Design of "Flash Loan" under Decentralized System

Xiaolei Ding[1,*], Lingwei Zhang[2], Shujuan Sun[3]

Corresponding author: Xiaolei Ding

{klausding@zufe.edu.cn[1,*], 1195494097@qq.com[2], 3041184396@qq.com[3]}

College of Finance Zhejiang University of Finance & Economics, Hangzhou, China

Abstract: In recent years, the decentralization system based on blockchain has ushered in rapid development, which presents the emerging trend of replacing the traditional financial system. The "flash loan," as a more experimental decentralized lending model, can realize capital loans without collateral. Influenced by a host of unfavorable factors represented by the economic downturn, small and micro enterprises in China are progressively facing the increasingly prominent problem of "difficulty in obtaining loans." In this context, although some banks in China have launched "flash loan" products, numerous reasons, such as high thresholds and strict audits, still make it difficult for small and micro enterprises to become their target audience. Hence, this paper intends to improve the design of the existing "flash loan" products, focusing on upgrading the related data management system and risk prevention system. Additionally, by constructing the form of virtual banks, on the background data management system with high confidentiality and the operation platform with high-risk control intensity, this research distributes the background reserve funds to virtual customers in the form of imitating regular banks and ensures the independence of the supply chain when it is applied to regular banks instead of virtual banks, thus providing a valuable reference for the promotion of decentralized lending model.

Keywords: Decentralized System; Blockchain; "Flash Loan"; Capital Loan; Virtual Bank

1 Introduction

The development of small and micro enterprises in China is closely connected with the steady progress of the national economy. Nevertheless, under the background of the continuous spread of major global public safety events and the drastic turbulence of the economic environment, it is difficult for small and micro enterprises to obtain appropriate financing to sustain their operation and development due to various restricted conditions such as small business scale, weak mortgage, and pledge ability. Meanwhile, under the centralized banking system, the vast majority of commercial banks will actively adopt risk control measures appropriate to their conditions based on the requirements of the central bank, rather than lending their idle funds to small and micro enterprises with low credit ratings, which makes most small and micro enterprises unable to obtain direct financing through banks[1].

In this regard, the emergence and vigorous development of the decentralized system based on the blockchain provides a brand-new idea to solve the above dilemma. More specifically, the blockchain-based "flash loan" can not only serve as the core technology to build a digital supply chain through the integration of financial technology and traditional supply chain[2], but also

ITEI 2022, December 23-25, Harbin, People's Republic of China

DOI 10.4108/eai.23-12-2022.2329208

broaden the financing channels of upstream, downstream, and upstream enterprises in the supply chain, lower their financing threshold and improve their financing efficiency, thus giving a new idea to the capital flow[3]. Moreover, under the premise of meeting the regulatory requirements, this model can be based on a well-checked contract algorithm to carry out more financial transactions, such as leverage hedging, liquidation, etc[4].

2 Functional Module and Technology Development Scheme of "Flash Loan"

Conceptually, a "flash loan" is a model in which both borrowing and repayment are made simultaneously without any mortgage of assets, with only a handling fee paid in a block transaction. With this product, users can use the borrowed assets for the agreed channels after completing the borrowing. At the end of the transaction, the user can repay the borrowed money and handling fee in time; otherwise, the transaction will be rolled back. By definition, only contractual transactions that are ultimately repayable can be further executed.

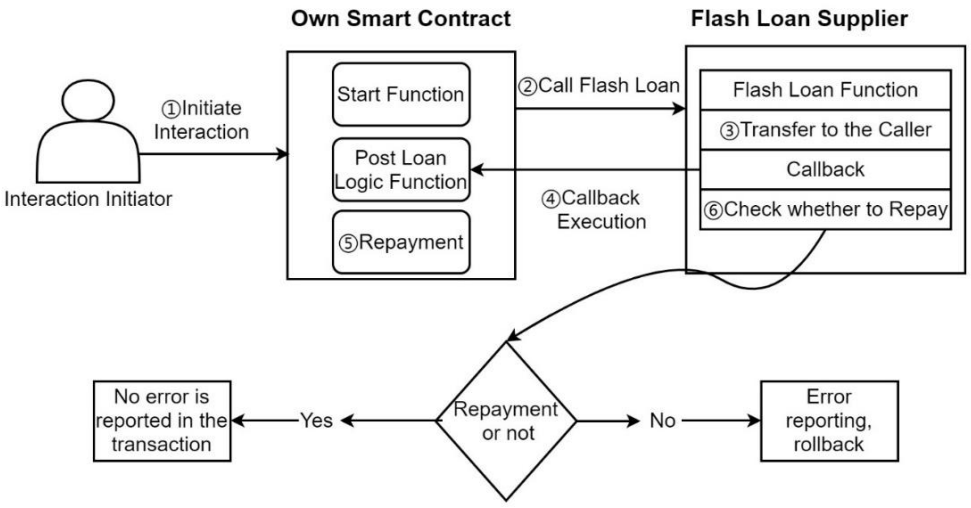

Fig. 1. Schematic Diagram of "Flash Loan"

