The Decentralized Financial Crisis

Lewis Gudgeon*, Daniel Perez*, Dominik Harz*, Benjamin Livshits* and Arthur Gervais*
* Department of Computing, Imperial College London

***Abstract*—The Global Financial Crisis of 2008, caused by the accumulation of excessive financial risk, inspired Satoshi Nakamoto to create Bitcoin. Now, more than ten years later, Decentralized Finance (DeFi), a peer-to-peer financial paradigm which leverages blockchain-based smart contracts to ensure its integrity and security, contains over 702m USD of capital as of April 15th, 2020. As this ecosystem develops, it is at risk of the very sort of financial meltdown it is supposed to be preventing. In this paper we explore how design weaknesses and price fluctuations in DeFi protocols could lead to a DeFi crisis. We focus on DeFi lending protocols as they currently constitute most of the DeFi ecosystem with a 76% market share by capital as of April 15th, 2020.**

First, we demonstrate the feasibility of attacking Maker's governance design to take full control of the protocol, the largest DeFi protocol by market share, which would have allowed the theft of 0.5bn USD of collateral and the minting of an unlimited supply of DAI tokens. In doing so, we present a novel strategy utilizing so-called *flash loans* that would have in principle allowed the execution of the governance attack in just *two transactions* and without the need to lock any assets. Approximately two weeks after we disclosed the attack details, Maker modified the governance parameters mitigating the attack vectors. Second, we turn to a central component of financial risk in DeFi lending protocols. Inspired by stress-testing as performed by central banks, we develop a stress-testing framework for a stylized DeFi lending protocol, focusing our attention on the impact of a *drying-up* of liquidity on protocol solvency. Based on our parameters, we find that with sufficiently illiquidity a lending protocol with a total debt of 400m USD could become undercollateralized within 19 days.

***Index Terms*—Cryptocurrencies, decentralized finance, stress-testing, financial crisis, governance attack, financial risk.**

I. Introduction

Blockchain technology emerged as a response to the Financial Crisis of 2007–8 [34].[1] The perception that banks had misbehaved resulted in a deterioration of trust in the traditional financial sector [17]. The causes of the crisis were several, but arguably chief among them was a lack of transparency regarding the amount of risk major banks were accumulating. When Lehman Brothers filed for bankruptcy, it had debts of 613bn USD, bond debt of 155bn USD and assets of 639bn USD [8]. Central to its bankruptcy was its exposure to subprime (i.e., bad quality) mortgages. This exposure was compounded by the fact that the bank had a leverage ratio[2] of 30.7x in 2007 [9].

From their inception, blockchain-based cryptocurrencies sought to provide a remedy to such crises: facilitating financial transactions without reliance on trusted intermediaries, shifting the power, and therefore, the ability to cause crisis through the construction of opaque and complex financial instruments, away from banks and financial institutions [34]. Ten years later, a complex financial architecture—the architecture of Decentralized Finance (DeFi)—is gradually emerging on top of existing blockchain platforms. Components in this architecture include those that pertain to lending, decentralized exchange of assets, and markets for derivatives (cf. Appendix A Table I) [20], [19], [45], [48], [16], [23].

DeFi architectures for lending require agents to post *security deposits* to fully compensate counter-parties for the disappearance of the agent. We assume that when an economically rational agent faces a choice between the repayment of a debt or the loss of collateral, given the absence of reputation tracking—on account of agent pseudonymity and the possibility of an agent using multiple addresses—the agent will choose the least costly option. Security deposits serve to guard against (i) *misbehavior* of agents, where the action that would maximize individual utility does not maximize social welfare, and (ii) external events, such as large exogenous drops in the value of a particular cryptocurrency [21]. Of all DeFi protocols, those with the most locked capital are for lending. As of April 15th, 2020, the largest protocol by capitalization, Maker [20], has c. 65% of all capital locked in DeFi, corresponding to 342.9m USD [41].

Governance is another crucial facet of DeFi protocols and we observe differing degrees of governance decentralization. For example, Maker uses its own token (MKR) to allow holders to vote on a contract that implements the governance rules. In contrast, Compound [19], the third largest protocol by market share, is centrally governed and a single account can shut down the system in case of a failure. Moreover, as in traditional finance, these protocols do not exist in isolation. Assets that are created in Maker, for example, can be used as collateral in other protocols such as Compound, dYdX [16], or in liquidity pools on Uniswap [48]. Indeed, the composability of DeFi — the ability to build a complex, multi-component financial sys-

[1]The first Bitcoin block famously outlines: "The Times 03/Jan/2009, Chancellor on brink of second bailout for banks".

[2]Defined as $\frac{\text{total assets}}{\text{equity}}$; the total assets were more than 30 times larger than what shareholders owned, indicating substantial debt.

978-1-7281-9390-8/20/$31.00 ©2020 IEEE
DOI 10.1109/CVCBT50464.2020.00005

tem on top of crypto-assets — is a defining property of open finance [42]. However, if the underlying collateral assets fail, all connected protocols will be affected as well: there is the possibility of financial contagion.

This paper. We focus on DeFi *lending* protocols, which constitute c. 76% of the DeFi market in capital terms. We consider two distinct but interconnected aspects of the attack and risk surface for collateral-based Defi lending protocols: (i) attacks on the governance mechanism and (ii) the economic security of such protocols in "black swan" [46] financial scenarios.

In relation to attacks on the governance mechanism, we examine an attack on Maker [20] which consists of an adversary amassing enough capital to seize full control of the funds within the protocol. Herein, we further consider two distinct attack strategies. We engaged in a process of responsible disclosure with Maker, which we detail, who since modified their governance parameters to mitigate the two attack strategies we present. The first attack strategy, crowdfunding, inspired by [31], covertly executed, was feasible within two blockchain blocks and required the attacker to lock c. 27.5m USD of collateral. This would have enabled an attacker to steal all 0.5bn USD of locked collateral in the protocol and mint an unlimited supply of DAI tokens. The second, novel, attack strategy utilized so-called flash loans and allows an adversary to amass the Maker collateral within a single transactions. This attack did not require locking of collateral and only required a few US dollars to pay for gas fees.

With respect to the economic security of collateralized DeFi lending protocols, with reference to our stylized model, we present the possibility of a DeFi lending protocol becoming undercollateralized (or insolvent) — where security deposits become smaller than the issued debt — as the result of a drying up of liquidity. Assuming rational economic agents, in such an under-collateralization event, the borrower would default on their debts, since the amount they have borrowed has become worth more than the amount they escrowed. Starting from formal definitions of the economic security constraints for DeFi lending platforms, we then use Monte Carlo simulation to stress-test their financial robustness. We submit that such stress-testing constitutes an important approach to bounding the economic security of DeFi lending protocols when formal security proofs are not obtainable and their security primarily depends on economic properties. We find that for plausible parameter ranges, a DeFi lending system could find itself undercollateralized. To the extent that other DeFi protocols allow agents to lend or trade the undercollateralized asset, financial contagion—where an economic shock spreads to other protocols—would be expected to result.

Contributions.

- **Governance attack on Maker (Section III).** With specific focus on the largest DeFi project by market share, Maker, we show how, prior to Maker implementing a parameter change, it was feasible to successfully steal the funds locked in the protocol covertly and within two blocks or within two transactions. By exploiting recent flash loan pool contracts, we show how an attacker with no capital (besides gas fees), would have been able to execute such an attack, if the flash loan pools would provide sufficient liquidity (which they did not at the time of writing).
- **Formal modeling of DeFi lending protocols (Section IV).** We provide definitions for economically-resilient DeFi lending protocols, introducing overcollateralization, liquidity, and counterparty risk as formal constraints. These definitions serve to formalize financial risk constraints for more than 93% of the funds locked in DeFi lending protocols as of April 15th, 2020 [41].
- **Financial stress-testing (Section V).** We develop a methodology to quantitatively stress-test a DeFi protocol with respect to its financial robustness, inspired by risk assessments performed by central banks in traditional financial systems. We simulate a price crash event with our stress-test methodology to a stylized DeFi lending protocol that resembles the largest DeFi lending protocols to-date, by volume: Maker, Compound, Aave and dYdX. We find, for plausible parameter ranges, that a DeFi lending protocol could become undercollateralized within 19 days.

II. Overview of Decentralized Finance

This section provides a definition of DeFi, describes the composability property of DeFi protocols, and states our assumptions regarding the underlying blockchain.

DeFi is an emergent field, with over 702m USD of total value locked in DeFi protocols as of April 15th, 2020 [41]. Table I in Appendix A presents a categorization of DeFi protocols, providing the three largest by locked USD in each case. We observe that Maker dominates the DeFi projects with a capitalization of over 342.9m USD. DeFi protocols mostly emerge for uses such as lending, decentralized exchange, and derivatives. We define DeFi as follows.

Definition II.1 (Decentralized Finance (DeFi))**.** a peer-to-peer financial system, which leverages distributed ledger-based smart contracts to ensure its integrity and security.

