A THEORY OF LENDING PROTOCOLS IN DEFI

MASSIMO BARTOLETTI AND ENRICO LIPPARINI

University of Cagliari, Cagliari, Italy
e-mail address: bart@unica.it

University of Cagliari, Cagliari, Italy
e-mail address: enrico.lipparini@unica.it

Abstract. Lending protocols are one of the main applications of Decentralized Finance (DeFi), enabling crypto-assets loan markets with a total value estimated in the tens of billions of dollars. Unlike traditional lending systems, these protocols operate without relying on trusted authorities or off-chain enforcement mechanisms. To achieve key economic goals such as stability of the loan market, they devise instead trustless on-chain mechanisms, such as rewarding liquidators who repay the loans of under-collateralized borrowers by awarding them part of the borrower's collateral. The complexity of these incentive mechanisms, combined with their entanglement in low-level implementation details, makes it challenging to precisely assess the structural and economic properties of lending protocols, as well as to analyze user strategies and attacks. Crucially, since participation is open to anyone, any weaknesses in the incentive mechanism may give rise to unintended emergent behaviours, or even enable adversarial strategies aimed at making profits to the detriment of legit users, or at undermining the stability of the protocol. In this work, we propose a formal model of lending protocols that captures the essential features of mainstream platforms, enabling us to identify and prove key properties related to their economic and strategic dynamics.

1. Introduction

Decentralized Finance (DeFi) refers to a collection of interoperable protocols run on permissionless blockchains that replicate traditional financial services without relying on centralized intermediaries. In this setting, *lending protocols* have established loan markets of crypto-assets that collectively manage tens of billions of dollars in value: as of June 2025, two of the main lending platforms, Aave and Compound, hold respectively ∼$25B and ∼$3B worth of crypto-assets [aav25a, com25a].

At an abstract level, lending protocols can be seen as state transition systems, where the system state keeps track of the credit and debit positions — abstractly modelled through *tokens* — associated with each user. Such system is partitioned into two components: the *user wallets*, which represent the tokens freely available for user disposal, and *lending pools*, which record the tokens available for lending as well as the outstanding credit and debit positions. For example, lending can be modelled as a transfer of tokens from the user's wallet to the lending pool, together with a contextual minting of *credit tokens* that represent the

Preprint submitted to
Logical Methods in Computer Science

user's claim. Dually, borrowing can be modelled as a transfer of tokens from the lending pool to the user's wallet, along with the minting of *debt tokens* that record the user's obligation.

A key distinguishing feature of decentralized lending protocols, compared to traditional lending systems, is the absence of off-chain enforcement mechanisms to prevent loan defaults. Instead, lending protocols rely entirely on *on-chain* mechanisms to incentivize, one the one hand, lenders to provide liquidity, and, on the other hand, borrowers to repay their loans. As in traditional finance, borrowing in decentralized lending protocols requires users to provide a collateral, and debts accrue interests over time. However, unlike traditional finance, decentralized lending protocols are open to all users, who can freely participate as *liquidity providers* — gaining from interests accrued on debts — and as *liquidators*, by repaying (part of) an under-collateralized loan in exchange for a discounted amount of the seized collateral. Another key difference is that all protocol parameters, such as the interest rate function, collateral and token prices, are algorithmically determined by smart contracts.

This openness, combined with the inherent complexity of the emergent behaviour resulting from interactions between users and lending pools, makes them an attractive target for adversaries. By exploiting weaknesses in their economic incentive mechanisms, adversaries can devise sophisticated attack strategies to extract undue profits, harm legitimate users, and, more broadly, undermine the stability of the protocol. Since real-world implementations of lending protocols are too complex for effective formal analysis, we need at least an abstract model of their behavior that can faithfully analyse such strategic aspects. Such model and analysis should offer relevant insights about the following research questions:

RQ1: What structural properties and invariants are enjoyed by lending pools?

RQ2: What is the economic effect of each individual interaction with a lending pool?

RQ3: Which strategies can be followed by rational users anticipating a forthcoming action?

RQ4: Which attacks are possible for adversaries with a large amount of capital?

Contributions. This paper proposes a formal analysis of lending protocols, focussing on the properties that arise through the interaction between users and lending pools. To this purpose, we introduce a new operational model that captures the state machine behavior of lending protocols by synthesizing the common features of leading implementations such as Aave and Compound.

More specifically, our contributions can be summarized as follows:

(1) A formal model of lending protocols that precisely captures their behavior as transitions in a state machine. Our model encompasses all typical interactions between users and lending pools, along with key economic features such as collateralization, exchange rates, token prices, and interest accruals (Section 2).

(2) An analysis of the fundamental *structural properties* of lending protocols, in the form of invariants on the machine states. (Section 3). In particular, we prove in Lemma 3.4 that exchange rates are preserved by all actions except interest accruals — which always increase them — and for the corner case where all the credits of a token are redeemed. Another crucial invariant is given by Theorem 3.6, which establishes that the total net worth of all users is preserved by all actions except price updates.

(3) An analysis of the economic effects of individual interactions with a lending protocol, both in terms of the change to the users' net worth (i.e., their *gain*) and collateralization (Section 4). In particular, Lemma 4.1 measures the gain of actions performed by users: it shows that the only action that affects a user's gain is the liquidation, which yields a positive gain for the liquidator and an equivalent loss for the liquidated borrower. Lemma 4.2 quantifies the effect of price updates on the users' net worth: it shows that users with lots of debts in a given token type would benefit from a price decrease, while those with lots of credits would suffer losses. Lemma 4.3 shows that a dual situation occurs for interest accruals. Lemma 4.4 measures the impact of user actions on the health factor. More specifically, Lemma 4.6 compares the effectiveness of adding more collateral versus repaying debts in order to increase one's health factor.

(4) An analysis of *strategic users* — those who aim at increasing their gain by leveraging partial knowledge of forthcoming actions in the lending protocol (Section 5). In particular, we investigate the strategies such users should follow when they anticipate future events such as liquidations (Theorem 5.1), price updates (Theorem 5.2 and Lemma 5.3), and interest accruals (Theorem 5.4). For liquidations and price updates, we show that a user can always front-run the impending action with their own transaction in order to achieve a higher gain. For interest accruals, instead, we show that — except in the simple case where the interest rate function is constant — there is no simple front-running strategy that guarantees a higher gain.

(5) An analysis of attacks to lending protocols, where adversaries use their capital to temporarily manipulate token prices or their utilization to obtain an advantage in further interactions with a lending pool (Section 6). More specifically, Theorem 6.1 shows an attack in which an adversary manipulates prices in order to borrow more tokens than what they should be allowed to. Theorem 6.2 shows another price manipulation attack, where the adversary causes other users to become under-collateralized and profits from their subsequent liquidation. In the other attacks, the adversary manipulates the *utilization* of some token — roughly defined as the ratio between the total debt in that token and its overall supply — to induce a variation in the interest rate applied to debts in that token. This variation is then exploited by the adversary in order to make a profit. Theorem 6.3 shows an attack where an adversary deposits tokens just before an interest accrual, in order to induce a decrease in the utilization, and so pay less interests on their debts. Theorem 6.4 shows instead an attack where the adversary borrows tokens before an interest accrual, in order to induce an increase in the utilization, and so benefit from a higher appreciation of their credits.

We discuss some limitations of our work in Section 7, related work in Section 8, and draw conclusions in Section 9. We include detailed proofs of our results in Appendix A to D.

2. Lending Protocols

We introduce a formal model of lending protocols, encompassing the common features implemented by the main lending platforms, and abstracting away some features that are inessential to understand their underlying economic mechanism. We discuss these abstractions and the limitations they induce in Section 7.

TABLE 1. Summary of notation.

A, B	Users	$XR_\Lambda(\mathsf{T})$	Exchange rate
$\mathsf{T}, \mathsf{T}^c, \mathsf{T}^d$	Token type (base,credit,debit)	$S_\omega(\mathsf{T}), S_\Lambda(\mathsf{T}^c), S_\Lambda(\mathsf{T}^d)$	Token supply
ω, ω'	Wallet states	$W_\Gamma(\mathsf{A})$	Net worth of A in Γ
Λ, Λ'	LP states	$H_\Gamma(\mathsf{A})$	Health factor of A in Γ
π, π'	Price functions	$g_\mathsf{A}(\Gamma, \mathsf{X})$	Gain of A upon firing X
X, X'	Transactions	T_{liq}	Liquidation threshold
Γ, Γ'	Blockchain states	R_{liq}	Liquidation reward

2.1. **Blockchain model.**

Users and tokens. We assume a denumerable set of *addresses* $\mathbb{A}$, ranged over by $\mathsf{A}, \mathsf{A}', \ldots$. Each user can participate in a lending protocol by using one or more addresses, which serve as pseudonyms for that user. Hereafter, at the cost of a little ambiguity we will often identify users with their addresses. We also assume a denumerable set of *base token types* $\mathbb{T}$, ranged over by $\mathsf{T}, \mathsf{T}', \ldots$. The notation $v{:}\,\mathsf{T}$ stands for v units of token type T, where v is a nonnegative real number ($v \in \mathbb{R}_0^+$). When users deposit tokens of type T into a lending pool, they receive in return a receipt of the deposit, which we model as *credit tokens* T^c. Dually, when users borrow tokens from a LP, we represent their debt as *debit tokens* T^d. We denote the universes of credit and debit tokens as $\mathbb{T}^c$ and $\mathbb{T}^d$, respectively.

Wallets. We model the users' *wallets* as a function that associates each base token type and each address to the token balance directly available to the user. Formally:

$$\omega : (\mathbb{T} \times \mathbb{A}) \to \mathbb{R}_0^+$$

Note that $\omega(\mathsf{T}, \mathsf{A})$ ranges over a continuous domain. While this differs from concrete lending protocol implementations, where token balances are discrete, our model abstracts them as nonnegative real numbers, thereby avoiding the need to account for rounding in balance-related operations. Hereafter, we use $v, v', \ldots$ to range over $\mathbb{R}_0^+$.

Lending pools. A lending pool (in short, LP) is intuitively formed by three components:

- a map from base token types to the balance of their reserves in the pool;
- a map from addresses to their associated credit tokens;
- a map from addresses to their associated debit tokens.

For notational convenience, rather than modelling a LP as a triple of functions, we model it as a function with domain the disjoint union of the domains of the three maps:

$$\Lambda : (\mathbb{T} \uplus (\mathbb{T}^c \times \mathbb{A}) \uplus (\mathbb{T}^d \times \mathbb{A})) \to \mathbb{R}_0^+$$

where we assume that Λ has finite support. We now introduce some notation to manipulate LPs. We denote by $\{x \mapsto y\}$ a partial function mapping x to y. Pointwise summation of functions is denoted by $+$ and $\sum$. When f is defined on x but g is not, then $(f+g)(x) = f(x)$. For example, if Λ maps each element of its domain to 0, then $\Lambda + \{\mathsf{T} \mapsto 2\}$ is the function that is equal to Λ in all points but T, where it takes value 2.

Prices. A price oracle is a function associating a strictly positive price to each base token:

$$\pi : \mathbb{T} \to \mathbb{R}^+$$

We use the previously introduced notation to describe price updates as well: for example, $\pi + \{\mathsf{T} \mapsto 0.1\}$ denotes the price function that coincides with π for all token types except for T, whose price is increased by 0.1.

Blockchain states. A blockchain state defines all the components that are needed to represent the interactions between users and LPs. Formally, we render a blockchain state as a triple $\Gamma = (\omega, \Lambda, \pi)$ containing the users' wallets ω, the LP state Λ, and a price oracle π.

2.2. Basic economic definitions.

Token supply. Given a wallet state ω and a base token type T, we denote by $S_\omega(\mathsf{T})$ the number of units of T in ω. We refer to $S_\omega(\mathsf{T})$ as the *supply of* T *in* ω. Similarly, given a LP state Λ, we denote by $S_\Lambda(\mathsf{T}^c)$ and $S_\Lambda(\mathsf{T}^d)$ the supply of a credit token T^c and of a debit token T^d, respectively. Formally:

$$S_\omega(\mathsf{T}) = \sum_{\mathsf{A}} \omega(\mathsf{T}, \mathsf{A}) \qquad S_\Lambda(\mathsf{T}^c) = \sum_{\mathsf{A}} \Lambda(\mathsf{T}^c, \mathsf{A}) \qquad S_\Lambda(\mathsf{T}^d) = \sum_{\mathsf{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \tag{2.1}$$

Exchange rate. The *exchange rate* of a token type T in a LP state Λ represents the share of deposited units of T (i.e., reserves plus debts) over the units of the associated credit tokens. Formally, we define the exchange rate $XR_\Lambda(\mathsf{T})$ as:

$$XR_\Lambda(\mathsf{T}) \;=\; \begin{cases} \dfrac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} & \text{if } S_\Lambda(\mathsf{T}^c) \neq 0 \\ 1 & \text{otherwise} \end{cases} \tag{2.2}$$

The intuition, which will be more clear once we define the rules for depositing and redeeming tokens, is to define the price $\pi(\mathsf{T}^c)$ of a credit token type T^c in Λ as:

$$\pi(\mathsf{T}^c) \;=\; XR_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T}) \tag{2.3}$$

Then, when a user deposits $v{:}\,\mathsf{T}$ into a LP, they will receive in exchange an amount $v^c{:}\,\mathsf{T}^c$ such that $v \cdot \pi(\mathsf{T}) = v^c \cdot \pi(\mathsf{T}^c)$. We will also see in Lemma 3.4 that the exchange rate increases upon interest accruals. Since this leads to a proportional increase of the price of credit tokens as per (2.3), users have a direct incentive to providing liquidity to the LP.

Net worth. We define the value of tokens in A's wallet as the sum of the amounts of the tokens in $\omega(\cdot, \mathsf{A})$ weighted by their price:

$$W_{\omega,\pi}(\mathsf{A}) \;=\; \sum_{\mathsf{T}} \omega(\mathsf{T}, \mathsf{A}) \cdot \pi(\mathsf{T}) \tag{2.4}$$

The value of A's credits in a LP is the sum of the amounts of all the credit tokens owned by A weighted by their price:

$$W^c_{\Lambda,\pi}(\mathsf{A}) \;=\; \sum_{\mathsf{T}\in\mathbb{T}} \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T}) \tag{2.5}$$

Similarly, the value of A's debts in a LP is the sum of the amount of A's debit tokens weighted by the price of the underlying base token:

$$W^d_{\Lambda,\pi}(\mathsf{A}) \;=\; \sum_{\mathsf{T}\in\mathbb{T}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}) \tag{2.6}$$

We then define the *net worth* of A in a blockchain state $\Gamma = (\omega, \Lambda, \pi)$ as the value of base tokens in A's wallet, plus the value of credits in the LP, minus the value of A's debt:

$$W_\Gamma(\mathsf{A}) \;=\; W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) \tag{2.7}$$

We will show in Theorem 3.6 a fundamental preservation property, i.e. the net worth is preserved by all LP actions (except for price updates).

In certain cases, it will be useful to refer to the net worth of a user *restricted* to a specific base token type T. We will write $W_\Gamma(\mathsf{A})|_\mathsf{T}$ to denote the quantity obtained by removing from $W_\Gamma(\mathsf{A})$ all the expressions that do not mention T, i.e.:

$$W_\Gamma(\mathsf{A})|_\mathsf{T} \;=\; \Big(\omega(\mathsf{T}, \mathsf{A}) + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_\Lambda(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \pi(\mathsf{T}) \tag{2.8}$$

Of course, the overall net worth of A is given by the sum of her restricted net worth over all the base token types:

$$W_\Gamma(\mathsf{A}) \;=\; \sum_{\mathsf{T}\in\mathbb{T}} W_\Gamma(\mathsf{A})|_\mathsf{T} \tag{2.9}$$

Net position. The net worth $W_\Gamma(\mathsf{A})$ does not perfectly reflect the financial position of A. On the one hand, A may have tokens deposited in a LP that she cannot redeem due to insufficient liquidity in the LP: as a result, her disposable wealth is lower than her net worth. On the other hand, A may owe debts to the LP without the LP being able to enforce their repayment: in this case, her disposable wealth is actually higher than her net worth. This situation arises when A has more debts than credits, i.e. her net position is negative. Formally, we define the *net position* of A as:

$$W^{c-d}_{\Lambda,\pi}(\mathsf{A}) \;=\; W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) \;=\; W_\Gamma(\mathsf{A}) - W_{\omega,\pi}(\mathsf{A}) \tag{2.10}$$

A negative net position represents the amount of debts that a user can *default*, i.e. that the LP cannot be guaranteed to recover.

Collateralization and health factor. Collateralization is a measure of a user's ability to repay their debts, defined as the ratio between the values of the user's credits and debts:

$$C_{\Lambda,\pi}(\mathsf{A}) \;=\; \begin{cases} \dfrac{W^c_{\Lambda,\pi}(\mathsf{A})}{W^d_{\Lambda,\pi}(\mathsf{A})} & \text{if } W^d_{\Lambda,\pi}(\mathsf{A}) > 0 \\ +\infty & \text{otherwise} \end{cases} \tag{2.11}$$

The idea is that credit tokens are not directly transferable by users, but rather are kept by the LP as a guarantee in case a borrower fails to repay her debt. As we will see, LPs allow users to borrow only if they are over-collateralized, featuring an incentive mechanism for borrowers to keep their debt sufficiently collateralized over time. More specifically, borrowers must maintain their collateralization above a given value $1/T_{\mathsf{liq}} \geq 1$ in order to avoid that their credit tokens are seized and distributed to other users in exchange for repaying their debt. The value $T_{\mathsf{liq}} < 1$ is a protocol parameter, called *liquidation threshold*.

The requirement that a user A has sufficient collateralization can be equivalently expressed by requiring that their *health factor* $H_{\Lambda,\pi}(\mathsf{A})$ is at least 1, where:

$$H_{\Lambda,\pi}(\mathsf{A}) \;=\; C_{\Lambda,\pi}(\mathsf{A}) \cdot T_{\mathsf{liq}} \tag{2.12}$$

Interest rates. As in traditional finance, loans in lending protocols accrue interest over time. We keep our model parametric with respect to interest rates, by introducing a function $I_\Lambda(\mathsf{T})$, which depends only on the LP state Λ and the token type T. Coherently to actual lending protocols [GWPK20], we assume that interest rates are strictly positive, and that the interest rate for a token T depends solely on the total reserves, credits, and debits denominated in T, independently of their distribution across user addresses. Formally, we require the interest rate function to respect the following constraints, for all T:

$$I_\Lambda(\mathsf{T}) > 0 \qquad\qquad \Lambda \sim_{\mathsf{T}} \Lambda' \implies I_\Lambda(\mathsf{T}) = I_{\Lambda'}(\mathsf{T}) \tag{2.13}$$

where we define the relation $\sim_{\mathsf{T}}$ between two LP states as:

$$\Lambda \sim_{\mathsf{T}} \Lambda' \quad \triangleq \quad \Lambda(\mathsf{T}) = \Lambda'(\mathsf{T}) \;\wedge\; S_\Lambda(\mathsf{T}^c) = S_{\Lambda'}(\mathsf{T}^c) \;\wedge\; S_\Lambda(\mathsf{T}^d) = S_{\Lambda'}(\mathsf{T}^d)$$

Although most of our results do not depend on the actual choice for of the interest rate function, in examples and in some specific results (e.g., Theorems 5.4, 6.3, and 6.4) we will consider a concrete instantiation, inspired by actual lending protocols such as Aave and Compound. There, the interest rate for a token T in a LP state Λ is a function of the *utilization* of T, which measures the fraction of units of T currently lent to users. Formally, the utilization of T in Λ is defined as 0 when $S_\Lambda(\mathsf{T}^d) = 0$, and otherwise:

$$U_\Lambda(\mathsf{T}) \;=\; \frac{S_\Lambda(\mathsf{T}^d)}{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)} \tag{2.14}$$

We then define the *linear utilization interest rate* as a linear function of the token utilization:

$$I_\Lambda(\mathsf{T}) \;=\; \alpha \cdot U_\Lambda(\mathsf{T}) + \beta \qquad \text{where } \alpha \geq 0,\ \beta > 0 \tag{2.15}$$

The idea is that if a token T is under-utilized, i.e. there are many available reserves in the LP compared to the debts in T, then the interest rate for T should be low, in order to incentivize users to borrow it. Instead, if a token is over-utilized, i.e. there are many debts in T compared to the available reserves, a higher interest rate discourages additional loans [GWPK20].

TABLE 2. Transactions.

$\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$	A deposits v units of T, receiving back units of credit token T^c
$\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$	A borrows v units of T
$\mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$	A repays v units on A's debt in T
$\mathsf{A}\colon \mathsf{rdm}(v\colon \mathsf{T}^c)$	A redeems v units of T^c, receiving back units of T
$\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}_0, {\mathsf{T}_1}^c)$	A repays v units of B's debt in T_0, seizing units of ${\mathsf{T}_1}^c$ from B
int	All loans accrue interests
$\mathsf{px}(\delta\colon \mathsf{T})$	Price of tokens T is increased/decreased by δ

2.3. **Semantics.** We formalise the interaction between users and LPs as a labelled transition system between blockchain states. Labels $\mathsf{X}, \mathsf{X}', \ldots$ represent *transactions*, which define the actions performed by users and by the environment. Transactions have the form displayed in Table 2. In the rest of the section we present the rules that define the state transitions. An extended example of the application of these rules follows in Section 2.4.

The rules below define state transitions of the form $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$. When such a transition exists, we say that X is *enabled* in Γ. We extend this relation to sequences of transactions: for an empty sequence ε we have $\Gamma \xrightarrow{\varepsilon} \Gamma$, and for a sequence $\boldsymbol{\mathcal{X}} = \mathsf{X}\boldsymbol{\mathcal{Y}}$ made of a head X and a tail $\boldsymbol{\mathcal{Y}}$ we define:

$$\Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma' \qquad \text{iff} \qquad \Gamma \xrightarrow{\mathsf{X}} \Gamma'' \text{ and } \Gamma'' \xrightarrow{\boldsymbol{\mathcal{Y}}} \Gamma'$$

We say that a blockchain state Γ_0 is *initial* when its LP state has no reserves, no credit tokens, and no debit tokens. We then say that a state Γ is *reachable* when there exists some initial Γ_0 and some sequence of transactions $\boldsymbol{\mathcal{X}}$ such that $\Gamma_0 \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma$.

Deposit. Any user A can deposit v units of a base token type T by performing the transaction $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$. For each deposit of T, the LP mints v^c units of the credit token T^c. The amount v^c is computed in such a way that the value in credit tokens obtained by A is equal to the value of the deposited base tokens, i.e., according to (2.3), $v^c \cdot \pi(\mathsf{T}^c) = v \cdot \pi(\mathsf{T})$.

$$\frac{\omega(\mathsf{T},\mathsf{A}) \geq v > 0 \qquad v^c = v/XR_\Lambda(\mathsf{T}) \qquad \Lambda' = \Lambda + \{\mathsf{T} \mapsto v\} + \{(\mathsf{T}^c,\mathsf{A}) \mapsto v^c\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{dep}(v:\mathsf{T})} (\omega - \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [DEP]}$$

The premise $\omega(\mathsf{T},\mathsf{A}) \geq v$ ensures that A's wallet contains at least v units of T. In the new blockchain state, the wallet state $\omega - \{(\mathsf{T},\mathsf{A}) \mapsto v\}$ records that $v\colon \mathsf{T}$ have been subtracted from A's wallet. In the premises, v^c is the amount of credit tokens assigned to A upon the deposit. In the new LP state Λ', the reserves of T are increased by v units, and the credits of A are increased by v^c units. We refer to users holding credit tokens as *creditors*.

Borrow. Any user can borrow units of a base token type T from an LP, provided that the LP has sufficient reserves of T, and that the user has enough collateral. In the rule premises, this is rendered by requiring that the borrower's health factor is at least 1 after the action.

$$\frac{\Lambda(\mathsf{T}) \geq v > 0 \qquad \Lambda' = \Lambda - \{\mathsf{T} \mapsto v\} + \{(\mathsf{T}^d,\mathsf{A}) \mapsto v\}) \qquad H_{\Lambda',\pi}(\mathsf{A}) \geq 1}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{bor}(v:\mathsf{T})} (\omega + \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [BOR]}$$

In the new blockchain state, $v{:}\,\mathsf{T}$ are added to A's wallet and removed from the LP reserves. Furthermore, the LP records $v{:}\,\mathsf{T}^d$ additional debit tokens for the borrower A.

Repay. Any user with a loan in tokens T can repay it (in part or as whole) by paying base tokens T to the LP. In exchange, the LP cancels part of the users' debt, by removing a number of debit tokens T^d equivalent to the number of base tokens paid to the LP.

$$\frac{\omega(\mathsf{T},\mathsf{A}) \geq v > 0 \qquad \Lambda(\mathsf{T}^d,\mathsf{A}) \geq v \qquad \Lambda' = \Lambda + \{\mathsf{T} \mapsto v\} - \{(\mathsf{T}^d,\mathsf{A}) \mapsto v\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{rep}(v:\mathsf{T})} (\omega - \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Rep]}$$

Redeem. Any debt-free user can redeem credit tokens T^c for an equal value of the underlying base tokens, provided that enough reserves of T are available in the LP. As in the deposit rule, the number v of units of the base token is computed in such a way to have $v^c \cdot \pi(\mathsf{T}^c) = v \cdot \pi(\mathsf{T})$, according to (2.3). Any user with non-zero debts can redeem credit tokens as long as it remains over-collateralized. This constraint does not apply to users without loans, as credit tokens are not used as collateral.

$$\frac{\begin{array}{c}\Lambda(\mathsf{T}^c,\mathsf{A}) \geq v^c > 0 \qquad v = v^c \cdot XR_\Lambda(\mathsf{T}) \qquad \Lambda(\mathsf{T}) \geq v \\ \Lambda' = \Lambda - \{\mathsf{T} \mapsto v\} - \{(\mathsf{T}^c,\mathsf{A}) \mapsto v^c\} \qquad H_{\Lambda',\pi}(\mathsf{A}) \geq 1\end{array}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{rdm}(v^c:\mathsf{T}^c)} (\omega + \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Rdm]}$$

The premise $\Lambda(\mathsf{T}^c,\mathsf{A}) \geq v^c$ requires that A has at least the amount of credit tokens that they want to redeem. The premise $\Lambda(\mathsf{T}) \geq v$ requires that the LP has enough reserves of base tokens T to give in return. The premise $H_{\Lambda',\pi}(\mathsf{A}) \geq 1$ requires that A remains over-collateralized after the action.

Interest Accrual. Interest accrual models the application of interest to loans. The action applies an interest to each loan, updating the debt of *all* users with a non-zero debt.

$$\frac{\Lambda' = \Lambda + \textstyle\sum_{\mathsf{T},\mathsf{A}} \Lambda(\mathsf{T}^d,\mathsf{A}) \cdot I_\Lambda(\mathsf{T})}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{int}} (\omega,\Lambda',\pi)} \text{ [Int]}$$

Formally, for each base token type T, the number of debit tokens T^d of each A is increased by $\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot I_\Lambda(\mathsf{T})$, which is strictly greter than zero by (2.13). Note that this action may either increase or decreases the health factor of users with debts, since both $W^d(\mathsf{A})$ and $W^c(\mathsf{A})$ increase upon the action. Unlike the previous actions, the label int omits the name of the address who signs the transaction. This is because interest accruals are meant to be triggered in a time-dependent fashion, e.g. once for each block.

