

Auto.gov: Learning-based On-chain Governance for Decentralized Finance (DeFi)

Jiahua Xu

jiahua.xu@ucl.ac.uk

UCL, Centre for Blockchain Technologies
DLT Science Foundation
London, UK

Yebo Feng

yebof@uoregon.edu

University of Oregon
Eugene, USA

Daniel Perez

daniel.perez@imperial.ac.uk
Imperial College London
London, UK

Benjamin Livshits

b.livshits@imperial.ac.uk

Imperial College London
UCL, Centre for Blockchain Technologies
DLT Science Foundation
London, UK

ABSTRACT

In recent years, decentralized finance (DeFi) has experienced remarkable growth, with various protocols such as lending protocols and automated market makers (AMMs) emerging. Traditionally, these protocols employ off-chain governance, where token holders vote to modify parameters. However, manual parameter adjustment, often conducted by the protocol's core team, is vulnerable to collusion, compromising the integrity and security of the system. Furthermore, purely deterministic, algorithm-based approaches may expose the protocol to novel exploits and attacks.

In this paper, we present "Auto.gov", a learning-based on-chain governance framework for DeFi that enhances security and reduces susceptibility to attacks. Our model leverages a deep Q-network (DQN) reinforcement learning approach to propose semi-automated, intuitive governance proposals with quantitative justifications. This methodology enables the system to efficiently adapt to and mitigate the negative impact of malicious behaviors, such as price oracle attacks, more effectively than benchmark models. Our evaluation demonstrates that Auto.gov offers a more reactive, objective, efficient, and resilient solution compared to existing manual processes, thereby significantly bolstering the security and, ultimately, enhancing the profitability of DeFi protocols.

CCS CONCEPTS

- Security and privacy → Web application security;
- Applied computing → Economics;
- Social and professional topics → Financial crime.

KEYWORDS

decentralized finance (DeFi), governance, reinforcement learning, DeFi protocol, price oracle attack

1 INTRODUCTION

Governance is a crucial aspect of blockchain-based systems, designed to ensure their stability, integrity, and security [14]. Despite blockchains' ability to store transaction histories without relying on trusted third parties, certain decisions in blockchain systems require an orchestration or *governance* processes. This requirement

applies to both chains such as Bitcoin and Ethereum (sometimes called layer-1 chains) as well as higher-level developments, such as *decentralized protocols*. One of the reasons behind the excitement surrounding blockchain is the emergence of DeFi [29] in the last two years.

DeFi protocols [11] (such as Aave, Compound, Uniswap, Curve) allow individuals to transact on the Ethereum chain, while exchanging tokens, borrowing, lending, etc. in a manner that does not require a bank or another trusted provider of this sort. DeFi protocols have now billions of dollars locked in them, with hundreds of millions of dollars in daily volume [30].

Because DeFi protocols are *parametrized*, a governance process is generally needed to adjust protocol parameters [8, 17, 19]. As an example, updating the collateral factor for a lending pool or changing a protocol's fee scheme is a governance process. As a norm, proposals on protocol changes are first posted on the protocol's forum, where they are discussed by the community. The decision of whether or not adopting a particular proposal is generally subjected

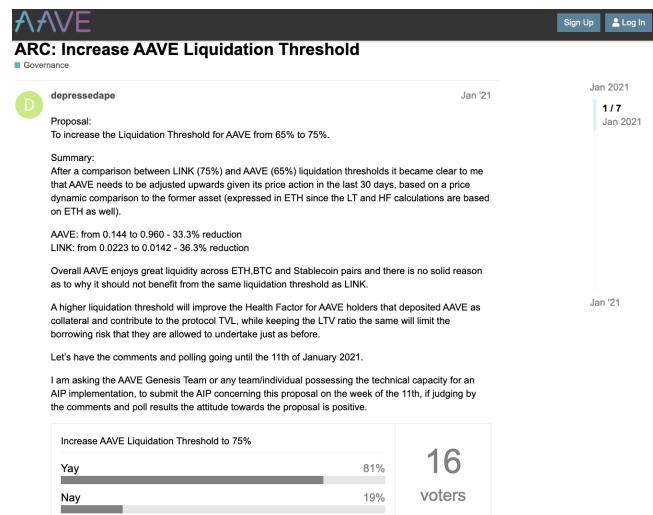


Figure 1: A post proposing to update a risk parameter

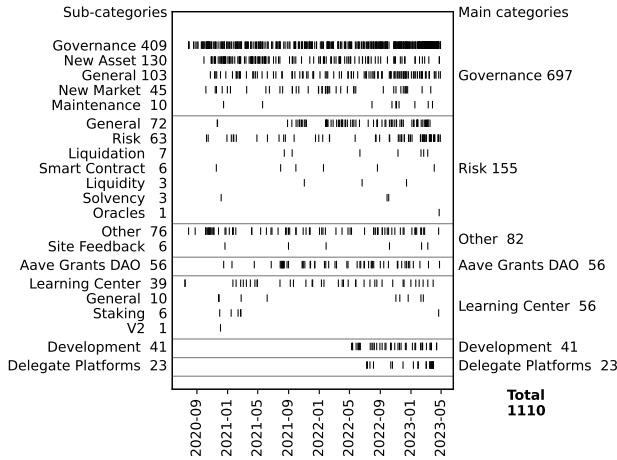


Figure 2: Statistics of posts on Aave governance forum

to a vote by holders of the governance tokens of the appropriate protocol and voting is done in the open [3] on platforms such as snapshot (snapshot.org) and Tally (tally.xyz).

As an example, Figure 1 exhibits an governance proposal. On 3 Jan 2021, a community member posted on the AAVE (the protocol) governance forum proposing to increase the liquidation threshold—one of the risk parameters—for the AAVE (the underlying token) market. The person justified his proposal by quoting the price performance of the AAVE token compared to a reference token LINK. The discussion of this specific thread lasted three weeks, eventually resulting in the rejection of the proposal.

Figure 2 shows the occurrences of forum posts under various categories, totalling 1,110 posts since July 2020 until April 2023. The discussion on smart-contract-level adjustment—e.g., value of risk parameters, or acceptance or depreciation of an asset as collateral—is typically under “Governance” and “Risk”, two of the most active main categories. Evidently from Figure 2, the governance forum, especially the above-mentioned two categories, has been increasingly used during the past year, indicating the growing significance in DeFi governance perceived by the community.

Regrettably, the existing governance execution, often centrally controlled by the core team, is highly susceptible to collusion, thereby jeopardizing the system’s integrity and security. Unfortunately, strictly deterministic, algorithm-driven methods [20] could expose the protocol to novel exploits and attacks, while the manual process—comprising proposing, discussing, and voting—can be not only labor-intensive and time-consuming but also ineffective [10]. As demonstrated in Appendix A, which presents the time series of risk parameter values juxtaposed with various crypto-assets’ market conditions on AAVE, the risk parameters often remain constant throughout the observation period despite significant fluctuations in price volatility, market liquidity (trading volume), and utilization ratio.

These challenges underscore the need for a refined governance process capable of bolstering the security of DeFi systems, providing motivation for this paper. Our objective is to automate certain aspects of the protocol governance. Specifically, using the AAVE

protocol mechanism for the environment setup, we apply DQN reinforcement learning (RL) to train a governance agent that can determine the optimal protocol parameter adjustment policy, under scenarios both with and without price oracle attacks.

Our evaluation demonstrates that the proposed RL-based governance agent can adapt to a specific DeFi environment and make robust, profitable decisions in just 20 minutes of training, using only the computing resources of a personal laptop. Once trained, the agent effortlessly outperforms benchmark strategies in terms of attack impact mitigation and ultimately profit generation. Overall, the agent is adept at striking a balance between ensuring the protocol’s safety and maximizing profits.

This paper makes the following contributions:

- To the best of our knowledge, this paper represents the first attempt to integrate DeFi security and economics with artificial intelligence (AI), uncovering the high potential of this interdisciplinary area for enhancing the security of DeFi protocols;
- We abstract a DeFi environment that models the interaction between the protocol, user and external market; the environment can be easily adjusted to apply to different types of DeFi protocols and accommodate various attack scenarios;
- We quantitatively demonstrate that (semi-)automated protocol parameter adjustment through RL is not only possible but also more efficient, effective, and secure compared to the existing manual process, allowing the system to adapt to and mitigate malicious behaviors more effectively;
- We simulate attack scenarios and show that the trained model remains robust against attacks, enhancing the overall security and ultimately profitability of DeFi systems.

The remainder of this paper is organized as follows. In Section 2, we introduce our environment modeling approach, followed by the environment initiation in Section 3. We then describe the development of the governance agent in Section 4. Our approach is evaluated in Section 5, and potential improvements are discussed in Section 6. Subsequently, we present related work in Section 7 and conclude our paper in Section 8. Our implementation is open-source and accessible at <https://github.com/xujiahuyz/auto-gov>.

2 ENVIRONMENT MODELING

We model and establish a simplified DeFi environment for our RL experiments. The environment consists of an aggregate market user and an AAVE-like lending protocol.

