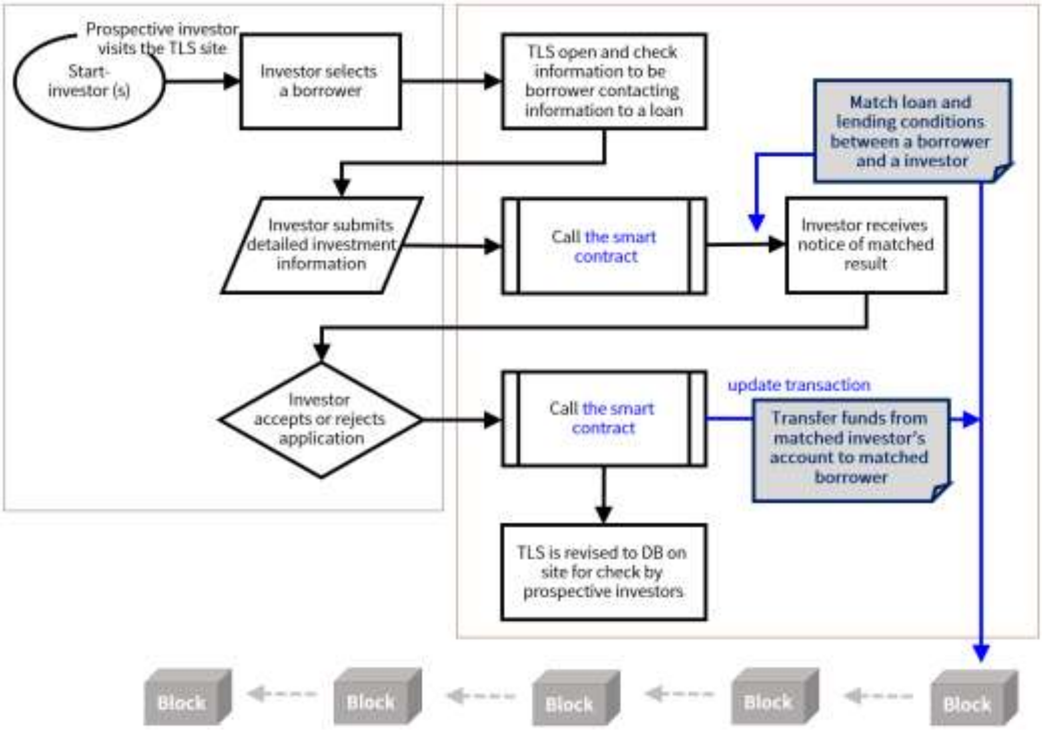

Prospective investor visits the TLS site
Start-investor (s)
Investor selects a borrower
TLS open and check information to be borrower contacting information to a loan
Match loan and lending conditions between a borrower and a investor
Investor submits detailed investment information
Call the smart contract
Investor receives notice of matched result
Investor accepts or rejects application
Call the smart contract
update transaction
Transfer funds from matched investor's account to matched borrower
TLS is revised to DB on site for check by prospective investors
Block
Block
Block
Block
Block

Figure 6. Investment Process Flow When an Investor Applies for an Investment

Once the investment is successfully made, the relevant transaction record is authenticated by the borrower and the investor before it is uploaded on the blockchain network. The uploaded information is transmitted to all participants, who can see all the information. When the invested amounts of money reach a target sum, the smart contract is approved by the administrator, and delivered to the borrower before the lending is activated. Furthermore, the amounts of money to be invested and to be repaid are automatically processed by the smart contract, which saves the trouble of manually checking the status of lending and investment.

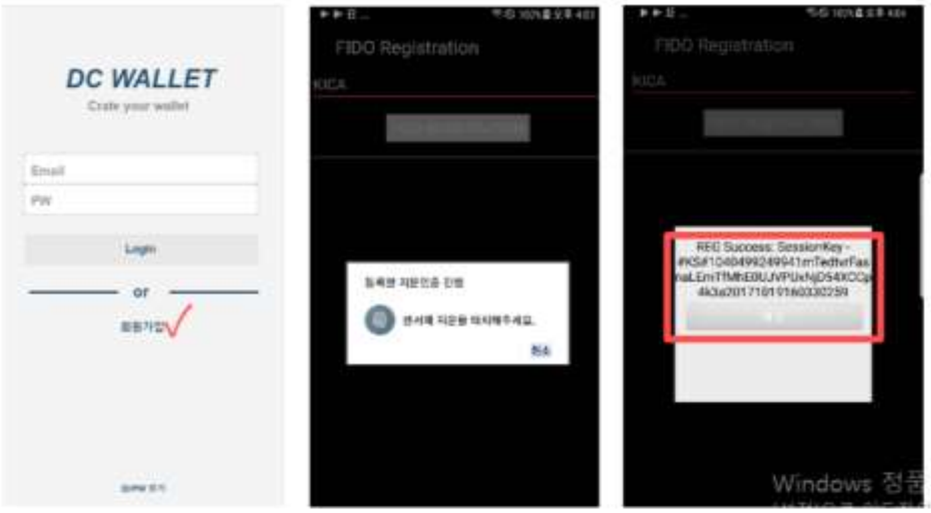
5. Prototype and Performance Testing

5.1. Prototype

To implement the proposed system's operating process, an authentication server node, a verification server node and a client node are included in the test-net setting. As part of the implementation environment, geth is installed on the server node to run Ethereum in the background. To store the loan information, both a private storage and the Ethereum blockchain as a test-net-based public storage are used.

