IJFANS INTERNATIONAL JOURNAL OF FOOD AND NUTRITIONAL SCIENCES
ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

DEFI ON PEER-TO-PEER LOAN MANAGEMENT MODEL USING SMART CONTRACTS ON BLOCKCHAIN

Dr. S. Jesssica Saritha

Assistant Professor, Dept of CSE, JNTUA College of Engineering Pulivendula.

Email ID: sjsaritha.cse@jntua.ac.in

Abstract:

This article explores the potential impact of Decentralized Finance (DeFi) and blockchain technology on the lending industry. By utilizing a peer-to-peer approach, DeFi can provide a more efficient, secure, and inclusive means of generating loans and conducting financial transactions. Unlike traditional banking systems, which are often slow and require extensive paperwork, a decentralized application (Dapp) can enable users to easily access loan services at any time. Additionally, the Dapp can offer lower interest rates in a transparent and secure environment. By revolutionizing the loan generation process, DeFi aims to provide users with greater flexibility, accessibility, and affordability when it comes to accessing financial services.

Keywords :

Solidity, Interplanetary File System(IPFS), Decentralized Finance, Loan Management System, Mortgage Security[CID].

I.INTRODUCTION

In recent times, the concept of decentralized finance has gained immense popularity owing to the advancements in blockchain technology. The traditional financial system has been disrupted by the decentralized nature of transactions, rendering intermediaries unnecessary. This transformation has revolutionized the way financial transactions are conducted, offering a more streamlined and efficient process. Now, individuals and businesses can make transactions without relying on traditional financial institutions, which is a significant step towards a more independent and secure financial future[1]. User security is a major challenge for privacy in the banking system. As technology continues to evolve, the challenges are being addressed, leading to the implementation of a blockchain-based financial system in the banking sector. The banking sector is responsible for connecting people with their money, and many banks are turning to the Ethereum blockchain to gain an advantage in controlling fraud during loan processes. This sector plays a crucial role in maintaining security and preventing attacks like the Punjab National Bank (PNB) Scam while approving loans. [2].

The decentralized financial system is commonly used by banks to manage loans and prevent fraud and scams. However, this system has some limitations when it comes to providing loans to customers. For example, system downtimes can occur when the server goes offline, and the loan application process can be time-consuming due to the decision-making involved. As a result, customers may lose hope of getting a loan within a reasonable timeframe. Business owners often fall victim to exploitation by lenders who provide loans with unfair interest rates, intermediaries, and heavy dependence on the

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

lender.

To address these issues, this paper proposes the design of a user-friendly decentralized application (DApp) that uses solidity-based smart contracts to provide a peer-to-peer lending platform using blockchain technology. This platform would not require any third-party involvement, such as banks[3].

This paper focuses on providing an efficient solution to this problem through our peer-to-peer lender-based payment system. This system provides fair interest rates and allows customers to specify the due date for loan repayment before receiving an Ethereum-based payment from the lender. The lender has access to the mortgage submitted by the borrower, which gives them the right to check the files or assets submitted through the IPFS file system. Borrowers receive a CID(Content Identifiers) token which is purely based on the content cryptographic hash to enter the mortgage address while requesting a loan.

If the borrower does not repay the loan according to the specified due date, the files submitted through the mortgage will be auctioned off by the lender. This process ensures that the lender is protected and that borrowers have the freedom to manage their loan repayment.

Traditional transaction systems and payment methods operate in a centralized manner, which requires continuous monitoring to provide loans to customers. For instance, the system needs to verify whether a user has previously taken a loan from any bank before they apply for a new one. This verification is authenticated using the user's PAN card, and the management then decides whether to grant the desired loan or not. In this system, everything is human-controlled, and there is involvement from third-party organizations. Additionally, withdrawing and depositing money is a time-consuming process[4].

In our research paper, we propose an automated transaction system that eliminates the need for third-party verification and banks by introducing Ethereum blockchain payment technology which is decentralized and on a peer-to- peer basis. Our system leverages a smart contract- based solution to ensure that all predefined terms and conditions are met during the generation of a transaction.