2.1 DeFi lending protocol—a primer

An AAVE-like DeFi lending protocol, in a nutshell, enables users to deposit their assets into one or more lending pools to earn interest and borrow assets from the same or other lending pools by collateralizing their deposited assets. The protocol is secured through overcollateralization and liquidation mechanisms. Specifically, a user’s aggregate borrow position must not exceed the aggregate loanable value backed by their collateral. The aggregate loanable value equals the sum of the collateralizing asset value discounted with each asset’s liquidation threshold, which is smaller than 1. If a user’s aggregate borrow position exceeds the aggregate loanable value, resulting in an “unhealthy” loan, the user’s collateral becomes

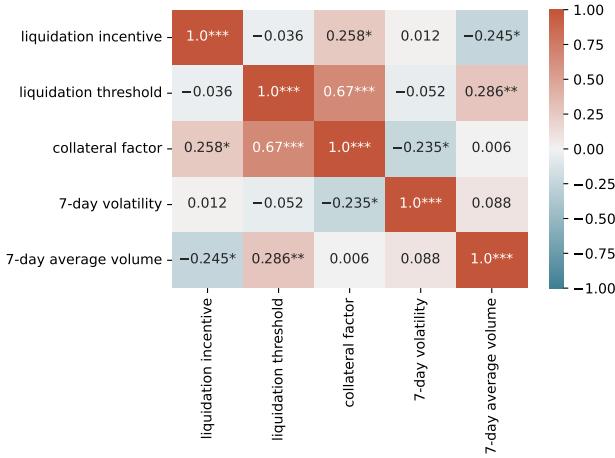


Figure 3: Correlation between risk parameters and asset risk metrics of assets of AAVE

immediately liquidatable by any network participant who repays (part of) the borrow position with a bonus. The bonus, designed to incentivize swift liquidation in case of an unhealthy loan, can be obtained as the collateral a liquidator receives equals the value of the loan they repay times the liquidation incentive, another risk parameter of the protocol that is typically set slightly greater than one (see Figure 13).

Despite these mechanisms in place to protect the protocol from insolvency, it is still exposed to the risk of undercollateralization. For instance, an abrupt drop in a collateralizing asset’s price against the borrow asset it backs may cause the user’s aggregate loanable value to fall below the collateral value, before the borrow position becomes liquidated. This makes defaulting on the loan the optimal and more likely choice for the user, leading to bad debt expenses. This situation tends to occur when the collateralizing asset is volatile against the borrow asset, and the collateral factor and/or liquidation threshold is high.

In addition to usual market movements, malicious market manipulation attacks can cause the protocol to become undercollateralized with even greater certainty. For example, an attacker can temporarily inflate the price of a collateralizing asset, allowing them to borrow more than they should with the intention of never repaying (see e.g., Section 3.2.1). The protocol would only “realize” that the loan is undercollateralized when the manipulated price later restores to its true value. This common attack vector in DeFi lending protocols is known as the “price oracle attack”. Assets with a thinner market are generally more vulnerable to price manipulation.

As demonstrated above, assets with higher price stability and market liquidity risks are more likely to cause protocol insolvency, all other factors being equal. Consequently, risk parameters are set on an asset-by-asset basis and may be adjusted, albeit with low historical frequency (see Figure 13), in the event of a significant change in the asset’s risk profile. The collateral factor and liquidation threshold should theoretically be set lower for assets with

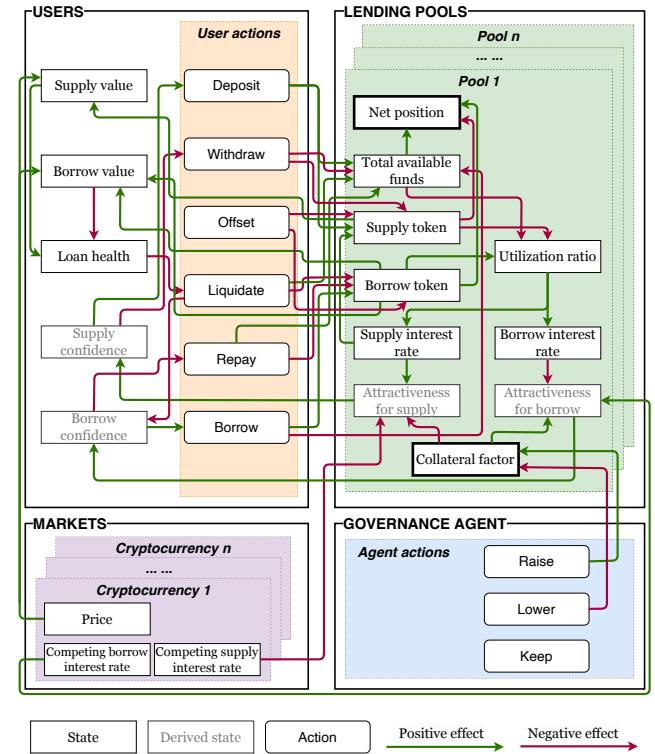


Figure 4: Action-state space of the simplified DeFi environment

higher price volatility, while the liquidation incentive should be set higher for assets with lower market liquidity.

Empirically, we observe a similar pattern. Figure 3 displays the correlation matrix between various risk parameters and asset risk metrics of assets listed on AAVE, calculated based on asset-day-level observations from January 2021 to April 2023. As expected, the collateral factor and liquidation threshold are negatively correlated with the asset’s price volatility, and the liquidation incentive is negatively correlated with the asset’s market liquidity.

2.2 Environment simplification

For the sake of simplicity and ease of experimentation, we make the following simplifications to the DeFi lending protocol:

- We include only three lending pools in the protocol, which are for WETH—the numeraire or the denominating asset of the protocol, USDC—a USD-pegged stablecoin, and TKN—some arbitrary token;
- We model only one market user, who behaves on behalf of the entire market;
- We make collateral factor the only adjustable protocol parameter by the RL agent, and assume liquidation threshold equals collateral factor;
- We do not consider liquidation incentive, as it is a zero-sum game among users (the liquidator wins and the borrower loses), and on an aggregate level, does not directly affect the protocol’s net position.

Figure 4 illustrates the complete action-state space of our RL environment, which we further elaborate in Section 2.3 and Section 2.4.

2.3 Actions a

2.3.1 Governance agent actions.

Raise / lower / keep collateral factor. When the governance agent raises, lowers or keeps the existing collateral factor of a specific lending pool, the pool’s collateral factor is increases, decreases or remains the same, respectively.

2.3.2 User actions.

Deposit. When a user deposits into a specific lending pool (namely, depositing WETH to the WETH pool, USDC to the USDC pool and so on), the pool’s total available funds increase by the deposited amount, and simultaneously, the same amount of interest-accruing supply tokens are minted.

Withdraw. When a user withdraws from a specific lending pool, the pool’s total available funds decrease by the withdrawn amount and the same amount of interest-accruing supply tokens are burned.

Borrow. When a user borrows from a specific lending pool, the pool’s total available funds decrease by the borrowed amount, and simultaneously, the same amount of interest-accruing borrow tokens are minted.

Repay. When a user repays, the pool’s total available funds increase by the repaid amount and the same amount of interest-accruing borrow tokens are burned.

Liquidate. In our simplified training environment, liquidating a borrow position updates the pool states (total available funds and interest-accruing borrow tokens) just like a repayment, but it also lowers the user’s borrow confidence.

Offset. Instead of repaying with the underlying asset, a user can also reduce the borrow position by surrendering the same amount of interest-accruing supply tokens of the same asset.

2.4 States S

2.4.1 Lending pool states.

Total available funds F_i . The total available funds of a lending pool i is the amount of its underlying token i remained in the pool available to be withdrawn or borrowed. From the accounting perspective, total available funds is on the asset side—equivalent to cash—of the pool’s balance sheet, and hence positively contributes to the pool’s net position Equation 1.

Supply tokens S_i . Supply tokens are interest-accruing tokens that keep track of the amount of funds a lending pool owes to the user throughout time. From the accounting perspective, supply tokens, bearing the nature of payables, are on the liability side of the pool’s balance sheet, and reduces the pool’s net position Equation 1. The number of supply tokens also negatively influences the utilization ratio of the pool. A user’s supply value within a pool equals the value of a user’s allocated supply tokens within that pool times the current price of the underlying token.

Borrow tokens B_i . Borrow tokens are interest-accruing tokens that keep track of the amount of funds the user owes to the lending pool throughout time. From the accounting perspective, borrow tokens, bearing the nature of receivables, are on the asset side of the pool’s balance sheet, and hence enhances the pool’s net position Equation 1. The number of borrow tokens also positively influences the utilization ratio of the pool. A user’s borrow value within a pool equals the value of a user’s allocated borrow tokens within that pool times the current price of the underlying token.

Bad debts D_i . While the lending protocol is generally secured by its overcollateralization and liquidation mechanism, under extreme market conditions, e.g. when the price of a collateral asset experiences a sudden drop, the protocol may still suffer from bad debts. Bad debts are the amount of funds that the lending protocol is unable to recover from the user; they occur when a user’s loan position is undercollateralized, leaving the user with no incentive to repay the loan and other network participants with no incentive to liquidate the position Equation 1. From the accounting perspective, bad debts are deemed expenses, and hence negatively contributes to the pool’s net position.

Net position N_i . The net position of lending protocol i measures the net worth of the lending protocol, calculated as:

$$N_i = F_i + B_i - S_i - D_i , \quad (1)$$

where F denotes the total available funds (Assets - Cash), B the borrow tokens (Assets - Receivables), S the supply tokens (Liabilities - Payables), and D the amount of bad debts (Expenses). The lending protocol becomes *insolvent* when its net position is negative.

Utilization ratio U_i . The utilization ratio of lending pool i is the ratio of the number of borrow tokens to the number of supply tokens, formally

$$U_i = \frac{B_i}{S_i} . \quad (2)$$

A low utilization ratio indicates capital inefficiency, while a high utilization ratio signals high liquidity risk of the pool. The utilization ratio is therefore used to determine the the pool’s supply and borrow interest rates through a pre-defined interest rate model, a monotone increasing function of the utilization ratio. When the utilization ratio is low, both the supply and borrow interest rates are low, in order to discourage supply and encourage borrow to drive the utilization ratio higher; when the utilization ratio becomes too high, both the supply and borrow interest rates increases exponentially, in order to discourage borrow and encourage supply to drive the utilization ratio lower and to mitigate liquidity risk.

Collateral factor C_i . The collateral factor of lending pool i determines the fraction of the user’s supply value within that pool that can be borrowed against. For example, if the collateral factor of a lending pool A is 0.2 and B 0.8, and a user has 100 supply value within pool A and 50 within pool B, then the user can borrow up to 60 ($= 100 \times 0.2 + 50 \times 0.8$) worth of funds across all lending pools. Conventionally, the collateral factor of each lending pool is manually adjusted by the protocol team based on the underlying token’s risk profile such as price volatility and level of centralization. The riskier an asset is deemed, the lower the collateral factor is set to be. A higher collateral factor means a higher borrowing

capacity, and hence a higher liquidity risk. Therefore, the collateral factor positively influences a pool's attractiveness for borrow, and negatively influences its attractiveness for supply.