On the TLS site where borrowers and investors access, applications are configured in HTML and JavaScript, and Web3.js library is used to communicate with the Ethereum node. Here, the smart contract program that sets the terms and conditions for loans is a code written in Solidity and distributed to the blockchain. The borrower information used in the prototype is assumed to be relevant to an undergraduate, with the borrower's loan information and identity records stored in the JSON format.

The figure below shows the user authentication using TLS FIDO incorporated in the blockchain. TLS generates FIDO's fingerprint authentication QR code, while the user uses the QR Scan menu on the TLS site to scan the QR and authenticate himself with the fingerprint registered on his smartphone. Upon completion of a successful authentication, a separate screen is displayed for processing.

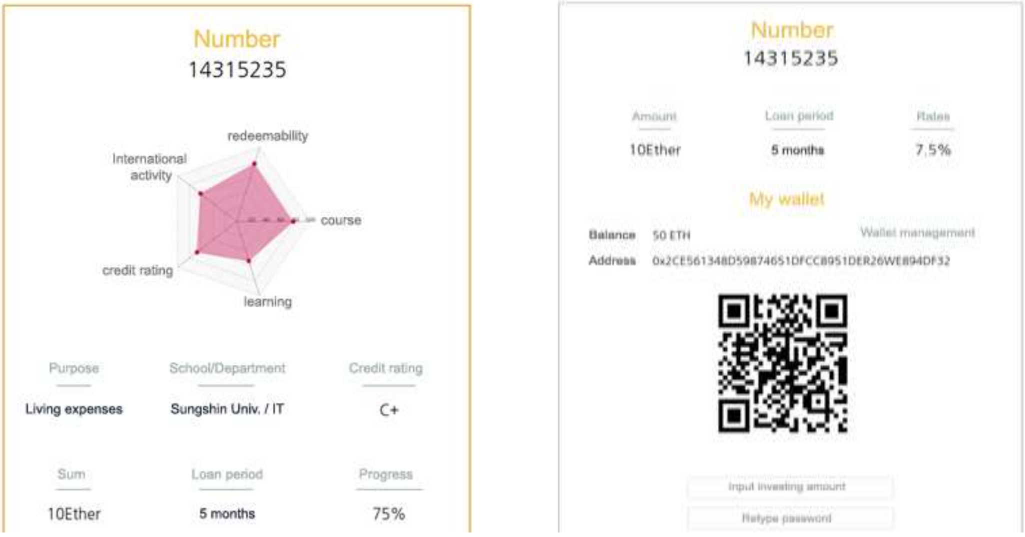


REG Success: SessionKey - #KS#1040499249941mTedtvFaanaLEmTfMhE0UJVPUxNjD54XOCq4k3a2017101016033022S9

Figure 7. User Authentication Using FIDO of the Trusted Lending System

A borrower applies for a loan, and the administrator approves the application. Then, TLS sets the terms and conditions to generate and distribute a smart contract, and the contract address is created. Once the input value and GAS expense are paid to the given contract address, a transaction (Singed T) takes place and runs.

Later on, an investor views the loan information uploaded in the blockchain, chooses to invest in a borrower, and invests a small amount of money. The amounts of money invested are automatically managed in the smart contract. Once the invested amounts reach a target sum, the administrator approves the loan.



Number
14315235

Purpose	School/Department	Credit rating
Living expenses	Sungshin Univ. / IT	C+

Sum	Loan period	Progress
10Ether	5 months	75%

(A) A Borrower Screen

Number
14315235

Amount	Loan period	Rates
10Ether	5 months	7.5%

My wallet

Balance 50 ETH
Address 0x2CE561348D598746510FCC8951DER26WE894DF32

(B) An Investor Screen

Figure 8. Website of the Trusted Lending System

5.2. Performance Testing and Anticipated Effect

This paper explores a trust-based lending system using blockchain. Blockchain has been well-documented with many relevant studies underway. Yet, as research on blockchain is still in its infancy, there is a paucity of articles on the implementation of blockchain.

Therefore, this paper implements a TLS system, and tests its qualitative safety. The safety of a blockchain-based P2P credit lending system is tested in terms of whether it meets the security requirements. The criteria for the test are three security components plus system performance (speed).

