(In-)Visible Risks of Blockchain-Based Financing for Capital Allocation Efficiency*

Dongkyu Chang† Kyoung Jin Choi‡ Keeyoung Rhee§

November 16, 2025

Abstract

We analyze how blockchain-based financing affects capital allocation to provide early guidance for DeFi regulation. Competition with conventional financial firms raises borrowing costs, incentivizing DeFi firms to shirk their responsibility for managing investors' funds. While blockchain technology enables collective monitoring, enhancing it without prudential regulation creates gambling dynamics: DeFi firms bet on evading detection when shirking, while investors bet on enforcing responsible behavior to secure higher repayments. Although an equilibrium exists where DeFi firms behave responsibly, it becomes less stable when investors are overly confident in coordinated monitoring, particularly in response to out-of-equilibrium offers with unexpectedly high shirk-inducing repayments.

Keywords: Blockchain, Decentralized Finance (DeFi), Fintech, Competition, Financial Stability, Disintermediation.

JEL Codes: D82, D86, G21, G23, G28

*We are gratuful to Elena Asparouhova, Jonathan Berk, Lin William Cong, Jungsuk Han, Evgeny Lyandres, Raghavendra Rau, Marzena Rostek, Gideon Saar, David Schoenherr, Harald Uhlig, and Marius Zoican, as well as participants at the NTU-CBADE Conference on Strategic Analysis and 2025 Global AI Finance Research Conference, and seminars at Seoul National University and Korea University for their helpful comments and discussions.

†City University of Hong Kong, Tat Chee Ave, Kowloon Tong, Hong Kong, e-mail:donchang@cityu.edu.hk,

‡Haskayne School of Business, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2N1N4, Canada, e-mail: kjchoi@ucalgary.ca,

§Correspondence, Sungkyunkwan University (SKKU), 25-2 Sungkyunkwan-Ro, Jongno-Gu, Seoul, 03063, Korea, e-mail: keeyoungrhee@g.skku.edu, contact number: +82-2-760-0433.

1 Introduction

Blockchain-based financing is often promoted as technological innovation that improves transparency and reduces information asymmetries. However, the mechanisms underlying this transparency are fundamentally different from those in conventional finance (Cong and He, 2019; Harvey, Ramachandran and Santoro, 2021; Park, 2025). Traditional oversight relies on legal enforcement, auditing, and third-party certification, where greater transparency typically enhances discipline. By contrast, blockchain monitoring is embedded in code, probabilistic, and decentralized: smart contracts are irreversible; governance is exercised through token-weighted voting in decentralized autonomous organizations (DAOs); and the likelihood of preventing or detecting misconduct increases only with the scale of investor participation.

These blockchain-driven features create a mechanism distinct from conventional transparency. Namely, they can simultaneously discipline and destabilize, fostering speculative dynamics that would not arise in standard financial settings. Recent crises in cryptocurrency exchanges—such as the collapse of Terra–Luna and the failure of FTX—revealed this paradox that blockchain-based markets are not perfectly insulated from inefficiency or instability, despite their unprecedented on-chain visibility. In fact, the very openness of blockchain systems can breed overconfidence among investors in their collective discipline, diverting capital to underperforming projects with unsustainable payouts. These cases raise a central question: under what conditions does blockchain-enabled monitoring improve capital allocation efficiency, and when does it instead amplify destabilizing speculation? To address this, we present a model that captures the strategic interaction between conventional finance firms, decentralized finance (DeFi) financial intermediaries, and investors, with a particular focus on the blockchain-specific mechanism of collective and probabilistic monitoring.

In the model, a regulated conventional financial firm and a blockchain-based DeFi firm compete for raising investor funds externally. The key innovation of our model lies in how the DeFi firm is monitored: rather than relying on regulatory enforcement, investors collectively enforce responsible behavior through blockchain validation. In our framework, the probability that the DeFi firm's shirking is detected increases with both the number of investors participating in the blockchain network and the efficiency of decentralized verification. This assumption captures the distinguishing features of the blockchain-based discipline mechanism—collective, probabilistic, and endogenously strengthened by investor participation.