Liquidation. When the health factor of a borrower B is below 1, any other user A with sufficient tokens can *liquidate* part of B's loan, in return for a discounted amount of credit tokens seized from B. The maximum seizable amount is bounded by B's balance of the credit token and by the ex-post health factor of B, which cannot exceed 1 after the action. The protocol parameter $R_{\mathsf{liq}} > 1$ represents the *reward factor*, which implies that the value of tokens obtained by the liquidator A is greater than the value of B's debt repaid.

$$\frac{\begin{array}{c}\omega(\mathsf{T}_0,\mathsf{A}) \geq v_0 > 0 \qquad \Lambda(\mathsf{T}_0^d,\mathsf{B}) \geq v_0 \qquad v_1^c = \frac{v_0}{XR_\Lambda(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)} \cdot R_{\mathsf{liq}} \qquad \Lambda(\mathsf{T}_1^c,\mathsf{B}) \geq v_1^c \\ \Lambda' = \Lambda + \{\mathsf{T}_0 \mapsto v_0\} + \{(\mathsf{T}_1^c,\mathsf{A}) \mapsto v_1^c\} - \{(\mathsf{T}_1^c,\mathsf{B}) \mapsto v_1^c\} - \{(\mathsf{T}_0^d,\mathsf{B}) \mapsto v_0\} \\ \mathsf{A} \neq \mathsf{B} \qquad H_{\Lambda,\pi}(\mathsf{B}) < 1 \qquad H_{\Lambda',\pi}(\mathsf{B}) \leq 1\end{array}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{liq}(\mathsf{B},v_0:\mathsf{T}_0,\mathsf{T}_1^c)} (\omega - \{(\mathsf{T}_0,\mathsf{A}) \mapsto v_0\},\Lambda',\pi)} \text{[Liq]}$$

Note that the amount v_1^c of credit tokens received by A is computed in such a way to equal the value of repaid debt, multiplied by the reward factor. That is, according to (2.3):

$$v_1^c \cdot \pi(\mathsf{T}_1^c) \;=\; v_1^c \cdot XR_\Lambda(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1) \;=\; v_0 \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}} \;>\; v_0 \cdot \pi(\mathsf{T}_0)$$

Price updates. The price of any base token can be increased/decreased by an amount $\delta \in \mathbb{R} \setminus \{0\}$, provided that the new price is still strictly positive:

$$\frac{\pi(\mathsf{T}) + \delta > 0}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{px}(\delta:\mathsf{T})} (\omega,\Lambda,\pi + \{\mathsf{T} \mapsto \delta\})} \text{[Px]}$$

Similarly to int, also the transition label $\mathsf{px}(\delta\colon \mathsf{T})$ is not linked to any address. This is because while in other actions the address in the label is the transaction signer, in a price update transaction we assume that the action can be performed only by a special user, acting as a price oracle.

Token swap. The actions considered so far fully characterise the behaviour of lending protocols. However, in order to be able to analyse the economic impact of strategies where users can also interact with the environment, we extend our transition system with an additional *swap* action, allowing users to exchange base tokens of type T_0 with a price-equivalent amount of tokens of another type T_1:

$$\frac{\omega(\mathsf{T}_0,\mathsf{A}) \geq v > 0 \qquad \omega' = \omega - \{(\mathsf{T}_0,\mathsf{A}) \mapsto v\} + \{(\mathsf{T}_1,\mathsf{A}) \mapsto v \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)}\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{swp}(v:\mathsf{T}_0,\mathsf{T}_1)} (\omega',\Lambda,\pi)} \text{[Swp]}$$

In practice, swap actions can be executed through centralized or decentralized exchange services. For example, Automated Market Makers (AMMs) are decentralized protocols that allow users to swap between two token types at an algorithmically determined exchange rate, and also serve as decentralized price oracles [AC20, BCL22]. In real-world settings, token swaps — especially when involving large amounts — typically result in price adjustments. For example, a large sale of a token is usually accompanied by a decrease of its price (e.g., in AMMs this price update is applied automatically as part of the swap action). In our [Swp] transition we assume that token prices are preserved: when necessary, we can still represent a price-updating swap action as an atomic sequence of [Swp] and [Px].

2.4. **An example.** We now illustrate our semantics through a simple example involving users A and B. We display their interactions in Figure 1, using an alternative representation of blockchain states for readability. Namely, we write a blockchain state as:

$$\mathsf{A}_1[w_1] \mid \cdots \mid \mathsf{A}_n[w_n] \mid [v_1\colon \mathsf{T}_1, \cdots, v_k\colon \mathsf{T}_k] \mid \pi$$

In this representation, a term $\mathsf{A}_i[w_i]$ includes the tokens of *all* kinds (base, credit, and debit) associated to A_i, while the term $[v_1\colon \mathsf{T}_1, \cdots, v_k\colon \mathsf{T}_k]$ describes the reserves of base tokens deposited in the LP. So, for example, the blockchain state (ω, Λ, π) where:

$$\omega = \{(\mathsf{T}_0, \mathsf{A}) \mapsto 1\} \qquad \Lambda = \{\mathsf{T}_0 \mapsto 2, \mathsf{T}_1 \mapsto 3, (\mathsf{T}_0^c, \mathsf{A}) \mapsto 4, (\mathsf{T}_1^c, \mathsf{B}) \mapsto 5, (\mathsf{T}_0^d, \mathsf{B}) \mapsto 6\}$$

would be represented in our sugared syntax as follows:

$$\mathsf{A}[1\colon \mathsf{T}_0, 4\colon \mathsf{T}_0^c] \mid \mathsf{B}[5\colon \mathsf{T}_1^c, 6\colon \mathsf{T}_0^d] \mid [2\colon \mathsf{T}_0, 3\colon \mathsf{T}_1] \mid \pi$$

We now discuss the state transitions in Figure 1. In the initial blockchain state, A has 100 units of T_0, B has 50 units of T_1, the LP has no reserves, and the price of both token types is 1. We assume that the protocol parameters are as follows: the liquidation threshold is $T_{\mathsf{liq}} = 2/3$, the liquidation reward is $R_{\mathsf{liq}} = 1.1$, and the interest rate function is utility-based and has parameters $\alpha = 0$ and $\beta = 0.12$, meaning that there is a constant interest factor $I_\Lambda(\mathsf{T}) = 12\%$ for all token types T.

- In steps 1 and 2, A and B deposit 50 units of T_0 and T_1, respectively, for which they receive equal amounts of credit tokens T_0^c and T_1^c.
- In step 3, B borrows 30: T_0, using his credit tokens T_1^c as collateral for the loan. The loan is permitted because the B's health factor after the action is above the safety threshold 1. Although B could have borrowed up to $W^c(\mathsf{B}) \cdot T_{\mathsf{liq}} = 50 \cdot 2/3 = 33.3$ units of T_0, given the collateral of 50: ${\mathsf{T}_1}^c$, here we assume that B decides to leave some margin to manage future price volatility and the accrual of interest, which could decrease B's health factor.
- In step 4, interest accrues on B's debt. Since the interest rate is 12%, B's debt on T_0 grows from 30 to 33.6.
- In step 5, B repays part of her debt, by paying 5: T_0 to the LP. In this way, B's health factor grows from 0.99 to 1.16, avoiding the risk of being immediately liquidated by A.
- In step 6, the price of T_0 is increased by 0.3: since the debt value is at the denominator in the formula of collateralization (2.11), this yields a decrease of B's health factor. This value drops to 0.89, crossing the threshold for liquidations.
- In step 7, A liquidates 11: T_0 of B's debt, obtaining in exchange $v_1^c\colon \mathsf{T}_1^c$, where:

  $$v_1^c = \frac{11}{XR(\mathsf{T}_1)} \cdot \frac{\pi'(\mathsf{T}_0)}{\pi'(\mathsf{T}_1)} \cdot R_{\mathsf{liq}} = \frac{11}{1} \cdot \frac{1.3}{1} \cdot 1.1 = 15.73$$

  Since the liquidation reward $R_{\mathsf{liq}} > 1$, the value in credit tokens obtained by A is greater than the value in base tokens she paid, making the liquidation profitable:

  $$11 \cdot \pi(\mathsf{T}_1) = 11 \cdot 1.3 = 14.3 \quad < \quad 15.73 \cdot XR(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1) = 15.73$$

  After the liquidation, B's health factor is increased (to 0.99), since B's debt value has decreased while the credit value has been preserved. Note that A could have not liquidated, e.g., 12: T_0, since doing so would have made B's health factor exceed the safety threshold.
- In step 8, A redeems 10: T_0^c, receiving 10.72: T_0 in exchange. Here, each unit of T_0^c is exchanged for $XR(\mathsf{T}_0) = {}^{36+17.6}/_{15.73+34.27} = 1.072$ units of T_0, due to accrued interests.

$$
\begin{aligned}
&\mathsf{A}[100\colon \mathsf{T}_0] \mid \mathsf{B}[50\colon \mathsf{T}_1] \mid [0\colon \mathsf{T}_0, 0\colon \mathsf{T}_1] \mid \pi = \{\mathsf{T}_0 \mapsto 1, \mathsf{T}_1 \mapsto 1\} \\
\xrightarrow{1.\ \mathsf{A}:\mathsf{dep}(50:\mathsf{T}_0)}\ &\mathsf{A}[50\colon \mathsf{T}_0, 50\colon \mathsf{T}_0^c] \mid \mathsf{B}[50\colon \mathsf{T}_1] \mid [50\colon \mathsf{T}_0] \mid \cdots \\
\xrightarrow{2.\ \mathsf{B}:\mathsf{dep}(50:\mathsf{T}_1)}\ &\mathsf{A}[\cdots] \mid \mathsf{B}[50\colon \mathsf{T}_1^c] \mid [50\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \cdots \\
\xrightarrow{3.\ \mathsf{B}:\mathsf{bor}(30:\mathsf{T}_0)}\ &\mathsf{A}[\cdots] \mid \mathsf{B}[30\colon \mathsf{T}_0, 30\colon \mathsf{T}_0^d] \mid [20\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \cdots && (H(\mathsf{B}) = 1.11) \\
\xrightarrow{4.\ \mathsf{int}}\ &\mathsf{B}[30\colon \mathsf{T}_0, 33.6\colon \mathsf{T}_0^d] \mid [20\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \cdots && (H(\mathsf{B}) = 0.99) \\
\xrightarrow{5.\ \mathsf{B}:\mathsf{rep}(5:\mathsf{T}_0)}\ &\mathsf{B}[25\colon \mathsf{T}_0, 28.6\colon \mathsf{T}_0^d] \mid [25\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \cdots && (H(\mathsf{B}) = 1.16) \\
\xrightarrow{6.\ \mathsf{px}(0.3:\mathsf{T}_0)}\ &\cdots \mid \pi' = \{\mathsf{T}_0 \mapsto 1.3, \mathsf{T}_1 \mapsto 1\} && (H(\mathsf{B}) = 0.89) \\
\xrightarrow{7.\ \mathsf{A}:\mathsf{liq}(\mathsf{B},11:\mathsf{T}_0,\mathsf{T}_1^c)}\ &\mathsf{A}[39\colon \mathsf{T}_0, 50\colon \mathsf{T}_0^c, 15.73\colon \mathsf{T}_1^c] \mid \mathsf{B}[25\colon \mathsf{T}_0, 34.27\colon \mathsf{T}_1^c, 17.6\colon \mathsf{T}_0^d] \mid && (H(\mathsf{B}) = 0.99) \\
&[36\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \pi' \\
\xrightarrow{8.\ \mathsf{A}:\mathsf{rdm}(10:\mathsf{T}_0^c)}\ &\mathsf{A}[49.72\colon \mathsf{T}_0, 40\colon \mathsf{T}_0^c, 15.73\colon \mathsf{T}_1^c] \mid \mathsf{B}[\cdots] \mid [25.28\colon \mathsf{T}_0, 50\colon \mathsf{T}_1] \mid \pi'
\end{aligned}
$$

FIGURE 1. Interactions between two users and a lending pool.

3. Structural properties of lending protocols

We establish in this section some structural properties of lending protocols, such as relevant invariants on their reachable states. As usual, free variables in statements are meant to be universally quantified; furthermore, blockchain states in the hypotheses are always assumed to be reachable. For simplicity, we will just write, for example, $\mathsf{X} \neq \mathsf{px}$ to mean that there exist no δ and T such that $\mathsf{X} = \mathsf{px}(\delta\colon \mathsf{T})$, and similarly for other transaction types.

First, we establish that the transition system is deterministic. This follows directly from the fact that, given a blockchain state Γ and a transaction X, there is at most one applicable rule. Determinism is a key property for blockchains, since it ensures that all the blockchain nodes can reconstruct the same state from a sequence of transactions.

Lemma 3.1 (Determinism). *If* $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$ *and* $\Gamma \xrightarrow{\mathsf{X}} \Gamma''$, *then* $\Gamma' = \Gamma''$.

Lemma 3.2 establishes that the amount of any base token is preserved by state transitions. The only exception is the [Swp] transition, which however does not "morally" break the invariant, since it represents the exchange of tokens between the user and an external service. By applying Lemma 3.2 inductively, it follows that base tokens are preserved along arbitrary sequences of transitions (not containing swaps).

Lemma 3.2 (Preservation of base tokens). *Let* $(\omega, \Lambda, \pi) \xrightarrow{\mathsf{X}} (\omega', \Lambda', \pi')$ *with* $\mathsf{X} \neq \mathsf{swp}$. *Then, for all* T*:*

$$S_\omega(\mathsf{T}) + \Lambda(\mathsf{T}) \;=\; S_{\omega'}(\mathsf{T}) + \Lambda'(\mathsf{T})$$

The following lemma gives a useful invariant on reachable LP states: if the LP has no credit tokens T^c, then it has neither reserves of T nor debit tokens T^d. Another invariant relating base, credit and debit tokens will be established later in (3.1).

Lemma 3.3. *If* $S_\Lambda(\mathsf{T}^c) = 0$, *then* $\Lambda(\mathsf{T}) = 0 = S_\Lambda(\mathsf{T}^d)$.

The exchange rate of any base token type T is preserved by all state transitions, except interest accruals and, in the case there are no debts in T, a redeem that reclaims the

entirety of the credits (bringing back the exchange rate to 1). When interests accrue, the exchange rate of T strictly increases whenever users have loans in T. By Equation (2.11), this guarantees that the credit token T^c will gain value (whenever the price of the underlying base token T is not decreased by a price update transition).

Lemma 3.4 (Monotonicity of exchange rate)**.** *Let* $(\omega, \Lambda, \pi) \xrightarrow{\mathsf{X}} (\omega', \Lambda', \pi')$*. Then, for all* T*:*

(a) *if* $\mathsf{X} = \mathsf{int}$ *and* $S_\Lambda(\mathsf{T}^d) > 0$*, then*

$$XR_{\Lambda'}(\mathsf{T}) \;=\; XR_\Lambda(\mathsf{T}) + \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} \cdot I_\Lambda(\mathsf{T}) \;>\; XR_\Lambda(\mathsf{T})$$

(b) *if* $\mathsf{X} = \mathsf{rdm}$*, and* $S_{\Lambda'}(\mathsf{T}^c) = 0$*, then* $XR_{\Lambda'}(\mathsf{T}) = 1$

(c) *otherwise,* $XR_{\Lambda'}(\mathsf{T}) = XR_\Lambda(\mathsf{T})$*.*

By (2.2), in initial blockchain states the exchange rate of each token is 1. Therefore, from the previous lemma it follows that in any reachable state the exchange rate of any token is always greater than or equal to 1. This is formalised by the following:

Corollary 3.5. $XR_\Lambda(\mathsf{T}) \geq 1$*.*

Together with (2.2), this corollary gives an upper bound to the supply of credit tokens in each reachable LP state. More precisely, the supply of T^c is bounded by the amount of reserves of T in the LP, plus the overall debt on T:

$$S_\Lambda(\mathsf{T}^c) \;\leq\; \Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d) \tag{3.1}$$

Note that, in the specific case where $\Lambda(\mathsf{T}) = 0 = S_\Lambda(\mathsf{T}^d)$, Equation (3.1) shows that also the inverse of Lemma 3.3 holds, i.e. under that hypothesis, we have that $S_\Lambda(\mathsf{T}^c) = 0$.

The following theorem establishes that the total net worth of all users remains constant throughout executions, except possibly when token prices are updated.

Theorem 3.6 (Preservation of net worth)**.** *For all* $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$ *such that* $\mathsf{X} \neq \mathsf{px}$*:*

$$\sum_{\mathsf{C} \in \mathbb{A}} W_{\Gamma'}(\mathsf{C}) = \sum_{\mathsf{C} \in \mathbb{A}} W_\Gamma(\mathsf{C})$$

4. Economic analysis of single transactions

In this section we exhaustively analyze how each action affects the net worth of users and their health factor. We will see that, among *user actions* (i.e., all the actions except int and px), the only action that can change the net worth of a user is the liquidation (positively if fired by the user, negatively if suffered by the user) — Lemma 4.1. Environment actions such as interest accruals and price updates, on the other hand, affect the net worth of users exposed to the relevant tokens — that is, users holding debt or credit tokens whose price or interest is modified by these actions. In particular, int always penalizes *debtors* (users who have debts), and benefits *creditors* (users who hold credit tokens) — Lemma 4.3. The action px, on the contrary, benefits debtors and penalizes creditors if the price goes down, while it penalizes debtors and benefits creditors if the price goes up — Lemma 4.2.

Besides maximizing gains, users are also compelled with reducing the risk of incurring in losses. In particular, a user should avoid being the subject of a liquidation. The risk of being liquidated depends on the health factor: indeed, to avoid liquidations, one's health

factor should not fall below 1. We will prove that deposits, repayments and liquidations increase the health factor of the user who fires them, while borrows and redeems decrease it — Lemma 4.4. In particular, we will see that, while in general repayments improve the health factor more than deposits, for users that are severely indebted it is better to deposit rather than repay — Lemma 4.6.

4.1. **Effect of transactions on net worth.** In order to study the economic impact of actions on users' net worth, we first define the *gain* of an address A upon firing a sequence of transactions $\boldsymbol{\mathcal{X}}$ from a state Γ:

$$g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) \;=\; W_{\Gamma'}(\mathsf{A}) - W_{\Gamma}(\mathsf{A}) \qquad \text{if } \Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma' \tag{4.1}$$

Note that the gain is well-defined, because if $\Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma'$ and $\Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma''$, then by determinism (Lemma 3.1) we must have $\Gamma' = \Gamma''$. When $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) < 0$, we will use the term *loss* to denote the value $|g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}})|$. Note that $\boldsymbol{\mathcal{X}}$ must not necessarily be performed by A, as it may include other users' actions, or environment actions.

Note that when some of the transactions in $\boldsymbol{\mathcal{X}}$ are not enabled in Γ, then the gain $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}})$ is not well-defined. In this case, with a slight abuse of notation, we will write $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}})$ to mean $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}')$, where $\boldsymbol{\mathcal{X}}'$ is the sequence of transactions obtained from $\boldsymbol{\mathcal{X}}$ by removing all the non-enabled transactions.

The following lemma shows that the only user action (i.e. all actions except int or px) that can change the net worth of users is liq. Such action increases the net worth of the liquidator and correspondingly decreases that of the liquidated address. In particular, the gain of the liquidator is proportional to the amount liquidated, and it coincides with the loss of the user being liquidated.

Lemma 4.1 (Gain from user actions)**.** *Let X be enabled in Γ, with $\mathsf{X} \notin \{\mathsf{int}, \mathsf{px}\}$. Then:*
(1) $g_{\mathsf{A}}(\Gamma, \mathsf{X}) = 0 \iff \mathsf{X}$ *is not a liquidation involving* A.
(2) $g_{\mathsf{A}}(\Gamma, \mathsf{X}) > 0 \iff \mathsf{X}$ *is a liquidation performed by* A;
(3) $g_{\mathsf{A}}(\Gamma, \mathsf{X}) < 0 \iff \mathsf{X}$ *is a liquidation suffered by* A;
In particular, if $\mathsf{X} = \mathsf{A}{:}\,\mathsf{liq}(\mathsf{B}, v{:}\,\mathsf{T}_0, \mathsf{T}_1^c)$, we have that:
(4) $g_{\mathsf{A}}(\Gamma, \mathsf{X}) = -g_{\mathsf{B}}(\Gamma, \mathsf{X}) = v \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}}$.

Note that the gain of A only depends on the value $v \cdot \pi(\mathsf{T}_0)$ being liquidated. This implies that the optimal strategy for a *non-strategic* user A — i.e., one who just wants to maximize their istantaneous gain — is to liquidate as much as possible, regardless of the users being liquidated and of the token types of the collateral received.

The following lemma shows how a user A benefits from (or gets damaged by) a price update of a token T. Specifically, the gain of A is given by the product between her wealth restricted to T and the ratio between the price variation and the old price of T. Recalling from (2.8) the definition of restricted wealth, we see that this gain is proportional to the amount of base tokens owned, plus the credits (adjusted by the exchange rate), and minus the debts, all multiplied by the price variation.

Lemma 4.2 (Gain from price updates)**.** *The gain of A upon a transaction $\mathsf{px}(\delta{:}\,\mathsf{T})$ in $\Gamma = (\omega, \Lambda, \pi)$ is given by:*

$$g_{\mathsf{A}}(\Gamma, \mathsf{px}(\delta{:}\,\mathsf{T})) \;=\; W_{\Gamma}(\mathsf{A})|_{\mathsf{T}} \cdot \frac{\delta}{\pi(\mathsf{T})} \;=\; \Big(\omega(\mathsf{T}, \mathsf{A}) + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \delta$$

Note that, when the price decreases (i.e. $\delta < 0$), the proportionality is of opposite sign, i.e. a user with lots of debts in T would benefit from the price decrease, while a user with lots of credits or base tokens would suffer losses.

The following lemma quantifies the effect of interest accruals on the users' gain. For each address A and token T, the gain of A is proportional to the interest accrued, to the price of T, and to the difference between the user credits in T (weighted by the ratio between the supply of debts and credits in T) and the user debts in T.

Lemma 4.3 (Gain from interest accruals)**.** *The gain of* A *upon a transaction* int *in* $\Gamma = (\omega, \Lambda, \pi)$ *is given by:*

$$g_{\mathsf{A}}(\Gamma, \mathsf{int}) \;=\; \sum_{S_\Lambda(\mathsf{T}^c)>0} \left(\frac{\Lambda(\mathsf{T}^c, \mathsf{A})}{S_\Lambda(\mathsf{T}^c)} \cdot S_\Lambda(\mathsf{T}^d) - \Lambda(\mathsf{T}^d, \mathsf{A}) \right) \cdot I_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T})$$

We additionally observe that the overall gain of A is given by the summation of the pointwise gains, as per (2.9). From that, we infer that A's gain *restricted* to a given token type T is positive if and only if A has credits in T and the ratio of A's credits in T over the total credits of T exceeds the ratio of A's debts over the total debit in T, i.e.:

$$g_{\mathsf{A}}(\Gamma, \mathsf{int})\,|_{\mathsf{T}} > 0 \quad \iff \quad \frac{\Lambda(\mathsf{T}^c, \mathsf{A})}{S_\Lambda(\mathsf{T}^c)} > \frac{\Lambda(\mathsf{T}^d, \mathsf{A})}{S_\Lambda(\mathsf{T}^d)}$$

In particular, this implies that pure creditors always have a gain from interest accruals.

4.2. **Effect of transactions on health factor.** We now study how user actions impact the health factor. The following lemma shows that deposits, repayments and liquidations increase users' health factor, while borrows and redeems decrease it.

Lemma 4.4 (Health factor from user actions)**.** *Let* $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$*, with* $\mathsf{X} = \mathsf{A}{:}\,\ell(\cdots)$*. Then:*

(1) $\ell \in \{\mathsf{dep}, \mathsf{rep}, \mathsf{liq}\} \implies H_{\Gamma'}(\mathsf{A}) \geq H_\Gamma(\mathsf{A})$
(2) $\ell \in \{\mathsf{bor}, \mathsf{rdm}\} \implies H_{\Gamma'}(\mathsf{A}) \leq H_\Gamma(\mathsf{A})$
(3) $\ell \in \{\mathsf{swp}\} \implies H_{\Gamma'}(\mathsf{A}) = H_\Gamma(\mathsf{A})$

Moreover, the inequalities in (1) *and* (2) *are strict if and only if* $W^d_\Gamma(\mathsf{A}) > 0$.

We have shown how actions performed by a user impact her health factor. It remains to study the effect of transactions that are not performed by the user, i.e. price updates, interest accruals, and liquidation suffered.

Price updates and interest accruals, depending on the state, can arbitrarily increase and decrease both the credits and the debts, hence it is quite clear that the health factor after these transactions can either increase or decrease.

For liquidations suffered, however, the ratio between the value of the liquidated debts and that of the seized credits is fixed, given by R_{liq}, hence it is not that straightforward to conclude whether the health factor of the liquidated user always increases, always decreases, or can either increase or decrease. While the previous lemma showed that the health factor of liquidators always increases, here we show that that of the liquidated address may either increase or decrease. It is not difficult to quantify the variation in the health factor of a borrower B who is suffering a liquidation, even though this is not particularly insightful.

For a liquidation $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}_0, \mathsf{T}_1^c)$ fired in Γ, the difference between the new and the old health factor of B is given by:

$$H_{\Gamma'}(\mathsf{B}) - H_\Gamma(\mathsf{B}) \;=\; \frac{\left(W_\Gamma^c(\mathsf{B}) - W_\Gamma^d(\mathsf{B}) \cdot {}^{R_{\mathsf{liq}}}\!/_{XR_\Gamma(\mathsf{T}_0)}\right) \cdot v \cdot \pi(\mathsf{T}_0) \cdot T_{\mathsf{liq}}}{W_\Gamma^d(\mathsf{B}) \cdot (W_\Gamma^d(\mathsf{B}) - v \cdot \pi(\mathsf{T}_0))}$$

The following example shows concrete cases where the health factor of the borrower increases or decreases upon a liquidation.