In this paper we make the assumption that agents are rational, that is, are agents who seek to maximize their expected utility. We assume that agents are pseudonymous.

A. DeFi Composability

DeFi protocols do not exist in isolation. Their open nature allows developers to create new protocols by composing existing protocols together. Some compare this approach with "Money Lego" [42]. As such, assets created through lending in one protocol can be reused as collateral

in other protocols in any kind of fashion. This creates a complex and intertwined system of assets and debt obligations. Moreover, a failure of a protocol that serves as backing asset to other protocols has a cascading effect on others. Indeed, a hallmark of financial crisis is that such events do not take place in isolation, but rather financial contagion takes place, where a shock affecting a few institutions spreads by contagion to the the rest of the financial sector, before affecting the larger economy [4].

B. Blockchain Model

A DeFi protocol operates on top of a layer-one blockchain, which provides standard ledger functionality [6], [5], [15], [38]. We assume that the underlying blockchain is able to provide finality [11], [32], construed as a guarantee that once committed to the blockchain a transaction cannot be modified or reversed. For this paper, we treat attacks on layer-one blockchains as orthogonal and as such we are not concerned with them.[3]

III. Governance Attack on Maker

In this section, we first present an attack on the governance mechanism of the Maker protocol [20]. We use a representation of the state of the Ethereum main network on February 7th and the Maker contract to simulate as realistically as possible how such an attack could take place. While focusing on a specific protocol, we submit that such a governance attack is representative of a new element of the attack surface for DeFi protocols more generally. Since we first analyzed this attack vector, the Maker protocol has been modified to mitigate this attack: we detail our interaction with the Maker team below. Although the basic idea of the attack had been briefly presented in a blog post [31], the *feasibility* of the attack has not been analyzed.

A. Disclosure to Maker

We engaged in a process of responsible disclosure with Maker, as detailed below.

- On February 7th, 2020 we reached out to the Maker team regarding our exposition of the feasibility of the governance attack.
- On February 14th the authors had a conference call with Maker, where we described our work. We agreed to giving the Maker team sight of this paper prior to our publication of it; we subsequently sent a draft of the paper on February 17th.
- On February 18th the authors further contacted Maker to describe how the use of flash loans increased the risk of the governance attack, offering a response window prior to publicizing this result within which Maker provided helpful feedback.

[3]Future work could consider the possibility of combining layer-one attacks with smart-contract attacks to increase their probability of success. For example, see the successful attack on Fomo3D [44].

After this exchange, on February 21st Maker announced that the Governance Security Module had been activated with a delay period of 24 hours [29], mitigating the vulnerability.

B. Background and Threat Model

The governance process relies on the MKR token, where participants have voting rights proportional to the amount of MKR tokens they lock within the voting system. MKR can be traded on exchanges [12].

Executive voting. Using executive voting, participants can elect an *executive contract*, defining a set of rules to govern the system, by staking (i.e., locking-up) tokens on it. Executive voting is continuous, i.e., participants can change their vote at any time and a contract can be newly elected as soon as it obtains a majority of votes. The elected contract is the only entity allowed to manipulate funds locked as collateral. If a malicious contract were to be elected, it could steal all the funds locked as collateral.

Defense mechanisms. Several defense mechanisms exist to protect executive voting. The *Governance Security Module* encapsulates the successfully elected contract for a certain period of time, after which the elected contract takes control of the system. At the time of first writing on February 7th, this period was set to zero [50]. This has subsequently been increased to 24 hours [28], see Section III-A. The *Emergency Shut Down*, which allows a set of participants holding a sufficient amount of MKR to halt the system. However, this operation requires a constant pool of 50k MKR tokens, worth 27.5M USD as of February 7th.[4]

Threat model. We assume the existence of a rational adversary i.e., one who would only engage in the attack if the potential returns are higher than the costs. In this attack, the costs are the amount of money that the adversary has to pay to have his contract elected as executive contract. The returns are the amount of money that the contract could steal or generate once it is elected. There are two ways in which electing an adversarial executive contract can financially benefit the adversary. First, the contract can transfer all the ETH collateral to the adversary's address. Second, the contract can mint new DAI tokens and transfer them to the adversary. The DAI tokens can then be traded until the DAI price crashes and effectively destroy the Maker system.

As of February 7th there were c. 150k MKR tokens used for executive voting and the current executive contract had 76k MKR tokens staked. We observed that the staked amount changes relatively often and the amount of tokens staked on the elected contract often dropped below 50k MKR tokens (eq. 27.5M USD). As of February 7th, there were c. 470M USD worth of ETH locked as collateral of the DAI supply, which an executive contract can dispose of

[4]We use the price of MKR on 2020-02-01, which was 550 USD.

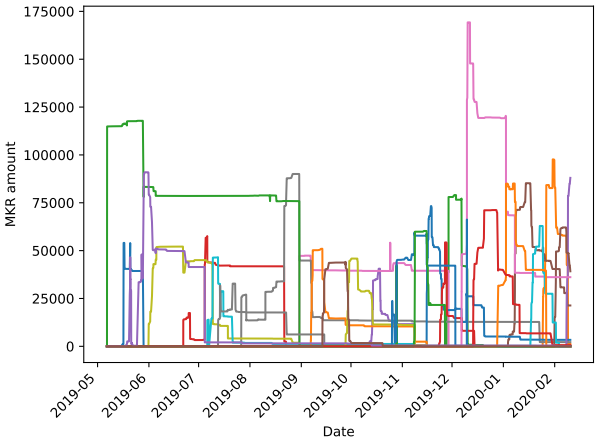

Fig. 1: Evolution of the amount of MKR tokens staked on different executive candidate contracts. We observe that at times the MKR amount of the executive contract dropped below 50k MKR.

freely. This shows that even before trading the DAI tokens, the attack would have been financially attractive.

C. Crowdfunding and Flash Loans

An adversary can choose between the two following strategies to amass the capital required for the governance attack.

Crowdfunding. Crowdfunding MKR tokens may allow users to lock their tokens in a contract and program the contract so that when the required amount of MKR tokens is reached, it stakes all its funds on a malicious executive contract. This would allow multiple parties to collaborate trustlessly on such an attack, while keeping control of their funds and while being assured that they will be compensated for their participation in it. [5]

Liquidity pools and flash loans. A shortcoming of the crowdfunding attack is the required coordination effort between the participants and the likely alerting of benevolent MKR members. Instead, an attack could use liquidity pools offering *flash loans* [3]. A flash loan is a *non-collateralized* loan that is valid within one transaction only. In the Ethereum Virtual Machine (EVM), a transaction can be reverted entirely if a condition in one part of the transaction is not fulfilled. A flash loan then operates as follows: a party creates a smart contract that (i) takes out the loan, (ii) executes some actions, and (iii) pays back the loan and, depending on the platform, interest.

The interesting aspect for our purposes is that if in step (ii) the execution of the actions fails or step (iii) the repayment of the loan cannot be completed, the EVM treats this loan as it never took place. Hence, under the assumption there is enough liquidity available in protocols such as dYdX [16] and Aave [2], an attacker could execute the MKR governance attack in step (ii), and, if successful, repay the flash loan in step (iii). Since the flash loan requires no collateral, the capital lock up cost for the attacker is significantly reduced. If there is enough liquidity available in these pools, the attacker might even not have to lock any tokens. Furthermore, the liquidity provider may have also profited from the execution of the attack, depending on in which protocol their tokens were locked. For example, in Aave as of February 7th they would have received an interest rate of 0.09% for each flash loan.

D. Practical Attack Viability

In this section, we use empirical data to show how such an attack could take place, and describe what the potential shortcomings could be. We first analyze all the transactions received by Maker's governance contract of as February 7th: `0x9ef05f7f6deb616fd37ac3c959a2ddd25a54e4f5`. Since the deployment of this contract, in May 2019, there were 24 different contracts which have been elected as executive contract (cf. Fig. 1). When a contract is elected as the executive contract, the total amount of staked MKR is, for a short period of time, distributed almost equally between the old and the new executive contract.[6] This serves to reduce the amount of tokens required for the attack by more than 50%.

One day after the first blog on this attack was published [31]), there was a sharp increase in the MKR staked on the executive contract, rising from c. 75k to c. 160k MKR at the beginning of December 2019. One token holder [22] in particular injected a large quantity of tokens—c. 66k MKR—potentially to help prevent an attack from occurring. [7]

E. The Attacks

The crowdfunding strategy. We inspected the amount of MKR transferred between January 1st, 2020 and February 8th, 2020. [8] We find a mean MKR transaction volume of c. 9k MKR tokens per day, corroborated by e.g. [12]. Given such volumes, an attacker accumulating 1k MKR tokens per day, for instance, would have sufficient tokens in less than 2 months. However, accumulating all the tokens in a single account would likely attract attention. Indeed, from our discussions with the Maker team, the large MKR token holders seem to be known.