Supply interest rate R_i^S . The supply interest rate of lending pool i is the interest rate that the lending pool pays to the user for supplying funds. A higher supply interest rate means a higher increasing speed for supply tokens due to interest accrual. The supply interest rate is set such that, at each step, the supply interest to be accrued can be fully covered by the borrow interest to be accrued with some spread $\Delta \in (0, 1)$:

$$R_i^S = R_i^B \cdot U_i \cdot (1 - \Delta). \quad (3)$$

Borrow interest rate R_i^B . The borrow interest rate of lending pool i is the interest rate that the user pays to the lending pool for borrowing funds. A higher borrow interest rate means a higher increasing speed for borrow tokens due to interest accrual. The borrow interest rate is set according to a pre-defined interest rate model, which in our environment, is set to be:

$$R_i^B = \frac{1}{b \cdot (1 - U_i)}, \quad (4)$$

where $b > 0$.

Attractiveness for supply. The attractiveness for supply of a lending pool is a derived state designed to model how a pool's states influence the user's willingness to supply funds to the entire lending protocol. A user's supply confidence in the lending protocol is positively affected by the aggregate attractiveness for supply of all lending pools in the protocol.

Attractiveness for borrow. The attractiveness for borrow of a lending pool is a derived state designed to model how a pool's states influence the user's willingness to borrow funds from the entire lending protocol. A user's borrow confidence in the lending protocol is positively affected by the aggregate attractiveness for borrow of all lending pools in the protocol.

2.4.2 User states.

Supply value V^S . The supply value of a user is the sum of user's supply value across all lending pools:

$$V^S = \sum_i (S_i \cdot P_i) \quad (5)$$

All other things equal, a higher supply value decreases the user's loan to value ratio, and hence increases the user's loan health.

Borrow value B^S . The borrow value of a user is the sum of user's borrow value across all lending pools:

$$B^S = \sum_i (B_i \cdot P_i) \quad (6)$$

All other things equal, a higher borrow value increases the user's loan to value ratio, and hence decreases the user's loan health.

Loan health. The loan health of a user is negatively related to the user's loan to value ratio. A healthy loan means the borrow value is backed by sufficient supply value, and an unhealthy loan triggers liquidation.

Supply confidence. The supply confidence of a user is a derived state designed to model a user's willingness to supply funds to the lending protocol. High supply confidence encourages the supply action, while low supply confidence more likely triggers the withdraw action.

Borrow confidence. The borrow confidence of a user is a derived state designed to model a user's willingness to borrow funds from the lending protocol. High borrow confidence encourages the borrow action, while low borrow confidence more likely triggers the repay action.

2.4.3 Market states.

Price P_i . The price of an underlying token of a lending pool i positively influences both the supply value and the borrow value of a user within that pool.

Competing supply interest rate $R_i^{S,c}$. The competing supply interest rate of an underlying token is the supply interest rate provided by the external market, representing the opportunity cost of supplying funds to the lending protocol i . A higher competing supply interest rate reduces the attractiveness for supply of the lending pool.

Competing borrow interest rate $R_i^{B,c}$. The competing borrow interest rate of an underlying token is the borrow interest rate provided by the external market. A higher competing borrow interest rate increases the attractiveness for borrow of the lending pool i .

2.5 Reward r

As the governance agent represents the interest of the lending protocol, we use the change in net position, a proxy of the protocol's profitability, to measure the performance of the governance agent.

3 ENVIRONMENT INITIATION

3.1 Asset price simulation

As discussed in Section 2.1, The reason for modeling three asset pools is to experiment how asset price volatilities might affect the RL agent's collateral factor determination. Two assets are insufficient to model one stable asset and one volatile asset; if Asset A is volatile against B, then B must be volatile against A. Thus, we need at least three assets to demonstrate the volatility effect on the collateral factor in a self-contained modelling environment. To this end, we include in the lending protocol environment three lending pools: WETH—which is the numeraire or the denominating asset of the protocol, USDC—which is a USD-pegged stablecoin, and TKN—which is some arbitrary token.

The initial prices—all denominated in WETH—of TKN, USDC and WETH are all normalized to 1. The token price time series P_t follow a geometric brownian motion with μ_t and σ_t that can be time-variant but are piece-wise constant within every step. The price update at each step can be formally expressed as:

$$P_t = e^{(\mu_t - \frac{\sigma_t^2}{2})t + \sigma_t W_t}, \quad (7)$$

where $W_t \sim N(0, 1)$.

As a numeraire, WETH has by definition $\mu_t \equiv 0, \sigma \equiv 0$, i.e. $P_t \equiv 1$. For USDC, we set $\mu_t \equiv 10^{-4}, \sigma_t \equiv 0.05$. For contrast, we set TKN to

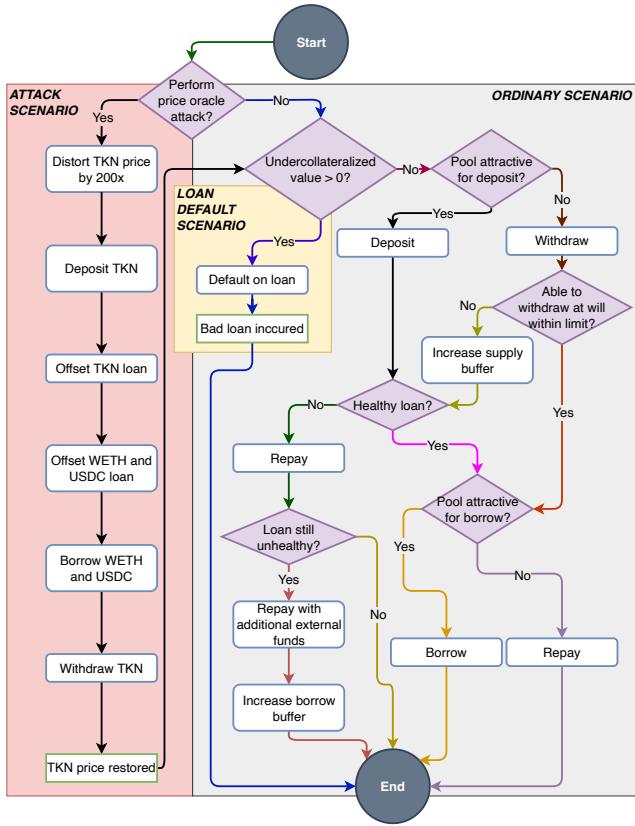


Figure 5: User reaction at each step of an episode

be most volatile, with $\mu_t \equiv 10^{-5}$ and $\sigma_t = 0.05 + \frac{(t-200)^2}{5 \times 10^5}$. Clearly, we attempt to synthesize TKN price such that it becomes gradually less volatile before day 200, and then increasingly more volatile.

3.2 User reaction simulation

Figure 5 illustrates the series of user’s reactions, pre-programmed in our model environment, according to the market condition as well as the user’s own financial status.

3.2.1 Attack scenario. In each episode, the model randomly select a certain number of steps where a price oracle attack will be performed before other ordinary actions from the market user.

At the step where an attack shall occur, the market user (who is now also an attacker) first inflates the price of TKN by 200 times. We are agnostic how the arbitrary price hike can take place, but theoretically this can be done through a flash loan attack (see Attack Procedure 1) for token assets with a relatively thin, low-liquidity market. The user then deposits all their available TKN to the lending pool to increase their supply token balance in TKN. Next, the user offsets their TKN loan with TKN supply tokens as much as possible, such that all the remaining TKN supply tokens can be used to back other, more valuable loans. The user subsequently offsets their WETH and USDC loans with the corresponding supply tokens as much as possible, such that the remaining WETH and USDC loans will be mainly backed by TKN with inflated price. The user

then seeks to borrow out as much additional WETH and USDC as possible from the lending pools, possibly depleting the pools before the faked borrow quota is used up. Finally, the user withdraws TKN to restore their initial TKN balance as much as possible.

Attack Procedure 1 Flash-loan-funded price oracle attack

- 1: **Flash Loan:** Borrow x_A token_A with a value equivalent to x_B token_B at market price.
- 2: **Swap:** Exchange x_A token_A for $x_B - \Delta_1$ token_B on an AMM, reducing the new price of token_A in terms of token_B to $\frac{x_B - \Delta_2}{x_A}$, with $\Delta_2 > \Delta_1 > 0$ due to slippage.
- 3: **Borrow:** Use $x_B - \Delta_1$ token_B as collateral to borrow $x_A + \Delta_3$ token_A from a lending platform using the AMM as their sole price oracle, ensuring that $\frac{x_B - \Delta_2}{x_A} < \frac{x_B - \Delta_1}{x_A + \Delta_3}$ to temporarily satisfy overcollateralization.
- 4: **Repay:** Return x_A token_A to repay the flash loan.

3.2.2 Loan default scenario. As described in Section 2.1, a user is likely to default on their loan if their undercollateralized value—defined as their total borrow value less total supply value—is positive, leaving them with no incentive to save their collateral by repaying the loan. As intended by the attacker, loan default is most likely to occur following a price oracle attack, although it may also happen, albeit much less likely, absent malicious behavior when simply the market is too volatile. When a loan is defaulted, the undercollateralized value will be treated as bad loan expenses, reducing the net position of the protocol (see Equation 1). Under major attacks when the attacker managed to borrow out a relatively large amount of WETH and USDC, the bad loan expenses can suffice to cause the protocol bankrupt, ending the episode prematurely.