Example 4.5. Consider a lending protocol with parameters $T_{\mathsf{liq}} = 2/3$, $R_{\mathsf{liq}} = 1.3$, and an utility-based interest rate function with $\alpha = 0$ and $\beta = 1/2$. Let Γ be an initial blockchain state where the following sequences of transactions are enabled:

$$\boldsymbol{\mathcal{X}} = \mathsf{B}\colon \mathsf{dep}(50\colon \mathsf{T})\;\; \mathsf{B}\colon \mathsf{bor}(30\colon \mathsf{T})\;\; \mathsf{int}\;\; \mathsf{A}\colon \mathsf{liq}(10\colon \mathsf{T}, \mathsf{B}, \mathsf{T})$$
$$\boldsymbol{\mathcal{Y}} = \mathsf{A}\colon \mathsf{dep}(90\colon \mathsf{T})\;\; \boldsymbol{\mathcal{X}}$$

In $\boldsymbol{\mathcal{X}}$, the health factor of the borrower B increases from 0.96 to 0.99 with the liquidation while in $\boldsymbol{\mathcal{Y}}$ is decreases from 0.82 to 0.80. This is because A's deposit (which is not present in $\boldsymbol{\mathcal{X}}$) has affected the exchange rate of T after the interest accrual: in $\boldsymbol{\mathcal{X}}$, such exchange rate is 1.3, while in $\boldsymbol{\mathcal{Y}}$ it is 1.1. This decrease in the exchange rate, caused by the reduced impact of B's debts on the ratio in (2.2), makes the value of B's credits decrease compared to $\boldsymbol{\mathcal{X}}$. Since the value of B's debts is preserved, this explains the decrease in B's health factor. See: `https://github.com/bitbart/lp-model/tree/main/examples-lmcs`. ◇

A user at risk of liquidation should try to immediately improve her health factor in order to avoid the losses coming from being liquidated. The following lemma compares the improvements that repays and deposits bring to the health factor.

Lemma 4.6 (Health factor: deposit *vs.* repay)**.** *Let* $\Gamma \xrightarrow{\mathsf{A}:\mathsf{dep}(v:\mathsf{T})} \Gamma_{dep}$ *and* $\Gamma \xrightarrow{\mathsf{A}:\mathsf{rep}(v:\mathsf{T})} \Gamma_{rep}$. *Then:*

$$H_{\Gamma_{rep}}(\mathsf{A}) \geq H_{\Gamma_{dep}}(\mathsf{A}) \quad \iff \quad v \cdot \pi(\mathsf{T}) \geq W_\Gamma^d(\mathsf{A}) - W_\Gamma^c(\mathsf{A})$$

From the previous lemma we see that repayments increase the health factor more than deposits if and only if the value transferred to the LP is greater than the difference between the value of debts of the user and the value of credit tokens held. In practice, this means that, for users with a positive net position — i.e., when $W_\Gamma^d(\mathsf{A}) < W_\Gamma^c(\mathsf{A})$ — it is more beneficial to repay instead of deposit. Instead, for users with negative net position, it could be more convenient to deposit, especially when the transferred value is small. This contradicts the statement contained in the Aave FAQs[1] for which "*By default, repayments increase your health factor more than deposits*".

5. Economic analysis of strategic players

All results in the previous section pertain to actions that have an immediate impact — either positive or negative — on a user. In contrast, in this section we consider more complex scenarios in which a user foresees a future event (e.g. int, px, or a liquidation against them). We study the *strategic* dimension of lending protocols: in particular, which actions should the user fire before the foreseen action takes effect in order to improve their net worth?

[1] `https://web.archive.org/web/20240914031752/https://docs.aave.com/faq/liquidations`

Conversely, if the user intends to execute a specific action, would it be better to fire it *before* or *after* the foreseen event?

We start by considering a game where a borrower A foresees that she is going to be liquidated. In order to avoid the liquidation, the only possibly helpful actions are those which increase A's health factor — by Lemma 4.4 — dep, rep and liq. We already know from Lemma 4.1 that liquidations performed by A increase her gain, so we limit our analysis to dep and rep. Theorem 5.1 shows that these actions are only helpful if they disable the liquidation fired against A; otherwise, they do not have any effect.

Theorem 5.1 (Strategy for impending liquidations)**.** *Let* A *and* $\Gamma = (\omega, \Lambda, \pi)$ *be such that* $H_\Gamma(\mathsf{A}) < 1$*, and let* liq *be a shorthand for an arbitrary liquidation on* A *enabled in* Γ*.*

Let $\mathsf{X} = \mathsf{A}{:}\,\ell(v{:}\,\mathsf{T})$ *with* $\ell \in \{\mathsf{dep}, \mathsf{rep}\}$*, and let* $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$*. Then:*

(1) *If* $\ell = \mathsf{dep}$*, then* $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) > g_\mathsf{A}(\Gamma, \mathsf{liq}) \iff v \geq \frac{XR_\mathsf{A}(\mathsf{T})}{\pi(\mathsf{T})} \cdot \left(\frac{W^d_{\Lambda,\pi}(\mathsf{A})}{T_\mathsf{liq}} - W^c_{\Lambda,\pi}(\mathsf{A}) \right)$

(2) *If* $\ell = \mathsf{rep}$*, then* $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) > g_\mathsf{A}(\Gamma, \mathsf{liq}) \iff v \geq \frac{1}{\pi(\mathsf{T})} \cdot \left(W^d_{\Lambda,\pi}(\mathsf{A}) - W^c_{\Lambda,\pi}(\mathsf{A}) \cdot T_\mathsf{liq} \right)$

The theorem also shows that, if A wants to minimize the parameter v, then she should choose dep if and only if $W^d_\Gamma(\mathsf{A}) \cdot (XR_\Gamma(\mathsf{T})/T_\mathsf{liq} - 1) \geq W^c_\Gamma(\mathsf{A}) \cdot (XR_\Gamma(\mathsf{T}) - T_\mathsf{liq})$, and choose rep otherwise.

Note that A cannot fire valid bor and rdm transactions in Γ, since, by hypothesis, A can be subject to liquidation, and so $H_\Gamma(\mathsf{A}) < 1$.

The following theorem shows how a user can take advantage of an incoming price update. It turns out that the only effective action is front-running the price update with a swap of the token affected by the price update. The rational strategy is to sell the token when its price is going to decrease, and to buy it otherwise.

Theorem 5.2 (Strategy for impending price updates)**.** *Let* $\mathsf{X} = \mathsf{A}{:}\,\ell(\cdots)$ *mentioning token* T*, let* $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$*, and let* px *be a shorthand for* $\mathsf{px}(\delta{:}\,\mathsf{T})$*. We have that:*

$$g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{px}) \circ g_\mathsf{A}(\Gamma, \mathsf{px}) = g_\mathsf{A}(\Gamma, \mathsf{px}\,\mathsf{X})$$

where the relation $\circ$ *is given by:*

$$\circ = \begin{cases} = & \text{if } \ell \in \{\mathsf{dep}, \mathsf{rep}, \mathsf{bor}, \mathsf{rdm}\} \\ > & \text{if } (\delta > 0 \text{ and } \ell = \mathsf{swp}(v{:}\,\mathsf{T}', \mathsf{T})) \text{ or } (\delta < 0 \text{ and } \ell = \mathsf{swp}(v{:}\,\mathsf{T}, \mathsf{T}')) \\ < & \text{if } (\delta < 0 \text{ and } \ell = \mathsf{swp}(v{:}\,\mathsf{T}', \mathsf{T})) \text{ or } (\delta > 0 \text{ and } \ell = \mathsf{swp}(v{:}\,\mathsf{T}, \mathsf{T}')) \end{cases}$$

More precisely, if Γ *has price function* π*, then:*

$$g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{px}) = g_\mathsf{A}(\Gamma, \mathsf{px}) + \sigma \cdot v \cdot \delta \cdot \left(\frac{\pi(\mathsf{T}')}{\pi(\mathsf{T})} \right)^\sigma \qquad \sigma = \begin{cases} 1 & \ell = \mathsf{swp}(v{:}\,\mathsf{T}', \mathsf{T}) \\ -1 & \ell = \mathsf{swp}(v{:}\,\mathsf{T}, \mathsf{T}') \end{cases}$$

Notice that in Theorem 5.2 we have not included the case $\ell = \mathsf{liq}$. Indeed, by Lemma 4.1 we already know that liq yields a positive gain, but only because of the liquidation reward. It is irrelevant to perform it before or after the price update (i.e. $g_\mathsf{A}(\Gamma, \mathsf{liq}\,\mathsf{px}) = g_\mathsf{A}(\Gamma, \mathsf{px}\,\mathsf{liq})$).

The previous theorem shows that, anticipating an increase in the price of T, the only single actions that a user A can perform to improve her net worth is to sell another token T' to buy T. But what if A is already fully exposed on T (i.e. she possesses only tokens in T)?

In traditional finance, traders can increase their exposition to a given asset via *financial options*: the trader buys a contract from a issuer, acquiring the right to buy from the issuer the underlying asset for a fixed *strike price* in the future. Hence, if in the future the market price of the asset exceeds the strike price, the trader can make a profit by buying the discounted asset from the issuer and resell it at market price. Some analogies between lending protocols and financial options has been investigated in [QEZ+24, SVTZ24].

The following lemma shows how A can exploit the lending protocol to increase her exposure to token T and benefit from a foreseen increase in the price of T, analogously what buyers do with financial options.

Lemma 5.3 (Strategy for impending price updates, II)**.** *Let:*

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})\;\; \mathsf{A}\colon \mathsf{bor}(v'\colon \mathsf{T}')\;\; \mathsf{A}\colon \mathsf{swp}(v'\colon \mathsf{T}', \mathsf{T})$$

be enabled in Γ*, and let* px *be a shorthand for* $\mathsf{px}(\delta\colon \mathsf{T})$ *with* $\delta > 0$*. We have that:*

$$g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}\,\mathsf{px}) \;>\; g_{\mathsf{A}}(\Gamma, \mathsf{px})$$

The following theorem considers a game in which A foresees an impending interest accrual. If we consider an arbitrary interest rate function, then there is no single action that A can fire before the interest accrual that is guaranteed to benefit her. Even if we limit to linear utility interest rate functions, i.e. $I_\Lambda(\mathsf{T}) = \alpha \cdot U_\Lambda(\mathsf{T}) + \beta$, as in (2.15), then A's strategy is not straightforward: depending on the state of the lending pool and on the parameters α and β, firing a given action before the interest accrual may be beneficial or detrimental for A. Indeed, we have that:

(i) deposits increase A's credit (which is going to appreciate after the interest accrual), but decrease the utilization (implying that the credit previously held by A is going to appreciate less);
(ii) borrows increase A's debt (which is going to increase after the interest accrual), but increase the utilization (implying that the credit previously held by A is going to appreciate more);
(iii) repayments, symmetrically to borrows, decrease A's debt, and decrease the utilization;
(iv) redeems, symmetrically to deposits, decrease A's credit but increase the utilization;
(v) liquidations behave similarly to deposits, with the only difference that the credits received are of a different token type than that of the deposited tokens, and of higher value; but this is not always enough to compensate for the lower credit appreciation.

Note that swaps do not interact with the lending pool whatsoever, hence firing them before or after an interest accrual is not going to have any impact in any case. In Section 6.2, we will show how an adversary can manipulate the utilization in order to increase her gain.

In the special case in which $\alpha = 0$, i.e. interest rates are constant and do not depend on the utilization, we can conclude that certain actions are surely going to benefit A (or, at most, have no impact), and other actions are surely going to penalize A (or, at most, have no impact). More specifically, deposits and repayments are beneficial, while borrows and redeems are detrimental. For liquidations, even in this case, there is no monotonicity.

Theorem 5.4 (Strategy for impending interest accruals)**.** *Assume that the lending protocol uses the linear utility interest rate function* $I_\Lambda(\mathsf{T}) = \alpha \cdot U_\Lambda(\mathsf{T}) + \beta$ *in* (2.15)*. Let* $\mathsf{X} = \mathsf{A}\colon \ell(\cdots)$ *mentioning token* T *with transaction parameter* v*.*

(1) *If the parameters* α *and* β *are arbitrary, then for every* $\ell \in \{\mathsf{dep}, \mathsf{bor}, \mathsf{rep}, \mathsf{rdm}, \mathsf{liq}\}$ *and for every* $\circ \in \{>, =, <\}$*, there exists* Γ *and* v *such that* $g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{int}) \circ g_{\mathsf{A}}(\Gamma, \mathsf{int})$*.*

(2) *If* $\alpha = 0$*, then:*
   (a) *if* $\ell \in \{\mathsf{dep}, \mathsf{rep}\}$*, then for all* Γ *and* v*,* $g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{int}) \geq g_{\mathsf{A}}(\Gamma, \mathsf{int})$
   (b) *if* $\ell \in \{\mathsf{bor}, \mathsf{rdm}\}$*, then for all* Γ *and* v*,* $g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{int}) \leq g_{\mathsf{A}}(\Gamma, \mathsf{int})$
   (c) *if* $\ell = \mathsf{liq}$*, then for all* $\circ \in \{\geq, \leq\}$*, there exist* Γ, v *such that* $g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{int}) \circ g_{\mathsf{A}}(\Gamma, \mathsf{int})$

Note that liq does not enjoy any monotonicity, not even in the case where $\alpha = 0$. Indeed, in certain situations it is beneficial to perform a liquidation before interests accrue, while in others, it is better to wait until after the interest accrual. This is due to the fact that higher overall amounts of debts imply higher exchange rates increases after int. In particular, given that credit tokens appreciate after an increase in exchange rates, a user who holds a high amount of credit tokens would benefit more from waiting interest rates to increase.

Example 5.5 (Liquidations and interest accruals)**.** Recall the sequence of transactions in Fig. 1 up to step 6 included. Assume that A anticipates that an int is going to happen, and she has to decide whether to liquidate B before the interests accrual or not. The convenience of liquidating B or not depends on the specific interest rate function. Consider e.g., the utility-based interest rate function in (2.15) in the simple case where $\alpha = 0$, that is, there is a constant interest rate β for each token type. If the interest increase is relatively low (e.g., $\beta = 10\%$), then the credit tokens held by A do not appreciate significantly, and so the liquidation reward is sufficiently high to incentivize A to liquidate B. However, if interest rates increase significantly (e.g. $\beta = 100\%$) or the liquidation bonus is very small, then the appreciation of the credit tokens held by A can be so impactful that the best strategy for A would be wait to liquidate B, so that the overall amount of debts will make the appreciation of the credit tokens higher enough to surpass the benefit given by the liquidation bonus. ⋄

6. Attacks

In this section we illustrate some attacks to lending protocols, which only require the adversary to own sufficient liquidity of certain tokens.

We start by considering *price manipulation attacks*, where an adversary uses their capital to trigger a temporary price fluctuation of a token handled by the lending pool (Section 6.1). More specifically, Theorem 6.1 shows an attack where the adversary's goal is to borrow more tokens than what they should be allowed to. Theorem 6.2 shows another attack where the adversary exploits a price manipulation to make a borrower under-collateralized and then liquidate her credit tokens.

Then, we consider *utilization attacks*, where an adversary manipulates the utilization of certain tokens to benefit from a change in the interest accrual (Section 6.2). More specifically, Theorem 6.3 shows an *under-utilization* attack in which an adversary deposits some tokens to decrease the utilization in order to pay less interests on her debts (penalizing creditors). Theorem 6.4 shows an *over-utilization attack* in which an adversary borrows some token to increase the utilization in order to gain more from the interest accrual (penalizing debtors).

Although these kinds of attacks are already known in literature [GPH+20, QZLG21, BCL21, MNW22, ZXE+23, ALFX24], our results are the first to formally establish general conditions under which they can occur.

In our results, we will make some simplifying assumptions on the credits or debts of the addresses involved in the attack, e.g. that the adversary has all the credits of a given token type, or none. This allows us to prove that the attacks always succeed, regardless of the actual token amounts invested by the adversary in the attack. In practice, even when such

conditions are not precisely met (e.g., the adversary does not possesses exactly *all* the credit tokens, but most of them), the attack will still succeed for suitable choices of the transaction parameters. It is possible to estimate such suitable values by using the formulas to compute the gain provided in Section 4. For the sake of clarity, and to provide a better intuition on the attacks, we will consider the cases in which the hypotheses hold.

6.1. **Price manipulation attacks.** In the decentralized setting, price oracles are usually implemented as smart contracts that determine the price of a token depending on an underlying market on that token. A typical implementation is given by constant-function Automated Market Makers (AMMs) [AC20], which realize a market on two or more token types, allowing users to swap tokens at an algorithmically-determined exchange rate that depends solely on the offer and supply of the supported tokens. For example, in the simple case of a constant-product AMM on two tokens T_0, T_1, swaps preserve the product of the reserves of the two tokens in the AMM. Accordingly, the price of T_0 w.r.t. T_1 is defined as the ratio between the reserves of T_1 and those of T_0 in the AMM. When a user swaps units of T_0, since the product of the reserves must remain constant, then after the swap the reserves of T_1 decrease, and so the price of T_0 will decrease as well. This design, in principle, makes AMMs suitable as price oracles, as users have an economic incentive to perform tokens swap in order to align the AMM token prices to external prices [BCL22].

In practice, relying on instantaneous AMM prices in a lending protocol can be insecure [WPG+22]. Indeed, an adversary with sufficient capital in a given token can induce significant price fluctuations of that token. This manipulated price can then be exploited in interactions with a lending protocol — as we will demonstrate below — before the adversary reverses the manipulation to restore the original price on the AMM. Formally, we model such a price manipulation attack as a sequence of transactions where the adversary fires a transaction $\mathsf{px}(\delta\colon \mathsf{T})$ to manipulate the price, then perform a sequence of interactions with the LP, and finally restores the original price by firing $\mathsf{px}(-\delta\colon \mathsf{T})$. We remark that the proposer-builder separation scheme currently adopted by Ethereum [HKTW23] makes is possible for an adversary to perform such transaction bundles atomically.

The following theorem shows an attack in which an adversary A manipulates price updates in order to borrow more tokens than what she should be allowed to. Specifically, after the attack, although A's gain remain constant, her net position becomes negative. This allows A to extract value from the LP by effectively defaulting on debt that is no longer backed by a sufficient collateral. Since the lending protocol cannot enforce repayments, the uncovered debt results in a loss for the pool.

Theorem 6.1 (Undercollateralized loan attack)**.** *Let* $\Gamma = (\omega, \Lambda, \pi)$*, and assume that* A *has no credits or debts with the LP, i.e.,* $W^c_\Gamma(\mathsf{A}) = W^d_\Gamma(\mathsf{A}) = 0$*. Consider the following sequence of transactions:*

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}\colon \mathsf{dep}(v_1\colon \mathsf{T}_1)\;\; \mathsf{px}(-\delta\colon \mathsf{T}_2)\;\; \mathsf{A}\colon \mathsf{bor}(v_2\colon \mathsf{T}_2)\;\; \mathsf{px}(\delta\colon \mathsf{T}_2)$$

where $0 < \delta < \pi(\mathsf{T}_2)$ *and* $v_2 = \frac{v_1}{XR_\Lambda(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_1)}{\pi(\mathsf{T}_2)-\delta} \cdot T_{\mathsf{liq}}$*. Let* $\Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma'$*. Then:*

(1) $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) = 0$
(2) $W^{c-d}_{\Gamma'}(\mathsf{A}) < 0$ *if and only if* $\delta > \pi(\mathsf{T}_2) \cdot (1 - T_{\mathsf{liq}})$

The theorem gives a lower bound for the price increase δ under which the attack does not have effect (i.e. the net position does not go negative). Note that, since δ can take values

in $(0, \pi(\mathsf{T}_2))$ and $0 < T_{\mathsf{liq}} < 1$, then there always exists a value for δ large enough to make the attack succeed.

The following theorem shows another attack, where the attacker A manipulates prices in order to make another user B under-collateralized and so make a gain from B's liquidation. In this attack, we assume that the collateral of B relies on a single token type T_1 (hypothesis 1), that B has debts only in T_2 (hypothesis 2), that the adversary has some tokens T_2 (hypothesis 3) and that B is not liquidatable in the current state (hypothesis 4).

Theorem 6.2 (Liquidation attack)**.** *Let $\Gamma = (\omega, \Lambda, \pi)$, and let A and B be such that:*
(1) $\Lambda(\mathsf{T}_1^c, \mathsf{B}) = v_c$ *and* $\Lambda(\mathsf{T}^c, \mathsf{B}) = 0$ *for all* $\mathsf{T} \neq \mathsf{T}_1$
(2) $\Lambda(\mathsf{T}_2^d, \mathsf{B}) = v_d$ *and* $\Lambda(\mathsf{T}^d, \mathsf{B}) = 0$ *for all* $\mathsf{T} \neq \mathsf{T}_2$
(3) $\omega(\mathsf{T}_2, \mathsf{A}) > 0$
(4) $H_\Gamma(\mathsf{B}) \geq 1$
Then, for every $\delta > 0$ sufficiently small, and for every $v_l > 0$ such that $v_l \leq \omega(\mathsf{T}_2, \mathsf{A})$, $v_l \leq v_d$ and $v_l < v_c \cdot \frac{XR_\Lambda(\mathsf{T}_1)}{R_{\mathsf{liq}}} \cdot \frac{\delta}{\pi(\mathsf{T}_2)}$, given the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{px}((-\pi(\mathsf{T}_1) + \delta){:}\,\mathsf{T}_1)\;\; \mathsf{A}{:}\,\mathsf{liq}(\mathsf{B}, v_l{:}\,\mathsf{T}_2, \mathsf{T}_1^c)\;\; \mathsf{px}((\pi(\mathsf{T}_1) - \delta){:}\,\mathsf{T}_1)$$

we have that $\boldsymbol{\mathcal{X}}$ is enabled in Γ, and $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) > 0$.

6.2. **Utilization attacks.** Utilization, defined previously in (2.14), gives an estimate of how much the reserves of a token are valuable, and are hence often used to determine interest rates: the higher the utilization, the higher the interest rate. This, however, exposes lending protocols to attacks where the adversary manipulates the utilization function in order to increase or decrease the interest rates to their advantage [BCL21].

We formalise in Theorem 6.3 an *under-utilization* attack, where an adversary deposits some tokens before an interest accrual in order to decrease the utilization of the token and pay less interests on her debts, and then immediately redeem her credits. Dually, Theorem 6.4 establishes conditions for an *over-utilization* attack, where an adversary borrows some tokens before the interest accrual in order to increase the utilization of the token and hence increase the appreciation of her credit tokens, and then immediately repays her debt. In both attacks, the adversary is not fairly participating in the dynamic of the lending protocol, but rather manipulating its intended behavior to increase her net worth.

The following theorem shows an under-utilization attack in which an adversary A manipulates the utilization of a token T. We assume that A has no credits (but possibly debts) in T. We also consider a user B who has credits (but no debts) in T. The attack consists in A firing a deposit immediately before an interest accrual, thus decreasing the utilization of T, and then redeeming her credits. This strategy benefits A in two ways: first, if A has debts, then a lower utilization implies a lower interest rate, hence reducing the increase of A's debt; secondly, given that A has now acquired credits in T, these credits appreciate and can be redeemed for a higher value. User B, on the contrary, gets penalized by A's attack, since a lower utilization implies a lower appreciation of her credits.

Theorem 6.3 (Under-utilization attack)**.** *Assume that the LP uses the linear utility interest rate function in* (2.15) *with $\alpha > 0$. Let $\Gamma = (\omega, \Lambda, \pi)$, and let A, B and T be such that:*
(1) $\Lambda(\mathsf{T}^c, \mathsf{A}) = 0$
(2) $\Lambda(\mathsf{T}^c, \mathsf{B}) > 0$ *and* $\Lambda(\mathsf{T}^d, \mathsf{B}) = 0$

Assume that the following sequence of transactions:

$$\mathscr{X} \;=\; \mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T}) \;\; \mathsf{int} \;\; \mathsf{A}\colon \mathsf{rdm}(v^c\colon \mathsf{T})$$

is enabled in Γ*, where* v^c *is the amount of credits held by* A *in the intermediate state before* rdm*. Then, we have that:*

$$g_{\mathsf{A}}(\Gamma, \mathscr{X}) > g_{\mathsf{A}}(\Gamma, \mathsf{int}) \qquad\qquad g_{\mathsf{B}}(\Gamma, \mathscr{X}) < g_{\mathsf{B}}(\Gamma, \mathsf{int})$$

If we drop the assumption that A does not possess any credit, then the attack does not necessarily succeed for *every* state of the lending pool for *every* value v, since the deposit decreases the appreciation of the credits already possessed by A. In such a case, there is a trade off between the lower appreciation of A's credits, on one side, and the reduction in the increment of A's debt, and the gains coming from the credit appreciation of the newly deposited tokens, on the other side. In general, the attack succeeds when A has plenty of debts in T but few credits. Precise relations between these values are established in the proof of Theorem 5.4.

The following theorem shows an over-utilization attack performed by an adversary A, which possesses *all* the credits in T (but not all the debts in T). We also consider another user B, which possesses debts in T (but not credit). Here, the adversary A borrows some tokens immediately before the interest accrual, thus increasing the utilization of the token T, and then immediately repays the loan. This strategy benefits A as a higher utilization implies a higher interest rate, and, since A is the only credits possessor, then *all* the overall debt increase in T correspond to an appreciation of A credits. Even though also the debts of A increase, since A is the only creditor, then this loss is matched by the gain coming from the appreciation of her credits. User B, on the contrary, gets penalized by the attack, since now her debts have increase more than they would have in the absence of the attack.

Theorem 6.4 (Over-utilization attack)**.** *Assume that the LP uses the linear utility interest rate function in* (2.15) *with* $\alpha > 0$*. Let* $\Gamma = (\omega, \Lambda, \pi)$*, and let* A, B *and* T *be such that:*

(1) $\Lambda(\mathsf{T}^c, \mathsf{A}) = S_\Lambda(\mathsf{T}^c)$ *and* $\Lambda(\mathsf{T}^d, \mathsf{A}) < S_\Lambda(\mathsf{T}^d)$
(2) $\Lambda(\mathsf{T}^d, \mathsf{B}) > 0$

Assume that the following sequence of transactions:

$$\mathscr{X} \;=\; \mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T}) \;\; \mathsf{int} \;\; \mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$$

is enabled in Γ*. Then, we have that:*

$$g_{\mathsf{A}}(\Gamma, \mathscr{X}) > g_{\mathsf{A}}(\Gamma, \mathsf{int}) \qquad\qquad g_{\mathsf{B}}(\Gamma, \mathscr{X}) < g_{\mathsf{B}}(\Gamma, \mathsf{int})$$

Similarly to the previous theorem, if we drop the assumption that A possesses *all* the credits in T, then the attack is not guaranteed to succeed for *every* state of the lending pool for *every* value v. Indeed, there is now a trade off between the increase in A's debt, and the increase in the appreciation of A's credits. In general, the attack succeeds when A has plenty of credits but few debts in T.

7. Limitations

For simplicity, our model of lending protocols abstracts away from certain functionalities and fine-grained details of real-world lending platforms. While these simplifications limit the direct applicability of our theory to existing systems, we believe that our results describe

ideal properties that lending protocols should satisfy – such as preservation of global net worth, incentives for liquidity providers and liquidators, etc.

We discuss here some of the key abstractions made in our model, using the Aave protocol implementation [aav20c] for reference.