[5] An (admittedly informal) poll on Twitter from late 2019 conducted by a user soon after this attack first appeared shows that several participants would be interested in such crowdfunding. See Fig. 6 in Appendix B.

[6] This was particularly visible at the end of November 2019 (80k MKR to 40k MKR) and in the middle of January 2020 (120k MKR to 45k MKR).

[7] It is unclear if the token holder was the Maker Foundation or some other party; in our discussion with Maker they stated they knew the identity of the token holder. The holder staked their tokens on the currently elected contract, making the attack more difficult to execute, before releasing the staked tokens approximately one month later. The token holder had more than sufficient tokens to execute the attack: were they malicious, they could have stolen the funds.

[8] See Appendix B, Fig. 7.

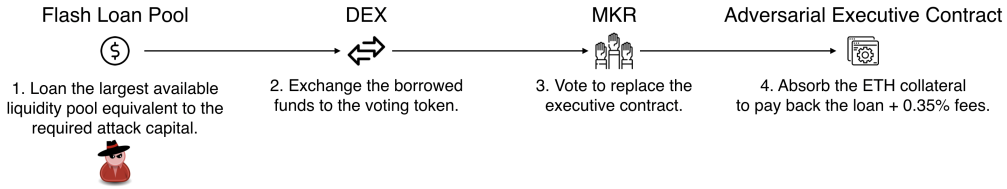

Fig. 2: Example flash loan attack against Maker. All steps can be executed within one transaction, under the assumption that the flash loan pool and DEX have sufficient liquidity available. To execute the attack, the adversary would not need upfront capital, besides the gas fees (estimated to amount to c. 15 USD).

To be covert, an attacker could try to accumulate tokens to multiple accounts without perceptibly changing the distribution of MKR tokens. On February 8th there were c. 5k accounts, holding a total of c. 272k MKR tokens.[9] Given that the attack is possible with 50k MKR tokens, an adversary could spread their tokens across e.g. 100 accounts with an average of 500 tokens each. However, one drawback of this approach is the requirement to vote from these 100 accounts. Voting for a contract costs on average 69k gas. Given the gas limit per block on Ethereum is 10 million, filling half of a block with voting transactions would allow votes from 10M/69k $\approx$ 72 contracts. Doing so would be inexpensive [40], meaning that an attacker would have been able to easily perform the whole attack in two blocks. In the second block, the attacker would finish voting for his malicious contract and execute the attack from the contract, which would leave only one block for anyone to react to the attack.

The flash loan strategy. Alternatively, to execute the governance attack without amassing tokens, the attacker could utilize liquidity pools to borrow the required tokens via a flash loan (e.g. via dYdX [16] or Aave [3]). [10] The attacker makes the following two transactions (cf. Fig. 2).

Transaction 1: Deploy the malicious governance contract and deploy the attack contract executing the flash loan.

Transaction 2: Call the attack contract deployed in Transaction 1 that executes the following steps.

1) Take out flash loan(s)(e.g. from Aave and dYdX) in the currency with the deepest markets for buying MKR tokens. As of February 7th this was ETH.
2) Sell the ETH loan for 50k MKR tokens on decentralized exchange(s).
3) Vote with the 50k MKR tokens to replace the current Maker governance contract with the malicious contract deployed in Transaction 1.
4) Mint DAI into an account chosen by the attacker.
5) Take out enough ETH from the Maker system to repay the flash loan.
6) Repay the flash loan with the required 0.09% interest to Aave and repay the flash loan to dYdX with minimal (1 WEI) interest.

In a naive approach, we could utilize the exchange rate for ETH to MKR to obtain that an attacker requires 114,746 ETH to execute the attack. However in practice, an attacker seeking to buy such a large quantity of MKR tokens would pay a greater price than this, forced to buying the tokens at the best remaining market price for each unit. As of February 14th, an attacker sourcing the required 50k MKR tokens from three different DEXs—38k MKR from Kyber, 11,500 MKR from Uniswap, and 500 MKR from Switcheo—would need a total of 378,940 ETH, 3.3x that of the naive estimate. [11] As of February 14th, the flash loan providers had insufficient pool liquidity: dYdX had c. 83,590 ETH and Aave had c. 13,670 ETH. However, on February 14th the ETH growth rate of Aave was 5.18% per day. Assuming the growth rate continued, it would have only taken *66 days* until enough liquidity was available in Aave.

F. Profitability Analysis

The crowdfunding strategy. With the crowd funding strategy, the profits from the attack could be split equally between the funding parties. The only cost are the 20 USD for including the transactions [40]. In return, the attackers could take away the 434,873 ETH in collateral in Maker plus 145m DAI, amounting to a net profit of 263m USD (as of February 7th). Additionally, the attackers could mint unlimited new DAI and use this to buy other cryptocurrencies available at centralized and decentralized exchanges.

The flash loan strategy. Assuming dYdX's and Aave's liquidity pools had accumulated the required 378,940 ETH to execute the attack, we can calculate the profitability as follows. The attacker obtains a total of 434,873 ETH in collateral from Maker as well as the 50k MKR tokens and the 22m DAI currently in circulation. The attacker needs to repay the 378,940 ETH loan with minimal interest (1 WEI for dYdX and 0.09% for Aave (265.82 ETH)). Furthermore, the attacker needs to pay for the gas fees for the two transactions. The second transaction involves various function calls to other contracts and will cost c. 15 USD equivalent of gas. However, by the end of the attack,

[9] Excluding the holders with a low balance (less than 1 MKR token), and a large balance (more than 5k MKR tokens).

[10] Aave is a protocol deployed on the Ethereum mainnet on January 8th, 2020, https://etherscan.io/tx/0x4752f752f5262fb11733e0136033f7d53cdc90971441750f606cf1594a5fde4f.

[11] For current liquidity and rates see https://dexindex.io/.

the attacker has c. 55k ETH, 50k MKR, and 145m DAI. This amounts to a net profit of 191m USD. Moreover, the attacker can design the attack smart contract such that the transaction is reverted if it becomes unprofitable. This makes the attack *risk free* from a cost perspective for the attacker. As pointed out above, the attacker can further create unlimited DAI to buy up existing liquidity on decentralized and centralized exchanges.

IV. DeFi Lending Protocols

After having presented a specific attack vector, we now turn to a generalization of the financial risk that exists for DeFi lending protocols. This section provides a formal system model for a DeFi lending system and characterizes system constraints. Appendix C Table II details the parameters for existing DeFi lending protocols that we seek to generalize in this section.

A. DeFi Lending Protocol Model

Overcollateralized borrowing allows an agent to provide an asset A as collateral to receive or create another asset B, of lower value, in return. The asset B, typically together with the payment of a fee, can be returned and the agent redeems its collateral in return. However, borrowed asset B may have different properties to asset A: for example, an agent might provide a highly volatile asset A and receive a price-stable asset B in return. Furthermore, a third asset C can serve as a governance mechanism, such as MKR. Holders of asset C are able to influence the rules of the DeFi lending protocol. In absence of a governance asset, DeFi lending protocols typically replace this function with a central privileged operator introducing counter-party risk.

At the agent level, a DeFi lending protocol permits agents $k \in K$ to escrow units of cryptocurrency i, c_i and borrow (or issue) units of another cryptocurrency d against that value. We formulate the constraints herein such that $i \in I$, where I denotes all the permissible collateral types. Appendix C Table II provides the collateral assets and liquidation ratios for DeFi protocols that account for 93% of the DeFi lending market. The prices of escrowed and borrowed assets are typically quoted with reference to an agreed quote currency, e.g. USD.

At the system level, a DeFi protocol is the aggregation of the individual acts of borrowing by agents, such that the system collateral of type i is given by $C_i = \sum_{k=1}^{K} c_{i,k}$ for K agents. We formally define an economically secure DeFi lending protocol as follows:

Definition IV.1 (Economically Secure DeFi lending protocol)**.** Assuming rational agents, a DeFi lending protocol is economically secure if it ensures that $\forall t$, with reference to a basis of value (e.g. USD), the total value of the system debt D at time t is smaller than the total value of all backing collateral types I ($\sum_{i=1}^{I} C_i$) at time t.

B. Economic Security Constraints

We now provide three constraints on the economic security of a DeFi lending protocol. These constraints apply to DeFi protocols which feature one or several collateral assets and which may additionally feature a reserve asset.

The Overcollateralization Constraint. Since the values of both the collateral assets and debt are subject to price fluctuations, overcollateralization seeks to ensure that there is *always* sufficient collateral to cover debt, i.e., to avoid insolvency.

Definition IV.2 (Overcollateralization)**.** When escrowed collateral c_i has a greater value with respect to a basis of value than the issued loan d.