We characterize all possible equilibria to analyze how investors' collective monitoring in the DeFi sector can foster both responsible behavior and destabilizing speculation, depending on each sector's relative competitiveness. A key determinant of equilibrium is investors' collective response to the DeFi firm's deviation. An individual investor's payoff from accepting the DeFi firm's deviation offer depends on how many other investors do the same, particularly when the offer incentivizes the DeFi's to shirk *ex post*. To capture this dynamic, we invoke two opposing refinement concepts: *coalition proofness* and *shirking proofness*. Under coalition proofness, the DeFi firm optimistically assumes that investors will respond to any shirk-inducing offer in the way most favorable to the firm, maximizing its deviation payoff. In contrast, shirking proofness reflects the most pessimistic out-of-equilibrium belief, under which the DeFi firm expects that any shirk-inducing deviation will be outright rejected. These refinements reflect two contrasting market sentiments regarding the DeFi firm's unexpected funding strategies, allowing us to analyze their implications for capital allocation efficiency by comparing equilibria under different refinements.

The DeFi firm's risk management strategy is shaped by its competitive (dis)advantage in the borrowing market and by the accuracy of blockchain-based monitoring. When the DeFi firm's investment yields a lower financial return than that of the conventional firm, an equilibrium arises in which the DeFi firm offers excessively high repayments, only to subsequently shirk for private benefits. Surprisingly, all investors still fund the DeFi firm, as they anticipate earning a higher financial return than what the conventional firm offers, owing to their collective monitoring of the DeFi firm's fund management.

Paradoxically, this equilibrium arises precisely when blockchain-based monitoring is most effective at detecting shirking. In this setting, both the DeFi firm and investors engage in a "catch-me-if-you-can" game. To outbid the conventional firm, the DeFi firm offers an exceptionally high share of financial returns. Yet, instead of settling for minimal financial gains, the DeFi firm—despite low odds—gambles on extracting private benefits from shirking while hoping to evade detection. Meanwhile, investors bet on enforcing responsible behavior through strong blockchain monitoring, expecting to secure a high repayment as their reward. This equilibrium is robust to any refinement, suggesting that enhanced blockchain monitoring alone may exacerbate inefficiencies in financial markets: capital is misallocated to underperforming investments, and borrowing DeFi firms mismanage funds for private benefits.

When the DeFi firm's investment yields a higher financial return, it has a stronger incentive to adhere to a prudent asset management strategy. In this case, the role of blockchain-based monitoring differs across equilibrium refinements. Under coalition proofness, an equilibrium in which the DeFi firm behaves responsibly arises only when blockchain monitoring is weak. Otherwise, the firm prefers to deviate from prudent management as it expects investors

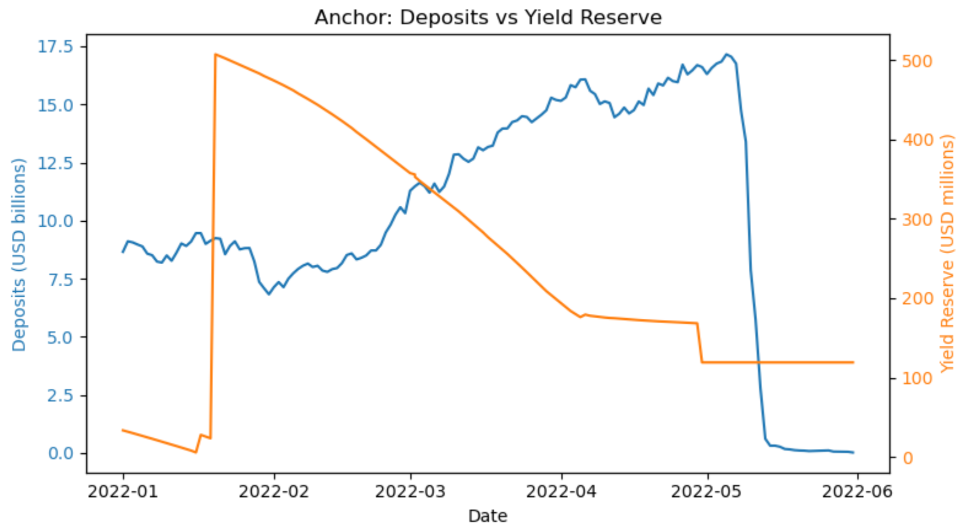

Figure 1 – Evolution of total deposits and yield reserve in Anchor, a major DeFi lending platform on the Terra blockchain, from January to May 2022. The blue line shows deposits (in billions of USD); the orange line shows the yield reserve (in millions of USD). The late-January 2022 spike in the yield reserve reflects Terraform Labs' injection of 450 million TerraUSD (UST; approximately $450 million at the time). Even as the reserve steadily depleted under the fixed 19.5% yield—visible to investors *on-chain* and *in real time*—deposits surged from under $10 billion to over $17 billion. This persistent deposit inflow, even amid apparent unsustainability, reflects the speculative dynamics modeled in our gambling equilibria. *Data sources:* classic Terra blockchain and DefiLlama (https://defillama.com/protocol/anchor).