II. LITERATURE REVIEW

Researchers from around the world have dedicated significant efforts to developing blockchain technology for an efficient loan management model on a peer-to-peer basis, as well as through the use of banks. They have addressed various factors and gained insights by proposing a system that ensures adherence to the principles of confidentiality, integrity, and availability (CIA) for security purposes. The system uses algorithms such as Proof of Work (PoW) and Proof of Authority (PoA) to ensure that the provided data is real, immutable, and authenticated [5].

Hegadi R (2023) is focusing on monitoring vulnerabilities found in smart contracts in Web3. These vulnerabilities include attacks on price manipulation, signature reply attacks, self-destructing attacks, overflow and underflow attacks, vulnerability on access control, and reentrancy attacks. The purpose of this research is to offer mitigating strategies and disseminate information about security attacks using smart contracts in the Web3 ecosystem, making it easier for borrowers to obtain loans from lenders. This will help users adapt to blockchain

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

technology while being mindful of potential security risks[6].

In a study by Zheng and Hao, they propose a Hyperledger-based peer-to-peer lending system (HyperP2PLS) to address irregularities in the P2P lending market. The performance analysis of the proposed system ensures safety, reliability, transparency, and efficiency[7]. The paper titled "Ethna" by Qingyang Yang delves into the P2P network of the Ethereum blockchain. Unlike Bitcoin, Ethereum utilizes a Kademlia Distributed Hash Table to manage its overall Peer-to-Peer Network. The researchers created a tool called "Ethereum Network Analyzer" to study the P2P network of the Ethereum blockchain and its topological features. This tool enables efficient data processing between the lender and the borrower while conducting a transaction[8].

In 2018, Huayun Tang, Yingying Jiao, and Butian Huang proposed a solution to the problem of classifying peer behavior in blockchain networks. Blockchain networks rely on a distributed set of peers or nodes that do not necessarily trust each other. It is crucial to identify unreliable peers to maintain network security and stability. To address this, the researchers introduced PeerClassifier, a deep-learning-based concept that accurately classifies peers based on their behavior patterns in terms of block validation and transaction processing[9]. Vana Kalogeraki and Dimitrios Gunopulos proposed a local search mechanism for retrieving information in peer-to-peer networks. This mechanism includes two search methods, namely Breadth First Search (BFS) and Intelligent Search. BFS is an extension of the Gnuttela protocol and is designed to minimize the number of searches in the network. Intelligent Search, on the other hand, uses the past behavior of the peer-to- peer network to improve scalability[10][11].

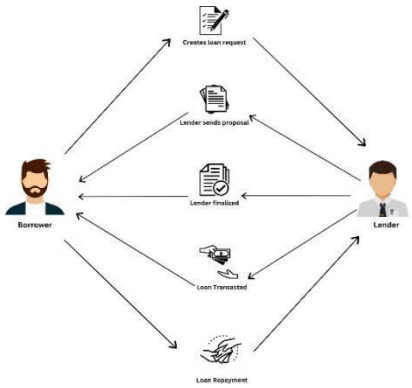
Ricardo Henriquez and Itai Cohen explore the payment transactions for providing mortgage finance between lenders and borrowers[12].

In their scholarly work published on December 8th, 2022, Wangcheng Yan and Wenjun Zhou delved into the challenges that arise in the P2P lending process, such as issues with the application platform and borrower collusion and herding. To address these concerns, they proposed integrating Blockchain technology with P2P lending processes, which can help reduce traditional finance originating fees and provide borrowers with optimal interest rates through the use of smart contracts. This innovative approach can serve as an alternative to traditional lending systems and has the potential to revolutionize the peer-to-peer lending process[13][14][15].

After reviewing various models proposed by researchers, we have developed a simplified peer- to-peer loan management model. This new model is highly efficient and secure, and it enables lenders to generate loans for borrowers using a secured file system accessed through the Interplanetary File System (IPFS). To ensure the loan is properly secured, we generate a mortgage address as a CID token. If the borrower is unable to repay the loan, the file will be auctioned off.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

III. METHODOLOGY



A. Workflow :

We have followed a workflow that has enabled us to establish a mutually beneficial Peer- to-Peer Loan management model between lenders and borrowers as described below:

Based on the figure presented above, it is evident that there are two parties involved in our Dapp - a borrower and a lender. The process can be compared to a request-response protocol, where the borrower requests a loan proposal. The lender then verifies the details provided by the borrower and decides whether or not to accept the request. If the request is accepted, the lender finalizes the proposal and transacts the loan payment as an acknowledgment to the borrower. The borrower then receives this acknowledgment and repays the loan amount later to the lender.