- *Governance.* In early implementations of Aave and Compond, administrators had the authority to set key economic parameters of the protocol, such as the interest rate function, liquidation threshold, and and liquidation reward. To mitigate the risk of administrators engaging in improper behavior, more recent versions of these platforms use *governance tokens*, distributed among liquidity providers, to collectively govern and update protocol parameters. In our model, we assume for simplicity that protocol parameters are fixed.
- *Deposits and collaterals.* Our [Dep] rule allows any user to add a new token type to the LP by just performing the first deposit of tokens of that type. In contrast, adding a new token type to an Aave LP must be authorized by the governance mechanisms. Additionally, our [Dep] rule, together with the definition of user collateralization (2.11), ensures that every deposit is automatically enabled as collateral. In contrast, Aave allows users to selectively disable specific deposited token types from being used as collateral.
- *Liquidations.* Our [Liq] rule allows liquidators to receive credit tokens in exchange for the repaid debt; if liquidators want to convert the credit tokens in the underlying base tokens, they must send a redeem transaction after the liquidation. In Aave, liquidators can also choose to receive the underlying base tokens directly. Furthermore, [Liq] allows liquidators to repay any fraction of the debt, with the only constraint that the borrower's health factor after the liquidation does not exceed 1. In Aave, instead, liquidations can repay up-to a 50% fraction of the debt [aav20a]. Since this constraint can be easily bypassed by splitting a liquidation into multiple actions, we have omitted it. Another difference is that in our model the protocol parameters T_{liq} (liquidation threshold) and R_{liq} (liquidation reward) are uniform across all token types. In contrast, Aave allows these parameters to vary by token, enabling the protocol to fine-tune incentives in selected tokens.
- *Interest accrual.* Our [Int] rule models the accrual of interest on loans as an update triggered by a privileged entity. This abstraction reflects the fact that the `int` action is not associated with any address, unlike other actions such as deposit or redeem. In lending protocol implementations, interest accruals are not executed on demand by privileged entities; instead, they occur automatically whenever a user performs an action that requires up-to-date debt amounts. To reduce execution costs, a single interest rate is applied over the entire period since the last accrual, which can introduce minor inaccuracies.
- *Price updates.* Our [Px] rule models the update of a token price performed by a price oracle. In contrast, Aave associates each token type with its own price oracle. This oracle is usually a smart contract that aggregates multiple independent sources, in order to mitigate the risk of price manipulation [GADH25].
- *Flash loans.* Lending platforms typically expose a flash loan functionality, which allows users to borrow arbitrary amounts of tokens without a collateral, provided that the borrowed funds are repaid within the same transaction. This transaction can bundle multiple actions performed by the same user: its atomicity guarantees that all operations — i.e. borrowing, using the borrowed tokens, and repaying the loan — must either complete successfully or be entirely reverted [aav20b]. Our model does not include flash loans, as they are usually meant to be used in combination with other protocols. Note that the possibility of obtaining large amounts of funds without providing a collateral is implicitly

assumed in the attacks in Section 6, where the adversary needs sufficient capital to obtain the desired manipulation of token prices or utilization.
- *Fees.* Aave requires users to pay fees for certain actions, such as borrowing and executing flash loans. These fees are accumulated in a reserve managed by the protocol's governance mechanisms and are intended to serve as a protection against unforeseen events.
- *Token amounts.* In our model, we let token amounts range over the continuous domain of non-negative real numbers. In contrast, real-world lending protocol implementations operate over a discrete domain, representing token amounts as fixed-size integers. As a result, all operations involving token amounts require rounding, which can introduce small inaccuracies and edge cases (and, possibly, attack vectors) abstracted away by our model.

8. Related work

Even though lending protocols have been extensively studied in recent years, only a few works base their analysis on formal, operational models that capture the interactions in lending protocols at the granularity of individual transactions. The work most closely related to ours is [BCL21], whose LP model served as a key inspiration for our model. Although both models encompass the same types of transactions (except swaps, which are not present in [BCL21]), the representation of LP and blockchain states are quite different. While, similarly to process algebras, [BCL21] renders states as parallel compositions of simple terms (e.g., an individual user wallet, a lending pool handling a single token type), in our model we gather all the components of the LP state (reserves, credit and debit maps) into a single function. Besides that, credits and debits are represented asymmetrically in [BCL21]: namely, credits are associated to users' wallets, while debits to LP states. These differences are not merely aesthetic, however, as they deeply impact the way states predicates are represented, and how states are updates. Overall, our design choices lead to a substantially clearer LP semantics and to more succinct proofs than [BCL21]. Another key difference lies in the comprehensiveness of the theoretical analysis. Compared to our work, the results in [BCL21] constitute a narrower subset: they include only simplified versions of exchange rate monotonicity (Lemma 3.4), net worth preservation (Theorem 3.6), and gain from user actions (Lemma 4.1). Our theoretical framework provides refined versions of these results, along with a thorough analysis of the effects of each individual actions and more complex strategies, supported by rigorous proofs for all statements.

Several works have focused on specific features of lending protocols, such as interest rate functions, price stabilization mechanisms, liquidation strategies, and flash loans.

Interest rate functions. The impact of interest rate functions on market liquidity and efficiency in lending protocols has been studied by [GWPK20], which provides an empirical analysis of the interest rate models employed by various protocols. The two main platforms Aave and Compound rely on static interest rate curves, which often struggle to adapt to rapid market changes such as major price fluctuations. Dynamic interest rates aiming at stabilizing utilization have been studied in various works [CSBS23, BNJ+24, BNWV24, NKV24, BCT25]. However, it has been observed that, although dynamic interest rates provide better utilization levels, they also increase the exposure to manipulation attacks [CEK23, BNWV24].

Prices. While, in our model, prices are simply modelled as a function from token types to non-negative real numbers, the literature has explored sophisticated price models and mechanism to mitigate price volatility. A taxonomy of various price stabilization mechanisms has been proposed in [MSS20]. The behaviour of lending protocols in times of high price volatility has been discussed in [GPH+20]. This work also uncovers a vulnerability in the governance design of MakerDAO that allowed attackers to utilize flash loans to steal funds from the contract. The performance of MakerDAO's oracles has been studied empirically in [GRB20], which also proposes alternate price feed aggregation models to improve oracle accuracy. The profitability competition for user deposits between staking in proof-of-stake systems and lending protocols has been studied in [Chi19, CE20]: when lending is believed to be more profitable than staking, users may shift deposits away from the staking contract of the underlying consensus protocol towards lending pools, thereby endangering the security of the system. The work [BEK24] studies the interaction between AMMs and LPs, analysing the impact of transaction costs, arbitrage opportunities, hedging of impermanent losses, and risk management. Price manipulation attacks, such as those presented in Section 6.1, have been formally characterized in [BMZ24] as instances of *MEV interference* between a contract (the lending pool) and its dependencies (the AMM serving as a price oracle). This interference allows the adversary interacting with the AMM to extract more value from the LP than would be possible by interacting with the LP alone.

Liquidations. A liquidation model intended to simulate interactions between lending pool liquidations and token exchange markets in times of high price volatility has been studied in [GPH+20]. The optimal bidding strategy for collateral liquidators in MakerDAO auctions has been studied in [DPT20]. The work [GPH+20] analyzed what happens when large price drops make many accounts under-collateralized. A key observation of this work is that if liquidators sell off collateral at an external market for units of the repaid token type, the limited market demand for collateral tokens may prevent liquidations from being executed. In the Compound protocol, liquidation efficiency has been studied through historical data [PWXL21], while the evolution of liquidatable and undercollateralized debt has been studied in [KCCM20] and the risk of financial contagion triggering a cascade of defaults in [TKWP23]. The impact of different liquidation strategies and protocol designs on the net position of borrowers has been studied in [BCJ+22]. Strategies to liquidate under-collateralized borrowers, such as those studied in Section 5, have been formally characterized as instances of Maximal Extractable Value (MEV) in [BZ25]. In particular, liquidations that do not exploit the knowledge of the mempool are classified by [BZ25] as a benign form of MEV. This classification aligns with the broader community consensus [Bar23, JG24, TMW+24], which views such liquidations as a necessary incentive mechanism to keep lending protocols aligned with their intended functionality.

Flash loans. An analysis of flash loans transactions in the main lending platforms has been conducted in [WWL+20]. Flash loans have been exploited in several attacks, as they enable attackers to have access to large amount of funds that can be used to initiate attacks [val20,har20,ori20,akr20]. Attacks such as pump and arbitrage and price manipulation have been studied in [QZLG21]. A framework for the automated synthesis of attacks that exploit flash loans has been proposed in [CBL24].

9. Conclusions

We have presented a formal model and analysis of decentralized lending protocols, based on common features synthesised from mainstream lending platforms such as Aave and Compound [aav25b, com25b]. Our theoretical investigation of lending protocols has provided answers to the following research questions:

(1) What structural properties and invariants are enjoyed by lending pools?
(2) What is the economic effect of each individual interaction with a lending pool?
(3) Which strategies can be followed by rational users anticipating a forthcoming action?
(4) Which attacks are possible for adversaries with a large amount of capital?

Overall, our formal model proved to be sufficiently granular to precisely reproduce and analyse known attacks from the literature, and at the same time streamlined enough to allow for succinct proofs. To the best of our knowledge, we are the first to have systematically studied the incentive mechanism of lending protocols at that level of granularity, providing a comprehensive analysis of user strategies. Most notably, we focused on strategies for front-running of impending transactions. In our analysis, we have observed that the dynamics of interest accruals are among the most complex aspects of the lending protocols, giving rise to different manipulation attacks and non-trivial user strategies.

Future work. Our analysis shows that lending protocols — despite the relative simplicity of the rules governing the semantics of individual actions — exhibit complex emergent behaviour. While the strategic properties and the attacks formalised in Sections 5 and 6 capture relevant aspects of these behaviour, it remains an open question whether more sophisticated strategies or attacks may exist. The search of strategies for reaching certain economic goals could be facilitated by specialised automatic tools. A relatively light-weight approach towards this goal is statistical model checking, a simulation-based technique that allows to observe the quantitative behavior of complex systems, based on statistical techniques to measure the confidence in the result produced. Some initial results regarding the application of this approach to lending protocols are in [BCJ+22], which studies how different liquidation strategies and choices of the protocol parameters T_{liq} and R_{liq} impact the net position of borrowers. A drawback of this approach — aside not guaranteeing 100% accuracy in the results — is that players' (probabilistic) strategies must be given as input to the simulator. Therefore, this technique does not seem suitable for automatically discovering, or ruling out the existence of, strategies that achieve given economic goals.

Another approach to inferring strategies and attacks in lending protocols is SMT-based bounded model checking. This technique involves encoding the semantics of lending protocols as a set of logical constraints and then querying whether there exists a sequence of transactions — up to a given length — that satisfies a specified property over blockchain states. While existing tools that apply SMT-based model checking to smart contracts written in real-world languages such as Solidity or Move are generally unable to verify — or even express — strategic properties [BCL25], a specialized tool built upon our abstract model could potentially offer greater expressiveness and effectiveness.

Acknowledgements. Work partially supported by project SERICS (PE00000014) under the MUR National Recovery and Resilience Plan funded by the European Union – NextGenerationEU, and by PRIN 2022 PNRR project DeLiCE (F53D23009130001).

References

[aav20a] Aave maximum liquidation amount, 2020. https://github.com/aave/aave-protocol/blob/efaeed363da70c64b5272bd4b8f468063ca5c361/contracts/lendingpool/LendingPoolLiquidationManager.sol#L181.

[aav20b] Aave v1 flashloan receiver interface, 2020. https://github.com/aave/aave-protocol/blob/efaeed363da70c64b5272bd4b8f468063ca5c361/contracts/flashloan/interfaces/IFlashLoanReceiver.sol#L11.

[aav20c] Aave v1 implementation, 2020. https://github.com/aave/aave-protocol/.

[aav25a] Aave markets website, 2025. https://app.aave.com/markets.

[aav25b] Aave website, 2025. https://www.aave.com.

[AC20] Guillermo Angeris and Tarun Chitra. Improved price oracles: Constant function market makers. In *ACM Conference on Advances in Financial Technologies (AFT)*, pages 80–91. ACM, 2020. https://arxiv.org/abs/2003.10001.

[akr20] Akropolis Defi attack, 2020. https://cryptonews.com/news/defi-akropolis-drops-20-following-a-usd-2m-heavy-hack-8299.htm.

[ALFX24] Sanidhay Arora, Yingjiu Li, Yebo Feng, and Jiahua Xu. SecPLF: Secure protocols for loanable funds against oracle manipulation attacks. In *ACM Asia Conference on Computer and Communications Security (ASIA CCS)*. ACM, 2024.

[Bar23] Mikolaj Barczentewicz. MEV on Ethereum: A policy analysis. ICLE White Paper, 2023.

[BCJ+22] Massimo Bartoletti, James Hsin-yu Chiang, Tommi A. Junttila, Alberto Lluch-Lafuente, Massimiliano Mirelli, and Andrea Vandin. Formal analysis of Lending Pools in Decentralized Finance. In *ISoLA*, volume 13703 of *LNCS*, pages 335–355. Springer, 2022.

[BCL21] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. SoK: Lending Pools in Decentralized Finance. In *Workshop on Trusted Smart Contracts*, volume 12676 of *LNCS*, pages 553–578. Springer, 2021.

[BCL22] Massimo Bartoletti, James Hsin-yu Chiang, and Alberto Lluch-Lafuente. A theory of Automated Market Makers in DeFi. *Logical Methods in Computer Science*, 18(4), 2022.

[BCL25] Massimo Bartoletti, Silvia Crafa, and Enrico Lipparini. Formal verification in Solidity and Move: Insights from a comparative analysis. In *Workshop on Formal Methods for Blockchains (FMBC)*, volume 129 of *OASIcs*, pages 3:1–3:18. Schloss Dagstuhl - Leibniz-Zentrum für Informatik, 2025.

[BCT25] Bastien Baude, Damien Challet, and Ioane Muni Toke. Optimal risk-aware interest rates for decentralized lending protocols. Working Papers hal-04971758, HAL, February 2025.

[BEK24] Werner Brönnimann, Pascal Egloff, and Thomas Krabichler. Automated market makers and their implications for liquidity providers. *Digital Finance*, 6(3):573–604, Sep 2024.

[BMZ24] Massimo Bartoletti, Riccardo Marchesin, and Roberto Zunino. DeFi composability as MEV non-interference. In *Financial Cryptography and Data Security*, volume 14745 of *LNCS*, pages 369–387. Springer, 2024.

[BNJ+24] Mahsa Bastankhah, Viraj Nadkarni, Chi Jin, Sanjeev Kulkarni, and Pramod Viswanath. Thinking Fast and Slow: Data-Driven Adaptive DeFi Borrow-Lending Protocol. In Rainer Böhme and Lucianna Kiffer, editors, *6th Conference on Advances in Financial Technologies (AFT 2024)*, volume 316 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 27:1–27:23, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[BNWV24] Mahsa Bastankhah, Viraj Nadkarni, Xuechao Wang, and Pramod Viswanath. Agilerate: Bringing adaptivity and robustness to defi lending markets. *CoRR*, abs/2410.13105, 2024.

[BZ25] Massimo Bartoletti and Roberto Zunino. A theoretical basis for MEV. In *Financial Cryptography and Data Security*, LNCS. Springer, 2025. To appear.

[CBL24] Zhiyang Chen, Sidi Mohamed Beillahi, and Fan Long. Flashsyn: Flash loan attack synthesis via counter example driven approximation. In *Proceedings of the IEEE/ACM 46th International Conference on Software Engineering*, ICSE '24, New York, NY, USA, 2024. Association for Computing Machinery.

[CE20] Tarun Chitra and Alex Evans. Why stake when you can borrow? *Available at SSRN 3629988*, 2020. https://arxiv.org/abs/2006.11156.

[CEK23] Tarun Chitra, Peteris Erins, and Kshitij Kulkarni. Attacks on dynamic defi interest rate curves, 2023.

[Chi19] Tarun Chitra. Competitive equilibria between staking and on-chain lending. *arXiv preprint arXiv:2001.00919*, 2019. https://arxiv.org/abs/2001.00919.

[com25a] Compound markets website, 2025. https://app.compound.finance/markets.

[com25b] Compound website, 2025. https://compound.finance/.

[CSBS23] Samuel Cohen, Leandro Sánchez-Betancourt, and Lukasz Szpruch. The economics of interest rate models in decentralised lending protocols. *SSRN Electronic Journal*, 01 2023.

[DPT20] Michael Darlin, Nikolaos Papadis, and Leandros Tassiulas. Optimal Bidding Strategy for Maker Auctions. *arXiv preprint arXiv:2009.07086*, 2020. https://arxiv.org/abs/2009.07086.

[GADH25] Robin Gansäuer, Hichem Ben Aoun, Jan Droll, and Hannes Hartenstein. Price oracle accuracy across blockchains: A measurement and analysis. In *International Workshop on Cryptoasset Analytics (CAAW)*, 2025.

[GPH+20] Lewis Gudgeon, Daniel Pérez, Dominik Harz, Benjamin Livshits, and Arthur Gervais. The decentralized financial crisis. In *Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 1–15. IEEE, 2020.

[GRB20] Wanyun Catherine Gu, Anika Raghuvanshi, and Dan Boneh. Empirical measurements on pricing oracles and decentralized governance for stablecoins. *Available at SSRN 3611231*, 2020. http://dx.doi.org/10.2139/ssrn.3611231.

[GWPK20] Lewis Gudgeon, Sam Werner, Daniel Perez, and William J Knottenbelt. DeFi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *ACM Conference on Advances in Financial Technologies*, pages 92–112, 2020.

[har20] Harvest Finance flashloan attack post-mortem, 2020. https://medium.com/harvest-finance/harvest-flashloan-economic-attack-post-mortem-3cf900d65217.

[HKTW23] Lioba Heimbach, Lucianna Kiffer, Christof Ferreira Torres, and Roger Wattenhofer. Ethereum's proposer-builder separation: Promises and realities. In *Proc. ACM on Internet Measurement Conference (IMC)*, pages 406–420. ACM, 2023.

[JG24] Yan Ji and James Grimmelmann. Regulatory implications of MEV mitigations. In *Financial Cryptography Workshops*, volume 14746 of *LNCS*, pages 335–363. Springer, 2024.

[KCCM20] Hsien-Tang Kao, Tarun Chitra, Rei Chiang, and John Morrow. An Analysis of the Market Risk to Participants in the Compound Protocol. 2020. https://scfab.github.io/2020/FAB2020_p5.pdf.

[MNW22] Torgin Mackinga, Tejaswi Nadahalli, and Roger Wattenhofer. TWAP oracle attacks: Easier done than said? In *IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pages 1–8. IEEE, 2022.

[MSS20] Amani Moin, Kevin Sekniqi, and Emin Gün Sirer. Sok: A classification framework for stablecoin designs. In *Financial Cryptography and Data Security*, volume 12059 of *LNCS*, pages 174–197. Springer, 2020.

[NKV24] Viraj Nadkarni, Sanjeev Kulkarni, and Pramod Viswanath. Adaptive Curves for Optimally Efficient Market Making. In Rainer Böhme and Lucianna Kiffer, editors, *6th Conference on Advances in Financial Technologies (AFT 2024)*, volume 316 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 25:1–25:22, Dagstuhl, Germany, 2024. Schloss Dagstuhl – Leibniz-Zentrum für Informatik.

[ori20] Origin Dollar attack, 2020. https://cryptonews.com/news/4th-major-defi-hack-in-a-month-origin-dollar-loses-usd-7m-8331.htm.

[PWXL21] Daniel Perez, Sam M. Werner, Jiahua Xu, and Benjamin Livshits. Liquidations: DeFi on a knife-edge. In *Financial Cryptography*, volume 12675 of *LNCS*, pages 457–476. Springer, 2021.

[QEZ+24] Kaihua Qin, Jens Ernstberger, Liyi Zhou, Philipp Jovanovic, and Arthur Gervais. Mitigating decentralized finance liquidations with reversible call options. In Foteini Baldimtsi and Christian Cachin, editors, *Financial Cryptography and Data Security*, pages 344–362, Cham, 2024. Springer Nature Switzerland.

[QZLG21] Kaihua Qin, Liyi Zhou, Benjamin Livshits, and Arthur Gervais. Attacking the DeFi ecosystem with flash loans for fun and profit. In *Financial Cryptography*, volume 12674 of *LNCS*, pages 3–32. Springer, 2021.

[SVTZ24] Lukasz Szpruch, Marc Vidales, Tanut Treetanthiploet, and Yufei Zhang. Pricing and hedging of decentralised lending contracts, 09 2024.

[TKWP23] Natkamon Tovanich, Myriam Kassoul, Simon Weidenholzer, and Julien Prat. Contagion in decentralized lending protocols: A case study of compound. In *Proceedings of the 2023 Workshop on Decentralized Finance and Security*, DeFi '23, page 55–63, New York, NY, USA, 2023. Association for Computing Machinery.

[TMW+24] Christof Ferreira Torres, Albin Mamuti, Ben Weintraub, Cristina Nita-Rotaru, and Shweta Shinde. Rolling in the shadows: Analyzing the extraction of MEV across layer-2 rollups. In *ACM SIGSAC Conference on Computer and Communications Security (CCS)*, pages 2591–2605. ACM, 2024.

[val20] Coindesk: Value DeFi attack, 2020. `https://www.coindesk.com/value-defi-suffers-6m-flash-loan-attack`.

[WPG+22] Sam Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J. Knottenbelt. SoK: Decentralized finance (DeFi). In *ACM Conference on Advances in Financial Technologies, (AFT)*, pages 30–46. ACM, 2022.

[WWL+20] Dabao Wang, Siwei Wu, Ziling Lin, Lei Wu, Xingliang Yuan, Yajin Zhou, Haoyu Wang, and Kui Ren. Towards understanding flash loan and its applications in DeFi ecosystem. *arXiv preprint arXiv:2010.12252*, 2020. `https://arxiv.org/abs/2010.12252`.

[ZXE+23] Liyi Zhou, Xihan Xiong, Jens Ernstberger, Stefanos Chaliasos, Zhipeng Wang, Ye Wang, Kaihua Qin, Roger Wattenhofer, Dawn Song, and Arthur Gervais. SoK: Decentralized Finance (DeFi) Attacks. In *IEEE Symposium on Security and Privacy*, pages 2444–2461. IEEE, 2023.

$$\frac{\omega(\mathsf{T},\mathsf{A}) \geq v > 0 \qquad v^c = {}^{v}\!/_{XR_\Lambda(\mathsf{T})} \qquad \Lambda' = \Lambda + \{\mathsf{T} \mapsto v\} + \{(\mathsf{T}^c,\mathsf{A}) \mapsto v^c\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{dep}(v:\mathsf{T})} (\omega - \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Dep]}$$

$$\frac{\Lambda(\mathsf{T}) \geq v > 0 \qquad \Lambda' = \Lambda - \{\mathsf{T} \mapsto v\} + \{(\mathsf{T}^d,\mathsf{A}) \mapsto v\}) \qquad H_{\Lambda',\pi}(\mathsf{A}) \geq 1}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{bor}(v:\mathsf{T})} (\omega + \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Bor]}$$

$$\frac{\omega(\mathsf{T},\mathsf{A}) \geq v > 0 \qquad \Lambda(\mathsf{T}^d,\mathsf{A}) \geq v \qquad \Lambda' = \Lambda + \{\mathsf{T} \mapsto v\} - \{(\mathsf{T}^d,\mathsf{A}) \mapsto v\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{rep}(v:\mathsf{T})} (\omega - \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Rep]}$$

$$\frac{\begin{array}{c}\Lambda(\mathsf{T}^c,\mathsf{A}) \geq v^c > 0 \qquad v = v^c \cdot XR_\Lambda(\mathsf{T}) \qquad \Lambda(\mathsf{T}) \geq v \\ \Lambda' = \Lambda - \{\mathsf{T} \mapsto v\} - \{(\mathsf{T}^c,\mathsf{A}) \mapsto v^c\} \qquad H_{\Lambda',\pi}(\mathsf{A}) \geq 1\end{array}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{rdm}(v^c:\mathsf{T}^c)} (\omega + \{(\mathsf{T},\mathsf{A}) \mapsto v\},\Lambda',\pi)} \text{ [Rdm]}$$

$$\frac{\Lambda' = \Lambda + \sum_{\mathsf{T},\mathsf{A}} \Lambda(\mathsf{T}^d,\mathsf{A}) \cdot I_\Lambda(\mathsf{T})}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{int}} (\omega,\Lambda',\pi)} \text{ [Int]}$$

$$\frac{\begin{array}{c}\omega(\mathsf{T}_0,\mathsf{A}) \geq v_0 > 0 \qquad \Lambda(\mathsf{T}_0^d,\mathsf{B}) \geq v_0 \qquad v_1^c = \frac{v_0}{XR_\Lambda(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)} \cdot R_{\mathsf{liq}} \qquad \Lambda(\mathsf{T}_1^c,\mathsf{B}) \geq v_1^c \\ \Lambda' = \Lambda + \{\mathsf{T}_0 \mapsto v_0\} + \{(\mathsf{T}_1^c,\mathsf{A}) \mapsto v_1^c\} - \{(\mathsf{T}_1^c,\mathsf{B}) \mapsto v_1^c\} - \{(\mathsf{T}_0^d,\mathsf{B}) \mapsto v_0\} \\ \mathsf{A} \neq \mathsf{B} \qquad H_{\Lambda,\pi}(\mathsf{B}) < 1 \qquad H_{\Lambda',\pi}(\mathsf{B}) \leq 1\end{array}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{liq}(\mathsf{B},v_0:\mathsf{T}_0,\mathsf{T}_1^c)} (\omega - \{(\mathsf{T}_0,\mathsf{A}) \mapsto v_0\},\Lambda',\pi)} \text{ [Liq]}$$

$$\frac{\pi(\mathsf{T}) + \delta > 0}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{px}(\delta:\mathsf{T})} (\omega,\Lambda,\pi + \{\mathsf{T} \mapsto \delta\})} \text{ [Px]}$$

$$\frac{\omega(\mathsf{T}_0,\mathsf{A}) \geq v > 0 \qquad \omega' = \omega - \{(\mathsf{T}_0,\mathsf{A}) \mapsto v\} + \{(\mathsf{T}_1,\mathsf{A}) \mapsto v \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)}\}}{(\omega,\Lambda,\pi) \xrightarrow{\mathsf{A}:\mathsf{swp}(v:\mathsf{T}_0,\mathsf{T}_1)} (\omega',\Lambda,\pi)} \text{ [Swp]}$$

FIGURE 2. LP semantics.

APPENDIX A. PROOFS FOR SECTION 3

In this and the following appendices we provide detailed proofs for all your statements. These proofs are presented in the order in which the statements appear in the paper, even though this order does not always reflect their logical dependencies. To clarify the relationship among our statements, Figure 3 displays a graph of the dependencies: an arrow $a \to b$ means that the proof of statement a depends on statement b. Note that this graph is acyclic.

For quick reference, we also summarize the semantics of LPs in Figure 2.