Denoting the overcollateralization factor as $\lambda_i \geq 0$, such that each collateral type has its own minimum collateralization ratio, and the price and quantity of an asset as $P()$ and $Q()$ respectively, the margin M of overcollateralization at time t at the system level[12] is as follows (summing over agents $k \in K$ and collateral types $i \in I$). A protocol designer faces a trade-off. If the parameter λ_i is too low, volatile markets may mean that the protocol becomes undercollateralized. However, if it is too high, then there is significant capital market inefficiency, with more capital than necessary in escrow, leading to opportunity costs of capital.

$$M_t = (1+\lambda_i)\sum_{k=1}^{K}\sum_{i=1}^{I} P_{c_{i,k,t}} Q_{c_{i,k,t}} - \sum_{k=1}^{K} d_{k,t} \qquad (1)$$

Clearly, $M_t \geq 0 \iff \sum_{k=1}^{K} d_{k,t} \leq (1+\lambda_i)\sum_{k=1}^{K}\sum_{i=1}^{I} P_{c_{i,k,t}} Q_{c_{i,k,t}}$. Should $M < 0$, then the margin of overcollateralization is negative and therefore the system as a whole is undercollateralized.

In addition, a protocol may have another pool of reserve liquidity available, enabling it to act as a lender of last resort.[13] For example, one such pool of collateral could be constituted by governance tokens Π for the protocol itself.[14] In a DeFi protocol, participants can have voting power in proportion to the number of governance tokens they hold. The total value of this pool of collateral is given by $P(\Pi)Q(\Pi)$, and thus adding this into the margin of overcollateralization for the system yields:

$$M_t = (1+\lambda_i)\sum_{k=1}^{K}\sum_{i=1}^{I} P_{c_{i,k,t}} Q_{c_{i,k,t}} + P_{\Pi,t} Q_{\Pi,t} - \sum_{k=1}^{K} d_{k,t} \quad (2)$$

Therefore, at the system level, the necessary condition for economic security in terms of overcollateralization is $M_t \geq 0$. In the event that $(1+\lambda_i)\sum_{k=1}^{K}\sum_{i=1}^{I} P_{c_{i,k,t}} Q_{c_{i,k,t}} < \sum_{k=1}^{K} d_{k,t}$, the reserve asset

[12]The system level perspective looks at the aggregates of assets and liabilities; depending on the protocol the ability to use one asset to cross-subsidize an undercollateralized other asset may be restricted.

[13]If a protocol does not have this, $Q_{\Pi,t} = 0$.

[14]MKR tokens in the case of Maker.

Π of a protocol can be used as a *lender of last resort* to buy the collateral value. If $M < 0$ even the liquidation of all of the primary collateral asset and reserve asset would be insufficient to cover the total system debt. Since tt is possible that the collateral and reserve assets are correlated[15], the ability of a reserve asset to recapitalize a system may be limited in the event of a sharp price drops. Absent any additional protocol specific defense mechanisms, this would constitute a catastrophic system failure since the borrowed funds would become worthless as they would no longer be redeemable.

The Liquidity Constraint. In an illiquid market, liquidating a collateral asset may only be possible with a significant *haircut*, where the collateral is sold at a discount. Following [36], we define market liquidity as follows.

Definition IV.3 (Market liquidity)**.** A measure of the extent to which a market can facilitate the trade of an asset at short notice, low cost and with little impact on its price.

The liquidity available in a market implies a security constraint: in expectations, over a certain time horizon, DeFi marketplaces can offer enough liquidity that in the event of a sustained period of negative price shocks, a protocol will be able to liquidate its collateral quickly enough to cover its outstanding debt liabilities.

For a time interval $[0, T]$ this can be expressed as:

$$\int_0^T \mathbb{E}[\Omega] d\Omega \leq \mathbb{E}[\Omega_{max}] \tag{3}$$

where Ω denotes the total notional traded value, i.e., the (average) price multiplied by the quantity for each trade. For a given trade ω of size q, $\omega = \bar{p}q$; aggregating these trades for a total number of trades J provides $\Omega = \sum_{j \in J}^{J} \omega_j$. Ω_{max} denotes the maximum notional value that could be sold off during a period of distress in the financial markets.

In the event of a severe price crash, on the assumption that a protocol is collateralized to a representative 150%, we assume a protocol will seize 100% of the debt value from the collateral pool, and seek to sell this collateral as quickly as possible on a market pair to the debt asset. Once a buyer has traded the debt asset d for the collateral, the protocol could then burn the debt d, effectively taking it out of circulation, offsetting the liability. Therefore, the impact that negative price shocks would have on a DeFi lending protocol, and how quickly they materialize, depend on liquidity available on all collateral/debt pairs. In the event of a liquidity crisis, the demand for liquidity outstrips supply[16], such that equation (3) is binding. Indeed, if equation 3 is binding there are not enough buyers in the market to buy the ETH that is for sale.

The Counterparty Risk Constraint. DeFi lending protocols are not fully decentralized on account of, for instance, the possibility of oracle attacks (which could cause a flash-crash), as well as privileged access to the smart contracts. Therefore it is necessary to either assume the "operator" of the protocol is honest, or that the operator only offers the services of the protocol provided they are profitable for them. We formally model this counterparty risk by assuming that its existence in a given protocol creates a risk premium, ψ, such that for an agent deciding between earning a return in a DeFi lending protocol vs elsewhere, the expected return in the DeFi protocol (r_D), once adjusted for the risk premium (ψ), must be higher than an outside return r_f. Formally, we have participation constraint $r_D - \psi > r_f$. This constraint is a participation constraint, and in Section V we assume that this inequality holds, such that agents have already chosen to participate in the protocol.

There exists an inherent trade-off in counterparty risk. On the one hand, governance mechanisms implemented through voting allow for a certain degree of decentralization whereby multiple protocol participants can influence the future direction of a protocol. Depending on the distribution of tokens, this may reduce the risk of one party becoming malicious. However, it also opens the door to attacks on the voting system, as we introduced in Section III. On the other hand, a single 'benevolent dictator' who controls the governance mechanism can prevent the attacks introduced in Section III. Yet this requires trusting that this central entity does not lose or expose its private keys controlling access to the smart contracts governing the protocol and that this central party cannot be bribed to behave maliciously.

V. Stress-Testing DeFi Lending

This section considers the financial security of a generic DeFi lending protocol, stress-testing the architecture to quantitatively assess its robustness as inspired by central banks [37], [43].

A. Stress-Testing Framework

Central banks conduct stress tests of banking systems to test their ability to withstand shocks. For example, in an annual stress test, the Bank of England examines what the potential impact would be of an adverse scenario on the banking system [37]. The hypothetical scenario is a "tail-risk" scenario, which seeks to be broad and severe enough to capture a range of adverse shocks. Following such best practice, we devise and implement a stress-test of the DeFi architecture.

B. Simulation Approach

We leverage the generic DeFi lending protocol architecture as developed in Section IV-A. We focus on a single

[15]There is evidence that crypto-assets display high intra-class correlation, limiting the advantage of diversification [26].

[16]Indeed, such liquidity crises were at the heart of the Financial crisis of 2007-8, as the value of many financial instruments traded by banks fell sharply without buyers [1].

collateral asset here for tractability, but this analysis can be extended lending protocols which rely on overcollateralization by multiple volatile collateral assets in combination with reserve assets. In part reflecting Appendix C Table II, we make the following assumptions about the initial state of the system.

1) The lending protocol allows users to deposit ETH as their single source of collateral c_i.
2) The lending protocol has 1m tokens of a generic reserve asset, which at the start of the simulation has the same price as ETH but with exactly half of the historical standard deviation of ETH taken over the sample period.
3) By arbitrage among borrowers, before the crash the lending protocol as a whole is collateralized to $\lambda_i + \epsilon$, i.e., just above the minimum collateralization ratio.
4) At the start of the crisis, the protocol has a collateralization ratio of exactly 150%, such that every USD of debt is backed by 1.50 USD of collateral.
5) Each unit of debt d^k maintains a peg of 1:1 to the US dollar, allowing us to abstract from the dynamics of maintaining the peg.
6) At the start of the sell-off, it is possible to sell 30,000 ETH per day without having an impact on price.[17].
7) The amount of reserve asset Π is fixed at the start of the sell-off at 1m units.
8) System debt levels range from 100m USD to 400m USD, seeking to approximately reflect the levels of capital escrowed in DeFi protocols as in Appendix C Table I.

Next, we detail the methodology we follow to obtain our simulation results.

Price simulation. Firstly, we obtain OHLCV data at daily frequency [14], focusing on the period January 1st, 2018 to February 7th, 2020, incorporating the large fall in the ETH price in early 2018. We present the evolution of ETH close prices in Appendix D Fig. 8 and a histogram of log returns in Appendix D Fig. 9. Perhaps the most notable element is the decline in the ETH/USD price over the course of 2018, with the price of ETH falling from an all-time-high of 1,432.88 USD to c. 220 USD as of February 7th, 2020. Taking parameters from this historical data[18], we use Monte Carlo simulation to capture how the ETH and reserve prices may be expected to evolve over the next 100 days. Monte Carlo simulation leverages randomness to produce a range of outcomes of a stochastic system. We simulate 5,000 randomly generated paths, using a geometric Brownian motion, specified with the following equation.

$$P_{c_{i,t}} = P_{c_{i,0}} \exp\left[(\mu_i - \frac{\sigma_i^2}{2})t + \sigma_i W_t\right] \tag{4}$$

W_t denotes a Wiener process [51] and for collateral type i μ_i denotes the drift and σ_i denotes the volatility.[19] Of the 5,000 simulations, our subsequent analysis is focused on the iteration which yields the fastest undercollateralization event. By focusing on this worst-case, we test the DeFi lending protocol with a "black swan" event, representing a severe challenge to its robustness.