B. Model Building :

The proposed research model aims to simplify the loan generation process between the lender and borrower. The borrower creates a loan request, which the lender verifies against the mortgage. After verifying, the lender sends their proposal to the borrower, who can then accept the loan. If the loan is approved, it will be transacted to the borrower's account and can be repaid later. This platform has been designed to be user-friendly, secure, and transparent as it is built on the Ethereum blockchain. Researchers may employ various methodologies in their studies. In our case, we have chosen the mortgage-based algorithm principle as our methodology to secure the loan management process. This will help to prevent any fraudulent activities as the system is completely decentralized and transparent.

C. Technology Stack :

Ethereum and Solidity are used for generating smart contracts. Truffle is used for compiling the smart contract, and Ganache is used for deploying the Smart Contract. Metamask is used to access Ethereum-enabled Dapps. Infura serves as a cloud platform, and Web3 serves as the user interface with jQuery and JavaScript.

IV. IMPLEMENTATION

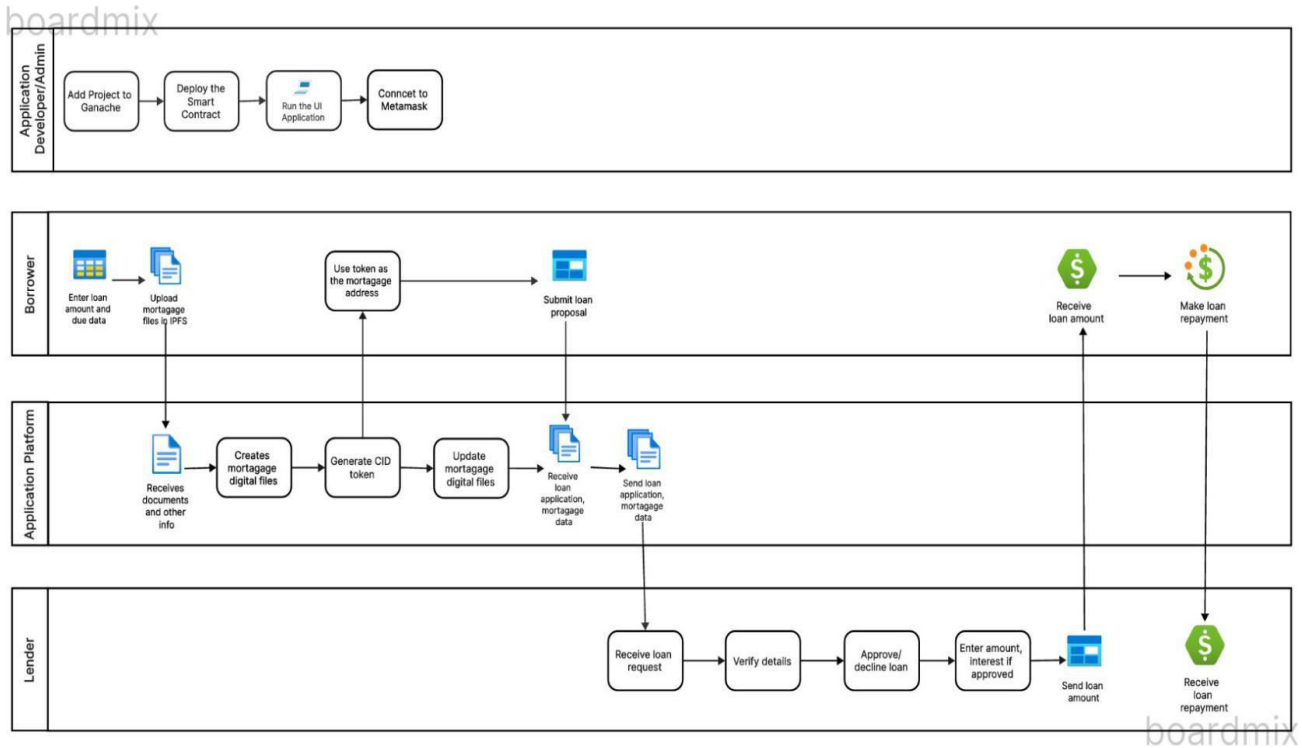
To implement the Loan Management Model, the first step is to gather the necessary data from different sources for developing a Decentralized Application (DApp). In this analysis, we used Solidity to create a Smart Contract at the backend, which enables the provision of loans on a peer-to-peer basis through our application platform. We used Infura as the cloud platform and Metamask as the crypto wallet for improved security. For compiling and deploying our project, we used

