Liquidity risks in the decentralized finance protocol Aave

Selim Cirikka , Oğuzhan Ersoy , Zekeriya Erkin
TU Delft

Abstract

Protocols for Loanable Funds (PLFs) are lending protocols that exist in the Decentralized Finance (DeFi) ecosystem. They provide users the opportunity of lending and borrowing of cryptocurrencies. The economic model used to ensure liquidity in these protocols are variable parameters and incentives to reach an optimal equilibrium and overcollateralization to make trust between participants unnecessary. However, the design of this protocol can show signs of illiquidity in which the safeguards of the protocol do not function as expected in times of an unfavourable market.

In this paper, the liquidity of Aave, one of the biggest PLFs, is empirically examined. A game theoretical model is used to analyze the behaviour of participants to the various incentives in the protocol. Firstly, the potential points of failure in case of a bear market with a volatile asset are evaluated. Secondly, the mechanisms for mitigation of illiquidity in the Aave protocol are examined. Ultimately, diversification of the assets in the safety module is proposed to increase the efficiency of the safety module and therefore decrease the risk of illiquidity in the protocol.

1 Introduction

With the increase of popularity in decentralized finance (DeFi) protocols, the protocols which offer lending services stand out as the most prominent protocols. They have locked in the highest proportion of the value in the DeFi ecosystem with around $35B of the in total $46.19B [1]. These protocols, which henceforth will be noted as Protocols for Loanable Funds (PLFs), offer their participants the possibility of depositing their cryptocurrencies in exchange for interest. These deposited assets can subsequently be borrowed in exchange for interest. Some of the more notable examples of PLFs are Aave [2], Compound [3] and MakerDAO [4].

The possibility of offering these lending services in a decentralized way depends on two requirements. Firstly, the protocol has to guarantee the safety of the assets of a depositor in the trustless DeFi ecosystem. Secondly, incentives have to be created for participants to provide liquidity to the protocol. This economic framework, in which depositors are matched with borrowers, is different compared to how loaning is handled in the conventional way through banks, which does not match depositors with borrowers [5]–[7].

As a consequence, PLFs face, besides technical challenges [8]–[11], design challenges regarding incentives and agent behaviour [11]–[14]. PLFs have to design the protocol in such a way as to provide incentives to participants to provide liquidity. It has to do this while simultaneously having to safeguard the technical and economic safety of the protocol.

This design can, in adverse market situations, lead to depositors not being able to withdraw their assets and leaving the protocol illiquid [14]–[16]. It is therefore fundamental to gain a deeper understanding of the behaviour of agents and the mitigation in place against these periods of downward pressure. The research question that is answered in this work is thus: ”How can the inability of withdrawing caused by illiquidity be mitigated in the Aave protocol during a bear market with a volatile asset?”.

In this paper, firstly a game theoretic model is used to systematically study the potential liquidity risks that lay in the Aave protocol. Secondly, using the model, aggravating factors are pinpointed and a potential negative deflationary spiral is hypothesized. Finally, improvements on the mitigation in Aave are proposed.

Related work In [9], Werner et al. give a overview of DeFi in general. It provides the primitives seen in DeFi in conjunction with economic and technical security risks in DeFi. In [17], Amler et al. give a similar overview with the addition of the challenges that DeFi face. Challenges such as security, scalability, privacy and regulation. In [6], Gudgeon et al. give a introduction on PLFs and look into the interest rates of Compound, Aave and dYdX and their behaviour since inception. Furthermore, the efficiency and interconnection of these markets is investigated. Bartoletti et al. [18] give a formal model of PLFs and a discussion on the role of PLFs in DeFi combined with potential attack vectors. In [14], Gudgeon et al. look into governance attacks on PLFs through the use of flash loans and stress test a hypothetical PLF showcasing the subsequent solvency. Kao et al. [13] analyse the market risk of participants of the Compound protocol through the use of simulations and a model. Gauntlet [19] analyse the market risk of participants in Aave in a similiar manner as Kao et al.

Our contributions can be summarized as:

- A game theoretic model of agent behaviour in PLFs (used on Aave) is given.
- A theoretical deflationary spiral is presented.
- An empirical analysis of the safety module in Aave.

Paper organization The rest of this paper is organized in the following manner. Section 2 gives the necessary background information on DeFi and Aave. Section 3 present a game theoretic model. Section 4 uses this model to illustrate a potential deflationary spiral. Section 5 showcases the results of empirical analysis of historical data. Lastly, Section 6 will give a summary and conclusion.