System simulation. We propose a simple model for the decline in liquidity over time as follows.

$$L = L_0 \exp(-\rho t) \tag{5}$$

where L_0 denotes the initial amount of ETH that can be sold per day. Intuitively, this equation captures the notion that in the event that the protocol attempts to sell large volumes each period, the amount of liquidity available in the next period will be lower.

In this simulation approach, we make a simplification by not modeling the impact that selling large volumes of collateral will have on the price of the collateral asset. It is highly likely that in such a sell-off scenario, the selling of large volumes would serve to endogenously push the price lower. Therefore what we present here represents an upper bound on the price behavior: in reality, the price drop may be even worse than the one we examine.

C. Simulation Results

We start with the Monte Carlo simulation of the correlated asset paths, before considering the impact this would have on a DeFi lending protocol and an ecosystem of multiple lending protocols.

Monte Carlo Price Simulation. To capture the effects of different correlations between the collateral asset and the reserve asset, we consider three different extents of correlation between the collateral and reserve asset: (i) strong, positive correlation (0.9), (ii) weak, positive correlation (0.1) and (iii) strong negative correlation (-0.9). We then generate correlated asset paths during the Monte Carlo simulation process. In this section we report results for strong correlation, but include those for weak correlation and strong negative correlation in Appendix E.

Fig. 3 shows the results of 5,000 runs of the Monte Carlo simulator for the ETH price, and Appendix E Fig. 10 shows the results for the reserve asset price in the presence of strong positive correlation in the asset price returns. The starting prices of assets as used in the simulator is the close price of ETH/USD on February 7th, 2020.

[17]This assumption is based on the 24-hour volume of ETH/DAI across markets listed on CoinGecko on February 7th, 2020, and as such is only a rough proxy for the market liquidity. We use this figure only as a baseline for parameterization and to highlight the theoretical possibility of illiquidity causing default.

[18]For the daily ETH/USD price data we find mean log returns of 0.001592 and standard deviation 0.050581, parameter values which have been independently verified.

[19]In this estimation, we draw shocks from the normal distribution, as is standard in GBM. Since performing a Jarque-Bera test [24] over the sample period suggests that the log-returns are non-normal, it is possible that in our estimation we underestimate the impact of heavy tails. Therefore, we present a best-case upper bound; in practice, undercollateralization could precipitate more quickly.

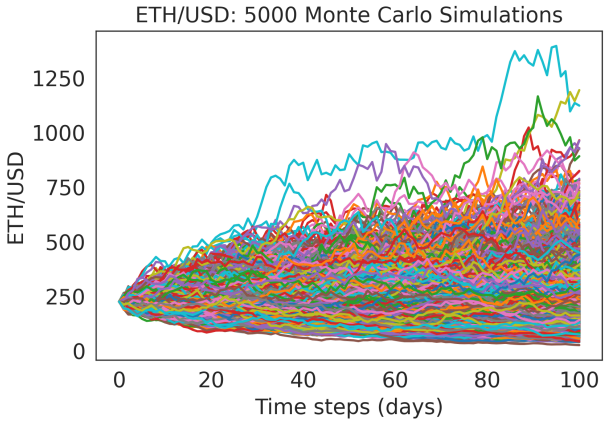

Fig. 3: Monte Carlo forecast of ETH prices over the next 100 days from February 7th, 2020.

We isolate the simulation which yields the fastest undercollateralization event.[20] In Appendix E Fig. 11 it is clear that in this worst case scenario for the ETH/USD price, the price of the reserve asset similarly falls. This illustrates the risk of using a reserve asset which is positively correlated with the collateral asset: if the price of the collateral asset falls, relative to the same basis of value the reserve asset value is likely to fall, limiting the ability of a DeFi lending protocol to recapitalize itself.

Impact on Collateral Margin. We take the simulation yielding the fastest undercollateralization event and consider the impact this would have on the collateral margin of a DeFi lending protocol. The main results of this are presented in Fig. 4. Plotted with solid lines is the evolution of the total collateral margin (comprising the collateral and the reserve asset) over time as the prices of the collateral asset and reserve asset decline. The dashed lines indicate how the amount of system debt evolves through time, on the assumption that at the start of the 100 day period, the protocol seeks to sell off all of the debt. The speed at which the debt can be liquidated through the sale of its backing collateral in turn depends on the available liquidity in the market for which we consider 3 cases:

1) constant liquidity (such that it is possible to sell a constant amount of ETH every day at the average daily price)
2) mild illiquidity (where the illiquidity parameter is arbitrarily set to some low level $\rho = 0.005$)
3) illiquidity, such that $\rho = 0.01$.

Where the initial system debt level is 100m USD, regardless of the liquidity parameter, the collateral margin does not become negative. However, at higher levels of debt, we see that the margin gets closer to 0, and once the debt level reaches 400m USD, the margin does indeed fall below 0, such that the protocol is undercollateralized overall. In the fourth panel of Fig. 4 we see that after 19 days of the protocol attempting to liquidate as much debt as possible, due to illiquidity it is unable to liquidate in time and the margin becomes negative. This would constitute a crisis in a DeFi protocol: each unit of debt would not have sufficient collateral backing, and rational agents would walk away from the protocol without repaying their debt.[21] Notably, the results presented in the Appendix E show that a weakly correlated reserve asset is able to slow or prevent the collateral margin from becoming negative (see Appendix E Fig. 13) while a strongly negative correlation between the assets is actually able to bolster the collateral margin (see Appendix E Fig. 15).

For the case where the collateral and reserve assets are strongly positively correlated, we consider how *quickly* a crisis may materialize for varying starting values of ETH liquidity and initial debt in Fig. 5. Fig. 5 shows that for a given amount of debt, the lower the starting liquidity (i.e., the amount that can be sold within 24 hours), the faster a negative margin precipitates. Similarly, for a fixed initial starting liquidity, the more debt there is in the system the faster the margin will become negative, down to below 15 days.

VI. Related Work

There is a paucity of directly related work. However, existing work can be divided into the following categories. A series of fundamental results in relation to the ability of non-custodial stablecoins to maintain their peg is provided in [25]. It is shown that stablecoins face deleveraging spirals which cause illiquidity during crises, and that stablecoins have *stable* and *unstable* domains. The model primarily involves the assumption of two types of agents in the marketplace: the stablecoin holder (who wants stability), and the speculator (who seeks leverage). The authors further demonstrate that such systems are susceptible to tail volatility. While unpublished, [10] uses option pricing theory to design dual-class structures that offer fixed income stable coins that are pegged to fiat currency. Further, [39] considers how one might build an asset-backed cryptocurrency through the use of hedging techniques.

VII. Conclusions

This paper has sought to demonstrate that, as they stand, DeFi lending protocols are liable to a variety of attack vectors. Firstly, we show the feasibility of an attack on the governance mechanism of Maker, finding that, prior to the fix implemented by Maker, provided an attacker was able to lock 27.5m USD of governance tokens they would have been able to steal all 0.5bn USD worth of collateral within two blocks. Therein we presented a novel strategy

[20] We plot the co-evolution of the asset price paths for strong correlation in Appendix E Fig. 11.

[21] In the event that strong-identities (i.e., where the mapping between an agent an an online identity is one-to-one and time invariant) are enforced on-chain, this calculus may change for agents, reducing the probability of a crisis by increasing the costs to the agent of reneging on their debt commitments. In this paper we proceed under the assumption that strong-identities are not enforced.