3.2.3 Ordinary scenario. In an ordinary scenario, the user deposits (withdraws) based on how attractive (unattractive) the lending pool is for depositing, which then depends on how much higher (lower) the lending interest rate and the collateral factor of the underlying asset of the lending pool is compared to the external market level. If the user decides that the lending pool is relatively unattractive, they will seek to withdraw liquidity. If they are not able to withdraw within limit at will—e.g., when their deposited funds are lent out by the protocol, leaving the pool with insufficient liquidity for large withdrawal—they will withdraw as much as possible but also increase their supply buffer, meaning they will supply less liquidity in the future steps for precaution even when the lending pool is attractive for depositing.

The user subsequently checks their loan health, i.e. whether their loan value has exceeded the aggregate loanable value backed by the collateral. If healthy, the user decides whether to borrow more or repay depending on how much more or less the lending pool’s borrow interest is compared to the market level. If unhealthy, the user tries to repay restore their loan health as much as they can in the first instance. If still unhealthy, additional external funds will be injected to the user’s account to repay the loan. This is to mimic the effect of liquidation, where the liquidator repays the loan on behalf of the borrower and seizes the latter’s collateral. Note that as discussed in Section 2.2, we only model one market user to represent the aggregate user behavior’s effect on the protocol. In that sense, a loan turning liquidatable can in fact directly increase

the liquidity of the lending pool. On the flip side, however, the user increases their borrow buffer every time their collateral becomes liquidatable, meaning they will borrow less in the future steps for precaution even when the lending pool is attractive for borrowing. In addition, the newly injected liquidity is still subject to withdrawal in the future steps should the lending protocol exhibits unattractive conditions for depositing.

3.3 Additional setups

3.3.1 Other DeFi environment parameters. We set the initial collateral factor for all three assets to be 0.8. We assume the external competing supply and borrow interest rates to be 0.05 and 0.15 per annum, respectively, for all three tokens. We additionally set the external competing collateral factors for WETH, USDC and TKN to be 0.7, 0.65 and 0. respectively.

The market user in the model has a starting balance of 20,000 units of WETH, USDC and TKN each, and initiates the three lending pools by depositing 15,000 units in each at time 0. We further assume that the market user has an initial safety supply margin and borrow margin both equal to 0.5, meaning they will supply and borrow half as much as they can initially. The supply and borrow buffers increase as the user experience withdrawal restrictions and liquidations as described in Section 3.2 and when the collateral factor is adjusted which leaves the user with an unstable impression of the protocol. The buffer values decrease if the user experience smooth supplies and borrows without restrictions or liquidations for over 20 steps consecutively.

3.3.2 Benchmark environment. The benchmark environment will be initiated exactly like the main training environment, including the price trajectories of all tokens, as well as at which steps an attack would occur. The only difference is that there is no governance agent in the benchmark environment, and the collateral factors will remain their initial value of 0.8 for all three tokens throughout each episode.

3.3.3 Random events and stochastic processes. The DeFi environment generates new price trajectories and time points of attacks for each episode, which will be equally applied to both the training and benchmark environments. Generating random events and stochastic processes for each episode ensures that the RL agent will not overfit to a particular price trajectory or attack timing, making the trained model more robust and generalizable.

4 DESIGN OF THE GOVERNANCE AGENT

In this section, we present the design and training process of the governance agent, which is responsible for making appropriate decisions for DeFi protocols.

4.1 Reinforcement learning-based agent

We employ reinforcement learning, an artificial intelligence approach for training agents to make optimal decisions in complex and uncertain environments (i.e., DeFi ecosystems) in the presence of attacks. Specifically, we use a deep reinforcement learning agent [26] to serve as the governance agent, enabling it to dynamically select the best action based on the current state of the DeFi protocols. This approach is well-suited for our purpose, as it enables

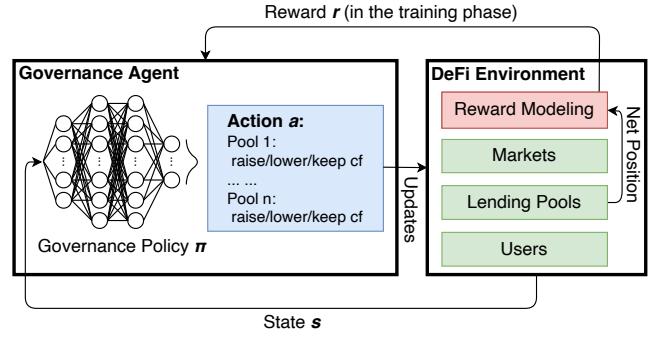


Figure 6: Architecture of the proposed system

the agent to learn from past experience and adapt its behavior to changing conditions in real-time. By leveraging a reinforcement learning agent, we can ensure that our protocol is flexible, adaptable, resilient to attacks, and able to optimize its behavior to maximize its performance under various scenarios. Figure 6 illustrates the architecture of our proposed approach.

Our goal is to train a policy π for the governance agent that tries to maximize the discounted, cumulative reward $R_{t_0} = \sum_{t=t_0}^{\infty} \gamma^{t-t_0} r_t$, where γ denotes the discount factor. We leverage deep Q-learning [28] to conduct the learning process for the governance agent, where a function $Q : S \times a \rightarrow \mathbb{R}$ can tell the agent what the reward would be. Then, the policy π of the governance agent can be represented as Equation 8, which always selects the action a that can maximize the value of the Q function.

$$\pi(S_t) = \arg \max_{a \in a} Q(S_t, a) \quad (8)$$

For each training update, we enforce that every Q function for the policy π follows the Bellman equation (Equation 9), where the difference between the two sides of the equality is known as the temporal difference error δ (Equation 10).

$$Q^\pi(S, a) = r + \gamma Q^\pi(S', \pi(S')) \quad (9)$$

$$\delta = Q(S, a) - (r + \gamma \max_a Q(S', a)) \quad (10)$$

Additionally, considering the potentially vast state space and the expected growth with the increasing number of lending pools, we employ a DQN [9] to serve as the policy network for the governance agent, enabling it to monitor multiple pools simultaneously. In a DQN, a deep neural network acts as an approximator for the Q -function. The DQN combines the strengths of both deep learning and Q-learning to tackle complex reinforcement learning problems with large state spaces, providing an efficient and robust approach for learning optimal policies.

Furthermore, to expedite the process of error elimination, we utilize Adam optimization [5] during training. Adam is an optimization algorithm that is commonly used to train deep neural networks. It is a variant of stochastic gradient descent (SGD) that adapts the learning rate for each weight in the network based on historical gradient information.

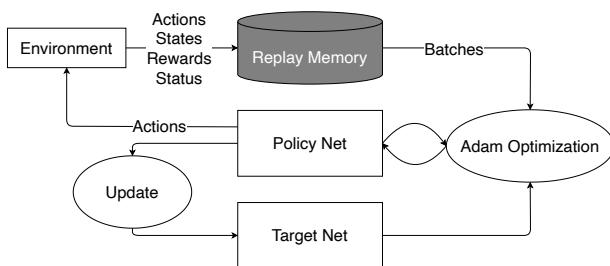
Algorithm 2 formalizes the training procedures including sampling, Adam optimization, and neural network updating, where g_t

Algorithm 2 High-level training procedure for the RL-based governance agent

```

1: Initialize DQN  $Q$ 
2: Initialize target network  $\hat{Q}$ 
3: Initialize experience replay memory  $D$ 
4: while not converged do
5:    $\epsilon \leftarrow$  new epsilon with  $\epsilon$ -decay           ▶ Sampling
6:   Choose an action  $a$  from  $S$  using policy  $\epsilon$ -greedy( $Q$ )
7:   Agent takes  $a$ , observe reward  $r$  and the next state  $S'$ 
8:   Store transition  $(S, a, r, S', is\_done)$  in  $D$ 
9:   if enough experience in  $D$  then           ▶ Learning
10:    Sample a batch of transitions from  $D$ 
11:    for every transition  $(S_i, a_i, r_i, S'_i, is\_done_i)$  in batch do
12:      if  $is\_done_i$  then
13:         $y_i \leftarrow r_i$ 
14:      else
15:         $y_i \leftarrow r_i + \gamma \max_{a' \in a} \hat{Q}(S'_i, a')$ 
16:      end if
17:       $\delta \leftarrow \frac{1}{N} \sum_{i=0}^{N-1} (Q(S_i, a_i) - y_i)^2$            ▶ Error
18:       $m_0 \leftarrow 0, v_0 \leftarrow 0, t \leftarrow 0$            ▶ Adam optimization
19:      while  $Q_t$  not converged do
20:         $t \leftarrow t + 1$ 
21:         $g_t \leftarrow \nabla_Q \delta_{t-1}$ 
22:         $m_t \leftarrow \beta_1 m_{t-1} + (1 - \beta_1) g_t$ 
23:         $v_t \leftarrow \beta_2 v_{t-1} + (1 - \beta_2) g_t^2$ 
24:         $\hat{m}_t \leftarrow \frac{m_t}{1 - \beta_1^t}$            ▶ Correcting bias
25:         $\hat{v}_t \leftarrow \frac{v_t}{1 - \beta_2^t}$ 
26:         $Q_t \leftarrow \prod_{\mathcal{F}, \sqrt{\hat{v}_t}} (Q_t - 1 - \frac{\alpha \hat{m}_t}{\sqrt{\hat{v}_t} + \mu})$            ▶ Updating
27:      end while
28:    end for
29:    Synchronize  $\hat{Q}$  with  $Q$  if reaches threshold
30:   end if
31: end while

```

**Figure 7: Operations for training the governance agent with the target network**

denotes the gradient at step t , m_t is the exponential moving average (EMA) of g_t , v_t is the EMA of g_t^2 , β_1 and β_2 are hyperparameters used in the moving averages of g_t^2 and g_t , α denotes the learning rate, and μ is a small number to prevent the denominator from becoming 0.