2 Background

2.1 Decentralized Finance

Decentralized finance (DeFi) is a form of finance which recently has gained steam, with a current total value locked of $46.19B at the time of writing [1]. It is a form of finance which does not require any intermediaries but instead makes use of smart contracts combined with blockchain technology.

Consequently, several traditional financial services (such as lending, margin trading, derivatives, exchanges) and experimental financial services (such as flash loans) can be offered in a decentral, trustless and transparent way in which anyone can participate [17]. These properties combined with the fact that these services are easy to use, low threshold services with potentially higher returns than classical institutions, might explain this sudden growth of DeFi services [20].

It is, however, still a technology in the infant stage. Finding security exploits is therefore almost an inevitability. Verily, DeFi has faced several attacks already [21]. These attacks have varied from coding errors [22], [23], to attacks which make use of the complex interconnection between the various DeFi services [8]. Besides malignant intents, the behaviour of agents in the protocol to a change in the protocol itself can also sometimes lead to unexpected consequences, such as stablecoin peg deviations and liquidations. [12]. A recent systematic overview of DeFi is given in [9].

2.2 Protocol for Loanable Funds

Protocol for Loanable Funds (PLFs) are protocols that facilitate lending between participants. They are a subset of the financial services offered in the DeFi ecosystem.

PLFs use pools to act as the lending market for participants, as opposed to keeping track of an order book. In these pools participants can deposit their assets, earning interest, or can borrow out of this pool, paying interest. These pools are implemented as smart contracts, which are Turing complete programs running on the Ethereum blockchain.

Smart contracts provide the link between depositor and borrower, however it does not provide safety for loan defaults. In conventional finance, a borrower provides collateral to ensure repayment of a loan in case of a default. Furthermore, the identity of the borrower is known which also is an incentive for the borrower to repay their debt. The identity of participants on the Ethereum blockchain is pseudonymous. As such, the safety is provided through overcollateralization. This entails that borrowers can merely borrow less than their deposited assets. In the scenario that the collateral of a borrower passes a threshold nearing an undercollateralized position, it will be liquidated by participants in the protocol for a premium. Intrinsically, this leads to debts being secured in case of loan defaults.

Besides safeguards against default, the protocol has to attract liquidity. In this steadily growing DeFi ecosystem, the protocols compete for liquidity. Therefore the protocols have to provide incentives for participants, in the form of competitive interest rates, governance tokens or special features such as flash loans or stable interest rates.

2.3 Aave

Aave is currently the PLF with the highest amount of locked assets in the DeFi ecosystem with a total of $8.62B [1]. It has seen a tremendous growth compared to one year ago, in which it had around $70M locked in the protocol. It provides pools for several assets, of which the biggest ones by far are the stablecoins USDC, DAI and USDT [24].

Every pool has its own parameters which one can fine-tune as to attract participants [25]. Liquidation threshold is one of the important parameters per pool. It signifies the point at which loans become undercollateralized. For example, a liquidation threshold of 80% signifies that if the loan were to rise above 80% of the value of the collateral deposited, that it will be available to be liquidated.

The interest rate is the main driver of behaviour. If the pool has very few borrowers but a high amount of deposits, then the borrow interest rate should be relatively low in comparison to the deposit interest rate. Vice versa, if the pool's liquidity is very scarce then depositing is encouraged through a high deposit interest rate and a high borrow interest rate. In essence, the protocol is trying to create an optimal utilization of the funds. The implementation of this idea is realized through a kinked interest rate [6], [26]. In the current implementation, the variable borrow rate vb_i is given by:

$$vb_i = \begin{cases} R_0 + \frac{U}{U_{optimal}} \cdot R_{slope1}, & \text{if } U < U_{optimal} \\ R_0 + R_{slope1} + \\ \frac{U - U_{optimal}}{1 - U_{optimal}} \cdot R_{slope2}, & \text{if } U > U_{optimal} \end{cases} \quad (1)$$

- R_0 is the base rate
- R_{slope1} the multiplier below optimal utilization
- R_{slope2} the multiplier above optimal utilization.
- U is the current utilization rate.
- $U_{optimal}$ is the optimal utilization rate.

If the utilization of the pool is above the optimum, than the borrow rate rises sharply to discourage further borrowing and encouraging the payment of outstanding loans. On the other hand, an utilization below the optimum is accompanied with a low borrow rate to encourage further borrowing.