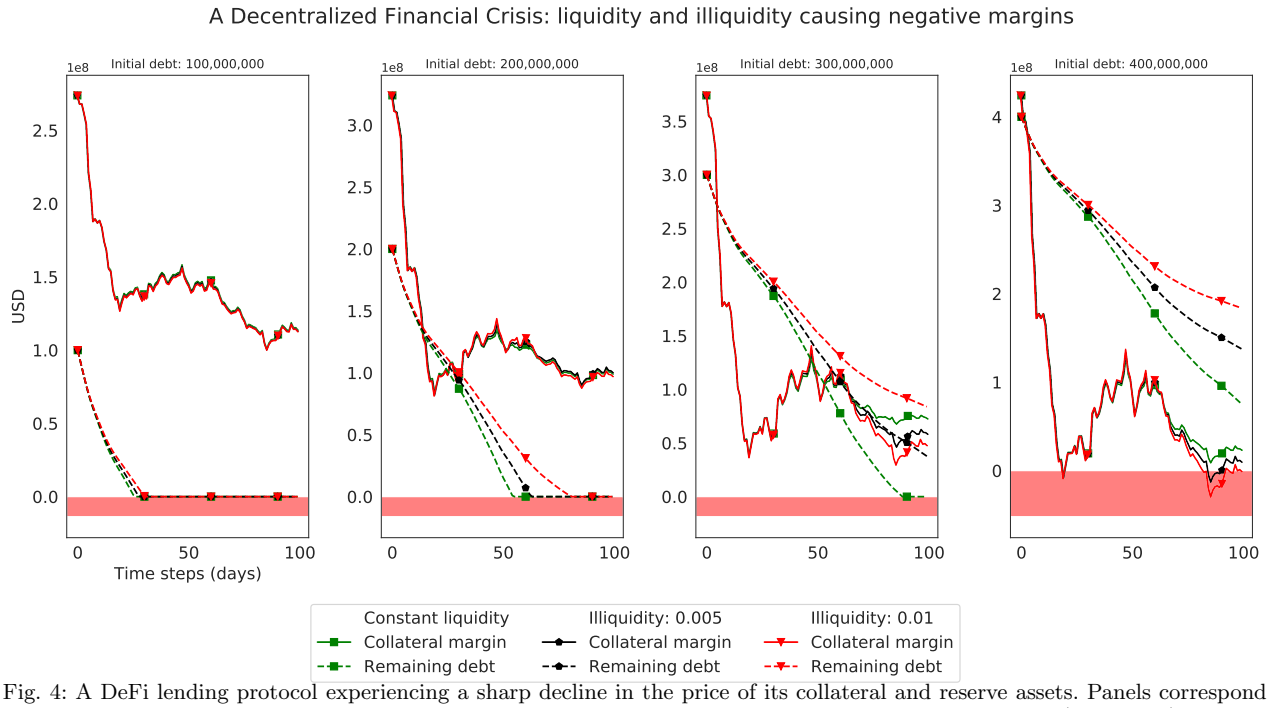

Fig. 4: A DeFi lending protocol experiencing a sharp decline in the price of its collateral and reserve assets. Panels correspond to four different levels of system debt, with each panel showing the evolution of the collateral margin (solid lines) and the total debt outstanding (dashed lines). Each panel also shows the consequences of different liquidity parameters. The margin becomes negative in panels 3 and 4— entering the red region below zero—the situation in which the lending protocol has become undercollateralized.

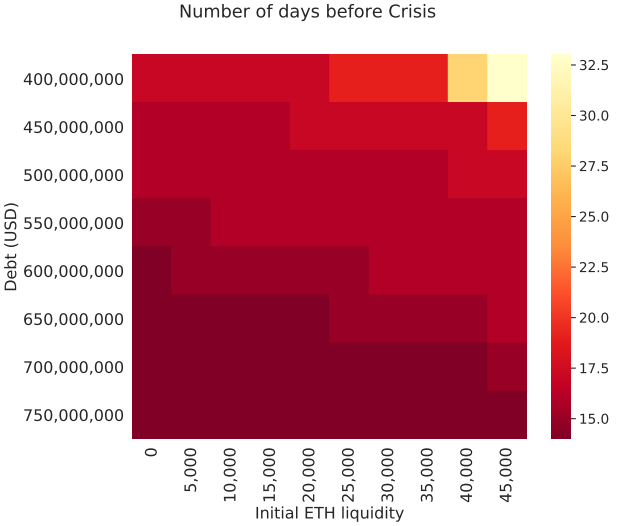

Fig. 5: Number of days before the collateral margin becomes negative, depending on the amount of system debt and the initial amount of ETH that can be sold within 24 hours.

that would have enabled an attacker to steal the collateral within two transactions without the need to escrow any assets.

Secondly, after providing formal constraints on the robust operation of a DeFi lending protocol, we use simulations to show that a for given parameters a DeFi lending protocol may become under-collateralized. We describe the interrelation of market liquidity and outstanding debt, showing how the larger the debt, or the less liquid a market, the faster insolvency can occur. We also consider different levels of correlation between the collateral and the reserve asset in a DeFi lending protocol and show that having a reserve asset that is weakly positively correlated or indeed negatively correlated can help to ensure protocol solvency.

These two types of failure mode in a DeFi protocol are potentially mutually reinforcing. If the collateral and reserve assets of a DeFi lending protocol experience a sharp decline in price, the cost of acquiring enough governance tokens to undertake the governance attack would also likely fall. Conversely, should an actor undertake a governance attack, this would plausibly send shock waves throughout the DeFi ecosystem, serving to reduce the price of the collateral asset, in turn making undercollateralization more likely.

Acknowledgments

The authors thank the reviewers for their valuable comments to improve the paper, and MakerDAO for their feedback. This work has been partially supported by EPSRC Standard Research Studentship (DTP) (EP/R513052/1) and the Tezos Foundation.

References

[1] Three myths that sustain the economic crisis. *The Guardian*, Aug 2012.

[2] Aave. Aave Liquidity Pools. https://app.aave.com/borrow, 2020.

[3] Aave. Aave Protocol. https://github.com/aave/aave-protocol, 2020.

[4] Franklin Allen and Douglas Gale. Financial contagion. *Journal of political economy*, 108(1):1–33, 2000.

[5] Christian Badertscher, Peter Gaži, Aggelos Kiayias, Alexander Russell, and Vassilis Zikas. Ouroboros genesis: Composable proof-of-stake blockchains with dynamic availability. In *Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security*, pages 913–930, 2018.

[6] Christian Badertscher, Ueli Maurer, Daniel Tschudi, and Vassilis Zikas. Bitcoin as a transaction ledger: A composable treatment. In *Annual International Cryptology Conference*, pages 324–356. Springer, 2017.

[7] Bancor. Bancor. https://www.bancor.network/, 2020.

[8] BBC. BBC World Service, Aftershock Timeline. http://www.bbc.co.uk/worldservice/business/2009/09/090902_aftershock_timeline_noflash.shtml, 2009.

[9] Lehman Brothers. Lehman brothers holdings inc. plan trust – '10-k' for 11/30/07, 2007.

[10] Yizhou Cao, Min Dai, Steven Kou, Lewei Li, and Chen Yang. Designing stable coins. 2018.

[11] Miguel Castro and Barbara Liskov. Practical Byzantine Fault Tolerance. In *Proceedings of the Third Symposium on Operating Systems Design and Implementation*, number February, pages 173–186, 1999.

[12] CoinMarketCap. Maker (MKR) price, charts, market cap, and other metrics. https://coinmarketcap.com/currencies/maker/, 2020.

[13] Connext. Connext. https://connext.network/, 2020.

[14] CryptoCompare. Cryptocompare. https://www.cryptocompare.com/, 2020.

[15] Bernardo David, Peter Gaži, Aggelos Kiayias, and Alexander Russell. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 66–98. Springer, 2018.

[16] dYdX. dYdX. https://dydx.exchange/, 2020.

[17] Timothy C Earle. Trust, confidence, and the 2008 global financial crisis. *Risk Analysis: An International Journal*, 29(6):785–792, 2009.

[18] Erasure. A new staking protocol powered by NMR. https://erasure.world/, 2020.

[19] Compound Finance. Compound finance, 2019.

[20] The Maker Foundation. Makerdao. https://makerdao.com/en/, 2019.

[21] Dominik Harz, Lewis Gudgeon, Arthur Gervais, and William J Knottenbelt. Balance: Dynamic adjustment of cryptocurrency deposits. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1485–1502. ACM, 2019.

[22] i3nikolai. Note on MKR voting and distribution. https://www.reddit.com/r/MakerDAO/comments/enpad1/note_on_mkr_voting_and_distribution/, 2020.

[23] InstaDApp. InstaDApp: Trustless smart wallet for DeFi. https://instadapp.io/, 2020.

[24] Carlos M Jarque and Anil K Bera. A test for normality of observations and regression residuals. *International Statistical Review/Revue Internationale de Statistique*, pages 163–172, 1987.

[25] Ariah Klages-Mundt and Andreea Minca. (in) stability for the blockchain: Deleveraging spirals and stablecoin attacks. *arXiv preprint arXiv:1906.02152*, 2019.

[26] Aikaterina Koutsouri, Francesco Poli, Elise Alfieri, Michael Petch, Walter Distaso, and William Knottenbelt. Balancing cryptoassets and gold: A weighted-risk contribution index for the alternative asset space. *Mathematical Research for Blockchain Economy, Forthcoming*, 2019.

[27] Kyber. Kyber. https://kyber.network/, 2020.

[28] Maker. The Governance Security Module (GSM). https://blog.makerdao.com/governance-security-module-gsm/, 2019.