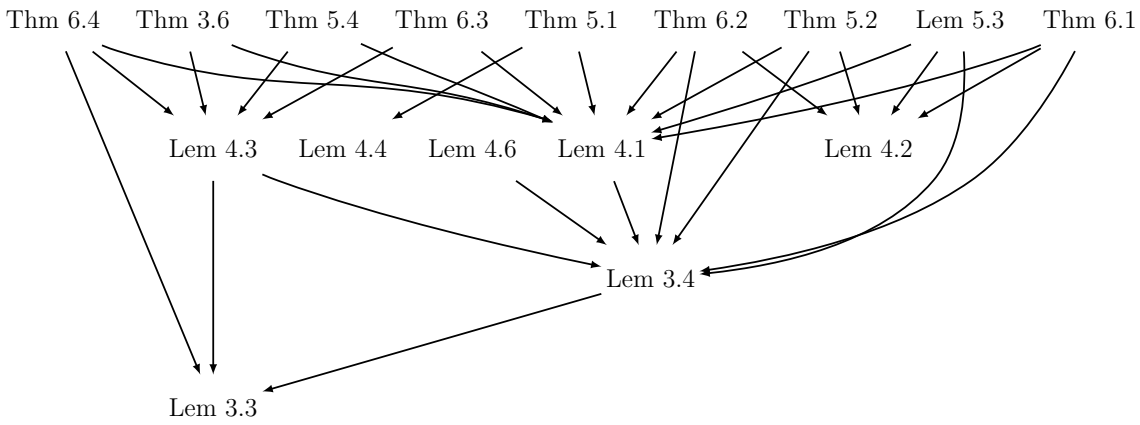

FIGURE 3. Dependencies among the statements.

Proof of Lemma 3.2. By inspection of the rules in Figure 2, it is immediate to observe that all the rules but [SWP] ensure that transition preserve the supply of base token types. □

Proof of Lemma 3.3. Let $\Gamma = (\omega, \Lambda, \pi)$ be a reachable state. We proceed by induction on the length of the trace to reach Γ. The base case holds trivially, since in initial LP states there are no tokens. For the inductive case, assume that $\Gamma \xrightarrow{\mathsf{X}} \Gamma' = (\omega', \Lambda', \pi')$ and that the statement holds in Γ. There are the following cases:

- $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$. We have that $S_{\Lambda'}(\mathsf{T}^c) > 0$, hence the thesis holds trivially.
- $\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$. We have that $\Lambda(\mathsf{T}) > 0$, so by hypothesis it must be $S_\Lambda(\mathsf{T}^c) > 0$. Since the [BOR] rule does not affect credit tokens, then $S_{\Lambda'}(\mathsf{T}^c) > 0$, hence the thesis holds trivially.
- $\mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$. We have that $S_\Lambda(\mathsf{T}^d) > 0$, hence by the induction hypothesis we must have $S_\Lambda(\mathsf{T}^c) > 0$. Since the [REP] rule does not affect credit tokens, then $S_{\Lambda'}(\mathsf{T}^c) > 0$, hence the thesis holds trivially.
- $\mathsf{A}\colon \mathsf{rdm}(v^c\colon \mathsf{T}^c)$. If $S_{\Lambda'}(\mathsf{T}^c) > 0$, then the thesis holds trivially. Otherwise, if $S_{\Lambda'}(\mathsf{T}^c) = 0$, then it must be $v^c = S_\Lambda(\mathsf{T}^c)$. Therefore, we have:

  $$\Lambda'(\mathsf{T}) = \Lambda(\mathsf{T}) - v^c \cdot XR_\Lambda(\mathsf{T}) = \Lambda(\mathsf{T}) - S_\Lambda(\mathsf{T}^c) \cdot XR_\Lambda(\mathsf{T}) \qquad \text{by [RDM] and hyp.}$$

  We have now two cases, depending on whether $S_\Lambda(\mathsf{T}^c) = 0$ or not. If $S_\Lambda(\mathsf{T}^c) = 0$, then by (2.2) we have that $XR_\Lambda(\mathsf{T}) = 1$. Furthermore, by the induction hypothesis we have that $\Lambda(\mathsf{T}) = 0 = S_\Lambda(\mathsf{T}^d)$. Therefore:

  $$\Lambda'(\mathsf{T}) = \Lambda(\mathsf{T}) - S_\Lambda(\mathsf{T}^c) = -S_\Lambda(\mathsf{T}^c) = 0$$
  $$S_{\Lambda'}(\mathsf{T}^d) = S_\Lambda(\mathsf{T}^d) = 0$$

  Otherwise, if $S_\Lambda(\mathsf{T}^c) > 0$, then by (2.2):

  $$\Lambda'(\mathsf{T}) = \Lambda(\mathsf{T}) - S_\Lambda(\mathsf{T}^c) \cdot \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} = -S_\Lambda(\mathsf{T}^d)$$

  Since $\Lambda'(\mathsf{T})$ cannot be negative, it must be $S_\Lambda(\mathsf{T}^d) = 0 = \Lambda'(\mathsf{T})$.
- $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v_0\colon \mathsf{T}_0, \mathsf{T}_1^c)$. We have two cases, depending on whether T is the repaid token T_0 or the base token underlying the credit token ${\mathsf{T}_1}^c$.

  - $\mathsf{T} = \mathsf{T}_0 \neq \mathsf{T}_1$. Assume that $S_{\Lambda'}({\mathsf{T}_0}^c) = 0$. Since the [Liq] transition does not affect the amount of ${\mathsf{T}_0}^c$, then it must be $S_\Lambda({\mathsf{T}_0}^c) = 0$. Then, the thesis follows by the induction hypothesis.
  - $\mathsf{T} = \mathsf{T}_1$. In this case thesis holds trivially, since $S_{\Lambda'}({\mathsf{T}_1}^c) \geq v_1^c > 0$ by the [Liq] rule.
- In all the other cases, the transition does not affect tokens T in the LP, hence the thesis follows directly from the hypothesis. □

Proof of Lemma 3.4. Let $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$, where $\Gamma = (\omega, \Lambda, \pi)$ and $\Gamma' = (\omega', \Lambda', \pi')$. We must prove that, for all T:

(a) if $\mathsf{X} = \mathsf{int}$, and $S_\Lambda(\mathsf{T}^d) > 0$, then

$$XR_{\Lambda'}(\mathsf{T}) \;=\; XR_\Lambda(\mathsf{T}) + \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} \cdot I_\Lambda(\mathsf{T}) \;>\; XR_\Lambda(\mathsf{T})$$

(b) if $\mathsf{X} = \mathsf{rdm}$, and $S_{\Lambda'}(\mathsf{T}^c) = 0$, then $XR_{\Lambda'}(\mathsf{T}) = 1$

(c) otherwise, $XR_{\Lambda'}(\mathsf{T}) = XR_\Lambda(\mathsf{T})$.

We proceed by cases on X. Note that, if $\mathsf{X} \neq \mathsf{int}$ but T does not appear in the transaction, then its exchange rate does not change. Hence, besides the case $\mathsf{X} = \mathsf{int}$, we only have to deal with transactions that mention T. There are the following exhaustive cases:

- $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$. Since the [Dep] rule increases the base tokens T, then $\Lambda'(\mathsf{T}) > 0$, and so by Lemma 3.3 it must be $S_{\Lambda'}(\mathsf{T}^c) > 0$. Then:

$$\begin{aligned}
XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{\Lambda(\mathsf{T}) + v + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c) + v/XR_\Lambda(\mathsf{T})} && \text{by [Dep]}\\
&= \frac{\Lambda(\mathsf{T}) + v + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c) \cdot XR_\Lambda(\mathsf{T}) + v} \cdot XR_\Lambda(\mathsf{T}) && \text{by arith.}\\
&= \frac{\Lambda(\mathsf{T}) + v + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c) \cdot \dfrac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} + v} \cdot XR_\Lambda(\mathsf{T}) && \text{by (2.2)}\\
&= XR_\Lambda(\mathsf{T}) && \text{by arith.}
\end{aligned}$$

- $\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$. Since the [Bor] rule increases the debit tokens T^d, then $S_{\Lambda'}(\mathsf{T}^d) > 0$, and so by Lemma 3.3 it must be $S_{\Lambda'}(\mathsf{T}^c) > 0$. Then:

$$\begin{aligned}
XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{(\Lambda(\mathsf{T}) - v) + (S_\Lambda(\mathsf{T}^d) + v)}{S_\Lambda(\mathsf{T}^c)} && \text{by [Bor]}\\
&= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.}\\
&= XR_\Lambda(\mathsf{T}) && \text{by (2.2)}
\end{aligned}$$

- int. For every A, we have that

$$\Lambda'(\mathsf{T}^d, \mathsf{A}) = \Lambda(\mathsf{T}^d, \mathsf{A}) + \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T}) = \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot (1 + I_\Lambda(\mathsf{T}))$$

The supply of credit tokens changes as follows:

$$\begin{aligned} S_{\Lambda'}(\mathsf{T}^d) &= \sum_{\mathsf{A} \in \mathbb{A}} \Lambda'(\mathsf{T}^d, \mathsf{A}) \\ &= \sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot (1 + I_\Lambda(\mathsf{T}) \\ &= \sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) + \sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T}) \\ &= S_\Lambda(\mathsf{T}^d) + \sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T}) \end{aligned}$$

The exchange rate changes as follows. If $S_\Lambda(\mathsf{T}^c) = 0$, then, by [Int] also $S_{\Lambda'}(\mathsf{T}^c) = 0$, and hence, by Equation (2.2), $XR_\Lambda(\mathsf{T}) = 1 = XR_{\Lambda'}(\mathsf{T})$. Otherwise, if $S_\Lambda(\mathsf{T}^c) \neq 0$, then $S_{\Lambda'}(\mathsf{T}^c) = S_\Lambda(\mathsf{T}^c) \neq 0$, and so:

$$\begin{aligned} XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)} \\ &= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d) + \sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T})}{S_\Lambda(\mathsf{T}^c)} && \text{by [Int]} \\ &= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} + \frac{\sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T})}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.} \\ &= XR_\Lambda(\mathsf{T}) + \frac{\sum_{\mathsf{A} \in \mathbb{A}} \Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_\Lambda(\mathsf{T})}{S_\Lambda(\mathsf{T}^c)} && \text{by (2.2)} \\ &= XR_\Lambda(\mathsf{T}) + \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} \cdot I_\Lambda(\mathsf{T}) && \text{by (2.1)} \end{aligned}$$

We now have the two following two cases:
- If $S_\Lambda(\mathsf{T}^d) = 0$, the second addend in the previous equation is equal to 0, hence $XR_{\Lambda'}(\mathsf{T}) = XR_\Lambda(\mathsf{T})$.
- If $S_\Lambda(\mathsf{T}^d) > 0$, since by Equation (2.13) $I_\Lambda(\mathsf{T}) > 0$, then the second addend is strictly positive, hence $XR_{\Lambda'}(\mathsf{T}) > XR_\Lambda(\mathsf{T})$.

- A: rep$(v\colon \mathsf{T})$. Since the [Rep] rule increases the base tokens T, then $\Lambda'(\mathsf{T}) > 0$, and so by Lemma 3.3 it must be $S_{\Lambda'}(\mathsf{T}^c) > 0$. Then:

$$\begin{aligned} XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)} \\ &= \frac{(\Lambda(\mathsf{T}) + v) + (S_\Lambda(\mathsf{T}^d) - v)}{S_\Lambda(\mathsf{T}^c)} && \text{by [Rep]} \\ &= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.} \\ &= XR_\Lambda(\mathsf{T}) && \text{by (2.2)} \end{aligned}$$

- $\mathsf{A}\colon \mathsf{rdm}(v\colon \mathsf{T}^c)$. We have two cases. First, consider the case $S_{\Lambda'}(\mathsf{T}^c) \neq 0$, i.e. $v \neq S_\Lambda(\mathsf{T}^c)$. Then:

$$\begin{aligned}
XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{\Lambda(\mathsf{T}) - v \cdot XR_\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c) - v} && \text{by [Rdm]}\\
&= \frac{\Lambda(\mathsf{T}) \cdot S_\Lambda(\mathsf{T}^c) - v \cdot XR_\Lambda(\mathsf{T}) \cdot S_\Lambda(\mathsf{T}^c) + S_\Lambda(\mathsf{T}^d) \cdot S_\Lambda(\mathsf{T}^c)}{(S_\Lambda(\mathsf{T}^c) - v) \cdot S_\Lambda(\mathsf{T}^c)} && \text{by arith.}\\
&= \frac{\Lambda(\mathsf{T}) \cdot S_\Lambda(\mathsf{T}^c) - v \cdot (\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)) + S_\Lambda(\mathsf{T}^d) \cdot S_\Lambda(\mathsf{T}^c)}{(S_\Lambda(\mathsf{T}^c) - v) \cdot S_\Lambda(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{\Lambda(\mathsf{T}) \cdot (S_\Lambda(\mathsf{T}^c) - v) + S_\Lambda(\mathsf{T}^d) \cdot (S_\Lambda(\mathsf{T}^c) - v)}{(S_\Lambda(\mathsf{T}^c) - v) \cdot S_\Lambda(\mathsf{T}^c)} && \text{by arith.}\\
&= XR_\Lambda(\mathsf{T}) && \text{by (2.2)}
\end{aligned}$$

  Otherwise, if $S_{\Lambda'}(\mathsf{T}^c) = 0$, then, by definition of exchange rate (2.2), $XR_{\Lambda'}(\mathsf{T}) = 1$.
- In the case of liq, since there are two tokens that appear in the rule, we will first consider the case in which the token T corresponds to the debt being repayed by the liquidator, and, secondly, the case in which the token T is the token whose associated credit tokens are seized and passed to the liquidator.
  - $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}, \mathsf{T}'^c)$, with $\mathsf{T} \neq \mathsf{T}'$.

$$\begin{aligned}
XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{(\Lambda(\mathsf{T}) + v) + (S_\Lambda(\mathsf{T}^d) - v)}{S_\Lambda(\mathsf{T}^c)} && \text{by [Liq]}\\
&= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.}\\
&= XR_\Lambda(\mathsf{T}) && \text{by (2.2)}
\end{aligned}$$

  - $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}', \mathsf{T}^c)$, with $\mathsf{T} \neq \mathsf{T}'$.

$$\begin{aligned}
XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)}\\
&= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d))}{S_\Lambda(\mathsf{T}^c) + v' - v'} && \text{by [Liq]}\\
&= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.}\\
&= XR_\Lambda(\mathsf{T}) && \text{by (2.2)}
\end{aligned}$$

– $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}, \mathsf{T}^c)$.

$$\begin{aligned} XR_{\Lambda'}(\mathsf{T}) &= \frac{\Lambda'(\mathsf{T}) + S_{\Lambda'}(\mathsf{T}^d)}{S_{\Lambda'}(\mathsf{T}^c)} && \text{by (2.2)} \\ &= \frac{(\Lambda(\mathsf{T}) + v) + (S_\Lambda(\mathsf{T}^d) - v)}{S_\Lambda(\mathsf{T}^c) + v' - v'} && \text{by [Liq]} \\ &= \frac{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} && \text{by arith.} \\ &= XR_\Lambda(\mathsf{T}) && \text{by (2.2)} \end{aligned}$$

- $\mathsf{px}(\delta\colon \mathsf{T})$ Price updates do not change the number of base/credit/debit tokens in the LP, hence the thesis holds trivially.
- $\mathsf{swp}(v\colon \mathsf{T}_1, \mathsf{T}_2)$ Swaps do not change the number of base/credit/debit tokens in the LP, hence the thesis holds trivially. □

Proof of Corollary 3.5. We must prove that $XR_\Lambda(\mathsf{T}) \geq 1$ for all reachable LP state Λ. Let $\Gamma = (\omega, \Lambda, \pi)$ be a reachable blockchain state. If Γ is initial, then $S_\Lambda(\mathsf{T}^c) = 0$, and so the second case of (2.2) applies, giving $XR_\Lambda(\mathsf{T}) = 1$. Otherwise, the statement follows by applying inductively Lemma 3.4. □

Proof of Theorem 3.6. We have to prove that, for every state Γ, and for every transition:

$$\Gamma = (\omega, \Lambda, \pi) \xrightarrow{\mathsf{X}} \Gamma' = (\omega', \Lambda', \pi)$$

such that $\mathsf{X} \neq \mathsf{px}$, we have that:

$$\sum_{\mathsf{C} \in \mathbb{A}} W_{\Gamma'}(\mathsf{C}) = \sum_{\mathsf{C} \in \mathbb{A}} W_\Gamma(\mathsf{C})$$

Since $\sum_{\mathsf{C}\in\mathbb{A}} g_\mathsf{C}(\Gamma, \mathsf{X}) = \sum_{\mathsf{C}\in\mathbb{A}}(W_{\Gamma'}(\mathsf{C}) - W_\Gamma(\mathsf{C}))$, we can equivalently prove that:

$$\sum_{\mathsf{C} \in \mathbb{A}} g_\mathsf{C}(\Gamma, \mathsf{X}) = 0$$

Note that Lemma 4.1 implies the thesis for all cases except $\mathsf{X} = \mathsf{int}$. Indeed, it states that:

- if X is not a liq, then the gain of the user A who fired the transaction is $g_\mathsf{A}(\Gamma, \mathsf{X}) = 0$, while the gain of the other users does not change.
- if X is a liq, say $\mathsf{X} = \mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}_0, \mathsf{T}_1^c)$, then the only non-zero gains are those of A and B, and $g_\mathsf{A}(\Gamma, \mathsf{X}) = -g_\mathsf{B}(\Gamma, \mathsf{X})$, i.e.:

$$\begin{aligned} \sum_{\mathsf{C} \in \mathbb{A}} g_\mathsf{C}(\Gamma, \mathsf{X}) &= \left(\sum_{\mathsf{C} \in \mathbb{A} \setminus \{\mathsf{A}, \mathsf{B}\}} g_\mathsf{C}(\Gamma, \mathsf{X}) \right) + g_\mathsf{A}(\Gamma, \mathsf{X}) + g_\mathsf{B}(\Gamma, \mathsf{X}) \\ &= 0 + g_\mathsf{A}(\Gamma, \mathsf{X}) - g_\mathsf{A}(\Gamma, \mathsf{X}) = 0 \end{aligned}$$

We now consider the case $\mathsf{X} = \mathsf{int}$. From Lemma 4.3, we have that, for all T, if $S_\Lambda(\mathsf{T}^c) = 0$, then for all A, $g_\mathsf{A}(\Gamma, \mathsf{int})|_\mathsf{T} = 0$; otherwise, if $S_\Lambda(\mathsf{T}^c) > 0$, for all A:

$$g_\mathsf{A}(\Gamma, \mathsf{int})|_\mathsf{T} = \left(\Lambda(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} - \Lambda(\mathsf{T}^d, \mathsf{A}) \right) \cdot \left(I_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T}) \right)$$

Let $c = I_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T})$. We have that:

$$\begin{aligned}
\sum_{\mathsf{C}\in\mathbb{A}} g_{\mathsf{C}}(\Gamma,\mathsf{int})|_{\mathsf{T}} &= \sum_{\mathsf{C}\in\mathbb{A}} \left(\Lambda(\mathsf{T}^c,\mathsf{C}) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} - \Lambda(\mathsf{T}^d,\mathsf{C})\right) \cdot c && \text{by (2.1)}\\
&= \left(\Big(\sum_{\mathsf{C}\in\mathbb{A}} \Lambda(\mathsf{T}^c,\mathsf{C})\Big) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} - \sum_{\mathsf{C}\in\mathbb{A}} \Lambda(\mathsf{T}^d,\mathsf{C})\right) \cdot c && \text{by arith.}\\
&= \left(S_\Lambda(\mathsf{T}^c) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} - S_\Lambda(\mathsf{T}^d)\right) \cdot c && \text{by (2.1)}\\
&= 0 && \text{by arith.}
\end{aligned}$$

The thesis follows from (2.9). □

Appendix B. Proofs for Section 4

Proof of Lemma 4.1. Let $\mathsf{X} \notin \{\mathsf{int},\mathsf{px}\}$ be enabled in Γ. We have to prove that:
(1) $g_{\mathsf{A}}(\Gamma,\mathsf{X}) = 0$ iff X is not a liquidation involving A.
(2) $g_{\mathsf{A}}(\Gamma,\mathsf{X}) > 0$ iff X is a liquidation performed by A;
(3) $g_{\mathsf{A}}(\Gamma,\mathsf{X}) < 0$ iff X is a liquidation suffered by A;
and, in the case $\mathsf{X} = \mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}_0, \mathsf{T}_1^c)$, that:
(4) $g_{\mathsf{A}}(\Gamma,\mathsf{X}) = -g_{\mathsf{B}}(\Gamma,\mathsf{X}) = v \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}}$.

Assume that the state transition is given by:

$$\Gamma = (\omega,\Lambda,\pi) \xrightarrow{\mathsf{X}} \Gamma' = (\omega',\Lambda',\pi)$$

In order to prove the first three points, we proceed by cases on X. The last point will follow from the cases concerning liq.

First, consider the case in which A does not appear in X. In this case, the amount of base tokens, credits, and debts held by A do not change. Since, by hypothesis, $\mathsf{X} \neq \mathsf{px}$, the token prices do not change too, and hence $W_{\omega',\pi}(\mathsf{A}) = W_{\omega',\pi}(\mathsf{A})$ and $W^d_{\Lambda',\pi}(\mathsf{A}) = W^d_{\Lambda,\pi}(\mathsf{A})$. For $W^c_{\Lambda',\pi}(\mathsf{A})$, we have to consider possible changes in the exchange rates. By Lemma 3.4 and the hypothesis that $\mathsf{X} \neq \mathsf{int}$, we know that the exchange rate of a token type T can only change if X is a rdm that reclaims the entirety of the credits in T. If this is the case, since by hypothesis A does not appear in X, in means that A had no credits in T, i.e. $W^c_{\Lambda,\pi}(\mathsf{A})|_{\mathsf{T}} = 0 = W^c_{\Lambda,\pi}(\mathsf{A})|_{\mathsf{T}}$, hence $W^c_{\Lambda',\pi}(\mathsf{A}) = W^c_{\Lambda,\pi}(\mathsf{A})$.

Now let's consider the following exhaustive cases in which A appears in X:

- $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$. We have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)}\\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}'} \Lambda'(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}') \cdot \pi(\mathsf{T}') - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.5)}\\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}'} \Lambda'(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}') \cdot \pi(\mathsf{T}') - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by Lem. 3.4}\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T})\Big) + \Big(\sum_{\mathsf{T}' \neq \mathsf{T}} \Lambda(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}') \cdot \pi(\mathsf{T}')\\
&\qquad + (\Lambda(\mathsf{T}^c, \mathsf{A}) + v^c) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T})\Big) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by [Dep]}\\
&= W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}) + W^c_{\Lambda,\pi}(\mathsf{A}) + v^c \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith. + (2.5)}\\
&= W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}) + W^c_{\Lambda,\pi}(\mathsf{A}) + v \cdot \frac{XR_{\Lambda}(\mathsf{T})}{XR_{\Lambda}(\mathsf{T})} \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by def. } v^c\\
&= W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}) + W^c_{\Lambda,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by Lem. 3.4}\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.}\\
&= W_{\Gamma}(\mathsf{A}) && \text{by (2.7)}
\end{aligned}$$

- $\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$. We have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)}\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T})\Big) + W^c_{\Lambda,\pi}(\mathsf{A}) - \Big(W^d_{\Lambda,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T})\Big) && \text{by [Bor]}\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.}\\
&= W_{\Gamma}(\mathsf{A}) && (2.7)
\end{aligned}$$

- $\mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$. We have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)}\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T})\Big) + W^c_{\Lambda,\pi}(\mathsf{A}) - \Big(W^d_{\Lambda,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T})\Big) && \text{by [Rep]}\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.}\\
&= W_{\Gamma}(\mathsf{A}) && \text{by (2.7)}
\end{aligned}$$

- $\mathsf{A}\colon \mathsf{rdm}(v^c\colon \mathsf{T}^c)$. By rule [Rdm], let $v = v^c \cdot XR_{\Lambda}(\mathsf{T})$. We have now two subcases.
  If $S_{\Lambda'}(\mathsf{T}^c) > 0$, then by Lemma 3.4 it follows that $XR_{\Lambda'}(\mathsf{T}) = XR_{\Lambda}(\mathsf{T})$, and so we have:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)}\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T})\Big) + \Big(W^c_{\Lambda,\pi}(\mathsf{A}) - v^c \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T})\Big) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by [Rdm]}\\
&= W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) + W^c_{\Lambda,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by def. } v\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.}\\
&= W_{\Gamma}(\mathsf{A}) && \text{by (2.7)}
\end{aligned}$$

Otherwise, if $S_{\Lambda'}(\mathsf{T}^c) = 0$, then it means that $v^c = S_\Lambda(\mathsf{T}^c) = \Lambda(\mathsf{T}^c, \mathsf{A})$, and by Lemma 3.4 it follows that $XR_{\Lambda'}(\mathsf{T}) = 1$. Hence, we have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) \\
&\quad + \sum_{\mathsf{T}' \neq \mathsf{T}} \Lambda'(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}') \cdot \pi(\mathsf{T}') && \text{by } \Lambda'(\mathsf{T}^c, \mathsf{A}) = 0 \\
&= W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) \\
&\quad + \sum_{\mathsf{T}' \neq \mathsf{T}} \Lambda(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}') \cdot \pi(\mathsf{T}') && \text{by [RDM]} \\
&= W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) \\
&\quad + \sum_{\mathsf{T}'} \Lambda(\mathsf{T}'^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}') \cdot \pi(\mathsf{T}') - \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by arith.} \\
&= W_{\omega,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - W^d_{\Lambda,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) \\
&\quad - \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by arith.} \\
&= W_{\Gamma}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - v^c \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by (2.7), } v^c = \Lambda(\mathsf{T}^c, \mathsf{A}) \\
&= W_{\Gamma}(\mathsf{A}) + v \cdot \pi(\mathsf{T}) - v \cdot \pi(\mathsf{T}) && \text{by def. } v^c \\
&= W_{\Gamma}(\mathsf{A}) && \text{by arith.}
\end{aligned}$$

- $\mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v_0\colon \mathsf{T}_0, \mathsf{T}_1^c)$, where $\mathsf{B} \neq \mathsf{A}$. We have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)} \\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}} \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) \cdot \pi(\mathsf{T}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.5)} \\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}} \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by Lem. 3.4} \\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v_0 \cdot \pi(\mathsf{T}_0)\Big) + \sum_{\mathsf{T} \neq \mathsf{T}_1} \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) \\
&\quad + \Big(\Lambda(\mathsf{T}_1{}^c, \mathsf{A}) + v_1^c\Big) \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by [LIQ]} \\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v_0 \cdot \pi(\mathsf{T}_0)\Big) \\
&\quad + \Big(W^c_{\Lambda,\pi}(\mathsf{A}) + v_1^c \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1)\Big) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith. and (2.5)} \\
&= W_{\omega,\pi}(\mathsf{A}) - v_0 \cdot \pi(\mathsf{T}_0) + W^c_{\Lambda,\pi}(\mathsf{A}) \\
&\quad + v_0 \cdot \frac{1}{XR_{\Lambda}(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)} \cdot R_{\mathsf{liq}} \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by def. } v_1^c \\
&= W_{\omega,\pi}(\mathsf{A}) - v_0 \cdot \pi(\mathsf{T}_0) + W^c_{\Lambda,\pi}(\mathsf{A}) + v_0 \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}} - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.} \\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) + (R_{\mathsf{liq}} - 1) \cdot v_0 \cdot \pi(\mathsf{T}_0) && \text{by arith.} \\
&= W_{\Gamma}(\mathsf{A}) + (R_{\mathsf{liq}} - 1) \cdot v_0 \cdot \pi(\mathsf{T}_0) && \text{by (2.7)}
\end{aligned}$$