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

Truffle and Ganache. During the design process, we questioned the trust between the lender and the borrower. This led us to implement a mortgage-based algorithm that stores the asset, which is confidential from the borrower, in a distributed file storage called IPFS (Interplanetary File System). IPFS is a peer-to-peer file-sharing system that uses Content addressing to uniquely address the file in a global namespace. The following is the BPMN diagram for our application.

BPMN Diagram:

The Corresponding BPMN Diagram is shown below:



Business Process Modelling and Notation (BPMN) is a method used to analyze the flow of our application and it clearly describes each step of the designed application.

Application Stages

The BPMN diagram for our application is organized into four stages: Application Developer/Admin, Borrower, Application Platform, and Lender.

i. Application Developer/Admin:

In the first stage, the project's admin (who is also the developer) will add the source code file - which is the truffle config file - into Ganache. This will run the local blockchain in the "Add projects" section and compile the code using the following commands to build a smart contract:

1. truffle init
2. truffle test
3. truffle migrate --reset

Once the code is compiled, the admin should update the javascript file in the front-end source directory using the application binary interface code and the address that is present in the build files. After that, the admin should run the project and connect their 12-digit wallet with Metamask to perform transactions.

ii. Borrower:

From the Borrower's Perspective, we can see how borrowers can interact with the decentralized application (dapp) for
period:= Repayment period in months
calcMonthlyPayment(amount, rate, period)
M = amount * (rate * (1 + rate)^period) / ((1 + rate)^period - 1)

process payment(payment Amount)

remainingAmount:= amount - (payment amount - payment amount * rate)

checkLatePayment(dueDate, lastPaymentTime) return (block. timestamp > dueDate + grace-period)

IV. RESULT AND ANALYSIS

The proposed system is designed to provide loans on a peer-to-peer basis in a more user-friendly way. The system provides security using a mortgage- based algorithm, which is specified using the equation:borrowing loans.

The borrower will enter the desired loan amount and the due date for repayment to the lender. They can choose from multiple lenders based on their interest rates. Additionally, the borrower is required to enter the CID address of their mortgage which is stored in a distributed file storage system called IPFS.
Before submitting the loan proposal, the borrower needs to use tokens as collateral to verify the security and trustworthiness of the mortgage address.

iii. Application Platform :

During this stage, the mortgage documents will be received and a digital file will be created, which will generate a CID token.

Whenever a borrower submits a loan proposal, this stage deals with receiving the mortgage data for the loan application in its entirety. This data will then be used to perform the loan transaction.

iv. Lender :

When navigating to the lender section of our decentralized application, you can verify borrower data and send loan proposals to them at a favorable interest rate. Once the loan is approved, borrowers will need to repay the loan by the specified due date. Failure to do so will result in the mortgage being revoked and auctioned off immediately. Our user-friendly interface makes it easy to complete all of these steps in one place.

Algorithm for 30-day installment plan:

//Parameters

amount := Initial loan amount
rate := Monthly interest rate (decimal)

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

$$M = \frac{P * r * (1+r)n}{(1+r)n(-1)}$$

Where :

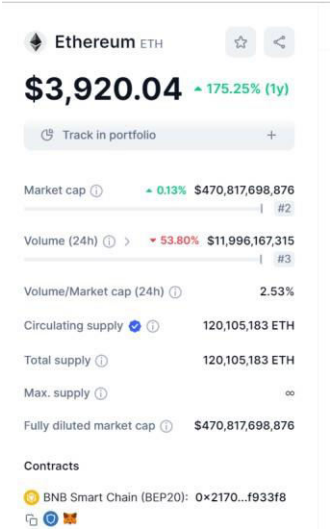
- M is the overall payment every month.
- P is the principal amount (i.e., the loan balance at an initial point).
- r is the interest rate, and
- n represents the no. of payments in total.