2.1 Functional Module

Blockchain Application Module

At present, corporate loans in China are based on credit guarantees, whereas third-party intermediaries play an important role in the audit of transaction credit. This situation has led to the financial sector facing the following pain points at this stage: a) it is difficult to verify the authenticity of assets and transaction information, with prominent information asymmetry exposed; b) inefficiencies resulting from complex cross-institutional financial transaction business processes; c) cross-border operation of Internet finance has posed corresponding challenges to the traditional centralized risk management and supervision model.

Against this background, the emergence of blockchain has endowed numerous scenarios in the traditional Internet where online convergence is difficult due to trust granularity or trust cost issues with the possibility of available convergence innovation. Additionally, the tamper-resistant and traceable nature of blockchain makes it possible to fully record the full lifecycle of data in a trusted data flow environment built by blockchain.

Smart Contract Module

After building the digital assets on the blockchain, it is imperative to manage the data assets. Smart contract based on blockchain technology is the key to data asset management, with their security related to the security of users' digital assets on the blockchain platform[5]. Smart contracts have a life cycle covering four processes, encompassing the generation, release, execution, and realization of contracts.

To put it concretely, during the process of contract generation, contract specification and contract verification play a vital role, in which the former is agreed upon by domain experts, while the latter needs to be carried out on virtual machines. Both of them must ensure consistency between the contract text and the code. Essentially, the contract release process is similar to the transaction release in BTC, which requires the consensus and verification of multiple nodes. In the process of contract execution based on "event triggering", the smart contract will periodically traverse the state machine and trigger conditions of each contract, thereby pushing the contracts that meet the trigger conditions to the verification queue. Furthermore, while changing the status (such as allocation and transfer) and value of digital objects, the contract realization process can realize the programming and deployment of objects on the blockchain by giving them digital characteristics.

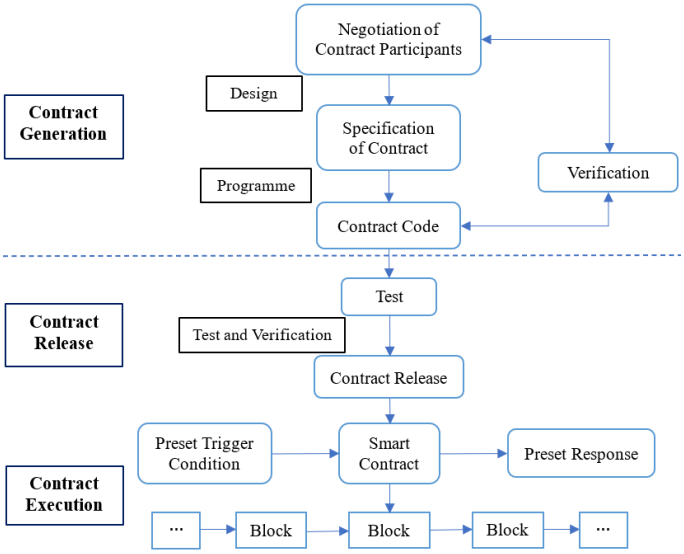

Fig. 2. Life Cycle of Smart Contracts

Visualization Module

Once the construction of the bottom-layer and back-end systems is completed, the underlying applications will be more in favor of the developer personnel model, but the systems required for the "flash loan" are mainly for ordinary personnel. In this case, it only needs to see the current status of the whole blockchain network and the current transaction situation, or inquire about the specific situation of a transaction, etc. Therefore, complementary structures can be built for the blockchain browser, thus presenting the content with greater attention or importance in a visual form.

2.2 Technology Development Scheme

Systemic Technology

The back-end management platform of the virtual bank is built in FISCO BCOS, using the virtual digital currency platform as the bottom layer. Given that the platform's audience is not professionals, an easy-to-understand front-end platform containing registration, login, and operating process pages for customers can be built. Furthermore, the design of the business layer can be carried out, including the setting of a host of contents such as the bottom chain administrator, system administrator, institutional node user, regular user, etc., of the blockchain, as well as the code of the implementation rules that can be triggered and executed set on the blockchain in the form of a smart contract. Moreover, the other contents of building the platform also incorporate authorization design, SDK use, micro-service design, supporting security audit, placing-order encryption scheme, etc. At last, the connection and interworking between each other will be further implemented according to the interaction platform.