Recalling that $v_0 > 0$, $\pi(\mathsf{T}_0) > 0$ and $R_{\mathsf{liq}} > 1$, we obtain:

$$g_{\mathsf{A}}(\Gamma, \mathsf{X}) \;=\; (R_{\mathsf{liq}} - 1) \cdot v_0 \cdot \pi(\mathsf{T}_0) \;>\; 0$$

- $\mathsf{B}\colon \mathsf{liq}(\mathsf{A}, v\colon \mathsf{T}_0, \mathsf{T}_1^c)$, where $\mathsf{B} \neq \mathsf{A}$. We have that:

$$
\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && (2.7)\\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}} \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) \cdot \pi(\mathsf{T}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.5)}\\
&= W_{\omega',\pi}(\mathsf{A}) + \sum_{\mathsf{T}} \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by Lem. 3.4}\\
&= W_{\omega,\pi}(\mathsf{A}) + \Big(\sum_{\mathsf{T}\neq\mathsf{T}_1} \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T})\\
&\quad + (\Lambda(\mathsf{T}_1{}^c, \mathsf{A}) - v_1^c) \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1)\Big) - \Big(W^d_{\Lambda,\pi}(\mathsf{A}) - v_0 \cdot \pi(\mathsf{T}_0)\Big) && [\textsc{Liq}]\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - v_1^c \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1)\\
&\quad - W^d_{\Lambda,\pi}(\mathsf{A}) + v_0 \cdot \pi(\mathsf{T}_0) && \text{(arith. + (2.5))}\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - v_0 \cdot \frac{1}{XR_{\Lambda}(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)} \cdot R_{\mathsf{liq}} \cdot XR_{\Lambda}(\mathsf{T}_1) \cdot \pi(\mathsf{T}_1)\\
&\quad - W^d_{\Lambda,\pi}(\mathsf{A}) + v_0 \cdot \pi(\mathsf{T}_0) && \text{(def. } v_1^c)\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}} - W^d_{\Lambda,\pi}(\mathsf{A}) + v_0 \cdot \pi(\mathsf{T}_0) && \text{(Lemma 3.4)}\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) + (1 - R_{\mathsf{liq}}) \cdot v_0 \cdot \pi(\mathsf{T}_0) && \text{(arith.)}\\
&= W_{\Gamma}(\mathsf{A}) + (1 - R_{\mathsf{liq}}) \cdot v_0 \cdot \pi(\mathsf{T}_0) && (2.7)
\end{aligned}
$$

  Recalling that $v_0 > 0$, $\pi(\mathsf{T}_0) > 0$ and $R_{\mathsf{liq}} > 1$, we obtain:

$$g_{\mathsf{A}}(\Gamma, \mathsf{X}) \;=\; (1 - R_{\mathsf{liq}}) \cdot v_0 \cdot \pi(\mathsf{T}_0) \;<\; 0$$

  This case, together with the previous one, proves that, if $\mathsf{X} = \mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v\colon \mathsf{T}_0, \mathsf{T}_1^c)$, then $g_{\mathsf{A}}(\Gamma, \mathsf{X}) = -g_{\mathsf{B}}(\Gamma, \mathsf{X}) = v \cdot \pi(\mathsf{T}_0) \cdot R_{\mathsf{liq}}$ Note that $g_{\mathsf{B}}(\Gamma, \mathsf{X})$ is obtained from this case by switching A and B.
- $\mathsf{swp}(v\colon \mathsf{T}_0, \mathsf{T}_1)$, with $v' = v \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)}$. We have that:

$$
\begin{aligned}
W_{\Gamma'}(\mathsf{A}) &= W_{\omega',\pi}(\mathsf{A}) + W^c_{\Lambda',\pi}(\mathsf{A}) - W^d_{\Lambda',\pi}(\mathsf{A}) && \text{by (2.7)}\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}_0) + v' \cdot \pi(\mathsf{T}_1)\Big) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by } [\textsc{swp}]\\
&= \Big(W_{\omega,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T}_0) + v \cdot \frac{\pi(\mathsf{T}_0)}{\pi(\mathsf{T}_1)} \cdot \pi(\mathsf{T}_1)\Big) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by def. } v'\\
&= W_{\omega,\pi}(\mathsf{A}) + W^c_{\Lambda,\pi}(\mathsf{A}) - W^d_{\Lambda,\pi}(\mathsf{A}) && \text{by arith.}\\
&= W_{\Gamma}(\mathsf{A}) && \text{by (2.7)}
\end{aligned}
$$

□

Proof of Lemma 4.2. Let $\Gamma = (\omega, \Lambda, \pi)$, and let $p = \pi(\mathsf{T})$. Then, given $\mathsf{X} = \mathsf{px}(\delta\colon \mathsf{T})$, by (2.8) we have to prove that:

$$g_{\mathsf{A}}(\Gamma, \mathsf{X}) = \Big(\omega(\mathsf{T}, \mathsf{A}) + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \delta$$

Assume that the state transition is given by:

$$\Gamma = (\omega, \Lambda, \pi) \xrightarrow{\mathsf{X}} \Gamma' = (\omega', \Lambda', \pi')$$

First, note that, since only the price of T changes, it trivially holds that $W_{\Gamma'}(\mathsf{A})\,|_{\mathsf{T}'} = W_{\Gamma}(\mathsf{A})|_{\mathsf{T}'}$ for every $\mathsf{T}' \neq \mathsf{T}$. Hence, $g_{\mathsf{A}}(\Gamma, \mathsf{X}) = g_{\mathsf{A}}(\Gamma, \mathsf{X})|_{\mathsf{T}}$, and so we can restrict to analyse $g_{\mathsf{A}}(\Gamma, \mathsf{X})|_{\mathsf{T}} = W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} - W_{\Gamma}(\mathsf{A})|_{\mathsf{T}}$. The wealth of A in the old state Γ is given by:

$$\begin{aligned}
W_{\Gamma}(\mathsf{A})|_{\mathsf{T}} &= W_{\omega,\pi}(\mathsf{A})|_{\mathsf{T}} + W^{c}_{\Lambda,\pi}(\mathsf{A})|_{\mathsf{T}} - W^{d}_{\Lambda,\pi}(\mathsf{A})|_{\mathsf{T}} && \text{by (2.7)}\\
&= \omega(\mathsf{T},\mathsf{A}) \cdot p + (\Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot p) - (\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot p) && \text{by (2.4),(2.5),(2.6)}\\
&= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big) \cdot p && \text{by arith.}
\end{aligned}$$

while for the new state, we have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} &= W_{\omega',\pi}(\mathsf{A})|_{\mathsf{T}} + W^{c}_{\Lambda',\pi}(\mathsf{A})|_{\mathsf{T}} - W^{d}_{\Lambda',\pi}(\mathsf{A})|_{\mathsf{T}} && \text{by (2.7)}\\
&= \omega'(\mathsf{T},\mathsf{A}) \cdot (p+\delta) + \Lambda'(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) \cdot (p+\delta)\\
&\quad - \Lambda'(\mathsf{T}^d,\mathsf{A}) \cdot (p+\delta) && \text{by (2.4),(2.5),(2.6)}\\
&= \omega(\mathsf{T},\mathsf{A}) \cdot (p+\delta) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) \cdot (p+\delta)\\
&\quad - \Lambda(\mathsf{T}^d,\mathsf{A}) \cdot (p+\delta) && \text{by [Px] and (3.4)}\\
&= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big) \cdot (p+\delta) && \text{by arith.}
\end{aligned}$$

Summing up:

$$\begin{aligned}
g_{\mathsf{A}}(\Gamma,\mathsf{X}) &= g_{\mathsf{A}}(\Gamma,\mathsf{X})|_{\mathsf{T}} && \text{by previous observation}\\
&= W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} - W_{\Gamma}(\mathsf{A})|_{\mathsf{T}} && \text{by (4.1)}\\
&= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big) \cdot \delta && \text{by arith.}
\end{aligned}$$

□

Proof of Lemma 4.3. Let $\Gamma = (\omega, \Lambda, \pi)$. We have to prove that the gain of a user A upon an int transaction in Γ w.r.t. T is given by:

$$g_{\mathsf{A}}(\Gamma, \mathsf{int})_{|\mathsf{T}} = \begin{cases} \left(\Lambda(\mathsf{T}^c,\mathsf{A}) \cdot \dfrac{S_{\Lambda}(\mathsf{T}^d)}{S_{\Lambda}(\mathsf{T}^c)} - \Lambda(\mathsf{T}^d,\mathsf{A})\right) \cdot \Big(I_{\Lambda}(\mathsf{T}) \cdot \pi(\mathsf{T})\Big) & \text{if } S_{\Lambda}(\mathsf{T}^c) > 0 \\ 0 & \text{otherwise} \end{cases}$$

Assume that the state transition is given by:

$$\Gamma = (\omega, \Lambda, \pi) \xrightarrow{\mathsf{X}} \Gamma' = (\omega', \Lambda', \pi)$$

By unfolding the definition of W and its components with (2.4)—(2.7), we have that:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} &= W_{\omega',\pi}(\mathsf{A})|_{\mathsf{T}} + W^{c}_{\Lambda',\pi}(\mathsf{A})|_{\mathsf{T}} - W^{d}_{\Lambda',\pi}(\mathsf{A})|_{\mathsf{T}}\\
&= \omega'(\mathsf{T},\mathsf{A}) \cdot \pi'(\mathsf{T}) + \Lambda'(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) \cdot \pi'(\mathsf{T}) - \Lambda'(\mathsf{T}^d,\mathsf{A}) \cdot \pi'(\mathsf{T})\\
&= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - \Big(\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot (1 + I_{\Lambda}(\mathsf{T}))\Big)\Big) \cdot \pi(\mathsf{T}) \qquad \text{(B.1)}
\end{aligned}$$

We have two subcases. If $S_\Lambda(\mathsf{T}^c) > 0$, by Lemma 3.4 and (B.1) we obtain:

$$W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} = \left(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot \left(XR_\Lambda(\mathsf{T}) + \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} \cdot I_\Lambda(\mathsf{T})\right) - \left(\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot (1 + I_\Lambda(\mathsf{T}))\right)\right) \cdot \pi(\mathsf{T}) \tag{B.2}$$

and so we obtain the following gain restricted to T:

$$\begin{aligned}
g_{\mathsf{A}}(\Gamma,\mathsf{X})|_{\mathsf{T}} &= W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} - W_\Gamma(\mathsf{A})|_{\mathsf{T}} && \text{by (4.1)}\\
&= \left(\Lambda(\mathsf{T}^c,\mathsf{A}) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} \cdot I_\Lambda(\mathsf{T}) - \left(\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot I_\Lambda(\mathsf{T})\right)\right) \cdot \pi(\mathsf{T}) && \text{by (B.2)}\\
&= \left(\Lambda(\mathsf{T}^c,\mathsf{A}) \cdot \frac{S_\Lambda(\mathsf{T}^d)}{S_\Lambda(\mathsf{T}^c)} - \Lambda(\mathsf{T}^d,\mathsf{A})\right) \cdot \left(I_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T})\right) && \text{by arith.}
\end{aligned}$$

Otherwise, if $S_\Lambda(\mathsf{T}^c) = 0$, then, by Lemma 3.4 we have that $XR_{\Lambda'}(\mathsf{T}) = XR_\Lambda(\mathsf{T})$, and by Lemma 3.3 we have that $\Lambda(\mathsf{T}^d,\mathsf{A}) = 0$. Hence we have:

$$\begin{aligned}
W_{\Gamma'}(\mathsf{A})|_{\mathsf{T}} &= \left(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - \left(\Lambda(\mathsf{T}^d,\mathsf{A}) \cdot (1 + I_\Lambda(\mathsf{T}))\right)\right) \cdot \pi(\mathsf{T}) && \text{by (B.1)}\\
&= \left(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T})\right) \cdot \pi(\mathsf{T}) && \text{by Lem. 3.3}\\
&= \left(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_\Lambda(\mathsf{T})\right) \cdot \pi(\mathsf{T}) && \text{by Lem. 3.4}\\
&= W_\Gamma(\mathsf{A})|_{\mathsf{T}} && \text{by (2.7)}
\end{aligned}$$

from which we have the thesis $g_{\mathsf{A}}(\Gamma,\mathsf{X})|_{\mathsf{T}} = 0$. □

Proof of Lemma 4.4. Let $\mathsf{X} = \mathsf{A}{:}\,\ell(\cdots)$, and let $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$. We have to prove that:

- $\ell \in \{\mathsf{dep},\mathsf{rep},\mathsf{liq}\} \implies H_{\Gamma'}(\mathsf{A}) \geq H_\Gamma(\mathsf{A})$
- $\ell \in \{\mathsf{bor},\mathsf{rdm}\} \implies H_{\Gamma'}(\mathsf{A}) \leq H_\Gamma(\mathsf{A})$
- $\ell \in \{\mathsf{swp}\} \implies H_{\Gamma'}(\mathsf{A}) = H_\Gamma(\mathsf{A})$

and the inequalities are strict if and only if $W^d_\Gamma(\mathsf{A}) > 0$.

Let $\Gamma = (\omega,\Lambda,\pi)$ and let $\Gamma' = (\omega',\Lambda',\pi')$. Note that since we are excluding px, the prices remain constant, and so $\pi' = \pi$. Recall the the health factor is defined by:

$$H_{\Lambda,\pi}(\mathsf{A}) = \begin{cases} \dfrac{W^c_{\Lambda,\pi}(\mathsf{A})}{W^d_{\Lambda,\pi}(\mathsf{A})} \cdot T_{\mathsf{liq}} & \text{if } W^d_{\Lambda,\pi}(\mathsf{A}) > 0 \\ +\infty & \text{otherwise} \end{cases}$$

We start by noting that, if $W^d_{\Lambda,\pi}(\mathsf{A}) = 0$, the health factor cannot increase, and it decreases if and only if A's debts increase (i.e. they become strictly positive). Otherwise, if $W^d_{\Lambda,\pi}(\mathsf{A}) = 0$, we have that:

(1) if the credits increase and the debts do not change, the health factor *increases*;
(2) if the credits do not change and the debts decrease, the health factor *increases*;
(3) if the credits decrease and the debts do not change, the health factor *decrease*;
(4) if the credits do not change and the debts increase, the health factor *decreases*;
(5) if the credits and the debts do not change, the health factor *remains constant*.

We then analyse the change in A' credits and debts based on ℓ:

- $\ell = \mathsf{dep}$: credits increase and debts do not change (case 1).
- $\ell = \mathsf{bor}$: debts increase and credits do not change (case 4).
- $\ell = \mathsf{rep}$: debts decreases and credits do not change (case 2).
- $\ell = \mathsf{rdm}$: credits decrease and debts do not change (case 3).
- $\ell = \mathsf{liq}$: credits increase and debts do not change (case 1).
- $\ell = \mathsf{swp}$: the credits and the debts do not change (case 5). □

Proof of Lemma 4.6. Let $\Gamma_0 \xrightarrow{\mathsf{A}:\mathsf{dep}(v:\mathsf{T})} \Gamma_1$ and $\Gamma_0 \xrightarrow{\mathsf{A}:\mathsf{rep}(v:\mathsf{T})} \Gamma_1'$. We have to prove that:

$$H_{\Gamma_1'}(\mathsf{A}) \geq H_{\Gamma_1}(\mathsf{A}) \text{ if and only if } v \cdot \pi(\mathsf{T}) \geq W^d_{\Gamma_0}(\mathsf{A}) - W^c_{\Gamma_0}(\mathsf{A})$$

Let $\Gamma_0 = (\omega_0, \Lambda_0, \pi_0)$, let $\Gamma_1 = (\omega_1, \Lambda_1, \pi_1)$, and let $\Gamma_1' = (\omega_1', \Lambda_1', \pi_1')$. By Lemma 3.4, we have that both transitions preserve the exchange rate, i.e. $XR_{\Lambda_1}(\mathsf{T}) = XR_{\Lambda_0}(\mathsf{T}) = XR_{\Lambda_0}(\mathsf{T})$.

We first compute the health factor in Γ_1. First, note that $W^d_{\Lambda_0,\pi}(\mathsf{A}) > 0$, since the rule [Rep] is enabled in Γ_0 and its premise requires that the repayer has a strictly positive debit. Since dep does not modify the debts, then $W^d_{\Lambda_1,\pi}(\mathsf{A}) = W^d_{\Lambda_0,\pi}(\mathsf{A}) > 0$. Therefore:

$$\begin{aligned}
H_{\Gamma_1}(\mathsf{A}) &= \frac{W^c_{\Lambda_1,\pi}(\mathsf{A})}{W^d_{\Lambda_1,\pi}(\mathsf{A})} \cdot T_{\mathsf{liq}} && \text{by (2.12)} \\
&= \frac{\sum_{\mathsf{T}_i} \Lambda_1(\mathsf{T}_i{}^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)}{\sum_{\mathsf{T}_i} \Lambda_1(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i)} \cdot T_{\mathsf{liq}} && \text{by (2.5),(2.6)} \\
&= \frac{\left(\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}_i{}^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)\right) + v/XR_{\Lambda_0}(\mathsf{T}) \cdot XR_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T})}{\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i)} \cdot T_{\mathsf{liq}} && \text{by [Dep]} \\
&= \frac{\left(\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}_i{}^c, \mathsf{A}) \cdot XR_{\Lambda_0}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)\right) + v \cdot \pi(\mathsf{T})}{\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i)} \cdot T_{\mathsf{liq}} && \text{by Lem. 3.4} \\
&= \frac{W^c_{\Lambda_0,\pi}(\mathsf{A}) + v \cdot \pi(\mathsf{T})}{W^d_{\Lambda_0,\pi}(\mathsf{A})} \cdot T_{\mathsf{liq}} && \text{by (2.5),(2.6)}
\end{aligned}$$

We then compute the health factor in Γ_1'. There are two subcases, depending on whether A repays the entirety of her debts or not.

If A repays all her debts, i.e. $v = \Lambda_0(\mathsf{T}^d, \mathsf{A})$, then $v \cdot \pi(\mathsf{T}) = W^d_{\Lambda_0}(\mathsf{A}) \geq W^d_{\Lambda_0}(\mathsf{A}) - W^c_{\Lambda_0}(\mathsf{A})$ and $W^d_{\Lambda_1',\pi}(\mathsf{A}) = 0$. Hence, by the definition of health factor, $H_{\Lambda_1'}(\mathsf{A}) = +\infty > H_{\Lambda_1}(\mathsf{A})$.

Otherwise, if A does not repay the entirety of her debts, we have that $W^d_{\Lambda'_1,\pi}(\mathsf{A}) > 0$, and the health factor in Γ'_1 is given by:

$$\begin{aligned}
H_{\Gamma'_1}(\mathsf{A}) &= \frac{W^c_{\Lambda'_1,\pi}(\mathsf{A})}{W^d_{\Lambda'_1,\pi}(\mathsf{A})} \cdot T_{\mathsf{liq}} && \text{by (2.12)}\\
&= \frac{\sum_{\mathsf{T}_i} \Lambda'_1({\mathsf{T}_i}^c, \mathsf{A}) \cdot XR_{\Lambda'_1}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)}{\sum_{\mathsf{T}_i} \Lambda'_1(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i)} \cdot T_{\mathsf{liq}} && \text{by (2.5),(2.6)}\\
&= \frac{\sum_{\mathsf{T}_i} \Lambda_0({\mathsf{T}_i}^c, \mathsf{A}) \cdot XR_{\Lambda'_1}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)}{\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i) - v \cdot \pi(\mathsf{T})} \cdot T_{\mathsf{liq}} && \text{by [Rep]}\\
&= \frac{\sum_{\mathsf{T}_i} \Lambda_0({\mathsf{T}_i}^c, \mathsf{A}) \cdot XR_{\Lambda_0}(\mathsf{T}_i) \cdot \pi(\mathsf{T}_i)}{\sum_{\mathsf{T}_i} \Lambda_0(\mathsf{T}^d, \mathsf{A}) \cdot \pi(\mathsf{T}_i) - v \cdot \pi(\mathsf{T})} \cdot T_{\mathsf{liq}} && \text{by Lem. 3.4}\\
&= \frac{W^c_{\Lambda_0,\pi}(\mathsf{A})}{W^d_{\Lambda_0,\pi}(\mathsf{A}) - v \cdot \pi(\mathsf{T})} \cdot T_{\mathsf{liq}} && \text{by (2.5) and (2.6)}
\end{aligned}$$

Let $A = W^c_{\Gamma_0}(\mathsf{A})$, let $B = W^d_{\Gamma_0}(\mathsf{A})$, and let $C = v \cdot \pi(\mathsf{T})$. Note that $B \geq C$ holds by the premise of [Rep]. In particular, in the case that $B = C$, then the health factor is by definition $+\infty$, which is greater than 0. So from now on, we only consider the case $B > C$. The proof follows from the following auxiliary result:

$$\forall A \in \mathbb{R},\ B > C > 0 \in \mathbb{R} \quad : \quad \frac{A}{B-C} \geq \frac{A+C}{B} \iff C \geq B - A \tag{B.3}$$

To prove (B.3), note that:

$$\begin{aligned}
\frac{A}{B-C} \geq \frac{A+C}{B} &\iff A \cdot B \geq (A+C) \cdot (B-C)\\
&\iff A \cdot B \geq A \cdot B - A \cdot C + B \cdot C - C^2\\
&\iff 0 \geq (-A + B - C) \cdot C\\
&\iff C \geq B - A
\end{aligned}$$

□

Appendix C. Proofs for Section 5

Proof of Theorem 5.1. Let A and Γ such that $H_\Gamma(\mathsf{A}) < 1$, and let liq be a shorthand for an arbitrary liquidation on A enabled in Γ.

Let $\mathsf{X} = \mathsf{A}\colon \ell(v\colon \mathsf{T})$ with $\ell \in \{\mathsf{dep}, \mathsf{rep}\}$, and $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$. Then we have to prove that:

(1) If $\mathsf{X} = \mathsf{dep}$, then $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) > g_\mathsf{A}(\Gamma, \mathsf{liq}) \iff v \geq \frac{XR_\Gamma(\mathsf{T})}{\pi_\Gamma(\mathsf{T})} \cdot \left(\frac{W^d_\Gamma(\mathsf{A})}{T_{\mathsf{liq}}} - W^c_\Gamma(\mathsf{A}) \right)$

(2) If $\mathsf{X} = \mathsf{rep}$, then $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) > g_\mathsf{A}(\Gamma, \mathsf{liq}) \iff v \geq \frac{1}{\pi_\Gamma(\mathsf{T})} \cdot \left(W^d_\Gamma(\mathsf{A}) - W^c_\Gamma(\mathsf{A}) \cdot T_{\mathsf{liq}} \right)$

Note that we have to cases:

- If after firing X the liq is still enabled, we have that $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) = g_\mathsf{A}(\Gamma, \mathsf{X}) + g_\mathsf{A}(\Gamma', \mathsf{liq}) = 0 + g_\mathsf{A}(\Gamma', \mathsf{liq}) < 0$ by Lemma 4.1.
- If after firing X the liq is not enabled anymore, we have that $g_\mathsf{A}(\Gamma, \mathsf{X}\,\mathsf{liq}) = g_\mathsf{A}(\Gamma, \mathsf{X}) = 0$ by Lemma 4.1.

Hence, we now compute the threshold values of v for which the liq gets disabled, i.e. for which $H_{\Gamma'}(\mathsf{A}) = 1$ (since by Lemma 4.4 both dep and rep increase the health factor, for higher values of v we have that $H_{\Gamma'}(\mathsf{A}) \geq 1$). Note that, if we consider a fixed liquidation on A with parameter v_l, then, in the case of $\ell = \mathsf{rep}$, it would be possible to disable the liq also by making the condition $\Lambda(\mathsf{T}^d, \mathsf{A}) \geq v_l$ false, by repaying a $v > \Lambda(\mathsf{T}^d, \mathsf{A}) - v_l$. However, in general, a user in danger of being liquidated does not precisely know the amount of debt that a liquidator will try to liquidate. For arbitrary values of v_l indeed, as it is in the hypothesis of the theorem, the only way to avoid being liquidated is making the health factor greater or equal to 1.

- If $\mathsf{X} = \mathsf{dep}$, then
$$H_{\Gamma'}(\mathsf{A}) = \frac{W^c_\Gamma(\mathsf{A}) + v/_{XR_\Gamma(\mathsf{T})} \cdot \pi_\Gamma(\mathsf{T})}{W^d_\Gamma(\mathsf{A})} \cdot T_{\mathsf{liq}}$$
hence we have that $H_{\Gamma'}(\mathsf{A}) \geq 1$ if and only if
$$v \geq \frac{XR_\Gamma(\mathsf{T})}{\pi_\Gamma(\mathsf{T})} \cdot \left(\frac{W^d_\Gamma(\mathsf{A})}{T_{\mathsf{liq}}} - W^c_\Gamma(\mathsf{A}) \right)$$
- If $\mathsf{X} = \mathsf{rep}$, then
$$H_{\Gamma'}(\mathsf{A}) = \frac{W^c_\Gamma(\mathsf{A})}{W^d_\Gamma(\mathsf{A}) - v \cdot \pi_\Gamma(\mathsf{T})} \cdot T_{\mathsf{liq}}$$
hence we have that $H_{\Gamma'}(\mathsf{A}) \geq 1$ if and only if
$$g_{\mathsf{A}}(\Gamma, \mathsf{liq}) \iff v \geq \frac{1}{\pi_\Gamma(\mathsf{T})} \cdot \left(W^d_\Gamma(\mathsf{A}) - W^c_\Gamma(\mathsf{A}) \cdot T_{\mathsf{liq}} \right)$$

Proof of Theorem 5.2. Let px be a shorthand for $\mathsf{px}(\delta\colon \mathsf{T})$. Let $\Gamma \xrightarrow{\mathsf{X}} \Gamma'$ with $\mathsf{X} = \mathsf{A}\colon \ell(\cdots)$ mentioning token T. We have to prove that:
$$g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{px}) \circ g_{\mathsf{A}}(\Gamma, \mathsf{px}) = g_{\mathsf{A}}(\Gamma, \mathsf{px}\,\mathsf{X}) \tag{C.1}$$
where the relation $\circ$ is given by:
$$\circ = \begin{cases} = & \text{if } \ell \in \{\mathsf{dep}, \mathsf{rep}, \mathsf{bor}, \mathsf{rdm}\} \\ > & \text{if } (\delta > 0 \text{ and } \ell = \mathsf{swp}(v\colon \mathsf{T}', \mathsf{T})) \text{ or } (\delta < 0 \text{ and } \ell = \mathsf{swp}(v\colon \mathsf{T}, \mathsf{T}')) \\ < & \text{if } (\delta < 0 \text{ and } \ell = \mathsf{swp}(v\colon \mathsf{T}', \mathsf{T})) \text{ or } (\delta > 0 \text{ and } \ell = \mathsf{swp}(v\colon \mathsf{T}, \mathsf{T}')) \end{cases}$$
More precisely, we have to prove that if Γ has price function π, then:
$$g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{px}) = g_{\mathsf{A}}(\Gamma, \mathsf{px}) + \sigma \cdot v \cdot \delta \cdot \left(\frac{\pi(\mathsf{T}')}{\pi(\mathsf{T})} \right)^\sigma \qquad \sigma = \begin{cases} 1 & \ell = \mathsf{swp}(v\colon \mathsf{T}', \mathsf{T}) \\ -1 & \ell = \mathsf{swp}(v\colon \mathsf{T}, \mathsf{T}') \end{cases}$$

Note that the rightmost equality in (C.1) is given by Lemma 4.1. Hence, we only have to prove the leftmost equality/inequality. Under the hypotheses of the theorem, we have:
$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{px}) &= g_{\mathsf{A}}(\Gamma, \mathsf{X}) + g_{\mathsf{A}}(\Gamma', \mathsf{px}) && \text{by (4.1)} \\ &= g_{\mathsf{A}}(\Gamma', \mathsf{px}) && \text{by Lem. 4.1} \\ &= \left(\omega'(\mathsf{T}, \mathsf{A}) + \Lambda'(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda'(\mathsf{T}^d, \mathsf{A}) \right) \cdot \delta && \text{by Lem. 4.2} \end{aligned}$$
We proceed from here by cases on ℓ:

- $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$.