In our project, the formula $M = P * r * \frac{(1+r)n}{(1+r)n(-1)}$ serves as the basis for implementing security measures tied to mortgage principles. Here, 'M' represents the monthly payment, 'P' denotes the principal amount, 'r' signifies the interest rate, and 'n' indicates the number of payments in total. By integrating this formula, we establish a systematic approach to calculating monthly mortgage payments, ensuring clarity and predictability for borrowers. Leveraging IPFS for storing mortgage- related data adds a layer of security and decentralization to the process, safeguarding sensitive information while enhancing accessibility and transparency for all stakeholders involved. Through this implementation, we achieve a robust and secure framework for managing mortgage- related transactions within our project.

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

The lender provides the borrower with a loan based on simple interest.

In our project, we utilized Ethereum-based loan transfers between lenders and borrowers through Metamask.



The figure above illustrates the price of Ethereum in the market over the past year.

The graph below illustrates the average transaction fee of Ethereum for the past year.

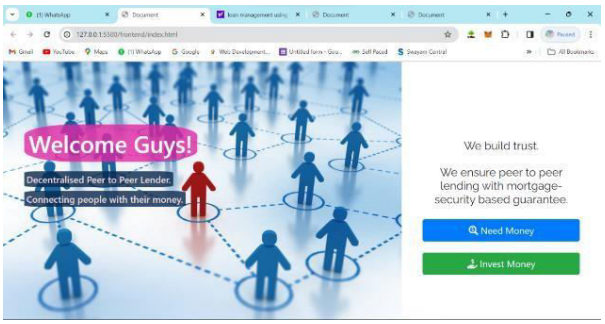
Our Dapp implementation offers the most efficient and reliable loan request process available. Users can count on our platform to provide a hassle-free experience when requesting a loan.

Analysis of Loan Management Model:

A.Access the front-end application

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

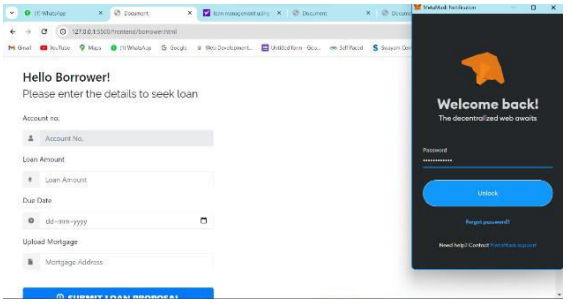
After deploying the smart contract and adding the project in Ganache, the first step is to enter into the dapp as shown below:



Click the "Need Money" button to borrow or the "Invest Money" button to lend.

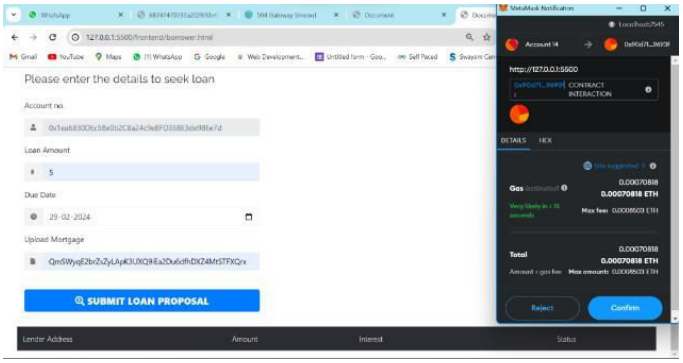
B. Connect to Metamask

When you open the borrower's page, you need to connect to Metamask to obtain the borrower's address as their account number.