to join the catch-me-if-you-can game. Under shirking proofness, by contrast, the DeFi firm never finds it optimal to deviate from its prudent asset management strategy, as it expects that investors will reject any out-of-equilibrium offer, regardless of the strength of blockchain monitoring. As a result, the DeFi firm always behaves prudently under shirking proofness.

Our model sheds light on why unsustainably high lending and staking rates often emerge and persist in DeFi markets, even when rational investors recognize both the risks and the high likelihood of collapse. Indeed, the catch-me-if-you-can gambling dynamic predicted by our model has been widely observed in DeFi lending markets, particularly during crypto bull runs. For example, during the 2021–2022 DeFi boom, many cryptocurrencies offered staking rewards exceeding 40–50%, reinforcing the speculative dynamics that characterized decentralized finance at the time.[1] These high rates clearly attracted many investors, tem-

[1]For instance, Axie Infinity's staking rewards mostly surpassed 50% during this period and occasionally exceeded 100%.

porarily driving up prices, even as the system was widely expected to collapse in the near future. The most striking example is Terra, where the Anchor Protocol sustained a 19.5% staking reward until the Terra-Luna collapse in May 2022—an interest rate that was clearly unsustainable for stablecoin lending (see Figure 1). Yet, despite recognizing the system's inevitable collapse, both investors and the Terra Foundation speculatively rode the Luna price rally, sustaining Terra's artificially high interest rates for months.[2] While the Terra–Luna collapse provides a vivid illustration of such dynamics, similar high-yield equilibria were observed across major DeFi lending platforms such as Aave and Compound during the 2021–2022 cycle, suggesting that the mechanism we highlight is not tied to a single event but reflects a broader and recurrent pattern in DeFi markets.

Our equilibrium analysis yields policy implications for mitigating moral hazard in unregulated technology sectors. A common policy proposal is to enhance blockchain infrastructure to improve monitoring capabilities. A key example is the introduction of Central Bank Digital Currencies (CBDCs), which could replace private cryptocurrencies to increase transparency and reduce fraud associated with unregulated digital assets (Gorton and Zhang, 2023; Rivadeneyra, Hendry and García, 2024). However, our findings suggest that such policies should be implemented with caution. If the DeFi sector lacks a substantial competitive advantage over conventional banking, merely enhancing blockchain monitoring could encourage riskier, gambling-like behavior among investors and DeFi firms, potentially destabilizing financial markets. Policymakers should therefore prioritize regulatory measures that strengthen DeFi firms' fiduciary duties. Without proper regulation, policies aimed at enhancing blockchain-based monitoring—such as the introduction of CBDCs—could inadvertently destabilize financial markets.

Like a well-designed CBDC, an effective stablecoin framework must pair transparency with robust prudential safeguards. Although CBDCs have not yet been implemented, they are widely expected to increase transparency and potentially spur disintermediation; privately issued stablecoins pose similar risks unless properly ring-fenced (Choi and Rhee, 2025). Recent U.S. legislation moves in this direction. In July 2025, Congress enacted the Guarding and Enabling the Nation's Infrastructure Using Stablecoins (GENIUS) Act—the first federal law establishing a licensing and reserve framework for payment stablecoins (U.S. Senate, 2025). By

[2] Notably, investors' confidence was further reinforced by the Luna Foundation Guard's accumulation of Bitcoin reserves—first inferred by on-chain analysts and later confirmed publicly in April 2022. Although these holdings were not directly integrated into the Anchor's on-chain yield mechanism, their visibility was widely interpreted as a form of enhanced monitoring capacity, reinforcing investors' belief that systemic safeguards had improved.

requiring one-to-one cash or T-bill reserves and *banning interest payments*, the Act seeks to (i) prevent deposit flight from the traditional banking system and (ii) curb the shirking behavior and capital misallocation that arise in the absence of prudential oversight. We therefore view the GENIUS Act as an early attempt to ring-fence stablecoins in much the same way that prudential rules would apply to a future CBDC.