Algorithm 3 Training with both primary networks and target networks

```

1: Input  $\epsilon, decay\_func1(), decay\_func2()$ 
2: Input  $target\_switch\_on\_point$ 
3:  $Ctr \leftarrow 0$ 
4: while training do
5:    $Ctr \leftarrow Ctr + 1$ 
6:   if  $\epsilon < target\_switch\_on\_point$  then
7:     Switch on the target network
8:      $\epsilon \leftarrow decay\_func2(\epsilon)$ 
9:     .....training.....           ▶ Train with target net
10:   else
11:     Switch off the target network
12:      $\epsilon \leftarrow decay\_func1(\epsilon)$ 
13:     .....training.....           ▶ Train without target net
14:   end if
15: end while

```

4.2 Target network

To prevent overfitting during training and enhance the agent's resilience to potential attacks, we have implemented a target network [26]. The target network is a critical component in the training process of DQNs. It consists of a separate neural network with the same architecture as the primary or online network, but with a distinct set of weights. The primary purpose of the target network is to provide more stable and consistent target values for the Q-learning updates. In our approach, the training procedure involves periodically copying the weights from the online network to the separate target network, as illustrated in Figure 7 and Algorithm 2. This technique helps improve stability and convergence, ultimately leading to more reliable and robust learned policies.

However, simply employing the target network may bring the following side effects:

- **Stability vs. Responsiveness:** The target network increases stability but reduces responsiveness, causing temporary mismatches between the online network's estimates and target values.
- **Delayed learning:** The infrequent updating of the target network may lead to slower training and temporary performance drops as the online network readjusts.
- **Overestimation bias:** Using a separate target network can help mitigate overestimation bias but may result in conservative Q-value estimations, causing temporary performance drops.

To address the disadvantages associated with the target network, we propose a novel approach for its implementation. Initially, we train the agent using only the primary network, resulting in accelerated early learning. After a certain amount of training, we introduce the target network and allow the epsilon value to decrease at a more gradual pace. This slower reduction in the epsilon value means that the agent explores the environment more slowly. This strategy can aid the agent in discovering more optimal solutions. By incorporating the target network later in the training process, we aim to balance the trade-offs among stability, responsiveness, and learning speed. Algorithm 3 illustrates this training procedure,

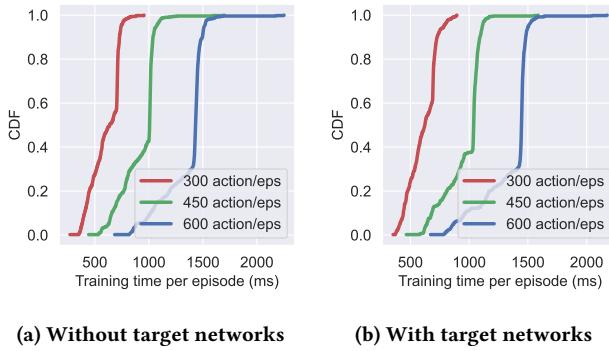


Figure 8: Cumulative distribution functions (CDFs) of training time per episode with different numbers of actions per episode

where we employ different ϵ decay functions for the primary and target networks, with the latter being slower.

4.3 Prioritized experience replay

To equip the governance agent with the ability to adapt to diverse DeFi environments, expedite the policy network’s training, and swiftly enhance its resistance to potential attacks, we have incorporated prioritized experience replay into our reinforcement learning agent.

Prioritized experience replay [25] enhances the standard experience replay technique, which uniformly stores and samples experiences during training. While experience replay helps break the correlation between consecutive samples and decrease update variance, prioritized experience replay assigns significance to each experience based on the discrepancy between actual and predicted Q-values. This approach increases the likelihood of sampling and learning from unexpected experiences or those with greater potential to boost the agent’s performance.

Once the DQN Q is fully converged and the governance agent is properly trained, the governance agent can be used for setting parameters for the lending pool individually, even without the reward feedback from the DeFi environment.

5 RESULTS

In this section, we outline the implementation specifics of our approach and present evaluation results concerning agent training, governance performance, and attack resistance.

5.1 hyperparameter tuning

Our approach is implemented using PyTorch [22] for the governance agent and OpenAI Gym [6] for the DeFi environment. The training evaluation processes are performed on a Mac laptop with an M1 Pro CPU and 32 GB of RAM.

Fine-tuning hyperparameters is also an essential part of training the governance agent. Due to space constraints, we skip the lengthy process of fine-tuning hyperparameters and list key hyperparameters that we use to generate results in Table 1.

Table 1: Key hyperparameters for the governance agent

DQN hidden layers	2	Learning rate	0.001
Neurons in hidden layer 1	256	Batch size	64
Neurons in hidden layer 2	256	Epsilon start	1
Input neurons	10×pool_num	Epsilon end	2e-3
Number of training episodes	850	Epsilon decay	5e-6
Target net switch on point	0.3	Gamma	0.95

5.2 Training of the governance agent

Our initial evaluation focuses on the training time per episode for the governance agent. As the agent may require retraining due to varying DeFi environments or modifications to specific protocols, the training speed substantially impacts the practicality of our approach.

Figure 8 depicts the cumulative distribution functions (CDFs) of training time per episode for varying numbers of actions. Training speed is crucial for the practicality of our approach, as the governance agent may need updating or retraining in response to different DeFi environments or protocol changes. The results demonstrate that for all three scenarios (i.e., 300, 450, and 600 actions per episode), the training time remains below 2000ms. With 300 actions per episode, the DQN can finish decision-making and training for each episode within just 1000ms. Our experiments indicate that a higher number of actions per training step can slightly enhance training quality but can also considerably prolong the training duration. Based on our findings, we determined that training with 450 actions per episode is adequate for the rapid and efficient training of the governance agent. Consequently, we utilize 450 actions per training episode in all subsequent evaluations, consistently yielding satisfactory results. Moreover, by comparing Figure 8a and Figure 8b, we observe that using target networks does not noticeably increase training time, as their time costs are very similar. As outlined in Table 1, the agent requires 850 episodes for full training, which translates to a total training time of approximately 21 minutes.

After landing on the appropriate hyperparameters, we train the governance agent for two scenarios, one without attacks, and one with price oracle attacks as described in Section 3.2 that occur in some random steps in each training episode. Figure 9 illustrates that price attacks are likely to, but not always, turn the lending

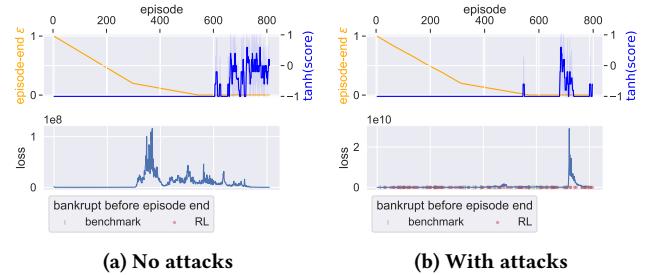
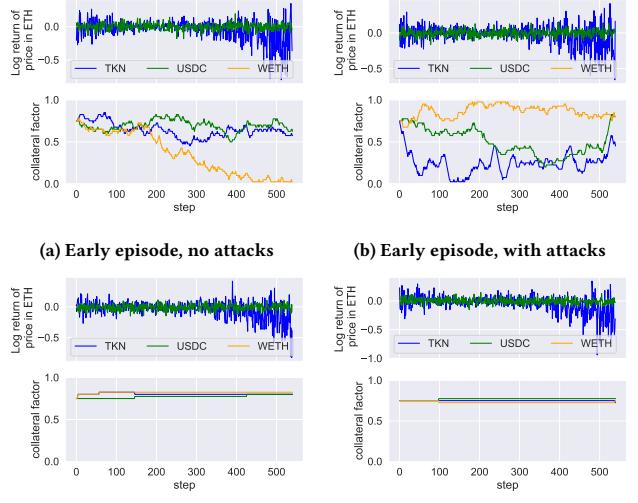


Figure 9: Change of epsilon, score, and loss with the increase of training steps



(c) Well-trained episode, no attacks (d) Well-trained episode, with attacks

Figure 10: Price trajectories and collateral factor adjustments of all tokens for selected episodes

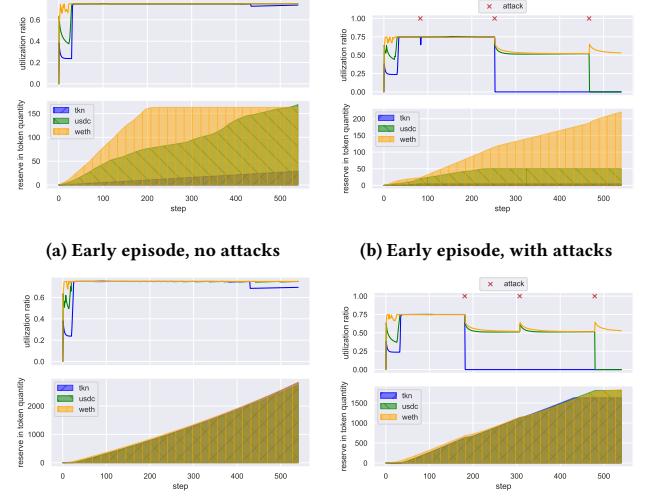
protocol bankrupt (marked at the bottom of Figure 9b), which ends the episode before the pre-determined maximal number of steps.

We proceed by evaluating the convergence speed of our governance agent’s training and the quality of the final decisions made by the trained agent. Figure 9 illustrates the changes in epsilon, losses, and scores (i.e., the cumulative rewards) as the number of training episodes increases. Since the score can fluctuate rapidly during the training process and various random factors can contribute to these fluctuations, we employ the Tanh estimator to normalize the scores [1]. Based on our experimental results, we have determined that the governance agent can be effectively trained with only 750 training episodes, each consisting of 450 actions. The losses may momentarily increase in the middle of the training, but they quickly decrease as the training progresses. Additionally, when combined with the information in Figure 8, the agent can rapidly adapt to a specific DeFi environment and make robust, profitable decisions within 20 minutes, using only the computing resources of a personal laptop. Overall, our findings suggest that our approach can effectively train a governance agent capable of making profitable and robust decisions in various DeFi environments in a timely and efficient manner.