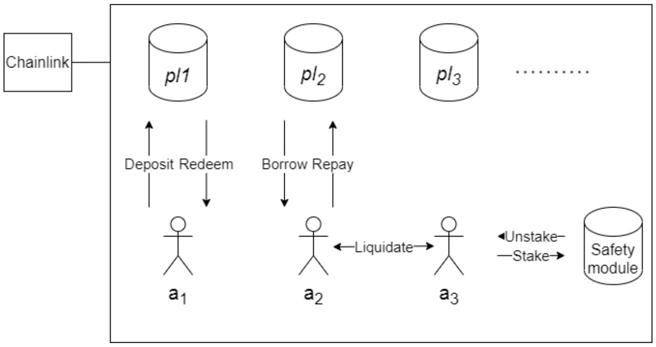

Figure 1: Overview of the Aave protocol

These parameters are set per market. The more risk averse markets have a relatively high $U_{optimal}$ and utilization threshold and a low R_0, R_{slope1} and R_{slope2} and the contrary holds for the more riskful markets [27].

Features The PLFs all compete for liquidity with each other and therefore try to stand out with distinct features. The prominent features of Aave are stable borrow rates and flash loans.

The stable borrow rate, in contrast to vb_i, is meant to stay constant. This is however a pseudo constant rate. If the stable rate diverges from the market rate, then it is still possible for this rate to be rebalanced [6], [27].

Flash loans are loans which do not require any collateral to be deposited. Instead, flash loans make use of the atomicity of the smart contracts to make sure that this loan does not default. A flash loan has to be repaid to the protocol in its entirety in the same transaction. The size of flash loans can, theoretically, entail the entire pool. Such an amount of assets has been the cause of some of the attacks on the DeFi ecosystem. By creating large imbalances with a sizeable flash loan, one can profit from these self-created imbalances through arbitrage [8], [28]. A closer look on flash loans is given in [29].

3 Model

The model, outlined in Tables 1 and 2, makes a connection between variables and the notable entities in a PLF. The model is based primarily on [26], [30], but is adjustable to more general PLFs as well. The main use case for this model will be to give a taxonomy of the PLF ecosystem. Reasoning about agent incentives and strategies can consequently be formalized. A visual overview is given in Figure 1.

Definition 1. For any pool pl_i, its utilization at time t, i.e the fraction between total loans of the pool, tb_i, and the deposits of the market, td_i, is calculated as:

$$u_{it} = \frac{tb_i}{td_i} \tag{2}$$

Definition 2. For any agent a_i, its health factor, i.e the ratio between the sum of its deposited assets times a diminishing factor (liquidation threshold) divided by the sum of its outstanding borrows, is calculated as:

Table 1: Model variables

Variable	Interpretation
a_i	Agent i
(a_i, d_j)	Deposited assets of agent i into pool j
(a_i, b_j)	Borrowed assets of agent i into pool j
c_i	Asset i
p_i	Price of asset i
pl_i	Pool i
tb_i	Total borrowed for pool i
td_i	Total deposited for pool i
$s_i = tb_i + td_i$	Total size of pool i
dpi_i	Deposit interest of pool i
vb_i	Variable borrow rate for pool i
u_{it}	Utilization ratio for pool i
Optimal utilization	80%
Liquidation threshold	80%
Loan to Value (LTV)	80%

Table 2: Agent actions

Variable	Interpretation
Dp (a_i, c_i)	a_i deposits c_i
Rdm (a_i, c_i)	a_i redeems c_i
Bor (a_i, c_i)	a_i borrows c_i
Rpy (a_i, c_i)	a_i repays their loan of c_i
Liq (a_i, a_j)	a_i liquidates the loan of a_j
Stk (a_i, c_{AAVE})	a_i stakes their AAVE asset in the safety module
UnStk (a_i, c_{AAVE})	a_i unstakes their AAVE assets from the safety module
Idle (a_i)	a_i does nothing

$$h_i = \frac{\sum_{j=1}^{n}(a_i, d_j) \cdot p_j \cdot \text{Liquidation threshold}}{\sum_{j=1}^{n}(a_i, b_j) \cdot p_j} \tag{3}$$

Whenever the agent's health factor < 1, its deposited collateral will be available to be liquidated by any other agent.

Model overview At $t = 0$, for all agents, assets and pools, the parameters, as noted in Table 1, are initialized. Subsequently, at every t:

1. Chainlink provides for each asset their value.
2. Aave updates the values for their assets.
3. Each agent chooses a strategy (Table 2).
4. Aave updates the market's parameters.