The rest of the paper proceeds as follows. Section 2 reviews the related literature. Section 3 describes the model. Section 4 analyzes ex-post incentives of risk-taking by financial firms in the model. Section 5 and 6 provide the full equilibrium analysis. Lastly, Section 8 provides concluding remarks. All proofs are relegated to the appendix.

2 Related Literature

Our analysis connects to a broader literature showing that monitoring technologies can both discipline behavior and generate distortions, underscoring a central challenge for regulatory design. Duflo et al. (2013), Greenstone et al. (2022), and Zou (2021) illustrate how stronger or more frequent monitoring reshapes incentives in unexpected ways. While these studies concern conventional settings—auditor independence, automated inspections, or intermittent enforcement—our study emphasizes that blockchain monitoring is distinctive: it is decentralized, probabilistic, and endogenous to investor participation. This feature makes it more prone to generating speculative equilibria, especially when investors are overconfident in their collective enforcement ability. The contrast with standard transparency effects also highlights why policy caution is warranted: enhancing blockchain monitoring without prudential safeguards may destabilize capital allocation rather than improve it.

In the blockchain and DeFi context, recent work highlights similar trade-offs. Cong and Mayer (2025) emphasize how digital currencies reshape strategic competition among nations, while Cong, Qu and Wang (2025) document that blockchain-based environmental monitoring in China reduced pollution but also induced firm relocation and economic contraction. Parallel developments in DeFi lending and token-based platforms likewise reveal both efficiency gains and new risks (Harvey, Ramachandran and Santoro, 2021; Capponi and Jia, 2025; Malinova and Park, 2023). Taken together, these studies underscore that blockchain technologies can discipline economic agents yet simultaneously generate new sources of inefficiency—an inherent tension that motivates our analysis.

This paper is related to the literature on competition between traditional banks and fintech firms. A broad set of studies shows that fintech platforms often gain advantages from superior data-processing and information technology—whether through payment competition, open banking, or improved screening and enforcement (Parlour, Rajan and Zhu, 2022; He, Huang and Zhou, 2023; Brunnermeier and Payne, 2024; Boualam and Yoo, 2022; Vives and Ye, 2025).[3] While this literature emphasizes data-driven screening efficiency, our study highlights a different mechanism: the entry of blockchain-based financing into the regulated financial sector. Here, competitive advantage derives not from superior information processing but from decentralized validation and monitoring, shifting the focus from screening to governance. This distinction broadens the standard bank–fintech competition framework and complements studies such as Fuster et al. (2019), Berg et al. (2020), Parlour, Rajan and Zhu (2022), Boualam and Yoo (2022), He, Huang and Zhou (2023), Brunnermeier and Payne (2024), and Vives and Ye (2025).

Our theory also contributes to the literature on market discipline (Flannery, 1998; Martinez Peria and Schmukler, 2001; Demirgüç-Kunt and Huizinga, 2004). We explore a new form of market discipline in the DeFi market, leveraging the transparency and automation of blockchain. Notably, this mechanism has emerged spontaneously within the market as a response to regulatory gaps, making it particularly significant. Our framework provides a lens for understanding the challenges faced by technology-driven industries that operate in relatively unregulated environments while seeking to attract investors. Importantly, the catch-me-if-you-can equilibrium arises when monitoring is enhanced under strong investor optimism. This result has important policy implications, showing that enhanced transparency alone does not necessarily lead to desirable outcomes unless accompanied by proper enforcement of fiduciary duties.

Our paper is broadly related to the literature on banking competition. While we do not attempt to review the vast body of work on this topic, much of the literature focuses on how competition affects banks' franchise value and, consequently, their risk-taking behavior, with implications for financial (in)stability (Allen and Gale, 2004; Allen, Carletti and Marquez, 2011; Beck, Demirgüç-Kunt and Levine, 2006; Boyd and De Nicolo, 2005; Egan, Hortaçsu and Matvos, 2017; Keeley, 1990; Martinez-Miera and Repullo, 2010; Repullo, 2004). Our contribution lies in examining a new channel of competitive pressure arising from decentralized financing, which can also contribute to financial instability. In particular, financial instabil-

[3] See also studies of the lending market competition among banks with asymmetric information on borrowers, such as Broecker (1990) and Hauswald and Marquez (2003). On the other hand, traditional banks are often modeled as having a comparative advantage in assessing collateral value (Brunnermeier and Payne, 2024) and achieving higher monitoring efficiency (Vives and Ye, 2025).

ity in our model does not stem solely from conventional financial firms' risk-taking in asset selection, as emphasized in the existing literature, but also from disintermediation, where all investors allocate their capital to DeFi firms that ultimately shirk ex post, while the regulated sector (including general fintech firms other than DeFi firms) selects a prudent asset.