C. Enter the details for the Loan proposal:

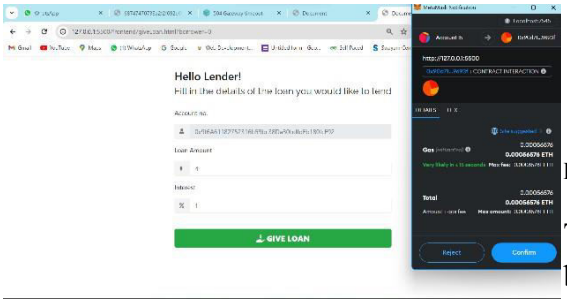
To submit the loan proposal, you must enter the loan amount. For example, you can type "5" to indicate an amount of 5 and due date for payment by the borrower. Additionally, you need to enter the CID generated for mortgage through IPFS.

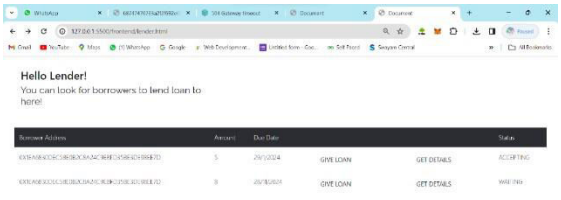


ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

D. Enter the details on the Lender Side :

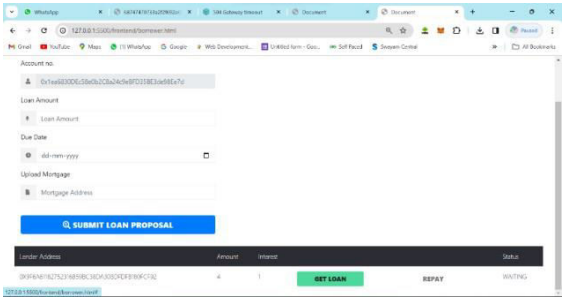
The lender must verify the borrower's details by clicking the "Get Details" button. Once verified, the lender can then enter the loan amount and interest rate to provide a loan to the borrower.





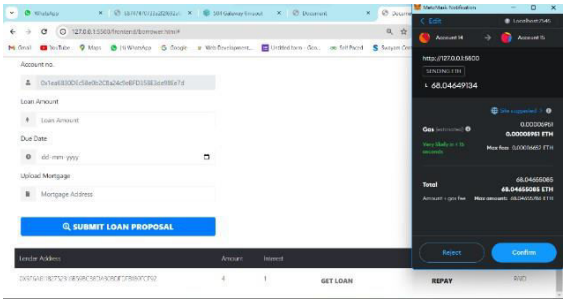
E. Accept the Loan :

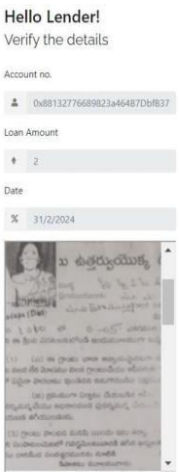
The borrower must click the "Get Loan" button to receive payment from MetaMask.



F. Repay the Loan :

The borrower must repay the loan and interest before the due date.





ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023

V. CONCLUSION

This paper presents the development of a decentralized peer-to-peer lending system that operates in a blockchain ecosystem. The system aims to provide efficient payment processing, fair interest rates, and time-saving capabilities. It allows for complete transparency by directly connecting borrowers to lenders without the need for any intermediary. The use of blockchain technology makes the lending process faster than traditional methods and immutable, which ensures that once the interest rate is set, it cannot be altered later. Moreover, in case of loan repayment, blockchain facilitates lenders to take prompt and efficient action on the mortgage submitted by the borrower.

Furthermore, the algorithm model based on loan management and mortgage can be applied to enhance security and transaction history. It is also possible to strengthen borrower authentication and transaction history between the lender and the borrower in the future.

REFERENCES :

[1] Betül Kaplan, Vahit Ferhan Benli & Elçin Aykaç Alp [March 4, 2023]- Blockchain Based Decentralized Lending Protocols: A Return Analysis Between S&P 500 and DeFi Assets(JOEEP).

[2] Arikumar K S,1, Deepak Kumar A, GowthamC, SahayaBeniPrathibac a,1, - Decentralized Loan Management Application Using Smart Contracts on Block Chain © 2021 open access by IOS Press.