5.3 Governance results

For each scenario with or without attacks, we select one early episode and one well-trained episode to demonstrate the training results. The early episode is the first episode that has the medium final score among all the episodes before the target net is switched on. The well-trained episode is the first episode that has the top 25 percentile final score among all the episodes with a positive score after the target net is switched on.

Figure 10 shows for selected episodes the RL governance agent’s collateral factor determination for each token vis-a-vis the tokens’ price movements. We observe that for scenarios either with or

**Figure 11: Lending pool state over time of the RL environment for selected episodes**

without attacks, the agent changes collateral factor randomly and frequently at the beginning. After the agent has been trained, the change of collateral factor becomes less frequent. This should be the correct learning outcome reacting to the design of the market user behavior that a change of collateral factor increases their supply buffer, which further decreases the funds available for borrowing and ultimately reduces the protocol’s revenue.

In addition, the agent tends to adopt a more aggressive strategy, i.e. making collateral factors higher, in the scenario without attacks than in the scenario with attacks. This behavior is intuitive, as a relatively smaller collateral factor can make the lending protocol more resistant to price attacks. The agent also appears to understand that, even when the possibility of attacks is present, but as long as they are infrequent, the collateral factor can still be set at a moderately high level to attract deposits and allow borrows, ultimately leading to higher profits. Being able to balance between keeping the protocol safe and maximizing profits is the key learning outcome of the governance agent. We also observe from the trained episodes that either WETH or USDC would end up with the highest collateral factor, and TKN the lowest. This order sometimes only appears towards the end of the episode, which is again intuitive as the pre-configured volatility of TKN (see Section 3.1) becomes increasingly high as the second half of the episode progresses. This is consistent with the theoretical grounding as well as the empirical findings (see Figure 3) that less volatile assets such as WETH and USDC should have higher collateral factors than more volatile ones such as TKN.

Figure 11 illustrate the utilization ratio and reserve quantity of the three token assets in the lending protocol for selected episodes. We observe under no attacks, the utilization ratios of all three tokens almost always remain at an optimal level of around 75%. This is likely driven by the correctly encoded market user reactions that tend to be borrow when the utilization ratio is low (hence low

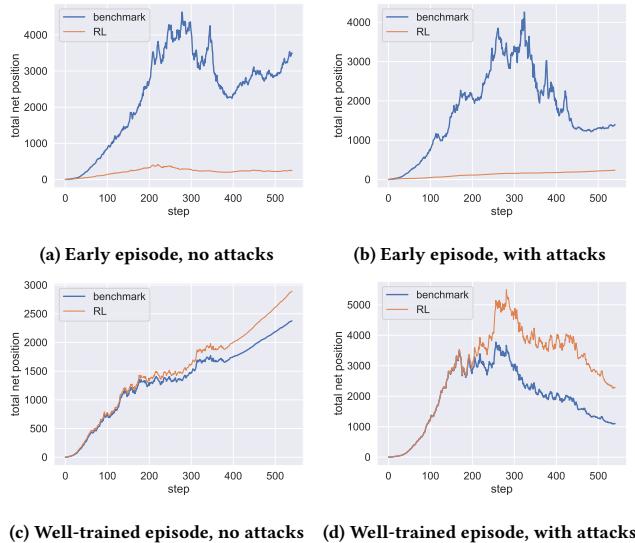


Figure 12: Protocol’s total net position over time of the RL environment compared with the benchmark environment for selected episodes

borrow interest) and supply when the utilization ratio is high (hence high supply interest), thus keeping the utilization ratio at a steady, equilibrated level. Under price oracle attacks, the utilization ratio of TKN goes down as the attacker always first offsets all TKN loans (see Section 3.2) and sometimes, when there are remaining underlying tokens of WETH and USDC in the protocol, the utilization ratio of those two assets goes up as the attacker tries to borrow them out. Comparing Figure 11c and Figure 11d with Figure 11a and Figure 10b, it is evident that the governance agent has learned to effectively increase the protocol reserve after being trained in scenarios both with and without attacks.

The training and learning outcome is most evident in Figure 12 where we observe that the RL agent underperforms the benchmark in terms of the size of the net position (calculated as in Equation 1) in the early episodes, but outperforms in the well-trained episodes, demonstrating the strong effectiveness of our model.

6 DISCUSSION

In this section, we explore some of the current limitations and potential areas for future improvement in our proposed approach.

6.1 Model improvement

Our model framework may be further improved by taking into account the following factors.

Higher fidelity. We can add complexity to the environment to make it more realistic. For example, instead of one aggregate market user, we can have multiple users with different risk appetites and different amount of capital. We also include more lending pools into the protocol and more risk parameters such as liquidation threshold and liquidation bonus.

User behavior inference. We use a set of pre-programmed rules to determine how the market user shall react under different conditions (Figure 5). To establish a more realistic module, one can first derive the actual underlying behavior pattern based on historical observations, which can then be encoded in the training environment.

More training dimensions. Instead of only training the governance agent to find the optimal collateral factor adjustment policy, we can also allow it to adjust other parameters such as other risk parameters and the interest rate model parameters.

More training scenarios. We can train the governance agent under various scenarios such as different market conditions (time-varying price volatility and competing interest rates etc) and different user behaviors.

More sophisticated machine learning techniques. We can apply more sophisticated machine learning models such as multi-agent reinforcement learning by allowing users to also be reinforcement learning agents with their own objectives.

6.2 Model extension

With some tweaks, our model can be easily extended to other lending protocols such as compound and dForce. Upon proper adjustment, the model can also be applied to other types of DeFi protocols such as AMMs. For example, the governance agent can learn to dynamically adjust AMM pool parameters—such as the amplification coefficient for Curve Finance¹—based on market conditions; and for almost all DeFi protocols, the governance agent can learn to optimally adjust the fee rate.

6.3 Implications for DeFi governance

Reinforcement learning based model further reduces human intervention in DeFi governance. It yields a more objective and data-driven decision making process. Furthermore, it eliminates the governance result being influenced by few top governance token holders, especially when the governance token concentrated in a few hands.

7 RELATED WORK

In this section, we introduce literature related to our work.

7.1 DeFi risks

Our work is in the first instance related to literature on quantitative DeFi risk management. Among the scant body of literature on this topic, [16] use agent-based modelling to stress-test the market risks to the Compound protocol participants. They demonstrate that the existing Compound liquidation mechanism can protect borrowers’ collateral as well as lenders’ funds even under volatile market conditions. They suggest the compound community to employ their simulation-based assessment to evaluate new assets to be introduced to the protocol. Their proposal assesses risks up-front, while our proposal focuses on reacting to current market conditions in an agile fashion based on a pre-trained model.

¹see e.g. <https://gov.curve.fi/t/evaluating-proposed-parameter-changes-for-fraxbp-vote-267/4317>

Our paper is also related to literature discussing DeFi risks in general. [4] formalize the main mechanisms of DeFi lending protocols, and describe the over- and under-collateralization risks associated to those protocols. [23] depict and anecdotal liquidation event on Compound and analyze its cause and lessons learned.

7.2 Collateralization and liquidation in traditional finance

Our work is also inspired by the abundant literature on traditional finance that studies the mechanics of collateralization and liquidation.

Almgren et al. [2] demonstrate how liquidity and transaction costs can be accounted for in a portfolio theory framework, and describe a valuation model for portfolios under liquidation.

Ramcharan [24] examines the liquidation with banks and finds that lower bank equity or liquidity results in lower liquidation value of bank-owned real estate collateral.

Chan et al. [7] theorize the equilibria of credit rationing, a phenomenon where lenders limit their supply of credit to borrowers. They find that unlimited collateral may nor may not eliminate credit rationing, depending on how a competitive equilibrium is conceptualized.

Oehmke [21] models collateral liquidations upon default of a repo borrower, and suggests repo lenders to consider their own balance sheet constraints when executing collateral sell-offs.

Vig [27] finds that the demand for collateralized debt decreases while the supply increases when the rights of creditors are strengthened. In the same vein, [12] find that high transferability of collateral results in a tighter linkage between leverage and asset tangibility (fixed assets as a fraction of total assets).

Through an array of case studies, [18] discover that in case of distressed loans, lenders rarely take possession of the collateral, but rather seek to be repaid through either refinancing or sale of the collateral.

7.3 Deep reinforcement learning for blockchain and crypto

Last but not least, our work is connected to the literature on deep reinforcement learning for blockchain and crypto.

Jiang et al. [15] apply a deep reinforcement learning framework to achieve a model-free portfolio optimization with crypto-assets.

Hou et al. [13] use deep reinforcement learning to automate attack analysis on blockchain incentive mechanisms.

8 CONCLUSION

Optimal, resilient governance has been long desired in the DeFi community. Despite its apparent advantages in terms of reactivity, objectivity, and empirical data support, deep RL has not been widely considered for governance purposes as an alternative to the current manual process. In this paper, we make this attempt by first abstracting a simplified but comprehensive DeFi environment to model the governance agent's reward function and then applying DQN RL to train the agent to find the optimal policy for protocol parameter adjustment. We use an AAVE-like lending protocol with

the likelihood price oracle attacks as an example, but our environment can be easily adjusted to apply to other protocol categories and account for different attack types.

Our results are promising: the trained agent successfully adapts to various scenarios, including those with and without attacks, demonstrating its capability to understand the consequences of setting different values and the necessity of assigning appropriate values based on the specific situation. Our experiment demonstrates the potential to replace the existing lengthy governance procedure, which is fully manual and may involve human bias, with an RL-based approach that emphasizes security. We anticipate that more and more DeFi protocols will adopt (a variation of) our model for their governance process, leading to a more secure and efficient ecosystem.