Lastly, our paper relates to the CBDC literature, as the introduction of CBDCs can lead to disintermediation (Ahnert, Hoffmann and Monnet, 2025; Andolfatto, 2021; Choi et al., 2021; Fernandez-Villaverde et al., 2021; Keister and Sanches, 2023; Kim and Kwon, 2023; Whited, Wu and Xiao, 2022; Williamson, 2022). Typically, concerns about disintermediation focus on the potential weakening of traditional banks' roles in deposit-taking and lending as individuals hold CBDCs directly with the central bank. Our paper offers a different perspective on this issue. Once CBDCs are introduced, DeFi platforms are likely to adopt them to enhance investor trust by incorporating legal tender into their systems. Given the inherently higher transparency of CBDCs compared to private cryptocurrencies, their adoption could significantly improve the visibility of fund flows and thereby strengthen monitoring. However, unless accompanied by proper enforcement of fiduciary duties, unintended consequences—such as the catch-me-if-you-can equilibrium or excessive risk-taking by conventional financial firms—could exacerbate disintermediation risks.

3 Model

We study an economy with two competing lending technologies: a regulated conventional financial sector and an unregulated DeFi sector. A unit mass of risk-neutral investors allocates capital between the two sectors. In the absence of DeFi, the conventional sector would undertake only prudent projects. The emergence of DeFi introduces IT-enabled competition in borrowing and lending, potentially reshaping the equilibrium allocation of funds. For clarity, we name the sectors' representative firms the *conventional financial firm* and the *DeFi firm*.

Although DeFi's share of total lending remains small today, it has exhibited triple-digit compound growth, and analysts expect an order-of-magnitude expansion as tokenization, stablecoins, and forthcoming CBDC rails mature. Anticipating this trajectory, we offer a forward-looking normative analysis to inform policy before DeFi reaches systemic scale.

The model unfolds as follows. Both the conventional and DeFi firms are assumed to be cashless and must raise external finance from investors, each endowed with one unit of capital. At the outset, the two firms compete for investors' funds by offering their contractual

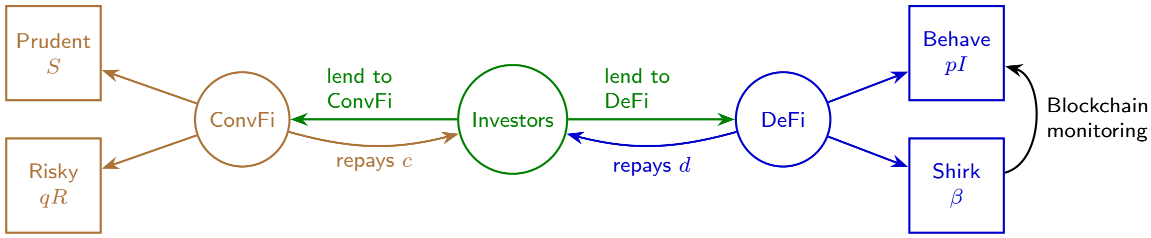

Figure 2 – Model Overview: "ConvFi" stands for the conventional financial firm.

terms *simultaneously*. Specifically, the conventional firm offers a contract that promises a repayment $c > 0$ contingent on the project success, while the DeFi firm issues securities at a unit price that repay $d > 0$ if its project succeeds. After observing these offers, all investors *simultaneously* allocate their capital by comparing the expected returns of the two securities. Once funded, each firm invests in its respective project. Investors who finance the DeFi firm engage in (imperfect) monitoring of its portfolio choices. Finally, project payoffs are realized and distributed according to the contracts specified at the funding stage. Figure 2 provides a stylized representation of the model.

In the next subsections, we provide further details on the investment and monitoring technologies, and we also develop the notation used throughout the paper.

3.1 The Conventional Financial Firm under Regulatory Oversight

We first emphasize that the term "conventional" does not imply technological backwardness. Rather, it refers to the firms operating under long-standing regulatory oversight, which may include technologically sophisticated entities using RegTech, Banking-as-a-Service (BaaS), APIs, and related tools.