Digital Currency Layer

While downloading the source code of the required blockchain system from Git, it is necessary to prepare the corresponding compilation environment and then start configuring the environment. Once the environment is configured, the associated construction can then be executed. Regarding the downloaded digital currency, this paper transforms it into the required currency through the related way represented by parameter adjustment. The same approach can be used to build virtual banks after building the digital currency. Nevertheless, it is strongly recommended to maintain the mobility of the virtual bank during its construction, i.e., to ensure that the virtual bank can eventually be removed and the entire process will not be affected when it is applied to the real bank.

Visualization Layer

A series of tools, such as Java Web, can be used to build visual pages, making the landing page, registration page, and operation flow page of the "flash loan" business available for display. After the user completes the operation process, the user information will reach the business layer through the interactive platform, thus judging how the relevant execution starts within a block. When the execution is finished, the user can see the corresponding results.

Block Layer

All transaction information eventually forms a structured account book, which is organized by the nodes of the blockchain in a certain way and at certain time intervals, and then stored in the

nodes of the blockchain. This structure that can be used to store transaction information is a block[6]. In addition to the transaction information, the block also stores some additional information to ensure the integrity and reliability of the transaction data. The block data is structured as follows:

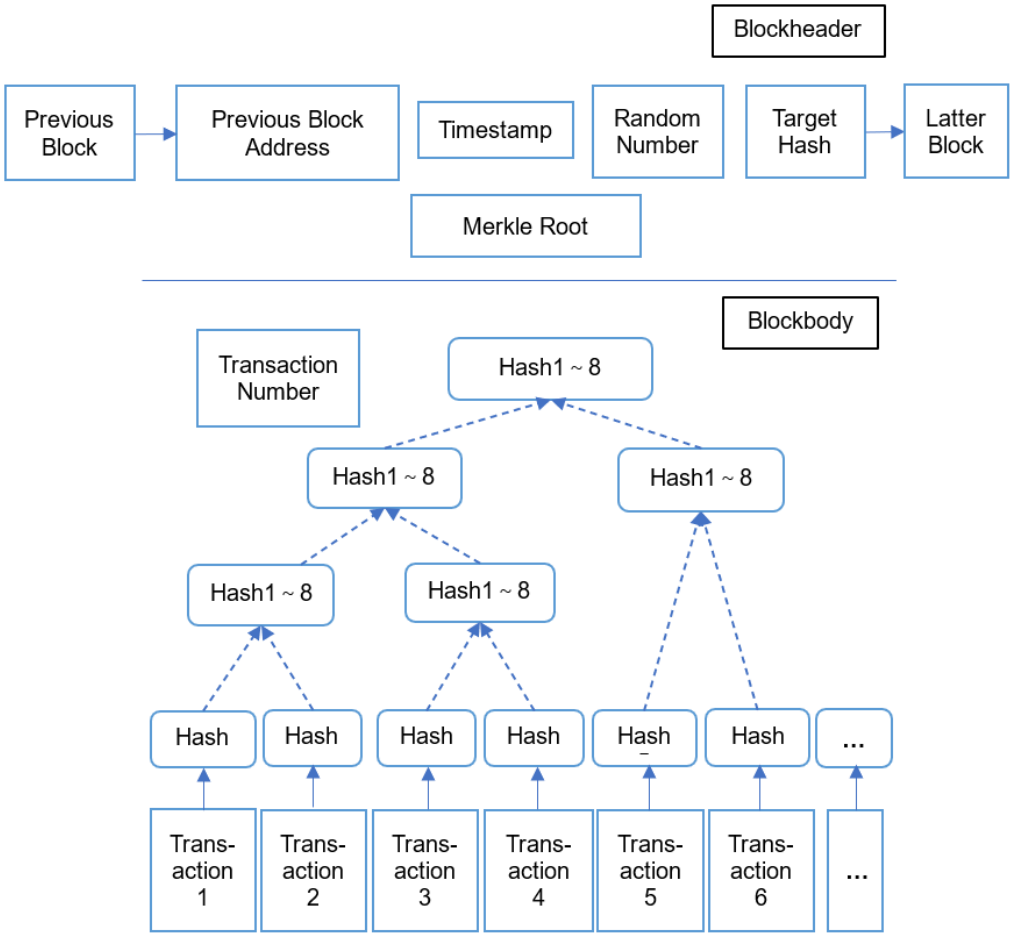

Fig. 3. Block Data Structure

Smart Contract Layer

This paper mainly applies the smart contract of Ethernet and Solidity language to deploy the written code to the blockchain code of the service layer[7]. Once deployed, the code will be stored on each node in the form of bytecodes. When a user requests to call a function, the call request will be included in the transaction and packaged on a block. Once the whole network has reached a consensus on the block, it means that the call is legal. In turn, EVM will call bytecode, which is responsible for accessing the bottom-layer state variables. If a bug occurs midway, a new smart contract must be deployed.