Assumptions The agents are presumed to be economically rational agents, wishing to maximize their total assets. As such, the agent will choose the strategy which maximizes:

$$\sum_{j=1}^{n}((a_i, d_j) \cdot p_j) + ((a_i, d_j) \cdot dpi_j) - ((a_i, b_j) \cdot vbi_j) \tag{4}$$

i.e the sum of all deposits into the protocol by the agent plus the earned interest on this deposit minus the interest that has to be paid for any outstanding loans.

Furthermore, the agents are presumed to be speculators who aim to profit with strategies which favour the short term. As a consequence, in Equation 4, the variable interest rate is used to calculate the profit instead of a stable interest rate.

The (pseudo)stable interest rate offers stability at the expense of a higher interest rate [27]. As the agents are speculators, the assumption is made that all the loans are established with a variable interest rate. Additionally, transaction fees are left out of the picture for simplicity of the model. Likewise, the markets are all initialized with the same utilization, liquidation and LTV parameters.

4 Liquidity

Equation 3 provides insight into the inner workings of a healthy PLF. Namely, as mentioned in Section 2, that the net worth of the collateral of a participant (times a liquidation threshold) should be worth more than the net worth of the outstanding loans. As a consequence, $\forall t, \forall i : td_i > tb_i$, i.e the protocol should at all times have a higher worth of deposits than of outstanding loans. In this state, the protocol is able to handle the usual actions of the agents such as borrowing assets or redeeming assets. In such a state the protocol is liquid. A more formal definition, adapted from [31], is the following:

Definition 3. A market is liquid if any amount of assets can be traded anytime within market hours, rapidly, with minimum loss of value and at competitive prices.

A state in which one is not able to borrow or redeem their deposited assets, would therefore be called an illiquid state. Preventing illiquidity is done through incentives. The variable borrow rate, vb_i (Equation 1), with its positively correlated deposit interest rate, dpi_i, change according to the current utilization, u_{it} (Equation 2) to make borrowing or depositing more or less attractive for agents.

4.1 Deflationary spiral

Illiquidity can manifest itself in two manners. If for some asset, c_i, the utilization ratio, u_{it} is close to or equal to 1, then some agents will not be able to borrow additional assets as all the deposited assets, td_i are loaned out. The second manifestation would be that the utilization ratio is greater than 1. In this scenario some agents will not be able to redeem their assets. While being unable to borrow is a inconvenience in the short term, not being able to withdraw your assets carries more risks such as a bank run [16].

Using the model in Section 3, a potential deflationary spiral is illustrated which depicts such a scenario in case of downward pressure on the market. This downward pressure is modeled as a constant depreciation of the deposits in the collateral. Namely, the price given by Chainlink to the protocol at $t + 1$ is less than the price given at t, namely $p_{i,t} > p_{i,t+1}$.

At $t = 0$, the markets are initialized such that $\forall i : u_{i0} < 1$, i.e the protocol is fully collateralized. Furthermore, we take a c_i used as collateral to borrow and corresponding p_i and pl_i to reason about this deflationary spiral. The assumptions of Section 3 also hold.

Depreciation: At $t = x$, Chainlink will report $p_{i,x}$, which by above assumption is less than $p_{i,x-1}$. This results in the net worth of an agent j to depreciate in the first term of Equation 4, i.e $(a_j, d_i) \cdot p_i$. Furthermore, the health factor of agent j will by Equation 3 depreciate as well.

Aave updates: If the health factor of agent j depreciates to < 1, the collateral of agent j, (a_j, d_i) will be available for liquidation by any other agent for a discount.

Agent strategy: After depreciation, the agents will have to choose a strategy (Table 2). With the aim of maximizing Equation 4, agent j can Idle(a_j) if it speculates p_i not to drop further and if the earned interest is more profitable than the depreciation of p_i. However, by our assumptions of downward pressure and economically rational speculators, Rdm(a_j, c_i) and Liq(a_j, a_k) are the rational choices compared to Idle(a_j) or Dp(a_j, c_i).

By equation 4, the interest $(a_i, d_j) \cdot dpi_j$ does not make up for the drop in valuation of the deposited assets $(a_i, d_j) \cdot p_j$. The average annual deposit rate for stablecoins is around 2% [2]. In comparison to the usual volatility in cryptocurrencies, ranging from +7% to -15% in in a 100-day period [32]. Therefore the long term interest gain is outweighed by downward pressure during a sufficiently long period of time. Rdm(a_j, c_i) will decrease your position in deposits and by aforementioned be more rational then maintaining your position through Idle(a_j) or increasing your position through Dp(a_j, c_i).