With this in mind, the conventional firm has two options for managing the funds it borrows. Specifically, it can invest in one of two types of financial assets, both of which exhibit constant returns to scale and require one unit of capital per unit of investment. If the conventional firm adopts a *prudent* risk management strategy, it selects a financial asset that guarantees a return of $S > 1$ per unit of investment. Alternatively, if the conventional firm engages in *excessive* financial risk, it invests in a riskier asset that yields a positive return of $R > 1$ with probability $q \in (0, 1)$ and zero otherwise. To capture the differing levels of risk between these two strategies, we impose the following assumption:

Assumption 1. $R > S > qR \geq 1$.

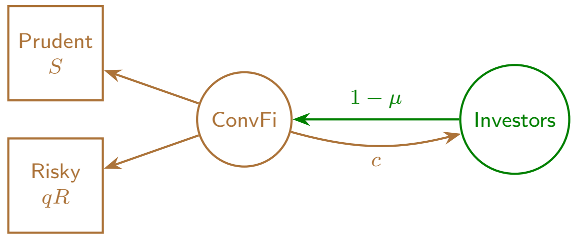

Figure 3 – The Conventional Firm: "ConvFi" stands for the conventional financial firm.

Figure 3 graphically represents the conventional firm's funding structure and its fund management strategy per unit capital, given that it is funded by investors with measure $1-\mu$. There are several observations regarding Assumption 1. First, the conventional firm earns a higher financial return when its excessive risk-taking strategy succeeds ($R > S$). However, from an ex-ante perspective, the prudent strategy generates a higher net present value (NPV) ($S > qR$). Therefore, in the absence of competition from the DeFi firm, the conventional firm would always choose the prudent risk-management strategy. That is, we implicitly assume the strict regulatory environment in the conventional financial sector that preserves financial stability. To avoid trivial cases, we also assume that both strategies yield positive NPVs, i.e., $S \geq 1$ and $qR \geq 1$. However, as we will see in the next subsection, the availability of an unregulated alternative can distort these incentives and affect the conventional firm's project choice through capital market competition.

3.2 The DeFi Firm under Decentralized Oversight

In contrast, the DeFi firm invests all of its funds in a single financial project, which also exhibits constant returns to scale. Specifically, the project requires one unit of capital per unit of investment and generates a return of $I > 1$ per unit with probability $p \in (0,1)$, provided the DeFi firm *behaves* responsibly in managing the project. If the DeFi firm *shirks*, the project yields zero return, but the firm enjoys a private benefit of $\beta > 0$ per unit of investment, which is not shared with investors. To ensure that investors can induce the DeFi firm to behave responsibly, we impose the following assumption:

Assumption 2. *$pI - 1 \geq \beta$.*

Without Assumption 2, the DeFi firm would *never* behave in any equilibrium. To see this, note that the DeFi firm must guarantee its investors a pecuniary payoff at least equal to one in order to attract any investment in the first place. Thus, $pI - 1$ is the upper bound of

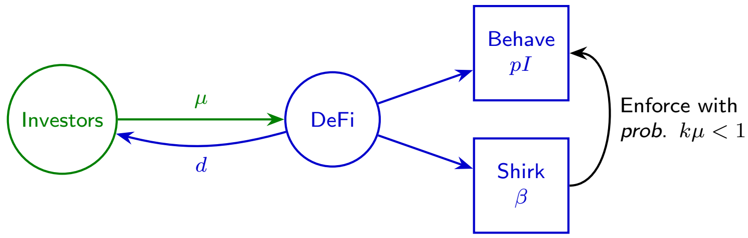

Figure 4 – The DeFi Firm.

the DeFi firm's payoff (per unit of capital) from behaving, which must be at least β to induce responsible behavior. Assumption 2 also implies $pI > \beta$, and hence it is socially optimal for the DeFi firm to behave rather than shirk.

Let $\mu \in [0, \phi]$ denote the fraction of investors who hold the security issued by the DeFi firm, where $\phi \in [0, 1]$ represents the total measure of securities issued.[4] We assume that if the DeFi firm shirks—i.e., deviates from responsible behavior—this misconduct is detected with probability μk. Here, $k \in (0, 1)$ measures the efficiency of blockchain-enabled monitoring. If shirking is detected, responsible behavior can be enforced at no cost. As previewed in the introduction, we capture blockchain-based monitoring through μ (the share of investors participating) and k (the efficiency of verification), with detection probability μk. Section 3.3 elaborates on the technical limits that bound k away from one, such as oracle dependence and the maximum extractable value (MEV).