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) - v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) + {}^{v}/_{XR_\Lambda(\mathsf{T})}) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by [Dep]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) - v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) + {}^{v}/_{XR_\Lambda(\mathsf{T})}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by Lem 3.4}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) && \text{by Lem. 4.2} \end{aligned}$$

- $\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$.

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - (\Lambda(\mathsf{T}^d,\mathsf{A}) + v)\Big)\cdot\delta && \text{by [Bor]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - (\Lambda(\mathsf{T}^d,\mathsf{A}) + v)\Big)\cdot\delta && \text{by Lem. 3.4}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) && \text{by Lem. 4.2} \end{aligned}$$

- $\mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$.

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) - v) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - (\Lambda(\mathsf{T}^d,\mathsf{A}) - v)\Big)\cdot\delta && \text{by [Rep]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) - v) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - (\Lambda(\mathsf{T}^d,\mathsf{A}) - v)\Big)\cdot\delta && \text{by Lem. 3.4}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) && \text{by Lem. 4.2} \end{aligned}$$

- $\mathsf{A}\colon \mathsf{rdm}(v^c\colon \mathsf{T}^c)$. Let $v = v^c \cdot XR_\Lambda(\mathsf{T})$. We have two subcases. If $S_{\Lambda'}(\mathsf{T}^c) > 0$, then:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) - v^c) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by [Rdm]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) - v^c) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by Lem. 3.4}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) && \text{by Lem. 4.2} \end{aligned}$$

  Otherwise, if $S_{\Lambda'}(\mathsf{T}^c) = 0$, then $v^c = \Lambda(\mathsf{T}^c, \mathsf{A})$, and so:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) - v^c) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by [Rdm]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) + v) + (\Lambda(\mathsf{T}^c,\mathsf{A}) - v^c) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) && \text{by Lem. 4.2} \end{aligned}$$

- $\mathsf{swp}(v\colon \mathsf{T}', \mathsf{T})$. Let $v' = v \cdot {}^{\pi(\mathsf{T}')}/_{\pi(\mathsf{T})}$. We have that:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma, \mathsf{X}\ \mathsf{px}) &= \Big((\omega(\mathsf{T},\mathsf{A}) + v') + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by [Swp]}\\ &= \Big((\omega(\mathsf{T},\mathsf{A}) + v') + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta && \text{by Lem. 3.4}\\ &= \Big(\omega(\mathsf{T},\mathsf{A}) + \Lambda(\mathsf{T}^c,\mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d,\mathsf{A})\Big)\cdot\delta + v'\cdot\delta && \text{by arith.}\\ &= g_{\mathsf{A}}(\Gamma, \mathsf{px}) + v'\cdot\delta && \text{by Lem. 4.2} \end{aligned}$$

Since $v' > 0$, we have that $g_{\mathsf{A}}(\Gamma, \mathsf{X}\mathsf{px}) \circ g_{\mathsf{A}}(\Gamma, \mathsf{px})$ whenever $\delta \circ 0$ for $\circ \in \{<, >\}$.

- $\mathsf{swp}(v\colon \mathsf{T}, \mathsf{T}')$. Let $v' = v \cdot {}^{\pi(\mathsf{T})}\!/_{\pi(\mathsf{T}')}$. We have that:

$$\begin{aligned}
g_{\mathsf{A}}(\Gamma, \mathsf{X}\,\mathsf{px}) &= \Big((\omega(\mathsf{T}, \mathsf{A}) - v') + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda'}(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \delta && \text{by [Swp]} \\
&= \Big((\omega(\mathsf{T}, \mathsf{A}) - v') + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \delta && \text{by Lem. 3.4} \\
&= \Big(\omega(\mathsf{T}, \mathsf{A}) + \Lambda(\mathsf{T}^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \delta - v' \cdot \delta && \text{by arith.} \\
&= g_{\mathsf{A}}(\Gamma, \mathsf{px}) - v' \cdot \delta && \text{by Lem. 4.2}
\end{aligned}$$

Since $v' > 0$, we have that $g_{\mathsf{A}}(\Gamma, \mathsf{X}\mathsf{px}) \circ g_{\mathsf{A}}(\Gamma, \mathsf{px})$ whenever $0 \circ \delta$ for $\circ \in \{<, >\}$. □

Proof of Lemma 5.3. Let px be a shorthand for $\mathsf{px}(\delta\colon \mathsf{T}_1)$, with $\delta > 0$, and consider the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}\colon \mathsf{dep}(v_1\colon \mathsf{T}_1)\ \mathsf{A}\colon \mathsf{bor}(v_2\colon \mathsf{T}_2)\ \mathsf{A}\colon \mathsf{swp}(v_2\colon \mathsf{T}_2, \mathsf{T}_1)$$

For all Γ such that $\boldsymbol{\mathcal{X}}$ is enabled in Γ, we prove that:

$$g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}\,\mathsf{px}) > g_{\mathsf{A}}(\Gamma, \mathsf{px})$$

We start by giving names to the intermediate states reached during the execution of $\boldsymbol{\mathcal{X}}$. Let:

$$\begin{aligned}
\Gamma = (\omega_0, \Lambda_0, \pi) &\xrightarrow{\mathsf{A}:\mathsf{dep}(v_1:\mathsf{T}_1)} \Gamma_1 = (\omega_1, \Lambda_1, \pi) \\
&\xrightarrow{\mathsf{A}:\mathsf{bor}(v_2:\mathsf{T}_2)} \Gamma_2 = (\omega_2, \Lambda_2, \pi) \\
&\xrightarrow{\mathsf{A}:\mathsf{swp}(v_2:\mathsf{T}_2,\mathsf{T}_1)} \Gamma_3 = (\omega_3, \Lambda_3, \pi)
\end{aligned}$$

Let $v_1' = v_2 \cdot {}^{\pi(\mathsf{T}_2)}\!/_{\pi(\mathsf{T}_1)}$. By the rules [Dep], [Bor] and [Swp], we have that:

$$\omega_1 = \omega_0 - \{(\mathsf{T}_1, \mathsf{A}) \mapsto v_1\} \qquad \Lambda_1 = \Lambda_0 + \{\mathsf{T}_1 \mapsto v_1\} + \{(\mathsf{T}_1^c, \mathsf{A}) \mapsto {}^{v_1}\!/_{XR_{\Lambda_0}(\mathsf{T}_1)}\}$$

$$\omega_2 = \omega_1 + \{(\mathsf{T}_2, \mathsf{A}) \mapsto v_2\} \qquad \Lambda_2 = \Lambda_1 - \{\mathsf{T}_2 \mapsto v_2\} + \{(\mathsf{T}_2^d, \mathsf{A}) \mapsto v_2\}$$

$$\omega_3 = \omega_2 - \{(\mathsf{T}_2, \mathsf{A}) \mapsto v_2\} + \{(\mathsf{T}_1, \mathsf{A}) \mapsto v_1'\} \qquad \Lambda_3 = \Lambda_2$$

We then estimate A's gain as follows:

$$\begin{aligned}
g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}\,\mathsf{px}) &= g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) + g_{\mathsf{A}}(\Gamma_3, \mathsf{px}) && \text{by (4.1)} \\
&= g_{\mathsf{A}}(\Gamma_3, \mathsf{px}) && \text{by Lem. 4.1} \\
&= \Big(\omega_3(\mathsf{T}_1, \mathsf{A}) + \Lambda_3({\mathsf{T}_1}^c, \mathsf{A}) \cdot XR_{\Lambda_3}(\mathsf{T}_1) - \Lambda_3({\mathsf{T}_1}^d, \mathsf{A})\Big) \cdot \delta && \text{by Lem. 4.2} \\
&= \Big(\omega_3(\mathsf{T}_1, \mathsf{A}) + \Lambda_3({\mathsf{T}_1}^c, \mathsf{A}) \cdot XR_{\Lambda_0}(\mathsf{T}_1) - \Lambda_3({\mathsf{T}_1}^d, \mathsf{A})\Big) \cdot \delta && \text{by Lem. 3.4} \\
&= \Big((\omega_0(\mathsf{T}_1, \mathsf{A}) - v_1 + v_1') \\
&\quad + (\Lambda_0({\mathsf{T}_1}^c, \mathsf{A}) + {}^{v_1}\!/_{XR_{\Lambda_0}(\mathsf{T}_1)}) \cdot XR_{\Lambda_0}(\mathsf{T}_1) - \Lambda_3({\mathsf{T}_1}^d, \mathsf{A})\Big) \cdot \delta && \text{by [Dep,Bor,Swp]} \\
&= \Big((\omega_0(\mathsf{T}_1, \mathsf{A}) + v_1') + \Lambda_0({\mathsf{T}_1}^c, \mathsf{A}) \cdot XR_{\Lambda_0}(\mathsf{T}_1) - \Lambda_3({\mathsf{T}_1}^d, \mathsf{A})\Big) \cdot \delta && \text{by arith.} \\
&= g_{\mathsf{A}}(\Gamma, \mathsf{px}) + v_1' \cdot \delta
\end{aligned}$$

Therefore, $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}\,\mathsf{px}) - g_{\mathsf{A}}(\Gamma, \mathsf{px}) = v_1' \cdot \delta > 0$. □

Proof of Theorem 5.4. Let $\mathsf{X} = \mathsf{A}\colon \ell(\cdots)$ mentioning token T with transaction parameter v. We have to prove that:

(1) If we do not make assumptions on the interest rate function $I_\Lambda(\mathsf{T})$, then we have that, for every $\ell \in \{\mathsf{dep}, \mathsf{bor}, \mathsf{rep}, \mathsf{rdm}, \mathsf{liq}\}$ and for every $\circ \in \{>, =, <\}$, there exists Γ_0 and v such that $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int}) \circ g_\mathsf{A}(\Gamma_0, \mathsf{int})$.
(2) If we assume a constant interest rate function, i.e. $I_\Lambda(\mathsf{T}) = r_\mathsf{T}$, then:
   (a) $\ell \in \{\mathsf{dep}, \mathsf{rep}\} \implies$ for all Γ_0 and v, $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int}) \geq g_\mathsf{A}(\Gamma_0, \mathsf{int})$
   (b) $\ell \in \{\mathsf{bor}, \mathsf{rdm}\} \implies$ for all Γ_0 and v, $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int}) \leq g_\mathsf{A}(\Gamma_0, \mathsf{int})$
   (c) $\ell \in \{\mathsf{liq}\} \implies$ for all $\circ \in \{\geq, \leq\}$, there exists Γ_0 and v such that $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int}) \circ g_\mathsf{A}(\Gamma_0, \mathsf{int})$

In order to prove the theorem, we proceed as follows. We explicitly compute the formula of the gain for each $\ell \in \{\mathsf{dep}, \mathsf{bor}, \mathsf{rep}, \mathsf{rdm}, \mathsf{liq}\}$. We then directly prove points (2.a) and (2.b), i.e. we show that the inequalities for the cases in which $\ell \in \{\mathsf{dep}, \mathsf{rep}, \mathsf{bor}, \mathsf{rdm}\}$ and $I_\Lambda(\mathsf{T}) = r_\mathsf{T}$ hold; moreover, we precisely determinate when the inequalities are strict or not. To prove the rest of the theorem, have to provide a counter-examples for each case. A counter-example consists of an interest rate function $I_\Lambda(\mathsf{T})$, a reachable state Γ_0, and a choice of parameter v such that $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int}) \circ g_\mathsf{A}(\Gamma_0, \mathsf{int})$ (for $\circ$ being one of $\{>, =, <\}$). Note that the points (2.a) and (2.b) already gives us 8 counter-example (for $\ell \in \{\mathsf{dep}, \mathsf{rep}\}$ we have the cases $\circ \in \{>, =\}$, and for $\ell \in \{\mathsf{bor}, \mathsf{rdm}\}$ we have the cases $\circ \in \{<, =\}$). For the remaining 7 cases, in order not to overload the proof with simple yet long computations, we provide the following link to the counter-examples: `https://github.com/bitbart/lp-model/tree/main/examples-lmcs/frontrun-int`.

Let $\Gamma_0 \xrightarrow{\mathsf{int}} \Gamma_1$ and $\Gamma_0 \xrightarrow{\mathsf{X}} \Gamma'_0 \xrightarrow{\mathsf{int}} \Gamma'_1$, and assume that the states are deconstructed as follows:

$$\Gamma_0 = (\omega_0, \Lambda_0, \pi_0) \qquad \Gamma'_0 = (\omega'_0, \Lambda'_0, \pi'_0) \qquad \Gamma_1 = (\omega_1, \Lambda_1, \pi_1) \qquad \Gamma'_1 = (\omega'_1, \Lambda'_1, \pi'_1)$$

First, we note that, for every $\mathsf{T}' \neq \mathsf{T}$, $g_\mathsf{A}(\Gamma_0, \mathsf{int})\,|_{\mathsf{T}'} = g_\mathsf{A}(\Gamma_0, \mathsf{X\ int})\,|_{\mathsf{T}'}$. Hence we will focus only on $g_\mathsf{A}(\Gamma_0, \mathsf{int})\,|_\mathsf{T}$ and $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int})\,|_\mathsf{T}$.

By Lemma 4.3 we have that:

$$g_\mathsf{A}(\Gamma_0, \mathsf{int})\,|_\mathsf{T} = \begin{cases} \left(\Lambda_0(\mathsf{T}_i{}^c, \mathsf{A}) \cdot \dfrac{S_{\Lambda_0}(\mathsf{T}_i{}^d)}{S_{\Lambda_0}(\mathsf{T}_i{}^c)} - \Lambda_0(\mathsf{T}_i{}^d, \mathsf{A})\right) \cdot I_{\Lambda_0}(\mathsf{T}_i) \cdot \pi_0(\mathsf{T}_i) & \text{if } S_\Lambda(\mathsf{T}^c) > 0 \\ 0 & \text{otherwise} \end{cases}$$

We now compute A's net worth in Γ'_1. We proceed by cases on X.

- $\mathsf{A}\colon \mathsf{dep}(v\colon \mathsf{T})$. Note that we have that $S_{\Lambda'}(\mathsf{T}^c) > 0$, since a successful dep generates a positive amount of credits.

  We have that:

$$\begin{aligned} g_\mathsf{A}(\Gamma_0, \mathsf{X\ int})\,|_\mathsf{T} &= g_\mathsf{A}(\Gamma_0, \mathsf{X})\,|_\mathsf{T} + g_\mathsf{A}(\Gamma'_0, \mathsf{int})\,|_\mathsf{T} \\ &= 0 + \left(\Lambda'_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda'_0}(\mathsf{T}^d)}{S_{\Lambda'_0}(\mathsf{T}^c)} - \Lambda'_0(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi'_0\mathsf{T}\right) && (4.1 + 4.3) \\ &= \left(\left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) + v/_{XR_{\Lambda_0}(\mathsf{T})}\right) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c) + v/_{XR_{\Lambda_0}(\mathsf{T})}} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right) && \text{by [Dep]} \end{aligned}$$

  We have two cases, depending on whether $S_\Lambda(\mathsf{T}^c) = 0$ or not.

  If $S_\Lambda(\mathsf{T}^c) = 0$, we have that $g_\mathsf{A}(\Gamma_0, \mathsf{int}) = 0\,|_\mathsf{T}$, and, from Lemma 3.3, that $S_{\Lambda_0}(\mathsf{T}^d) = 0$ (and so also $\Lambda_0(\mathsf{T}^d, \mathsf{A}) = 0$). Hence we obtain that also $g_\mathsf{A}(\Gamma_0, \mathsf{X\ int})\,|_\mathsf{T} = 0$.

Otherwise, we have that:

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = \left(\left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) + v/_{XR_{\Lambda_0}(\mathsf{T})}\right) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c) + v/_{XR_{\Lambda_0}(\mathsf{T})}} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda'_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}$$
$$- \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c)} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}$$

If we consider a constant interest rate, i.e. $I_{\Lambda'_0}(\mathsf{T}) = I_{\Lambda_0}(\mathsf{T})$, then

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = S_{\Lambda_0}(\mathsf{T}^d) \cdot \left(\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A}) + v/_{XR_{\Lambda_0}(\mathsf{T})}}{S_{\Lambda_0}(\mathsf{T}^c) + v/_{XR_{\Lambda_0}(\mathsf{T})}} - \frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)}\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}$$

This amount is positive, and it is equal to zero if and only if $S_{\Lambda_0}(\mathsf{T}^d) = 0$. Indeed, $I_{\Lambda_0}(\mathsf{T}) > 0$ and $\pi_0\mathsf{T} > 0$ by definition, and $\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A}) + v/_{XR_{\Lambda_0}(\mathsf{T})}}{S_{\Lambda_0}(\mathsf{T}^c) + v/_{XR_{\Lambda_0}(\mathsf{T})}} - \frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)} > 0$ follows from the simple mathematical fact that, given $A, B \in \mathbb{R}_{\geq 0}$ with $A < B$, and $C \in \mathbb{R}_{>0}$, then $\frac{A+C}{B+C} > \frac{A}{B}$.

- $\mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T})$. Note that a bor can only be fired if the reserves are non-zero, i.e. $\Lambda(\mathsf{T}) > 0$. By Lemma 3.3, this implies that $S_{\Lambda}(\mathsf{T}^c) > 0$. Moreover, after a successful bor, we have $S_{\Lambda'}(\mathsf{T}^d) > 0$. By Lemma 3.3, this implies that $S_{\Lambda'}(\mathsf{T}^c) > 0$.

  We have that:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} &= g_{\mathsf{A}}(\Gamma_0, \mathsf{X})|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma'_0, \mathsf{int})|_{\mathsf{T}} \\ &= 0 + \left(\Lambda'_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda'_0}(\mathsf{T}^d)}{S_{\Lambda'_0}(\mathsf{T}^c)} - \Lambda'_0(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi'_0\mathsf{T}\right) \qquad (4.1 + 4.3) \\ &= \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d) + v}{S_{\Lambda_0}(\mathsf{T}^c)} - \left(\Lambda_0(\mathsf{T}^d, \mathsf{A}) + v\right)\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right) \quad \text{by [Bor]} \end{aligned}$$

  Hence we have that

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d) + v}{S_{\Lambda_0}(\mathsf{T}^c)} - \left(\Lambda_0(\mathsf{T}^d, \mathsf{A}) + v\right)\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right)$$
$$- \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c)} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}$$

  If we consider a constant interest rate, i.e. $I_{\Lambda'_0}(\mathsf{T}) = I_{\Lambda_0}(\mathsf{T})$, then

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = v \cdot \left(\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)} - 1\right) \cdot \left(I_{\Lambda'_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right)$$

  which is ≤ 0, since $\Lambda_0(\mathsf{T}^c, \mathsf{A}) \leq S_{\Lambda_0}(\mathsf{T}^c)$.

- $\mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$. Note that a rep can only be fired if the exist some debts, i.e. $S_\Lambda(\mathsf{T}^d) > 0$, which, by Lemma 3.3, implies $S_\Lambda(\mathsf{T}^c) > 0$. Moreover, since rep does not impact credits, we have that $S_{\Lambda'}(\mathsf{T}^c) = S_\Lambda(\mathsf{T}^c) > 0$.

  We have that:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} &= g_{\mathsf{A}}(\Gamma_0, \mathsf{X})|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma_0', \mathsf{int})|_{\mathsf{T}} \\ &= 0 + \left(\Lambda_0'(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0'}(\mathsf{T}^d)}{S_{\Lambda_0'}(\mathsf{T}^c)} - \Lambda_0'(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0'\mathsf{T}\right) \qquad (4.1 + 4.3) \\ &= \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d) - v}{S_{\Lambda_0}(\mathsf{T}^c)} - \left(\Lambda_0(\mathsf{T}^d, \mathsf{A}) - v\right)\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right) \quad \text{by [Rep]} \end{aligned}$$

  Hence we have that

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} &= \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d) - v}{S_{\Lambda_0}(\mathsf{T}^c)} - \left(\Lambda_0(\mathsf{T}^d, \mathsf{A}) - v\right)\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right) \\ &\quad - \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c)} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T} \end{aligned}$$

  If we consider a constant interest rate, i.e. $I_{\Lambda_0'}(\mathsf{T}) = I_{\Lambda_0}(\mathsf{T})$, then

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = -v \cdot \left(\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)} - 1\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right)$$

  which is ≥ 0, since $\Lambda_0(\mathsf{T}^c, \mathsf{A}) \leq S_{\Lambda_0}(\mathsf{T}^c)$.

- $\mathsf{A}\colon \mathsf{rdm}(v\colon \mathsf{T})$. Note that a rdm can only be fired if the credits are non-zero, i.e. $S_\Lambda(\mathsf{T}^c) > 0$. There are two cases.

  In the first case, A redeems all the T-credits available in the lending pool. Then, $S_{\Lambda'}(\mathsf{T}^c) = 0$, and hence, by Lemma 3.3, also $S_{\Lambda'}(\mathsf{T}^d) = 0$. Since rdm does not affect debts, this implies that also $S_\Lambda(\mathsf{T}^d) = 0$. Hence we have that

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} &= g_{\mathsf{A}}(\Gamma_0, \mathsf{X})|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma_0', \mathsf{int})|_{\mathsf{T}} \\ &= 0 + 0 \qquad (4.1 + 4.3) \end{aligned}$$

  which implies that $g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} \leq 0$, since $g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} \geq 0$ (recall that, by hypothesis, $S_\Lambda(\mathsf{T}^d) = 0$).

  In the second case, A does not redeem all the T-credits available in the lending pool, i.e. $S_{\Lambda'}(\mathsf{T}^c) > 0$.

We have that:

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} &= g_{\mathsf{A}}(\Gamma_0, \mathsf{X})|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma_0', \mathsf{int})|_{\mathsf{T}} \\ &= 0 + \left(\Lambda_0'(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0'}(\mathsf{T}^d)}{S_{\Lambda_0'}(\mathsf{T}^c)} - \Lambda_0'(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0'\mathsf{T}\right) \qquad (4.1 + 4.3) \\ &= \left(\left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) - v/_{XR_{\Lambda_0}(\mathsf{T})}\right) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c) - v/_{XR_{\Lambda_0}(\mathsf{T})}} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot \left(I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0\mathsf{T}\right) \quad \text{by [Dep]} \end{aligned}$$

and hence

$$\begin{aligned} g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} &= \left(\left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) - v/_{XR_{\Lambda_0}(\mathsf{T})}\right) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c) - v/_{XR_{\Lambda_0}(\mathsf{T})}} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_0'}(\mathsf{T}) \cdot \pi_0\mathsf{T} \\ &\quad - \left(\Lambda_0(\mathsf{T}^c, \mathsf{A}) \cdot \frac{S_{\Lambda_0}(\mathsf{T}^d)}{S_{\Lambda_0}(\mathsf{T}^c)} - \Lambda_0(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T} \end{aligned}$$

If we consider a constant interest rate, i.e. $I_{\Lambda_0'}(\mathsf{T}) = I_{\Lambda_0}(\mathsf{T})$, then

$$g_{\mathsf{A}}(\Gamma_0, \mathsf{X}\ \mathsf{int})|_{\mathsf{T}} - g_{\mathsf{A}}(\Gamma_0, \mathsf{int})|_{\mathsf{T}} = S_{\Lambda_0}(\mathsf{T}^d) \cdot \left(\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A}) - v/_{XR_{\Lambda_0}(\mathsf{T})}}{S_{\Lambda_0}(\mathsf{T}^c) - v/_{XR_{\Lambda_0}(\mathsf{T})}} - \frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)}\right) \cdot I_{\Lambda_0}(\mathsf{T}) \cdot \pi_0\mathsf{T}$$

This amount is negative, and it is equal to zero if and only if $S_{\Lambda_0}(\mathsf{T}^d) = 0$. Indeed, $I_{\Lambda_0}(\mathsf{T}) > 0$ and $\pi_0\mathsf{T} > 0$ by definition, and $\frac{\Lambda_0(\mathsf{T}^c, \mathsf{A}) - v/_{XR_{\Lambda_0}(\mathsf{T})}}{S_{\Lambda_0}(\mathsf{T}^c) - v/_{XR_{\Lambda_0}(\mathsf{T})}} - \frac{\Lambda_0(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_0}(\mathsf{T}^c)} < 0$ follows from the simple mathematical fact that, given $A, B \in \mathbb{R}_{\geq 0}$ with $A < B$, and $C \in \mathbb{R}_{>0}$, then $\frac{A-C}{B-C} < \frac{A}{B}$.

Appendix D. Proofs for Section 6

Proof of Theorem 6.1. Let $\Gamma = (\omega, \Lambda, \pi)$, and assume that A has no credits or debts with the LP, i.e., $W_\Gamma^c(\mathsf{A}) = W_\Gamma^d(\mathsf{A}) = 0$. Consider the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}{:}\,\mathsf{dep}(v_1{:}\,\mathsf{T}_1)\ \ \mathsf{px}(-\delta{:}\,\mathsf{T}_2)\ \ \mathsf{A}{:}\,\mathsf{bor}(v_2{:}\,\mathsf{T}_2)\ \ \mathsf{px}(\delta{:}\,\mathsf{T}_2)$$

where $0 < \delta < \pi(\mathsf{T}_2)$ and $v_2 = \frac{v_1}{XR_\Lambda(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_1)}{\pi(\mathsf{T}_2) - \delta} \cdot T_{\mathsf{liq}}$. We have to prove that:

(1) $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) = 0$

(2) $W_{\Gamma'}^{c-d}(\mathsf{A}) < 0$ if $\Gamma \xrightarrow{\boldsymbol{\mathcal{X}}} \Gamma'$.