Table 1. Performance Testing Using Qualitative Safety

Security components	S.-Y. Oh, *et al.*[12]	B.-J. Park, *et al.*[13]	Y.-D. Seo, *et al.*[14]	TLS (Our system)
Consolidated authorization				✔
Confidential management	✔			✔
Ensuring data integrity	✔	✔	✔	✔
Supporting availability	✔		✔	✔
Transaction processing speed		✔		✔

Here, FIDO is used for the consolidated authorization, ensuring a convenient and secure authentication. Confidentiality refers to managing the data confidentiality with ease without compromising the performance. Given blockchain hardly ensures confidentiality, a private storage is used in this paper to separately store the encrypted confidential information. Also, as blockchain assures integrity in most research, the data integrity is assured in this paper as well. Availability refers to data being available to authorized users regardless of time and place. Blockchain participants are allowed to access the system and use the data. Finally, the Ethereum blockchain theoretically outpaces the more popular Bitcoin in terms of processing speed. Despite authentication and sign (digital signature) security features added to blockchain, there is no remarkable difference in processing speed.

6. Conclusion

This paper proposes a safe P2P crowdfunding system based on blockchain networks. The proposed system enhances security by deterring forgery with encryption of transaction information using blockchain. Also, using a smart contract for implementing a loan agreement, the proposed system automatically enables transactions in compliance with terms and conditions, prevents administrators from committing a fraud or forging agreements, and successfully authenticates crucial information in non-face-to-face transactions such as P2P crowdfunding. By virtue of the blockchain technology, the proposed system allows parties to a contract to view details of their agreement anytime, which will be conducive to settling any disputes.

Acknowledgments

This research was supported by the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2017-2015-0-00369) supervised by the IITP(Institute for Information & communications Technology Promotion).

References

[1] L. A. Tidwell, “peer-to-peer lending system for the promotion of social goals”, U.S. Patent US20100005018 A1, **(2010)**.

[2] H. Zhao, Y. Ge, Q. Liu, G. Wang, E. Chen and H. Zhang, “P2P Lending Survey: Platforms, Recent Advances and Prospects”, ACM Transactions on Intelligent Systems and Technology, vol. 8, no. 6, **(2017)**.

[3] E. M. Gerber and J. Hui, “Crowdfunding: Motivations and deterrents for participation”, ACM Transactions on Computer-Human Interaction, vol. 20, no. 6, **(2013)**.

[4] S.-C. Hsueh and C.-H. Kuo. “Effective Matching for P2P Lending by Mining Strong Association Rules”, Sapporo, Japan, **(2017)**.

[5] L. Xu, N. Shah, L. Chen, N. Diallo, Z. Gao, Y. Lu and W. Shi, “Enabling the Sharing Economy: Privacy Respecting Contract based on Public Blockchain”, Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, Abu Dhabi, United Arab Emirates, **(2017)**.

[6] K.-J. Kim and S.-P. Hong, “Study on Rule-based Data Protection System Using Blockchain in P2P Distributed Networks”, International Journal of Security and Its Application, vol. 10, no. 11, **(2016)**.

[7] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System”, https://bitcoin.org/bitcoin.pdf, **(2008)**.

[8] R. Neisse, G. Steri and I. Nai-Fovino, “A Blockchain-based Approach for Data Accountability and Provenance Tracking”, Proceedings of the 12th International Conference on Availability, Reliability and Security, Reggio Calabria, Italy, **(2017)**.

[9] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf and S. Capkun, “On the Security and Performance of Proof of Work Blockchains”, Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, **(2016)**.

[10] L. S. Sankar, M. Sindhu and M. Sethumadhavan, “Survey of consensus protocols on blockchain applications”, Proceedings of the 4th International Conference on Advanced Computing and Communication Systems, **(2017)**.

[11] Ethereum Project, https://www.ethereum.org/.

[12] S.-Y. Oh and C.-H. Lee, “Block Chain Application Technology to Improve Reliability of Real Estate Market”, The Jounal of Society for e-Business Studies, vol. 22, no. 1, **(2017)**.

[13] B.-J. Park, T.-J. Lee and J. Kwak, “Blockchain-Based IoT Device Authentication Scheme”, Journal of the Korea Institute of Information Security & Cryptology, vol. 27, no. 2, **(2017)**.

[14] Y.-D. Seo, J.-W. Kim, S.-H. Jeong and H.-S. Eom, “The implementation of secure export payment service using the Blockchain”, Korea Information Science Society, **(2016)**.

[15] H. Nielsen, Editor, “The Startup Funding Book”, NHN Ventures Aps Publishers, **(2017)**.

Authors

Kyoung-Jin Kim, she graduated with a B.S. in 2007, with a M.S. in 2009 and with a Ph.D. in 2013 from the Sungshin Women's University. She joined the Information Security lab as a postdoctoral fellow since 2016. She is actively involved in teach and research in information security at Sungshin Women's University, Korea. Her research interests focus on privacy protection, access control and blockchain.

Seng-Phil Hong, he received his BS degree in Computer Science from Indiana State University, and MS degree in Computer Science from Ball State University at Indiana, USA. He researched the information security for Ph.D at Illinois Institute of Technology from 1994 to 1997, He joined the Research and Development Center in LG-CNS Systems, Inc since 1997, and he received Ph.D. degree in computer science from KAIST University in Korea. He is actively involved in teach and research in information security at Sungshin Women's University, Korea. His research interests include access control, security architecture, privacy, e-business security, blockchain and fintech.