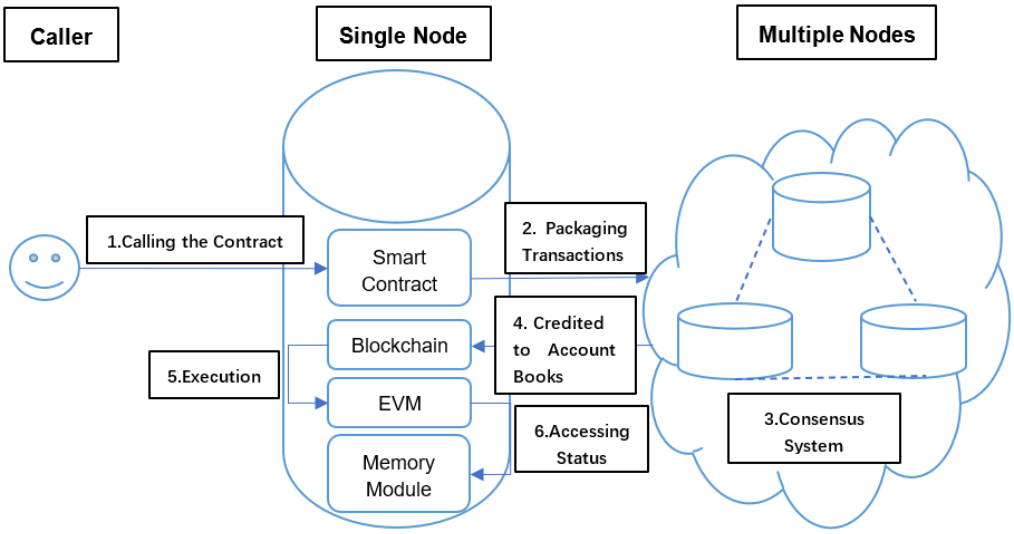

Fig. 4. Application Principle of Smart Contract

3 "Flash Loan" Solution to the Problem of "Difficulty in Obtaining Loan"

On the whole, the "Flash Loan" includes a wider range of enterprises and a lower entry threshold, whereby participants only need to set their loan-related parameters and other information, such as collection address and loan amount, in the process of carrying out the lending business on the virtual platform. At the beginning of the operation, not only will the procedure check the stock of the pool and the lending behavior, but it will also check the proper behavior of the lenders when they repay the funds, such as whether the loans are repayable with interest or not. If during the inspection process, it finds that the lender's repayment exceeds one block time or does not belong to the principal interest-bearing repayment behavior, it further will roll back all operations.

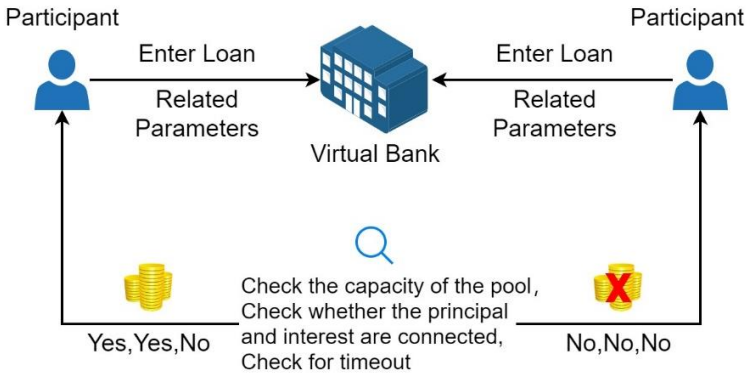

Fig. 5. Operation Flow of "Flash Loan"

3.1 Simple and Convenient Borrowing-related Interaction

The borrower only needs to copy and input the lender's smart contract address to the sender and input its blockchain address on the owner side to realize the interaction of loan contracts. Further, the borrower can obtain the corresponding funds from the lender in a short time by simply inputting the amount of the borrowing requested by the borrower. When the due date of repayment comes, the platform will automatically calculate the interest and principal payable by the borrower, sending a short message to remind the borrower to repay the relevant borrowing funds in a timely manner. If the borrower fails to repay in time, the platform will directly roll back and cancel the transaction of the loan.