Liq(a_j, a_k) is a rational choice as long as $(a_k, d_i) \cdot p_i \cdot$ (discount factor) $> (a_k, d_l) \cdot p_l$, i.e as long as the collateral of agent k has not dropped in price far enough that its worth is less than the outstanding loan of agent k.

Agent strategy — liquidation: If agent j decides to liquidate another agent k, then a_j will receive the c_i collateral from a_k. A speculator, fearing slippage or further depreciation of p_i, will immediately sell c_i on an exchange.

Agent strategy — redeeming: If agent j decides to redeem its own deposited c_i, then this will lead to an higher u_{it}. Likewise, a speculator fearing slippage or further depreciation of p_i, will immediately sell c_i on an exchange.

Aave updates: Depending on the agent strategies, new utilization ratios are calculated per pool. By beforementioned, the conclusion was that liquidation and redeeming are the dominant strategies. These strategies result in a net appreciation of the utilization ratio as deposits are redeemed out of the protocol or obtained with a discount through liquidation. Furthermore, as the utilization ratio, u_{it} appreciates for pl_i, the variable borrow interest rate and deposit interest rate appreciate according to Equation 1. If $u_{it} > u_{optimal}$, then it is in the interest of the protocol to promote depositing, repayments of loans and inhibiting further borrowing.

These two strategies, liquidation and redeeming, will further progress the depreciation of the asset c_i. As such, a vicious cycle is created which reinforces itself causing the asset c_i to land in a deflationary spiral (Figure 2).

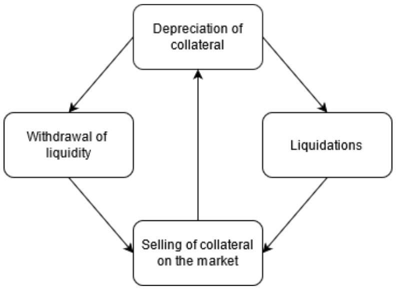

Figure 2: A deflationary spiral aggravated through liquidations and withdrawal of liquidity.

4.2 Undercollateralization

If this vicious cycle is upheld for long enough, it can cause a state of undercollateralization in which $tb_i > td_i$. This means that the loans are not fully backed up by the underlying collateral. If left as is, the pool could dry up while there is still outstanding debt in the protocol. This concretely means that some participants will not be able to redeem their assets as there is no asset in the pool to be redeemed. The debtors have no incentive to pay their outstanding loans.

Besides this deflationary spiral, there are several potential factors which can aggravate it.

- An high amount of the liquidity and governance tokens are in the hands of a few addresses [12], [33]. The deflationary spiral as portrayed is therefore more feasible as fewer agents are necessary to move high amounts of assets.
- Governance can work in the disinterest of the protocol. Governance is a mechanism to strive towards an even more decentral protocol. Participants of the protocol can vote on protocol wide parameters with their governance tokens. The Schelling point is however not always favouring the best interest of the protocol [34]. Keeping in mind the distribution of governance tokens combined with the fact that voting power is directly linked to the amount of governance tokens that one possesses, one can conclude that a few agents can act in their own interest through governance. Currently, the core team of Aave is still overseeing governance [35].
- Liquidations can make participants even less healthy and even less inclined to pay their debts. Liquidations are an mechanism to ensure that outstanding debts are paid. If the health factor of the agent however drops even more than the point of undercollateralization (through delayed liquidations caused by, for example, network congestion, oracle responsiveness etc. [10], [15]), then liquidations actually push the protocol and agent even more into insolvency and as such works counter-productive [19], [36].
- A high utilization ratio is seen naturally in the historical data of Aave, taking for example DAI (Figure 3). This is in accordance with [6] where such utilization ratios are also seen in other PLFs. This shows that protocol incentives are not always sufficient to reaching optimal utilization.

5 Safety Module

With the arrival of the governance framework in Aave in 2020, also came the arrival of a safety module. This safety module is meant to counteract periods of downfall. The principle idea behind the safety module is that users can stake their AAVE governance tokens and earn interest on them. In return, the protocol can use these staked AAVE tokens to provide liquidity in times of need. Whenever outstanding debts are at risk to be unprofitable for liquidation, then the protocol will slash and sell some of these staked AAVE tokens to provide liquidity. Furthermore, to prevent participants from unstaking in times of downfall periods, the protocol has setup a cooldown timer after which one can unstake. As of now, this cooldown period is 10 days. In conclusion, the risks that stakeholders carry are the risk that their assets can be slashed. The incentive to stake is provided through the potential of earning more AAVE tokens through interest.