[3] Nilo Legowo, Nubli Hawari, Taruly Karlina, Eric Tanuwijaya, Kanda Mahendra-6 Sept 2023- Design Smart Contract Based on Blockchain for Peer-to-Peer Lending Platform 2023 10th International Conference on ICT for Smart Society (ICISS).

[4] A. Jha, Shivani Dubey, Harshitha U Kumar-15 Mar 2023- Transaction System Based on Blockchain Technology using Smart Contract- International Journal Of Scientific Research In Engineering And Management.

[5] Franklin Allen and Anthony M. Santomero. The theory of financial intermediation. Journal of Banking and Finance, 21(11-12):1461–1485, 1998.

[6] Hegadi R, Akella S, Reddy K and Kumar C P. (2023). Analyzing and Mitigating Common Vulnerabilities in Smart Contracts in Web3 Ecosystem: A Comprehensive Study 2023 IEEE 2nd International Conference on Data, Decision and Systems (ICDDS).

[7] Zeng, X., Hao, N., Zheng, J., & Xu, X. (2019).
A consortium blockchain paradigm on hyper ledger-based peer-to-peer lending system. China Communications, 16, 38-50

[8] Taotao Wang, Chonghe Zhao, Qing Yang, Shengli Zhang-Ethna: Analyzing the Underlying Peer-to-Peer Network of Ethereum Blockchain- 2021 Journal IEEE Transactions on Network Science and Engineering

[9] Huayun Tang, Yingying Jiao, Butian Huang -
20 Nov 2018-Learning to Classify Blockchain Peers According to Their Behavior Sequences-
IEEE Access

[10] A Local Search Mechanism for Peer-to-Peer Networks- Vana Kalogeraki and Dimitrios Gunopulos.

[11] Xu, J., and Callan, J. Effective retrieval with distributed collections. Proc. of the 21st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (Melbourne, Australia, 1998), pp. 112–120.

[12] Henriquez, Ricardo and cohen, itai and Bittan, Netanel and Tulbassiyev, Kanat, Blockchain and Business Model Innovation: Designing a P2P Mortgage Lending System (April 14, 2019).

[13] Wangcheng Yan & Wenjun Zhou-Is blockchain a cure for peer-to-peer lending -8 Dec 2022.

[14] Harvey, C.R., Ramachandran, A. and Santoro, J., (2021), DeFi and the Future of Finance. John Wiley & Sons.

[15] Zetzsche, D. A., Arner, D. W., and Buckley,
R. P., (2020), Decentralized finance. Journal of Financial Regulation, 6(2), 172–203.

[16] Mark Andrew. The Changing Route of Owner Occupation: The Impact of Student Debt. Housing Studies, 25(1):39–62, 2010.

[17] Juan Benet. IPFS - Content Addressed, Versioned, P2P File System. CoRR, abs/1407.3561, 2014.
C. Baden-Fuller and M. S. Morgan. Business models as models. Long Range Planning, 43(2- 3):156–171, 2010.

[18] C. Lv, P. Cao, E. Cohen, K. Li, and S. Shenker. Search and replication in unstructured peer-to-peer networks. In ICS, 2002.

[19] Transaction System Based on Blockchain Technology using Smart Contract-A. Jha, Shivani Dubey, Harshitha U Kumar-15 Mar 2023

Financial investment trust mechanism based on smart contract-W. Xiong, Danping Wan28 Jul 2023.

[20] Smart Contracts and Decentralized Finance- Kose John, L. Kogan, Fahad Saleh-31 Jul 2023 Journal: SSRN Electronic Journal

[21] A Detailed Study of Blockchain and DApps- Sourav Verma, Sonali Dash, Ankita Joshi + 1 more authors-6 Oct 2022-Journal:2022 International Conference on Cyber Resilience (ICCR).

Sven C. Berger and F. Gleisner. Emergence of Financial Intermediaries in Electronic Markets: The Case of Online P2P Lending. Business Research, 2(1):39–65, 2009

ISSN PRINT 2319 1775 Online 2320 7876
 UGC CARE Listed (Group -I) Journal Volume 12, Iss 07, 2023