3.2 Higher Safety

The platform code applies a callback function that protects the lender's interests in a timely manner. When the borrower enters the repayment amount, the platform will automatically check whether the specific amount is the same as the lending amount after deducting interest and corresponding handling fees. If the platform finds that the two are different and the borrower fails to pay the remaining amount and handling fee and interest in a timely manner, it will immediately implement the rollback mechanism and interrupt any transaction related to the borrowing amount on the digital currency electronic payment (DC/EP henceforth) information platform based on the wallet address of its blockchain, with the borrowing amount returned to the lender in full.

3.3 Faster Application Speed

In China, the future safe and reliable DC/EP trading platform will be further built and improved, on which anyone can register with a real name to obtain a DC/EP wallet. Benefiting from this, the "flash loan" platform is in a position to screen user information and calculate their credit qualifications and loan risks based on the address of the blockchain wallet, thereby completing the approval within minutes at the earliest. On the other hand, the platform will detect the amount in the smart contract address created by the lender. Once it meets the platform's minimum access requirements, the request can be quickly granted to facilitate rapid interaction between lenders and borrowers within the platform.

3.4 Accessibility of Loans of Any Amount Without Collateral

With blockchain technology as the core, the "flash loan" itself has a high degree of security and visualization, and all participants' transactions can be queried. Concurrently, not only can the rollback times of the wallet address reflect the credit qualification of the wallet owner, but also the lender's funds will automatically return to the previously-set smart contract after the rollback. Consequently, the lender does not need the borrower to provide any collateral as his or her credit guarantee. On the same note, the security and transparency of the blockchain are conducive to ensuring the trust of both borrowers and lenders, and increasing the transaction frequency, intending to play the positive role of idle funds in social development more effectively.

4 Conclusion

As outlined above, based on the form of building a decentralized virtual bank and a "flash loan" financing platform, this paper discusses the implementation mode and value significance of "flash loan." In particular, through the integration of the digital currency layer, the visualization layer, as well as the block layer, the platform improves the authenticity and effectiveness of the asset transaction information, thus providing the interactive parties with visual credit qualifications. More importantly, the construction of the "flash loan" platform is beneficial to effectively alleviate the financing difficulties faced by small and micro enterprises, and promote the flow of social idle capital, thus ultimately further expanding the application scope of DC/EP.

References

[1]X. Yang, "Blockchain-Based Supply Chain Finance Design Pattern," 2021 13th International Conference on Intelligent Human-Machine Systems and Cybernetics (IHMSC) pp. 200-203, 2021.

[2] C. Y. Kim and K. Lee "Risk management to cryptocurrency exchange and investors guidelines to prevent potential threats" Proc. Int. Conf. Platform Technol. Service (PlatCon) pp. 1-6, 2018.

[3] L. Zhou, X. Y. Zhong, J. Liu and M. J. Xia, "Game Analysis of "Blockchain+Supply Chain Finance" Mode in Empowering Small and Micro Enterprises' Financing," 2021 International Conference on Computer, Blockchain and Financial Development (CBFD) pp. 396-400, 2021.

[4] K. Qin, L. Zhou and A. Gervais, "Quantifying Blockchain Extractable Value: How dark is the forest?," 2022 IEEE Symposium on Security and Privacy (SP) pp. 198-214, 2022.

[5] H. Tian et al., "Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3928-3941, 2021.

[6] A. Zamyatin D. Harz J. Lind P. Panayiotou A. Gervais and W. Knottenbelt "XCLAIM: Trustless interoperable cryptocurrency-backed assets" Proc. IEEE Symp. Secur. Privacy (S&P) pp. 193-210, 2019.

[7] L. Lys, A. Micoulet and M. Potop-Butucaru, "Atomic Swapping Bitcoins and Ethers," 2019 38th Symposium on Reliable Distributed Systems (SRDS) pp. 372-3722, 2019.

[8] S. Badruddoja, R. Dantu, Y. He, K. Upadhayay and M. Thompson, "Making Smart Contracts Smarter," 2021 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) pp. 1-3, 2021.

[9] C. Jiang and C. Ru, "Application of Blockchain Technology in Supply Chain Finance," 2020 5th International Conference on Mechanical, Control and Computer Engineering (ICMCCE) pp. 1342-1345, 2020.

[10]W. Sun, "Application of Blockchain Technology in the Supply Chain Finance," 2022 7th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA) pp. 205-209, 2022.