To prove Item (1), consider the sequence of transitions:

$$\Gamma \xrightarrow{\mathsf{X}_1 = \mathsf{A}:\mathsf{dep}(v_1:\mathsf{T}_1)} \Gamma_1 \xrightarrow{\mathsf{X}_2 = \mathsf{px}(-\delta:\mathsf{T}_2)} \Gamma_2 \xrightarrow{\mathsf{X}_3 = \mathsf{A}:\mathsf{bor}(v_2:\mathsf{T}_2)} \Gamma_3 \xrightarrow{\mathsf{X}_4 = \mathsf{px}(\delta:\mathsf{T}_2)} \Gamma'$$

Note that if X_1 is not enabled in Γ, then by the hypothesis that A has no credits in Γ then also X_3 will not be enabled, and so $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) = 0$. Otherwise, if X_1 is enabled in Γ but X_3 is not

enabled in Γ_2, then the effects of X_2 and X_4 cancel out, and then $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) = g_{\mathsf{A}}(\Gamma, \mathsf{X}_1) = 0$ by Lemma 4.1. Finally, in case all the transactions in $\boldsymbol{\mathcal{X}}$ are enabled, we have that:

$$
\begin{aligned}
g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) &= g_{\mathsf{A}}(\Gamma, \mathsf{X}_1) + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2) + g_{\mathsf{A}}(\Gamma_2, \mathsf{X}_3) + g_{\mathsf{A}}(\Gamma_3, \mathsf{X}_4) && \text{by (4.1)}\\
&= g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2) + g_{\mathsf{A}}(\Gamma_3, \mathsf{X}_4) && \text{by Lem. 4.1}\\
&= W_{\Gamma_1}(\mathsf{A})|_{\mathsf{T}_2} \cdot \frac{-\delta}{\pi(\mathsf{T}_2)} + W_{\Gamma_3}(\mathsf{A})|_{\mathsf{T}_2} \cdot \frac{\delta}{\pi(\mathsf{T}_2) - \delta} && \text{by Lem 4.2}\\
&= \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot -\delta\\
&+ \Big(\omega_3(\mathsf{T}_2, \mathsf{A}) + \Lambda_3(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_3}(\mathsf{T}_2) - \Lambda_3(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot \delta && \text{by (2.8)}\\
&= \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot -\delta\\
&+ \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + v_2 + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_3}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A}) - v_2\Big) \cdot \delta && \text{by [Bor]}\\
&= \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot -\delta\\
&+ \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_3}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot \delta && \text{by arith.}\\
&= \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot -\delta\\
&+ \Big(\omega_1(\mathsf{T}_2, \mathsf{A}) + \Lambda_1(\mathsf{T}_2^c, \mathsf{A}) \cdot XR_{\Lambda_1}(\mathsf{T}_2) - \Lambda_1(\mathsf{T}_2^d, \mathsf{A})\Big) \cdot \delta && \text{by Lem. 3.4}\\
&= 0 && \text{by arith.}
\end{aligned}
$$

To prove Item (2), observe that since by hypothesis $W_\Gamma^c(\mathsf{A}) = W_\Gamma^d(\mathsf{A}) = 0$, then in Γ' we have that:

$$
\begin{aligned}
W_{\Gamma'}^c(\mathsf{A}) &= \frac{v_1}{XR_\Lambda(\mathsf{T}_1)} \cdot \pi(\mathsf{T}_1)\\
W_{\Gamma'}^d(\mathsf{A}) &= v_2 \cdot \pi(\mathsf{T}_2) = \frac{v_1}{XR_\Lambda(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_1)}{\pi(\mathsf{T}_2) - \delta} \cdot T_{\mathsf{liq}} \cdot \pi(\mathsf{T}_2)
\end{aligned}
$$

Therefore:

$$
W_{\Gamma'}^{c-d}(\mathsf{A}) = W_{\Gamma'}^c(\mathsf{A}) - W_{\Gamma'}^d(\mathsf{A}) = \frac{v_1}{XR_\Lambda(\mathsf{T}_1)} \cdot \pi(\mathsf{T}_1) \cdot \Big(1 - \frac{T_{\mathsf{liq}} \cdot \pi(\mathsf{T}_2)}{\pi(\mathsf{T}_2) - \delta}\Big)
$$

This amount is negative if and only if

$$
\frac{T_{\mathsf{liq}} \cdot \pi(\mathsf{T}_2)}{\pi(\mathsf{T}_2) - \delta} > 1
$$

or, equivalently, since $0 < \delta < \pi(\mathsf{T}_2)$:

$$
\delta > \pi(\mathsf{T}_2) \cdot \Big(1 - T_{\mathsf{liq}}\Big)
$$

□

Proof of Theorem 6.2. Let $\Gamma = (\omega, \Lambda, \pi)$ and let A and B such that:

(1) $\Lambda(\mathsf{T}_1^c, \mathsf{B}) = v_c$, and $\Lambda(\mathsf{T}^c, \mathsf{B}) = 0$ for all $\mathsf{T} \neq \mathsf{T}_1$ (i.e. the collateral of B relies on a single token type T_1)
(2) $\Lambda(\mathsf{T}_2^d, \mathsf{B}) = v_d$, and $\Lambda(\mathsf{T}^d, \mathsf{B}) = 0$ for all $\mathsf{T} \neq \mathsf{T}_2$ (i.e. B has debts only in T_2)
(3) $\omega(\mathsf{T}_2, \mathsf{A}) > 0$
(4) $H_\Gamma(\mathsf{B}) \geq 1$ (i.e. B cannot be liquidated in Γ)

Then, for every $\delta > 0$ sufficiently small, and for every $v_l > 0$ such that $v_l \leq \omega(\mathsf{T}_2, \mathsf{A})$, $v_l \leq v_d$ and $v_l < v_c \cdot \frac{XR_\Lambda(\mathsf{T}_1)}{R_{\mathsf{liq}}} \cdot \frac{\delta}{\pi(\mathsf{T}_2)}$, given the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{px}((-\pi(\mathsf{T}_1)+\delta)\colon \mathsf{T}_1)\;\; \mathsf{A}\colon \mathsf{liq}(\mathsf{B}, v_l\colon \mathsf{T}_2, \mathsf{T}_1^c)\;\; \mathsf{px}((\pi(\mathsf{T}_1)-\delta)\colon \mathsf{T}_1)$$

it holds that:

(1) $\boldsymbol{\mathcal{X}}$ is enabled in Γ
(2) $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) > 0$

We start by giving names to the intermediate states reached during the execution of $\boldsymbol{\mathcal{X}}$:

$$\begin{aligned}
\Gamma = (\omega, \Lambda, \pi) &\xrightarrow{\mathsf{X}_1 = \mathsf{px}((-\pi(\mathsf{T}_1)+\delta):\mathsf{T}_1)} \Gamma_1 = (\omega_1, \Lambda_1, \pi_1) && \omega_1 = \omega, \Lambda_1 = \Lambda \\
&\xrightarrow{\mathsf{X}_2 = \mathsf{A}:\mathsf{liq}(\mathsf{B}, v_l:\mathsf{T}_2, \mathsf{T}_1^c)} \Gamma_2 = (\omega_2, \Lambda_2, \pi_2) && \pi_2 = \pi_1 \\
&\xrightarrow{\mathsf{X}_3 = \mathsf{px}((\pi(\mathsf{T}_1)-\delta):\mathsf{T}_1)} \Gamma_3 = (\omega_3, \Lambda_3, \pi_3) && \omega_3 = \omega_2, \Lambda_3 = \Lambda_2
\end{aligned}$$

We first prove Item (1). Of course, both price updates are enabled whenever $\delta > 0$, so in order to prove that $\boldsymbol{\mathcal{X}}$ is enabled in Γ we only need to prove that the liquidation is enabled in Γ_1. We check that all the premises of [Liq] hold:

- $\omega_1(\mathsf{T}_2, \mathsf{A}) \geq v_l > 0$ is given by the conditions on v_l
- $\Lambda_1(\mathsf{T}_2^d, \mathsf{B}) \geq v_l$ is given by the conditions on v_l
- $\Lambda_1(\mathsf{T}_1^c, \mathsf{B}) \geq \frac{v_l}{XR_{\Lambda_1}(\mathsf{T}_1)} \cdot \frac{\pi_1(\mathsf{T}_2)}{\pi_1(\mathsf{T}_1)} \cdot R_{\mathsf{liq}}$ is given by the fact that $\pi_1(\mathsf{T}_2) = \delta$, $\pi_1(\mathsf{T}_1) = \pi(\mathsf{T}_1)$, and $v_l < v_c \cdot \frac{XR_\Lambda(\mathsf{T}_1)}{R_{\mathsf{liq}}} \cdot \frac{\delta}{\pi(\mathsf{T}_2)}$.
- $H_{\Gamma_1}(\mathsf{B}) < 1$ is given by the fact that
$$H_{\Gamma_1}(\mathsf{B}) = \frac{v_c \cdot \pi_1(\mathsf{T}_1)}{v_d \cdot \pi_1(\mathsf{T}_2)} \cdot R_{\mathsf{liq}} = \frac{v_c \cdot \delta}{v_d \cdot \pi(\mathsf{T}_2)} \cdot R_{\mathsf{liq}}$$
which, for δ sufficiently small, is strictly less than 1.
- $H_{\Gamma_2}(\mathsf{B}) \leq 1$ is given by the fact that
$$\begin{aligned}
H_{\Gamma_2}(\mathsf{B}) &= \frac{\left(v_c - \frac{v_l}{XR_{\Lambda_1}(\mathsf{T}_1)} \cdot \frac{\pi_1(\mathsf{T}_2)}{\pi_1(\mathsf{T}_1)} \cdot R_{\mathsf{liq}}\right) \cdot \pi_1(\mathsf{T}_1)}{(v_d - v_l) \cdot \pi_1(\mathsf{T}_2)} \cdot R_{\mathsf{liq}} && \text{by [Liq]} \\
&= \frac{\left(v_c - \frac{v_l}{XR_{\Lambda}(\mathsf{T}_1)} \cdot \frac{\pi(\mathsf{T}_2)}{\delta} \cdot R_{\mathsf{liq}}\right) \cdot \delta}{(v_d - v_l) \cdot \pi(\mathsf{T}_2)} \cdot R_{\mathsf{liq}} && \text{by Lem. 3.4} \\
&= \frac{v_c \cdot \delta - \frac{v_l}{XR_{\Lambda}(\mathsf{T}_1)} \cdot \pi(\mathsf{T}_2) \cdot R_{\mathsf{liq}}}{(v_d - v_l) \cdot \pi(\mathsf{T}_2)} \cdot R_{\mathsf{liq}} && \text{by arith.}
\end{aligned}$$
which, for δ sufficiently small, is less or equal to 1 (note that δ bounds v_l).

We now prove Item (2). Since by the previous point all transactions are enabled, we have that:

$$
\begin{aligned}
g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) &= g_{\mathsf{A}}(\Gamma, \mathsf{X}_1) + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2) + g_{\mathsf{A}}(\Gamma_2, \mathsf{X}_3) && \text{by (4.1)}\\
&= W_{\Gamma}(\mathsf{A})|_{\mathsf{T}_1} \cdot \frac{-\pi(\mathsf{T}_1) + \delta}{\pi(\mathsf{T}_1)} + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2) + W_{\Gamma_2}(\mathsf{A})|_{\mathsf{T}_1} \cdot \frac{\pi(\mathsf{T}_1) - \delta}{\delta} && \text{by Lem. 4.2}\\
&= \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (-\pi(\mathsf{T}_1) + \delta)\\
&\quad + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)\\
&\quad + \Big(\omega_2(\mathsf{T}_1, \mathsf{A}) + \Lambda_2(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda_2}(\mathsf{T}_1) - \Lambda_2(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (\pi(\mathsf{T}_1) - \delta) && \text{by (2.8)}\\
&> \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (-\pi(\mathsf{T}_1) + \delta)\\
&\quad + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)\\
&\quad + \Big(\omega_1(\mathsf{T}_1, \mathsf{A}) + \Lambda_1(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda_2}(\mathsf{T}_1) - \Lambda_1(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (\pi(\mathsf{T}_1) - \delta) && \text{by [Liq]}\\
&= \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (-\pi(\mathsf{T}_1) + \delta)\\
&\quad + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)\\
&\quad + \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda_2}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (\pi(\mathsf{T}_1) - \delta) && \text{by [Px]}\\
&= \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (-\pi(\mathsf{T}_1) + \delta)\\
&\quad + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)\\
&\quad + \Big(\omega(\mathsf{T}_1, \mathsf{A}) + \Lambda(\mathsf{T}_1^c, \mathsf{A}) \cdot XR_{\Lambda}(\mathsf{T}_1) - \Lambda(\mathsf{T}_1^d, \mathsf{A})\Big) \cdot (\pi(\mathsf{T}_1) - \delta) && \text{by Lem. 3.4}\\
&= g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2) && \text{by arith.}\\
&> 0 && \text{by Lem. 4.1}
\end{aligned}
$$

□

Proof of Theorem 6.3. Let $\Gamma = (\omega, \Lambda, \pi)$, and let A, B and T be such that:
(1) $\Lambda(\mathsf{T}^c, \mathsf{A}) = 0$ and
(2) $\Lambda(\mathsf{T}^c, \mathsf{B}) > 0$ and $\Lambda(\mathsf{T}^d, \mathsf{B}) = 0$
Then, let $\boldsymbol{\mathcal{X}}$ be the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}{:}\,\mathsf{dep}(v{:}\,\mathsf{T}) \;\; \mathsf{int} \;\; \mathsf{A}{:}\,\mathsf{rdm}(v^c{:}\,\mathsf{T})$$

where v^c is the amount of credits held by A in the intermediate state before rdm.

Assuming $\boldsymbol{\mathcal{X}}$ is enabled in Γ, and that the lending protocol uses the linear utility interest rate function in (2.15) with $\alpha > 0$, we have to prove that:

- $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}}) > g_{\mathsf{A}}(\Gamma, \mathsf{int})$,
- $g_{\mathsf{B}}(\Gamma, \boldsymbol{\mathcal{X}}) < g_{\mathsf{B}}(\Gamma, \mathsf{int})$

We start by giving names to the intermediate states reached during the execution of $\boldsymbol{\mathcal{X}}$:

$$\begin{aligned}\Gamma = (\omega, \Lambda, \pi) &\xrightarrow{\mathsf{X}_1 = \mathsf{A}:\mathsf{dep}(v:\mathsf{T})} \Gamma_1 = (\omega_1, \Lambda_1, \pi)\\ &\xrightarrow{\mathsf{X}_2 = \mathsf{int}} \Gamma_2 = (\omega_2, \Lambda_2, \pi)\\ &\xrightarrow{\mathsf{X}_3 = \mathsf{A}:\mathsf{rdm}(v^c:\mathsf{T})} \Gamma_3 = (\omega_3, \Lambda_3, \pi)\end{aligned}$$

First note that, for every $\mathsf{T}' \neq \mathsf{T}$, it trivially holds that $g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}})\,|_{\mathsf{T}'} = g_{\mathsf{A}}(\Gamma, \mathsf{int})\,|_{\mathsf{T}'}$ and $g_{\mathsf{B}}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}'} = g_{\mathsf{B}}(\Gamma, \mathsf{int})|_{\mathsf{T}'}$. Hence, we only focus on the gains restricted to T.

By hypothesis, we have that $S_\Lambda(\mathsf{T}^c) > 0$ and $S_\Lambda(\mathsf{T}^d) > 0$. Since dep does not decrease the supply of credits nor that of debts, we also have that $S_{\Lambda_1}(\mathsf{T}^c) > 0$ and $S_{\Lambda_1}(\mathsf{T}^d) > 0$. Moreover, since $\Lambda(\mathsf{T}^d, \mathsf{B}) = 0$ and the deposit fired by A does not impact the credits of B, we also have $\Lambda_1(\mathsf{T}^d, \mathsf{B}) = 0$

The gain of A is given by:

$$\begin{aligned}
g_{\mathsf{A}}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}} &= g_{\mathsf{A}}(\Gamma, \mathsf{X}_1)|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + g_{\mathsf{A}}(\Gamma_2, \mathsf{X}_3)|_{\mathsf{T}} && \text{by (4.1)}\\
&= 0 + g_{\mathsf{A}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + 0 && \text{by Lem. 4.1}\\
&= \left(\frac{\Lambda_1(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_1}(\mathsf{T}^c)} \cdot S_{\Lambda_1}(\mathsf{T}^d) - \Lambda_1(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by Lem. 4.3}\\
&= \left(\frac{\Lambda(\mathsf{T}^c, \mathsf{A}) + v/_{XR_\Lambda(\mathsf{T})}}{S_\Lambda(\mathsf{T}^c) + v/_{XR_\Lambda(\mathsf{T})}} \cdot S_\Lambda(\mathsf{T}^d) - \Lambda(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by [Dep]}\\
&= \left(\frac{v/_{XR_\Lambda(\mathsf{T})}}{S_\Lambda(\mathsf{T}^c) + v/_{XR_\Lambda(\mathsf{T})}} \cdot S_\Lambda(\mathsf{T}^d) - \Lambda(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by hyp.}\\
&> -\Lambda(\mathsf{T}^d, \mathsf{A}) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by arith.}\\
&= -\Lambda(\mathsf{T}^d, \mathsf{A}) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d)}{(\Lambda(\mathsf{T}) + v) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by (2.15) + [Dep]}\\
&> -\Lambda(\mathsf{T}^d, \mathsf{A}) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d)}{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by arith.}\\
&= g_{\mathsf{A}}(\Gamma, \mathsf{int})|_{\mathsf{T}} && \text{Lem. 4.3 + hyp.}
\end{aligned}$$

The gain of B is given by:

$$\begin{aligned}
g_{\mathsf{B}}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}} &= g_{\mathsf{B}}(\Gamma, \mathsf{X}_1)|_{\mathsf{T}} + g_{\mathsf{B}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + g_{\mathsf{B}}(\Gamma_2, \mathsf{X}_3)|_{\mathsf{T}} && \text{by (4.1)}\\
&= 0 + g_{\mathsf{B}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + 0 && \text{by Lem. 4.1}\\
&= \left(\frac{\Lambda_1(\mathsf{T}^c, \mathsf{B})}{S_{\Lambda_1}(\mathsf{T}^c)} \cdot S_{\Lambda_1}(\mathsf{T}^d) - \Lambda_1(\mathsf{T}^d, \mathsf{B})\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by Lem. 4.3}\\
&= \frac{\Lambda_1(\mathsf{T}^c, \mathsf{B})}{S_{\Lambda_1}(\mathsf{T}^c)} \cdot S_{\Lambda_1}(\mathsf{T}^d) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by hyp.}\\
&= \frac{\Lambda(\mathsf{T}^c, \mathsf{B})}{S_\Lambda(\mathsf{T}^c) + v/_{XR_\Lambda(\mathsf{T})}} \cdot S_\Lambda(\mathsf{T}^d) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d)}{(\Lambda(\mathsf{T}) + v) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by [Dep]}\\
&< \frac{\Lambda(\mathsf{T}^c, \mathsf{B})}{S_\Lambda(\mathsf{T}^c)} \cdot S_\Lambda(\mathsf{T}^d) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d)}{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by arith}\\
&= g_{\mathsf{B}}(\Gamma, \mathsf{int})|_{\mathsf{T}} && \text{by Lem. 4.3}
\end{aligned}$$

□

Proof of Theorem 6.4. Let $\Gamma = (\omega, \Lambda, \pi)$, and let A, B and T be such that:
(1) $\Lambda(\mathsf{T}^c, \mathsf{A}) = S_\Lambda(\mathsf{T}^c)$ and $\Lambda(\mathsf{T}^d, \mathsf{A}) < S_\Lambda(\mathsf{T}^d)$
(2) $\Lambda(\mathsf{T}^d, \mathsf{B}) > 0$
Then, let the following sequence of transactions:

$$\boldsymbol{\mathcal{X}} \;=\; \mathsf{A}\colon \mathsf{bor}(v\colon \mathsf{T}) \;\; \mathsf{int} \;\; \mathsf{A}\colon \mathsf{rep}(v\colon \mathsf{T})$$

be enabled in Γ. If $I_\Lambda(\mathsf{T})$ is a linear utility interest rate function with $\alpha > 0$, then:
- $g_\mathsf{A}(\Gamma, \boldsymbol{\mathcal{X}}) > g_\mathsf{A}(\Gamma, \mathsf{int})$,
- $g_\mathsf{B}(\Gamma, \boldsymbol{\mathcal{X}}) < g_\mathsf{B}(\Gamma, \mathsf{int})$

We start by giving names to the intermediate states reached during the execution of $\boldsymbol{\mathcal{X}}$:

$$\begin{aligned}\Gamma = (\omega, \Lambda, \pi) &\xrightarrow{\mathsf{X}_1 = \mathsf{A}:\mathsf{bor}(v:\mathsf{T})} \Gamma_1 = (\omega_1, \Lambda_1, \pi)\\ &\xrightarrow{\mathsf{X}_2 = \mathsf{int}} \Gamma_2 = (\omega_2, \Lambda_2, \pi)\\ &\xrightarrow{\mathsf{X}_3 = \mathsf{A}:\mathsf{rep}(v:\mathsf{T})} \Gamma_3 = (\omega_3, \Lambda_3, \pi)\end{aligned}$$

First note that, for every $\mathsf{T}' \neq \mathsf{T}$, it trivially holds that $g_\mathsf{A}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}'} = g_\mathsf{A}(\Gamma, \mathsf{int})|_{\mathsf{T}'}$ and $g_\mathsf{B}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}'} = g_\mathsf{B}(\Gamma, \mathsf{int})|_{\mathsf{T}'}$. Hence, we only focus on the gains restricted to T.

By hypothesis, we have that $S_\Lambda(\mathsf{T}^d) > 0$, and, by Lemma 3.3, also $S_\Lambda(\mathsf{T}^c) > 0$. Since bor does not decrease the supply of credits nor that of debit tokens, we also have that $S_{\Lambda_1}(\mathsf{T}^c) > 0$ and $S_{\Lambda_1}(\mathsf{T}^d) > 0$.

The gain of A is given by:

$$\begin{aligned}
g_\mathsf{A}(\Gamma, \boldsymbol{\mathcal{X}})|_\mathsf{T} &= g_\mathsf{A}(\Gamma, \mathsf{X}_1)|_\mathsf{T} + g_\mathsf{A}(\Gamma_1, \mathsf{X}_2)|_\mathsf{T} + g_\mathsf{A}(\Gamma_2, \mathsf{X}_3)|_\mathsf{T} && \text{by (4.1)}\\
&= 0 + g_\mathsf{A}(\Gamma_1, \mathsf{X}_2)|_\mathsf{T} + 0 && \text{by Lem. 4.1}\\
&= \left(\frac{\Lambda_1(\mathsf{T}^c, \mathsf{A})}{S_{\Lambda_1}(\mathsf{T}^c)} \cdot S_{\Lambda_1}(\mathsf{T}^d) - \Lambda_1(\mathsf{T}^d, \mathsf{A})\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by Lem. 4.3}\\
&= \left(\frac{\Lambda(\mathsf{T}^c, \mathsf{A})}{S_\Lambda(\mathsf{T}^c)} \cdot \Big(S_\Lambda(\mathsf{T}^d) + v\Big) - \Big(\Lambda(\mathsf{T}^d, \mathsf{A}) + v\Big)\right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by [BOR]}\\
&= \Big(S_\Lambda(\mathsf{T}^d) + v - \Lambda(\mathsf{T}^d, \mathsf{A}) - v\Big) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d) + v}{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by hyp.}\\
&> \Big(S_\Lambda(\mathsf{T}^d) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot \left(\alpha \cdot \frac{S_\Lambda(\mathsf{T}^d)}{\Lambda(\mathsf{T}) + S_\Lambda(\mathsf{T}^d)} + \beta\right) \cdot \pi(\mathsf{T}) && \text{by arith.}\\
&= \Big(S_\Lambda(\mathsf{T}^d) - \Lambda(\mathsf{T}^d, \mathsf{A})\Big) \cdot I_\Lambda(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by (2.15)}\\
&= g_\mathsf{A}(\Gamma, \mathsf{int})|_\mathsf{T} && \text{Lem. 4.3 + hyp.}
\end{aligned}$$

Note that the hypothesis that $S_\Lambda(\mathsf{T}^d) > \Lambda(\mathsf{T}^d, \mathsf{A})$ is necessary to show the strict inequality. Otherwise, we would have $g_\mathsf{A}(\Gamma, \boldsymbol{\mathcal{X}})|_\mathsf{T} = 0 = g_\mathsf{A}(\Gamma, \mathsf{int})|_\mathsf{T}$.

We now compute the gain of B. Note that, since by hypothesis $\Lambda(\mathsf{T}^c, \mathsf{A}) = S_\Lambda(\mathsf{T}^c)$, then $\Lambda(\mathsf{T}^c, \mathsf{B}) = 0$, and, since the borrow fired by A does not affect the credits of B, then we also

have $\Lambda_1(\mathsf{T}^c, \mathsf{B}) = 0$. The gain:

$$
\begin{aligned}
g_{\mathsf{B}}(\Gamma, \boldsymbol{\mathcal{X}})|_{\mathsf{T}} &= g_{\mathsf{B}}(\Gamma, \mathsf{X}_1)|_{\mathsf{T}} + g_{\mathsf{B}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + g_{\mathsf{B}}(\Gamma_2, \mathsf{X}_3)|_{\mathsf{T}} && \text{by (4.1)} \\
&= 0 + g_{\mathsf{B}}(\Gamma_1, \mathsf{X}_2)|_{\mathsf{T}} + 0 && \text{by Lem. 4.1} \\
&= \left(\frac{\Lambda_1(\mathsf{T}^c, \mathsf{B})}{S_{\Lambda_1}(\mathsf{T}^c)} \cdot S_{\Lambda_1}(\mathsf{T}^d) - \Lambda_1(\mathsf{T}^d, \mathsf{B}) \right) \cdot I_{\Lambda_1}(\mathsf{T}) \cdot \pi(\mathsf{T}) && \text{by Lem. 4.3} \\
&= -\Lambda_1(\mathsf{T}^d, \mathsf{B}) \cdot \left(\alpha \cdot \frac{S_{\Lambda_1}(\mathsf{T}^d)}{\Lambda_1(\mathsf{T}) + S_{\Lambda_1}(\mathsf{T}^d)} + \beta \right) \cdot \pi(\mathsf{T}) && \text{by hyp.} \\
&= -\Lambda(\mathsf{T}^d, \mathsf{B}) \cdot \left(\alpha \cdot \frac{S_{\Lambda}(\mathsf{T}^d) + v}{\Lambda(\mathsf{T}) + S_{\Lambda}(\mathsf{T}^d)} + \beta \right) \cdot \pi(\mathsf{T}) && \text{by [Bor]} \\
&< -\Lambda(\mathsf{T}^d, \mathsf{B}) \cdot \left(\alpha \cdot \frac{S_{\Lambda}(\mathsf{T}^d)}{\Lambda(\mathsf{T}) + S_{\Lambda}(\mathsf{T}^d)} + \beta \right) \cdot \pi(\mathsf{T}) && \text{by arith.} \\
&= g_{\mathsf{B}}(\Gamma, \mathsf{int})|_{\mathsf{T}} && \text{by Lem. 4.3}
\end{aligned}
$$

□