Figure 4 illustrates the DeFi firm's stylized fund-management strategy when it is funded by investors of measure μ. It is worth noting that the DeFi firm faces a tradeoff when determining its fund size. On the one hand, since the DeFi firm's net income per unit of capital is positive, its payoff from behaving increases with investment size. On the other hand, borrowing from a greater number of investors enhances blockchain-based monitoring, making it more difficult for the DeFi firm to extract private benefits from shirking. Consequently, the DeFi firm may voluntarily limit its fund size to balance these competing factors and maximize its overall payoff. However, the success of such self-regulation hinges on the effectiveness of decentralized oversight.

However, as we show in Appendix A, the DeFi firm always finds that scaling up its investment from a current size improves its profitability, even though such a strategy reduces the likelihood that shirking goes undetected. Thus, without loss, we may focus on the cases

[4] ϕ corresponds to the maximum funding the DeFi firm seeks. This constraint becomes relevant under coalition-proofness but is not required under shirking-proofness, as explained later.

where the DeFi firm issues the maximum volume of securities even if the market does not clear, i.e., $\phi = 1$. Consequently, we use μ throughout to denote the total size of funds the DeFi firm raises through bond issuance. Lastly, we streamline the equilibrium analysis by assuming that the conventional firm resolves indifference by prudently managing its asset risk, while the DeFi firm resolves indifference by behaving responsibly.

The key economic friction in the DeFi sector is therefore the inability of investors to perfectly enforce responsible fund management ex post. While the binary choice between behaving and shirking in our model is stylized, real-world DeFi platforms exhibit closely related incentive problems: once capital is raised, project insiders or validators may take actions that benefit themselves at the expense of lenders. The effectiveness of investor monitoring, and thus the credibility of responsible behavior, ultimately depends on how DeFi protocols implement governance, transparency, and technical safeguards. These issues motivate the next subsection, where we explain how our parameters μ and k capture the technological foundations and limits of decentralized oversight in practice.

3.3 Decentralized Oversight: Technical Foundations and Limits

This subsection elaborates the technical underpinnings of μ and k, linking our parameterization to practical blockchain mechanisms such as smart contracts, oracles, and validator incentives. When funding a DeFi firm, investors are concerned about whether the firm manages the project responsibly—especially in the absence of regulatory oversight. In decentralized finance, smart contracts play a role analogous to legal contracts in traditional finance, codifying governance and enforcement rules in publicly visible code. However, unlike legal contracts, they cannot be reversed or externally enforced once deployed. This irreversibility creates scope for what we call *shirking*: actions that deviate from responsible governance but remain technically feasible within the protocol. For instance, in lending platforms such as Aave or Compound, shirking may involve manipulating oracle feeds, exploiting unaudited or poorly designed smart contracts, or failing to enforce collateral liquidation rules. More broadly, developers or insiders may take advantage of design loopholes or incentive misalignments, resulting in governance failures, scams, or protocol exploits.[5] Similar incentive problems also arise at the validation layer: front-running and other forms of MEV extraction—such as sandwich attacks or liquidation arbitrage—are not prohibited in most jurisdictions, allowing validators

[5]For a detailed discussion of risks associated with smart contracts, see Harvey, Ramachandran and Santoro (2021), Ferreira and Li (2025), and Landsman et al. (2025), among others.

under Proof-of-Stake to extract private gains.[6] These factors limit the reliability of decentralized oversight and, importantly, reduce the effectiveness of blockchain-based monitoring even when transaction data are transparently recorded on-chain.

To mitigate these vulnerabilities, the blockchain ecosystem incorporates various self-monitoring and incentive mechanisms. Consensus protocols such as Proof of Work, Proof of Stake, Proof of History, and Proof of Authority are designed to preserve ledger integrity, while additional mechanisms such as validator slashing or token burning deter misconduct. Furthermore, many DeFi protocols rely on collective, community-driven monitoring that leverages blockchain transparency. Decentralized Autonomous Organizations (DAOs), for example, use public forums to debate and evaluate governance proposals prior to voting (see Figure 9 and Figure 10 in Appendix G). These governance structures allow token holders to submit proposals, challenge suspicious behavior, and collectively enforce protocol rules. If a founding team attempts to exploit a loophole in a smart contract, investors can respond by submitting a governance proposal to amend or disable the contract.

In line with these self-monitoring and incentive systems, our modelling approach captures the idea that protocol integrity improves as more investors participate in governance. A larger μ—representing broader investor participation—raises the likelihood that shirking is detected and disciplined. In this sense, μ represents the *breadth* of decentralized oversight.