Observations There are two observations that can be made with regards to the efficiency of the safety module in mitigating periods of illiquidity.

Firstly, Equation 4 still holds with the addition of the safety module, as the AAVE token is an asset as any other asset. Any agent has incentive to stake AAVE assets and earn interest in order to maximize their profit. Unstaking is however always a possibility. The cooldown timer is at this moment in time 10 days. However, in simulated runs from [14], [19], PLFs become illiquid in as little as 19 days. Therefore agents could unstake their assets when the protocol needs it the most.

Secondly, the correlation of AAVE with the underlying protocol is highly positive (0.77 [19]) with Ethereum, the most used collateral in the protocol (84.9% [37]). This concretely means that the asset meant to function as backup collateral in times of prolonged deflation of the collateral, will actually drop in conjunction with said collateral. In simulated runs from [14], a higher correlation did indeed cause a faster state of illiquidity.

Case study Between 11 May 2021 and 23 May 2021, the value of cryptocurrencies dropped significantly. Ethereum lost around 43% and AAVE around %46. Taking the current size of the staking module as of 16 June 2021, namely $1,2B, this drop would amount to a remainder of $550M. This would amount to a loss of $645M, even without the protocol having made use of the safety module.

A diversification of the assets in the safety module can therefore be to the benefit of any reserve pool used in PLFs (Proof A.2). As an example, a composition made out of a split of 33% AAVE tokens, 33% SNX (A derivative DeFi protocol governance token) and a 33% DAI, would result in a remainder of $912M. This would amount to a loss of $280M instead (Calculations A.3).

There are catches to this diversification. Diversification would mean that Aave as a protocol takes a stake in protocols outside of its own. Depending on the aim of the protocol, this might be unwanted. The protocol might not wish to compose their safety module with the assets representing other protocols.

Secondly, the above example is not optimized in the general sense. While a low correlation is beneficial in times of downward pressure, it is not beneficial in times of appreciation of Ethereum. As such, the protocol has to make choices depending on how it wants the safety module to act in both of these situations.

6 Conclusion

In this paper, a model was given which gave a taxonomy of PLFs, protocols meant to provide lending services on the DeFi ecosystem. The agent incentives and protocol measures to provide correct incentives were mapped.

Using this model, the notion of liquidity was examined. A PLF has to find a balance between competitiveness and safety, tweaking its parameters accordingly while maintaining liquidity.

The model was also used to describe a deflationary spiral, in which misalignment of protocol incentives and agent strategies can lead to illiquidity, a state in which the protocol is left with outstanding debt not being able to provide its lending services. Asset distribution among few addresses, governance workings and liquidations were examined and pinpointed as hypothetically aggravating factors.

Lastly, the safety module of Aave was observed to have inefficient handling of its assets. Participants can unstake their assets in times of a downfall period. Furthermore, the AAVE asset used as reserve in this safety module is strongly correlated with Ethereum (0.77), the collateral used the most in AAVE (%84.9).

Diversifying the safety module can therefore lead to a more efficient use of the assets in the safety module. The downsides are that the protocol would have to have a stake in another protocol's assets. This might not be in accordance with the aims of the protocol. Secondly, this efficiency is only seen whenever the underlying collateral depreciates in price. However when the collateral appreciates the diversified safety module would appreciate less rapidly.

References

[1] *DeFi Pulse — The DeFi Leaderboard — Stats, Charts and Guides*, en. [Online]. Available: https://defipulse.com (accessed 22/05/2021).

[2] Aave, *Open Source DeFi Protocol*, en. [Online]. Available: https://aave.com/ (accessed 25/05/2021).

[3] Compound, *Compound*, en. [Online]. Available: https://compound.finance (accessed 27/05/2021).

[4] MakerDAO, *MakerDAO — An Unbiased Global Financial System*. [Online]. Available: https://makerdao.com (accessed 27/05/2021).

[5] J. Xu and N. Vadgama, "From banks to DeFi: the evolution of the lending market," Apr. 2021. [Online]. Available: http://arxiv.org/abs/2104.00970.

[6] L. Gudgeon, S. Werner, D. Perez and W. J. Knottenbelt, "DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency," in *AFT 2020 - Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 2020. DOI: 10.1145/3419614.3423254.