[29] Maker. Governance Security Module (GSM) vote. https://forum.makerdao.com/t/signal-request-should-we-have-another-executive-vote-regarding-the-governance-security-module/1209/25, 2020.

[30] MelonProject. Melon Project. https://github.com/melonproject/melon-lab/releases, 2020.

[31] Micah Zoltu. How to turn $20M into $340M in 15 seconds. https://medium.com/coinmonks/how-to-turn-20m-into-340m-in-15-seconds-48d161a42311, 2019.

[32] Andrew Miller, Yu Xia, Kyle Croman, Elaine Shi, and Dawn Song. The Honey Badger of BFT Protocols. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security - CCS'16*, (Section 3):31–42, 2016.

[33] Nexus Mutual. Nexus Mutual. https://nexusmutual.io/, 2020.

[34] Satoshi Nakamoto et al. Bitcoin: A peer-to-peer electronic cash system. 2008.

[35] Lighting Network. Lightning Network. https://lightning.network/, 2020.

[36] Kleopatra Nikolaou. Liquidity (risk) concepts: definitions and interactions. 2009.

[37] Bank of England. Stress testing the uk banking system: key elements of the 2019 annual cyclical scenario, 2019.

[38] Rafael Pass, Lior Seeman, and Abhi Shelat. Analysis of the blockchain protocol in asynchronous networks. In *Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pages 643–673. Springer, 2017.

[39] Alex Lipton Thomas Hardjono Alex Pentland. Digital trade coin (dtc): Towards a more stable digital currency. 2018.

[40] Daniel Perez and Benjamin Livshits. Broken metre: Attacking resource metering in evm. *arXiv preprint arXiv:1909.07220*, 2019.

[41] DeFi Pulse. The DeFi Leaderboard. https://defipulse.com/, 2019.

[42] DeFi Pulse. What is defi?, 2019.

[43] The Federal Reserve. Dodd-frank act stress tests. https://www.federalreserve.gov/supervisionreg/dfa-stress-tests.htm, 2019.

[44] SECBIT. How the winner got Fomo3D prize — A Detailed Explanation. https://medium.com/coinmonks/how-the-winner-got-fomo3d-prize-a-detailed-explanation-b30a69b7813f, 2018.

[45] Synthetix. Synthetix: Decentralized synthetic assets. https://www.synthetix.io/, 2020.

[46] Nassim Nicholas Taleb. *The black swan: The impact of the highly improbable*, volume 2. Random house, 2007.

[47] TokenSets. TokenSets. https://www.tokensets.com/, 2020.

[48] Uniswap. Uniswap. https://uniswap.io/, 2020.

[49] WBTC. Wbtc. https://www.wbtc.network/, 2020.

[50] Week in Ethereum News. Week in Ethereum News December 28, 2019. https://weekinethereumnews.com/week-in-ethereum-news-december-28-2019/, 2020.

[51] Norbert Wiener. Collected works, vol. 1, 1976.

Appendix

A. Existing DeFi protocols

	Project	Capital (USD)	Blockchain
Lending	Maker [20]	342.9m	Ethereum
	Compound [19]	91.6m	Ethereum
	Aave [3]	36.4m	Ethereum
DEX	Uniswap [48]	35.7m	Ethereum
	Bancor [7]	7.2m	Ethereum
	Kyber [27]	3.9m	Ethereum
Derivatives	Synthetix [45]	101.9m	Ethereum
	Nexus [33]	2.7m	Ethereum
	Erasure [18]	1.2m	Ethereum
Payments	Lightning [35]	6.5m	Bitcoin
	Connext [13]	12.1k	Ethereum
Assets	token Sets [47]	9m	Ethereum
	WBTC [49]	7.3m	Ethereum
	Melon [30]	221.9k	Ethereum

TABLE I: Existing DeFi projects [41] (April 15th, 2020).

B. Governance Attack on Maker

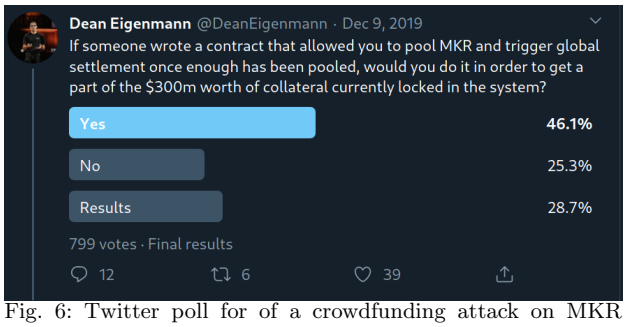

Fig. 6: Twitter poll for of a crowdfunding attack on MKR governance.

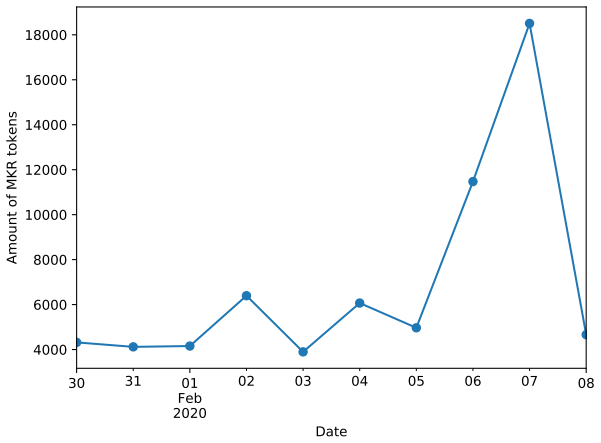

Fig. 7: Daily traded volume of MKR tokens between 2020-01-30 and 2020-02-08.

C. Parameters of DeFi lending platforms

Protocol	Collateral asset (liquidation ratio)	Reserve asset
Maker [20]	ETH (150%), BAT (150%), USDC (125%)	MKR
Compound [19]	ETH (133%), BAT (167%), DAI (133%) REP (250%), USDC (133%), ZRX (167%)	
Aave [3]	DAI (125%), USDC (125%), TUSD (125%) ETH (125%), LEND (154%), BAT (154%) KNC (154%), LINK (143%), MANA (154%) MKR (154%), REP (154%), WBTC (154%) ZRX (154%)	
dYdX [16]	ETH (115%), USDC (115%), DAI (115%)	

TABLE II: Parameters of DeFi lending platforms, comprising 93% of DeFi market as of April 15th, 2020.

D. Price data

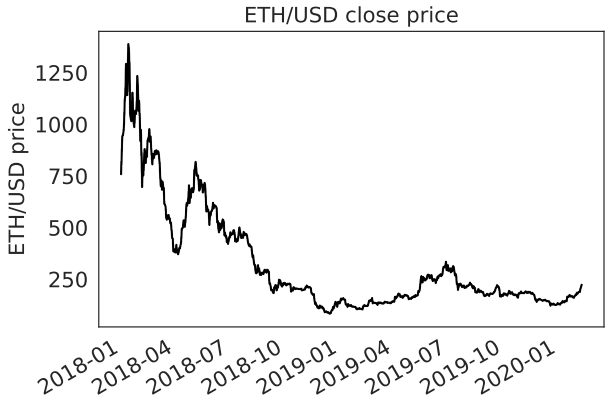

Fig. 8: Close prices for ETH/USD over the period January 1st, 2018 to February 7th, 2020.

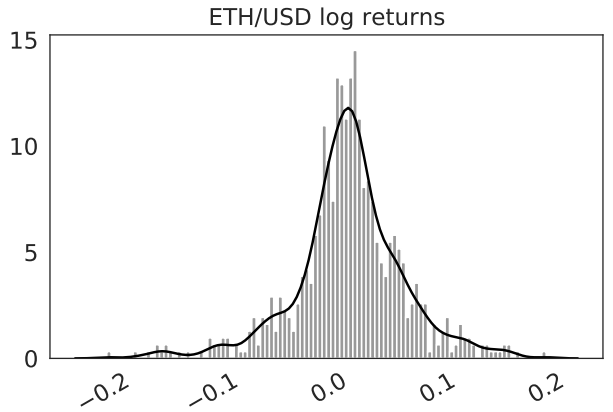

Fig. 9: Log returns for ETH/USD over the period January 1st, 2018 to February 7th, 2020.

E. Simulation results

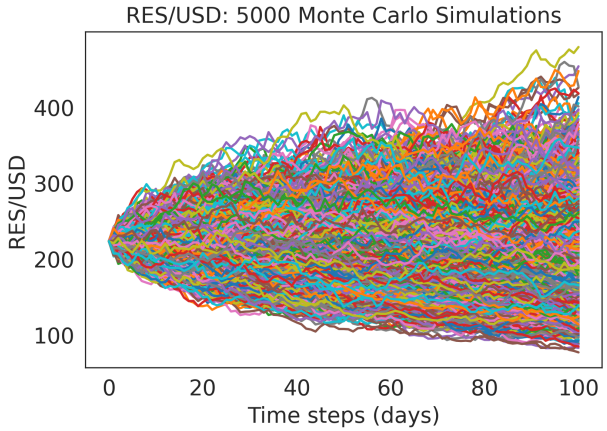

Fig. 10: Monte Carlo forecast of the reserve asset price over the next 100 days from February 7th, 2020.