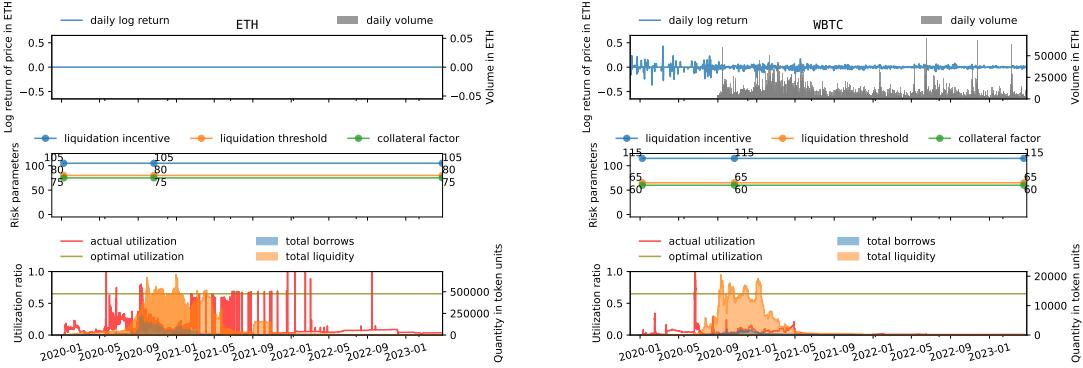
REFERENCES

- [1] Aslı AKILLİ and Hülya ATIL. 2020. Effect of Normalization Techniques On Data Mining Methods: Case Study for Dairy Cattle Data. *Veri Madenciliği Yöntemleri: Tarım Alanında Uygulamaları. Çanakkale: Rating Academy Ar-Ge Yazılım Yayıncılık Eğitim Danışmanlık ve Organizasyon Ticaret Limited Şirketi* (2020), 127–148.
- [2] Robert Almgren and Neil Chriss. 1999. Value under liquidation. *Risk* 12, 12 (1999), 61–63. <https://www.risk.net/infrastructure/1530394/value-under-liquidation>
- [3] Tom Barbereau, Reilly Smethurst, Orestis Papageorgiou, Alexander Rieger, and Gilbert Fridgen. 2022. DeFi, not so decentralized: The measured distribution of voting rights. (2022).
- [4] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch Lafuente. 2021. SoK: Lending Pools in Decentralized Finance. In *Lecture Notes in Computer Science*. Vol. 12676 LNCS. Springer, 553–578. https://doi.org/10.1007/978-3-662-63958-0_40
- [5] Sebastian Bock and Martin Weiß. 2019. A proof of local convergence for the Adam optimizer. In *2019 international joint conference on neural networks (IJCNN)*. IEEE, 1–8.
- [6] Greg Brockman, Vicki Cheung, Ludwig Pettersson, Jonas Schneider, John Schulman, Jie Tang, and Wojciech Zaremba. 2016. Openai gym. *arXiv preprint arXiv:1606.01540* (2016).
- [7] Yuk-Shee Chan and Anjan V Thakor. 1987. Collateral and Competitive Equilibria with Moral Hazard and Private Information. *The Journal of Finance* 42, 2 (6 1987), 345–363. <https://doi.org/10.1111/j.1540-6261.1987.tb02571.x>
- [8] Hassan Hamid Ekal and Shams N Abdul-wahab. 2022. DeFi Governance and Decision-Making on Blockchain. *Mesopotamian Journal of Computer Science* 2022 (2022), 9–16.
- [9] Jianqing Fan, Zhaoran Wang, Yuchen Xie, and Zhuoran Yang. 2020. A theoretical analysis of deep Q-learning. In *Learning for Dynamics and Control*. PMLR, 486–489.
- [10] Lewis Gudgeon, Daniel Perez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. 2020. The decentralized financial crisis. In *2020 crypto valley conference on blockchain technology (CVCBT)*. IEEE, 1–15.
- [11] Lewis Gudgeon, Sam Werner, Daniel Perez, and William J. Knottenbelt. 2020. DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency. In *The 2nd ACM Conference on Advances in Financial Technologies*. 92–112. <https://doi.org/10.1145/3419614.3423254>
- [12] Thomas W. Hall. 2012. The collateral channel: Evidence on leverage and asset tangibility. *Journal of Corporate Finance* 18, 3 (6 2012), 570–583. <https://doi.org/10.1016/j.jcorpfin.2011.12.003>
- [13] Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramèr, Giulia Fanti, and Ari Juels. 2019. SquirRL: Automating attack discovery on blockchain incentive mechanisms with deep reinforcement learning. (2019).
- [14] Johannes Rude Jensen, Victor von Wachter, and Omri Ross. 2021. How decentralized is the governance of blockchain-based finance: Empirical evidence from four governance token distributions. *arXiv preprint arXiv:2102.10096* (2021).
- [15] Zhengyao Jiang, Dixin Xu, and Jinjun Liang. 2017. A deep reinforcement learning framework for the financial portfolio management problem.
- [16] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. 2020. An analysis of the market risk to participants in the compound protocol. In *Third International Symposium on Foundations and Applications of Blockchains*. https://scfab.github.io/2020/FAB2020_p5.pdf
- [17] Aggelos Kiayias and Philip Lazos. 2022. SoK: blockchain governance. *arXiv preprint arXiv:2201.07188* (2022).
- [18] Ronald J. Mann. 1997. Strategy and Force in the Liquidation of Secured Debt. *Michigan Law Review* 96, 2 (11 1997), 159. <https://doi.org/10.2307/1290068>

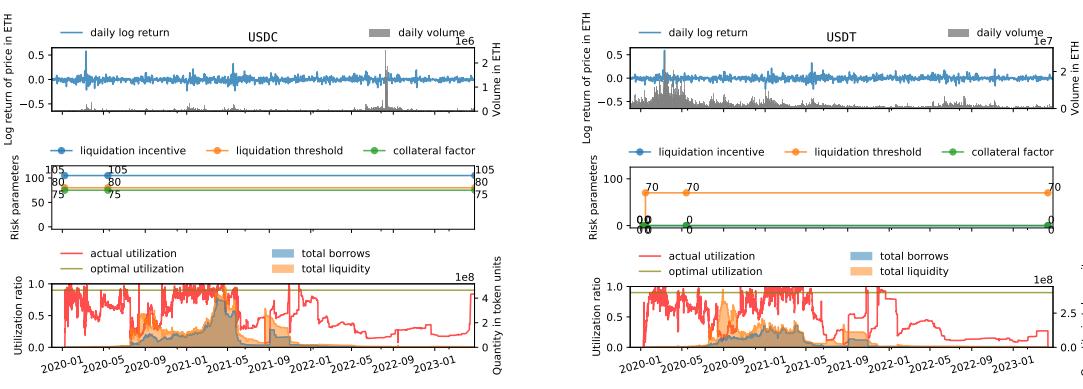
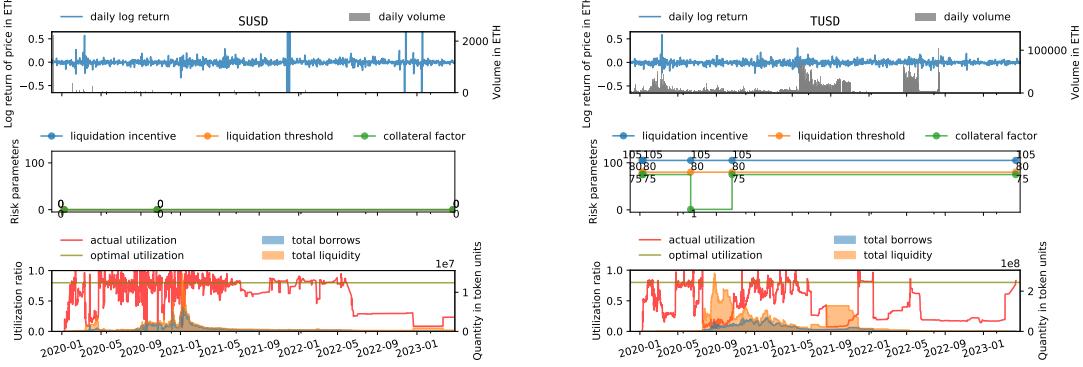
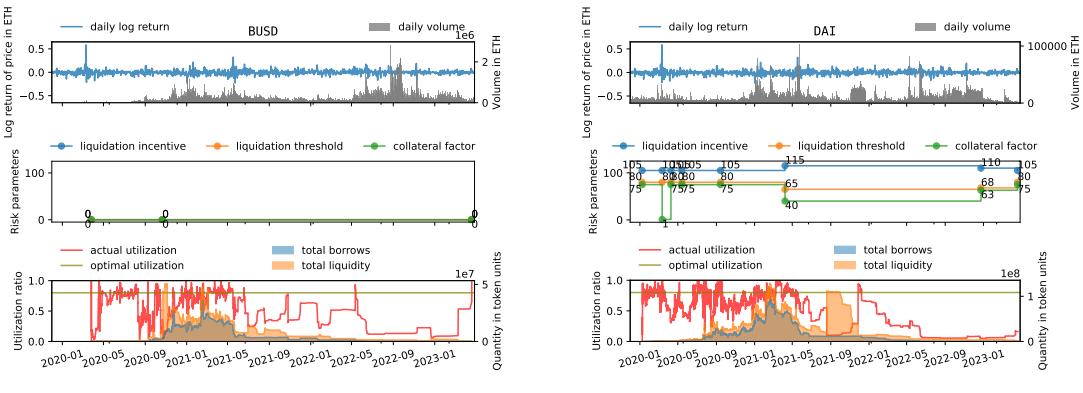
- [19] Vijay Mohan, Peyman Khezr, and Chris Berg. 2022. Voting with time commitment for decentralized governance: Bond voting as a Sybil-resistant mechanism. *Available at SSRN* (2022).
- [20] Kelsie Nabben. 2023. Governance by Algorithms, Governance of Algorithms: Human-Machine Politics in Decentralised Autonomous Organisations (DAOs). *puntOorg International Journal* 8, 1 (2023), 36–54.
- [21] Martin Oehmke. 2014. Liquidating illiquid collateral. *Journal of Economic Theory* 149, 1 (1 2014), 183–210. <https://doi.org/10.1016/j.jet.2013.02.001>
- [22] Adam Paszke, Sam Gross, Francisco Massa, Adam Lerer, James Bradbury, Gregory Chanan, Trevor Killeen, Zeming Lin, Natalia Gimelshein, Luca Antiga, et al. 2019. Pytorch: An imperative style, high-performance deep learning library. *Advances in neural information processing systems* 32 (2019).
- [23] Daniel Perez, Sam M. Werner, Jiahua Xu, and Benjamin Livshits. 2020. Liquidations: DeFi on a Knife-edge. (9 2020). <http://arxiv.org/abs/2009.13235>
- [24] Rodney Ramcharan. 2020. Banks’ Balance Sheets and Liquidation Values: Evidence from Real Estate Collateral. *The Review of Financial Studies* 33, 2 (2 2020), 504–535. <https://doi.org/10.1093/rfs/hhz056>
- [25] Tom Schaul, John Quan, Ioannis Antonoglou, and David Silver. 2015. Prioritized experience replay. *arXiv preprint arXiv:1511.05952* (2015).
- [26] Hado Van Hasselt, Arthur Guez, and David Silver. 2016. Deep reinforcement learning with double q-learning. In *Proceedings of the AAAI Conference on Artificial Intelligence*, Vol. 30.
- [27] Vikrant Vig. 2013. Access to Collateral and Corporate Debt Structure: Evidence from a Natural Experiment. *Journal of Finance* 68, 3 (6 2013), 881–928. <https://doi.org/10.1111/jofi.12020>
- [28] Christopher JCH Watkins and Peter Dayan. 1992. Q-learning. *Machine learning* 8 (1992), 279–292.
- [29] Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. 2021. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778* (2021).
- [30] Jiahua Xu and Yebo Feng. 2022. Reap the Harvest on Blockchain: A Survey of Yield Farming Protocols. *IEEE Transactions on Network and Service Management* (2022).