[7] Z. Jakab and M. Kumhof, "Banks are Not Intermediaries of Loanable Funds And Why this Matters," *SSRN Electronic Journal*, 2015, ISSN: 1556-5068. DOI: 10.2139/ssrn.2612050.

[8] K. Qin, L. Zhou, B. Livshits and A. Gervais, "Attacking the DeFi Ecosystem with Flash Loans for Fun and Profit," Mar. 2020. [Online]. Available: http://arxiv.org/abs/2003.03810.

[9] S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz and W. J. Knottenbelt, "SoK: Decentralized Finance (DeFi)," Jan. 2021. [Online]. Available: http://arxiv.org/abs/2101.08778.

[10] Blocknative, *Evidence of Mempool Manipulation on Black Thursday: Hammerbots, Mempool Compression, and Spontaneous Stuck Transactions*, en, Jul. 2020. [Online]. Available: https://www.blocknative.com/blog/mempool-forensics (accessed 27/05/2021).

[11] Zoltu, *How to turn $20M into $340M in 15 seconds*, Dec. 2019. [Online]. Available: https://medium.com/coinmonks/how-to-turn-20m-into-340m-in-15-seconds-48d161a42311 (accessed 27/05/2021).

[12] D. Perez, S. M. Werner, J. Xu and B. Livshits, "Liquidations: DeFi on a Knife-edge," Sep. 2020. [Online]. Available: http://arxiv.org/abs/2009.13235.

[13] H. T. Kao, T. Chitra, R. Chiang and J. Morrow, "An Analysis of the Market Risk to Participants in the Compound Protocol," *Third International Symposium on Foundations and Applications of Blockchain (FAB '20)*, 2020.

[14] L. Gudgeon, D. Perez, D. Harz, B. Livshits and A. Gervais, "The Decentralized Financial Crisis," in *Proceedings - 2020 Crypto Valley Conference on Blockchain Technology, CVCBT 2020*, 2020. DOI: 10.1109/CVCBT50464.2020.00005.

[15] E. Frangella, *Crypto Black Thursday: The Good, the Bad, and the Ugly*, Mar. 2020. [Online]. Available: https://medium.com/aave/crypto-black-thursday-the-good-the-bad-and-the-ugly-7f2acebf2b83 (accessed 27/05/2021).

[16] Alethio, *Illiquidity and Bank Run Risk in Defi*, Dec. 2019. [Online]. Available: https://medium.com/alethio/overlooked-risk-illiquidity-and-bank-runs-on-compound-finance-5d6fc3922d0d (accessed 27/05/2021).

[17] H. Amler, L. Eckey, S. Faust, M. Kaiser, P. Sandner and B. Schlosser, "DeFi-ning DeFi: Challenges & Pathway," Jan. 2021. [Online]. Available: http://arxiv.org/abs/2101.05589.

[18] M. Bartoletti, J. H.-y. Chiang and A. Lluch-Lafuente, "SoK: Lending Pools in Decentralized Finance," Dec. 2020. [Online]. Available: http://arxiv.org/abs/2012.13230.

[19] Gauntlet, "Market Risk Assessment. An analysis of the financial risk to participants in the Aave V1 and V2 protocols.," Tech. Rep., 2021.

[20] J. E.-T. Cheah, *What is DeFi and why is it the hottest ticket in cryptocurrencies?* en, Aug. 2020. [Online]. Available: http://theconversation.com/what-is-defi-and-why-is-it-the-hottest-ticket-in-cryptocurrencies-144883 (accessed 25/05/2021).

[21] *DeFi Hacks*. [Online]. Available: https://defihacks.wiki/ (accessed 25/05/2021).

[22] Quantstamp, *How the dForce hacker used reentrancy to steal 25 million*, Apr. 2020. [Online]. Available: https://quantstamp.com/blog/how-the-dforce-hacker-used-reentrancy-to-steal-25-million (accessed 25/05/2021).

[23] A. Munro, *Harvest Finance (FARM) hack explained simply*, en-AU, Oct. 2020. [Online]. Available: https://www.finder.com.au/harvest-finance-farm-hack-explained-simply (accessed 25/05/2021).

[24] Aave, *Markets*, en. [Online]. Available: https://app.aave.com/markets (accessed 28/05/2021).

[25] Aave, *Risk Parameters*. [Online]. Available: https://docs.aave.com/risk/asset-risk/risk-parameters (accessed 30/05/2021).

[26] Aave, *Whitepaper v1.0*, original-date: 2019-10-21T13:21:52Z, May 2021. [Online]. Available: https://github.com/aave/aave-protocol/blob/4b4545fb583fd4f400507b10f3c3114f45b8a037/docs/Aave_Protocol_Whitepaper_v1_0.pdf (accessed 27/05/2021).