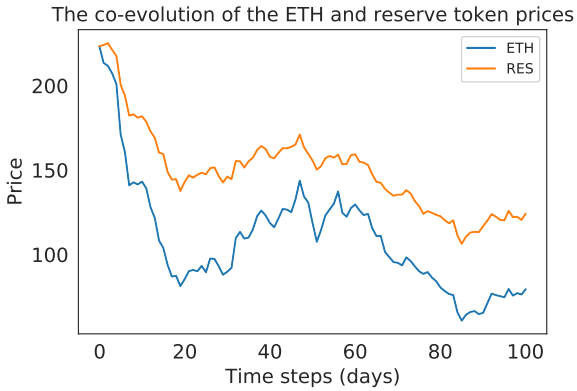

Fig. 11: For the simulation yielding the fastest undercollateralization event, the co-evolution of the ETH and reserve asset prices where the asset price returns are strongly positively correlated.

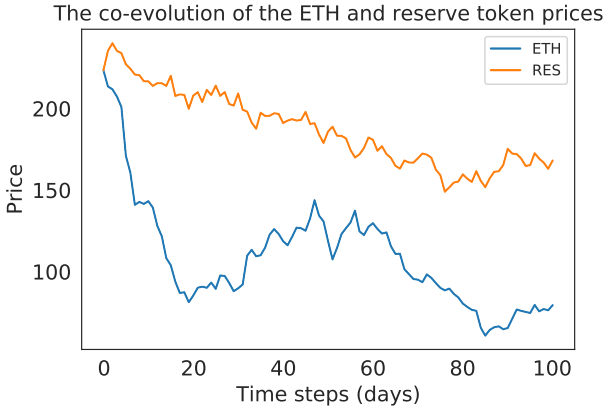

Fig. 12: For the simulation yielding the fastest undercollateralization event, the co-evolution of the ETH and reserve asset prices where the asset price returns are weakly positively correlated.

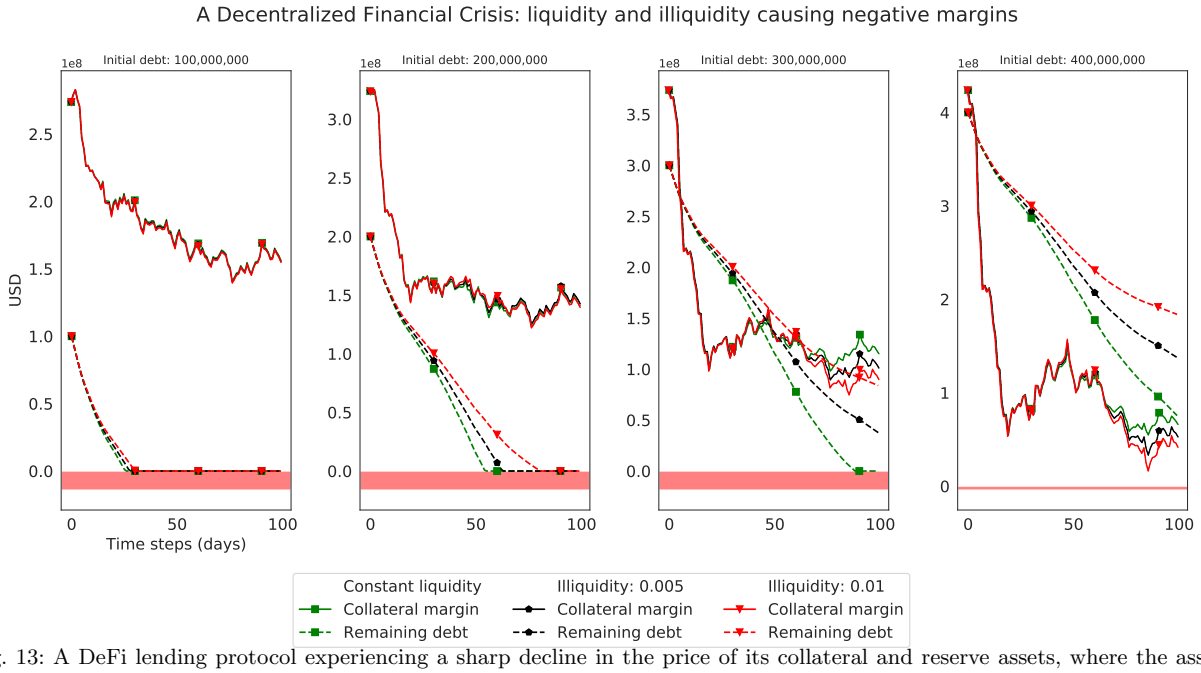

Fig. 13: A DeFi lending protocol experiencing a sharp decline in the price of its collateral and reserve assets, where the assets have a correlation of 0.1. Panels correspond to 4 different levels of system debt, with each panel showing the evolution of the collateral margin and the total debt outstanding. Each panel also shows the consequences of different liquidity parameters.

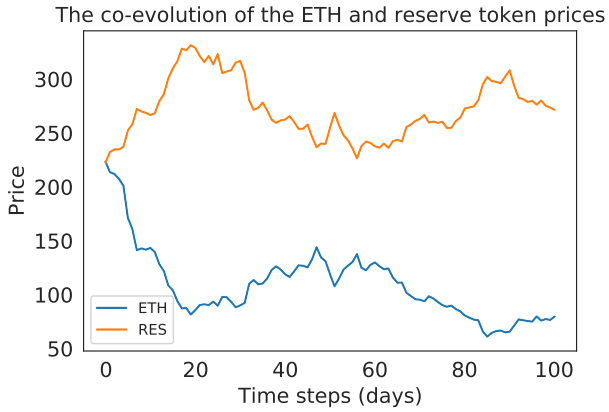

Fig. 14: For the simulation yielding the fastest undercollateralization event, the co-evolution of the ETH and reserve asset prices where the asset price returns are strongly negatively correlated.

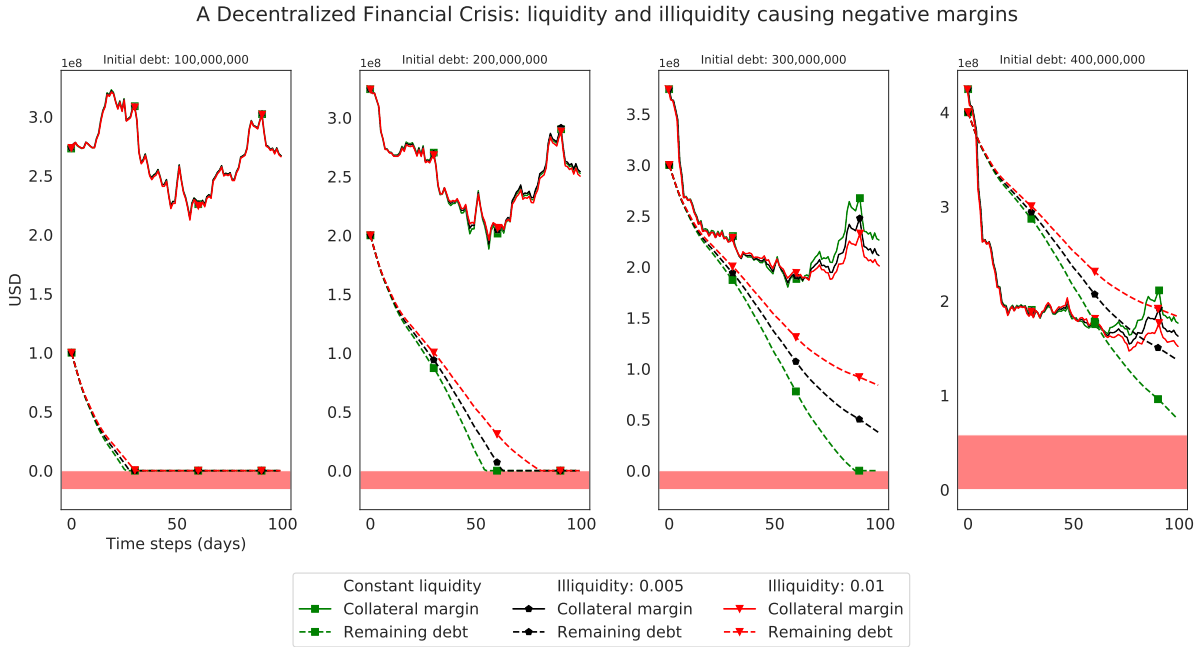

Fig. 15: A DeFi lending protocol experiencing a sharp decline in the price of its collateral asset with a negatively correlated reserve asset, where the assets have a correlation of -0.9. Panels correspond to 4 different levels of system debt, with each panel showing the evolution of the collateral margin and the total debt outstanding. Each panel also shows the consequences of different liquidity parameters.