How a Self-Sovereign Identity prevents overcollateralisation in Decentralised Finance

Harmen Kroon
TU Delft
H.M.Kroon@student.tudelft.nl

Abstract

1 Introduction

The field of Self-Sovereign Identity (SSI) is an increasingly important topic considering the increased demand of digital identification. Previous research has been done on multiple aspects which form the basis of establishing a digital identity; Security, Controllability and Portability [1].

Furthermore, a verifiable digital identity is a required feature for financial services that are operating in blockchain-based cryptocurrencies [2]. As decentralised finance is being developed further and with its popularity rising, the liquidity of digital markets have reached 25 billion USD [4] and monthly trading volumes have passed the trillion dollar mark in January 2021 [3].

The increase of adoption enlarges the demand for financial services that require more than is possible through the pseudonymous on-chain asset exchange. Financial capabilities of the cryptocurrency ecosystem are continuously extended through stacking of protocols and use of smart contracts to establish a decentralised autonomous organisation (DAO).

The basis of finance is founded by lending and borrowing, which has also been applied to the decentralized finance through Loanable Fund Markets [5, 6, 7]. These markets offer either flash loans or longer term collateralised loans. Flash loans are secured as a single transaction which can be reverted in case the loan defaults, whereas longer term loans are secured by fully collateralising the loan. This means that the value of a loan plus interest is needed to insure counterparty risk, in the form of defaulting or fluctations of asset value. The insurance that a borrower repays a loan is paramount to a healthy lending market. DeFi is anonymous or pseudonymous in nature and therefore lacks the background checking systems that are used by traditional lending companies.

A Self-Sovereign Identity with trusted attestations opens the door to a multitude of digital financial services while servicing as a big stick in order to transparently manage counterparty risk [2]. Such an SSI can safely and securely store a financial reputation score, much like a traditional credit score. Research on collateral reduction mechanisms have been done by [8] and [9], but is largely unexplored.

2 Problem Description

The main research question this paper tries to answer is as follows:

How can a Self-Sovereign Identity based reputation system dissuade overcollatoralisation in decentralised lending protocols?

In order to answer this question the following topics will be discussed in this paper. Firstly, the established peer to peer lending protocols and their reputation mechanisms are reviewed. Secondly, the most common credit score system (FICO[10]) and proposed adaptations for decentralized finance are discussed. Thirdly, an implementation is proposed based on these findings using a blockchain based SSI solution and both a credit score claim and a credit history evaluation. Finally, an experiment based on the proposed implementation is conducted and reviewed.

3 Lending protocols and their risk assessment

Flash loans are single transaction loans that require no collateral, but circumvent the risk by revoking the transaction if the borrower does not pay back.

Longer term loans in DeFi commonly require a collateral in order to secure the loan from risk of defaulting. A lending protocol is build on the assumption of self-centered anonymous financial agents that only act in their own benefit. Meaning that when it is financially favourable to default on a loan and take the loss on the collateral, an agent will take that approach. Due to volatility of cryptomarkets the value of a collateral can swing wide over the course of a loan. To prevent pulling out of a loan from happening a loan is always not just fully collateralized, but overcollateralized. In the case that the value of the provided collateral falls below the value of the loan a liquidation procedure ensures that capital is retrieved by selling of the collateral.

provide number/percentage, source

3.1 Overcollateralization

The biggest DeFi lending markets, like Aave, Maker and Compound, all require overcollateralization of loans and as such have set the standard. Issues with the requirement of collateral are the limited use cases and high barrier of entry. The use cases are limited to speculating on different crypto assets (80%) or financing DeFi projects. The barrier of entry is a huge repellent for widespread use of DeFi lending, as smaller speculators or non-crypto holders are barred from using theses services.

source

3.2 Uncollateralization

Efforts have been made to reduce collateral or even provide uncollateralized loans. Many collateral reduction mechanisms are based on building up a lending history and slowly reducing required collateral up to 100% (Balance [8], Promise [9]). The real strides are made in protocols that strive for lending with no collateral at all, similar to traditional lending. This requires a form of trust in the borrower, counter to that of the collateral provided trust used in secured loans.

TrueFi started out with a KYB approach and used "a whitelist of carefully selected funds vetted by the TrustToken team." and evolved into a credit rating system in v3. The TrueFi creditworthiness score (from 0 to 255) is based on five factors, Company Background, Repayment History, Operating & Trading History, Assets Under Management, Credit Metrics .

https://blog.trusttoke
truefi-the-defi-protocol-for-uncollateralized-lending-9bfd6594a48

https://blog.trusttoke
v3-credit-model-new-asset-support-a7cf73a37270

Aave has a feature called credit delegation that allows depositors to delegate borrowing power to other users. A delegator is encouraged to set up a legally binding contract with the delegatee outside of the protocol through a legal institution or through a smart contract like OpenLaw. .

https://www.coindesk
unsecured-borrowing-defi,
https://www.coindesk
launches-first-legal-dao-for-distributed-vc-investments

4 Identity management in Lending protocols

- MYKEY uses smart contracts to facilitate a consistent crosschain ID.

https://mykey.org/key

- Sidetree is a layer 2 protocol that enables a scalable W3C Decentralized Identifier anchored to any existing decentralized system.
- Bloom is an SSI solution with a build in credit score

https://w3c.github.io/did-core/

https://identity.foundation/sidetree/spec/

bloom.co

Union is a protocol that allows users to set up their own lending service to borrowers they assign as being trusted.

5 Experimental Setup and Results

6 Responsible Research

7 Discussion

8 Conclusions and Future Work

References

[1] A. Tobin & D. Reed, The inevitable rise of Self-Sovereign Identity, White paper, 2017.

[2] C. Harwick & J. Caton, What's holding back blockchain finance? On the possibilities of decentralized autonomous finance, The Quarterly review of Economics and Finance, 2020.

[3] A. Brauneis, R. Mestel, R. Riordan & E. Theissen, How to measure the liquidity of cryptocurrency markets?, Journal of Banking & Finance, 2021.

[4] S. Werner et al., Systemization of Knowledge: Decentralized Finance (DeFi), Imperial College London, 2021

[5] AAVE protocol whitepaper, AAVE, 2021

[6] R. Leshner & G. Hayes, Compound: The Money Market Protocol, Whitepaper, 2019

[7] M. Bartoletti, J. Chiang & A. Lluch-Lafuente, Systemization of Knowledge: Lending pools in decentralized finance, 2020

[8] D. Harz et al., Balance: Dynamic Adjustment of cryptocurrency deposits, Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security, pp. 1485 1502, 2019

[9] D. Harz et al., Promise: Leveraging future gains for collateral reduction, IACR Cryptol, vol. 2020, p. 532, 2020

[10] N. Jain, T. Agrawal, P. Goyal, V. Hassija, A Blockchain-Based distributed network for Secure Credit Scoring, 10‘9 5th International Conference on Signal Processing, Computing and Control (ISPCC), 2019, pp. 306-312, doi: 10.1109/ISPCC48220.2019.8988510