[27] Aave, *Borrow Interest Rate*. [Online]. Available: https://docs.aave.com/risk/liquidity-risk/borrow-interest-rate (accessed 30/05/2021).

[28] J. Crawley, *BurgerSwap Hit by Flash Loan Attack Netting Over $7M*, en, May 2021. [Online]. Available: https://www.coindesk.com/burgerswap-flash-loan-attack (accessed 29/05/2021).

[29] D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang and K. Ren, "Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem," Oct. 2020. DOI: 10.1145/3457977.3460301. [Online]. Available: http://arxiv.org/abs/2010.12252%20http://dx.doi.org/10.1145/3457977.3460301.

[30] A. Klages-Mundt and A. Minca, "While Stability Lasts: A Stochastic Model of Stablecoins," 2021. [Online]. Available: https://arxiv.org/abs/2004.01304.

[31] K. Nikolaou, "Liquidity (Risk) Concepts: Definitions and Interactions," *ECB Working Paper*, no. 1008, 2009.

[32] Barchart, *ETHUSD - Ethereum - USD Cryptocurrency Technical Analysis*, en. [Online]. Available: https://www.barchart.com/crypto/quotes/%5EETHUSD/technical-analysis (accessed 25/06/2021).

[33] M. Nadler and F. Schär, "Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution," 2020.

[34] Aave, *Base stable rate oracle update and improvements in Aave V2 - Risk*, en, Dec. 2020. [Online]. Available: https://governance.aave.com/t/base-stable-rate-oracle-update-and-improvements-in-aave-v2/1879 (accessed 16/06/2021).

[35] Aave, *Governance*. [Online]. Available: https://docs.aave.com/aavenomics/governance (accessed 16/06/2021).

[36] OpenZepellin, *Aave Protocol Audit*. [Online]. Available: https://blog.openzeppelin.com/aave-protocol-audit/ (accessed 16/06/2021).

[37] johaya, *Aave Risk V2*, en. [Online]. Available: https://duneanalytics.com/johaya/aave-risk-v2 (accessed 16/06/2021).

[38] Aavewatch, *Aave live statistics*, en. [Online]. Available: https://aavewatch.com/ (accessed 26/06/2021).

[39] CoinMarketCap, *Cryptocurrency Prices, Charts And Market Capitalizations*, en. [Online]. Available: https://coinmarketcap.com/ (accessed 26/06/2021).

A Appendix

A.1 Figures

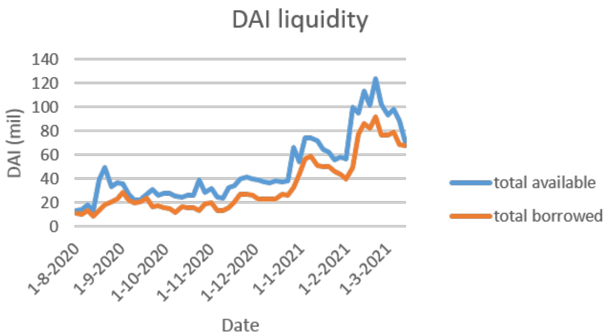

Figure 3: Historic utilization in the DAI pool. (Data points obtained from: [38])

A.2 Proofs

Proof. The total net worth of the safety module consists of cryptocurrencies c_i multiplied by their accompanying price p_i.

$$\sum_{i=1}^{n} c_i \cdot p_i \tag{5}$$

Furthermore every c_i has a accompanying Pearson correlation with Ethereum, cor_i, signifying the amount of price movement that p_i will move jointly with $p_{ethereum}$.

A composition of c_i with the lowest cor_i will therefore show the least amount of price movement in reaction to the price movement of Ethereum.

By Equation 5, the highest net worth of the safety module, in case of a downwards price movement of Etheurem, is realized through the c_i with the lowest cor_i as their p_i will drop the least.

As such the net worth of the safety module composed of c_i with a cor_i lower than AAVE, will be strictly larger than a safety module consisting of only AAVE.

□

A.3 Calculations

Table 3: Price history of the coins used for the calculations in Section 5. (Price data obtained from: [39])

	11 May 2021	23 May 2021	Correlation with Ethereum
Ethereum	$ 3575	$ 1525	1
AAVE	$479	$ 220	0.77
DAI	$1	$1	-0.26
SNX	$14	$12	0.7