APPENDIX

A CRYPTO-ASSET MARKETS ON AAVE

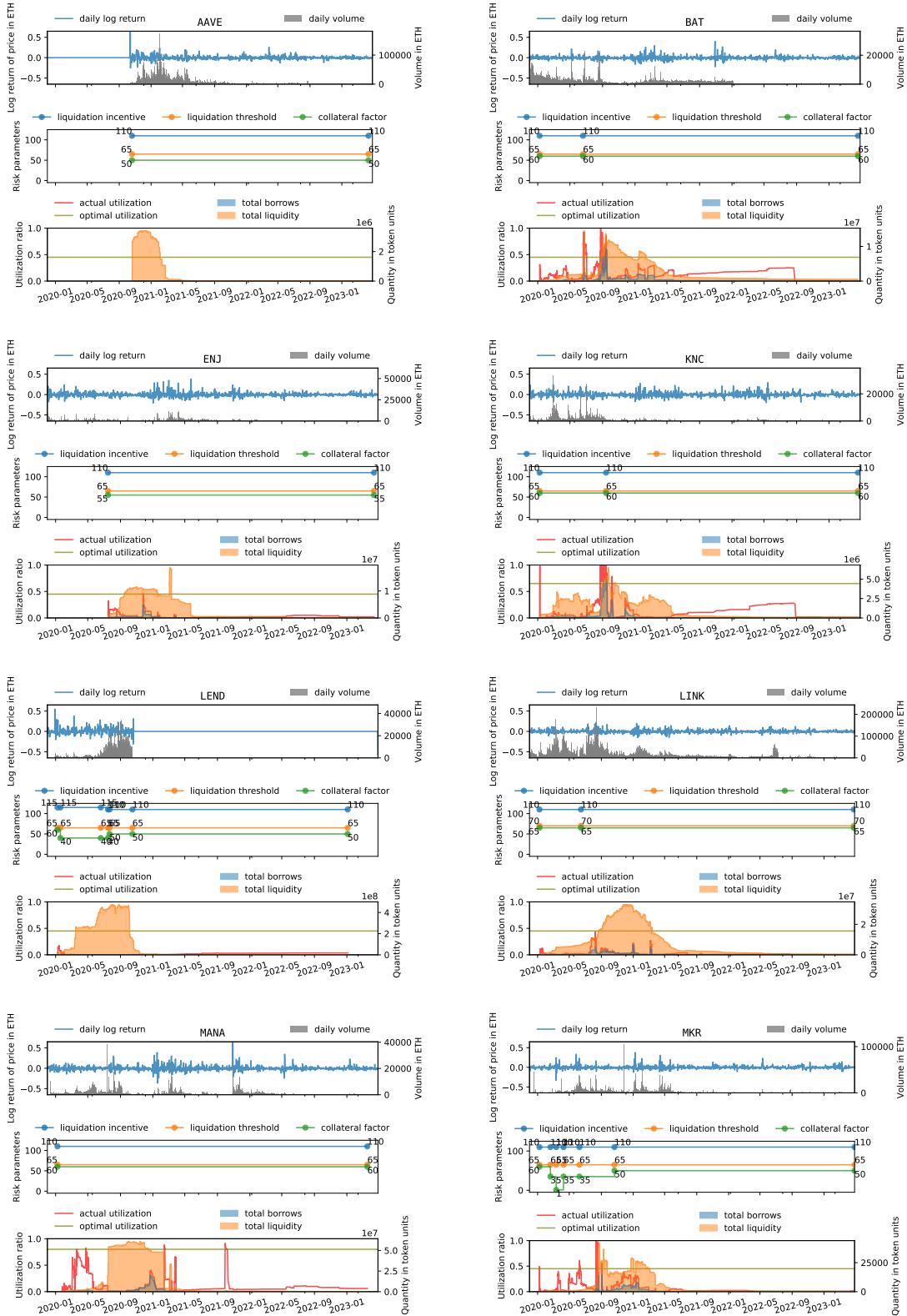


(a) Distributed ledger consensus-layer tokens



(b) USD-pegged stablecoins

Auto.gov: Learning-based On-chain Governance for Decentralized Finance (DeFi)



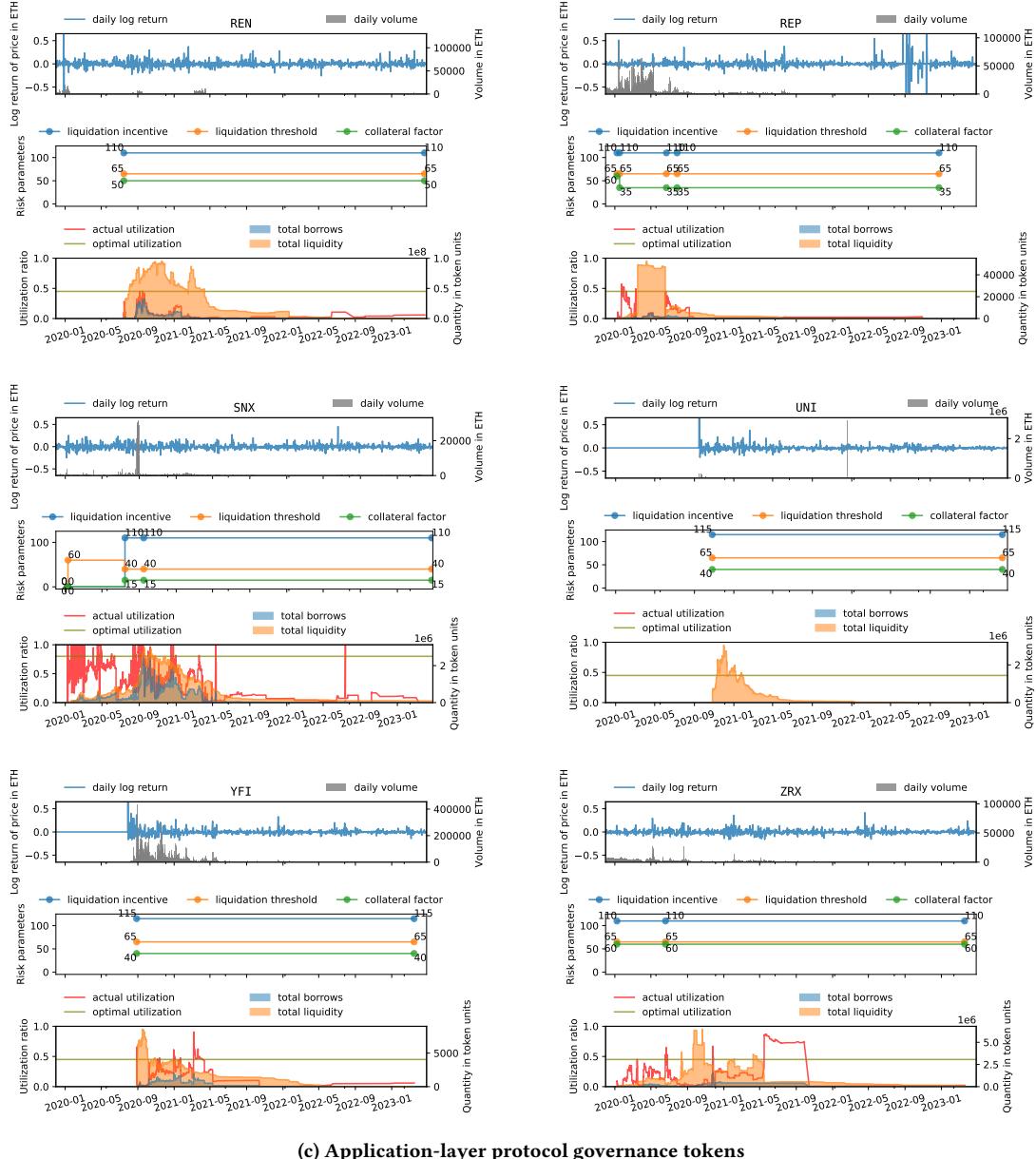


Figure 13: Time series of states of lending pools and market conditions of their corresponding underlying assets on AAVE