However, decentralized monitoring is inherently limited in the absence of formal regulation and specialized technical expertise. These limitations are reflected in the assumption that $\mu k < 1$ for any $\mu \in [0, 1]$, emphasizing that perfect detection is rarely attainable. Many DeFi proposals involve complex smart contracts that require advanced technical understanding, and although governance discussions occur in public spaces (see again Figure 9 and Figure 10), most investors lack the coding and security expertise needed to evaluate them thoroughly. Rapid innovation, opaque contract architectures, and the persistent oracle problem—which exposes protocols to inaccurate or manipulable off-chain data sources—further reduce the effectiveness of collective monitoring. Consequently, the efficiency parameter k is constrained not only by decentralized network design but also by the inherent technical complexity of modern DeFi systems.

In summary, while greater participation (μ) increases the likelihood that misconduct is detected, the overall monitoring effectiveness is fundamentally bounded by k, which captures the technological and institutional limits of blockchain-based governance. This simple rep-

[6] See Mazorra, Reynolds and Daza (2022), Öz et al. (2024) for MEV-related vulnerabilities.

resentation abstracts from regulatory interventions, which we later incorporate in the policy discussion (Section 7) as factors affecting β (moral hazard) and k (monitoring efficiency).

4 Ex-post Risk-taking Incentives

Having established the technological and institutional foundations of monitoring in the DeFi sector, we now return to the economic implications for risk-taking behavior. In our framework, the parameters μ and k determine how effectively investors can detect and discipline shirking. These monitoring capabilities interact directly with the contractual terms offered by the conventional financial firm and the DeFi firm, shaping their incentives to behave responsibly or to take excessive risks once funds are raised. In this section, we characterize these ex-post incentives and show how borrowing terms (B, F) determine the strategic choices of the two firms.

To establish equilibria by backward induction, we first analyze how the ex-post risk-taking behavior of conventional and DeFi firms is shaped by the terms of external financing. Suppose that the conventional firm finances its investment of size $1-\mu$ under financial repayment c per unit of capital. If the conventional firm prudently manages its asset risk, it will get the expected payoff $(1-\mu)(S-c)$. Otherwise, if the conventional firm adopts the excessive risk strategy, it will get the expected payoff $(1-\mu)q(R-c)$. Hence, the conventional firm will prudently manage its asset risk if and only if $S-c \geq q(R-c)$, or equivalently,

$$c \leq \bar{c} := \frac{S-qR}{1-q}, \tag{1}$$

where we assume that the conventional firm breaks a tie by prudently managing the fund whenever indifferent. The cutoff $\bar{c}$ lies below both S and R (i.e., $\bar{c} < S < R$).

Next, suppose that the DeFi firm raises funds of size μ at repayment d. If the DeFi firm behaves responsibly, it obtains the expected payoff $\mu p(I-d)$. If the DeFi firm shirks, the investors enforce responsible behavior with probability $k\mu$, while the firm obtains the private benefit from shirking with probability $1-k\mu$. Hence, the DeFi firm's expected payoff from shirking is $\mu[k\mu p(I-d)+(1-k\mu)\beta]$. The DeFi firm finds it optimal to behave responsibly if and only if $\mu p(I-d) \geq \mu[k\mu p(I-d)+(1-k\mu)\beta]$, or equivalently,

$$d \leq \bar{d} := I - \frac{\beta}{p}, \tag{2}$$

where we assume that the DeFi firm breaks a tie by behaving whenever indifferent.

Lemma 1.

(i) Suppose the conventional firm raises funds of size $1 - \mu \in [0, 1]$ *under a contract with repayment* c*. Then it manages its asset risk prudently if and only if* $c \leq \bar{c}$*.*

(ii) Suppose the DeFi firm raises funds of size $\mu \in [0, 1]$ *by selling securities with repayment* d*. Then it behaves responsibly if and only if* $d \leq \bar{d}$*.*

Lemma 1-(i) aligns with the findings in the literature on the risk-shifting behavior of financial institutions under high borrowing costs (Keeley, 1990; Boyd and De Nicolo, 2005). For the conventional firm, a high repayment c allows investors to claim a disproportionately large share of investment returns, leaving the firm with little net income from prudent risk management. This creates an incentive for the conventional firm to engage in excessive risk-taking to maximize its private gains. In the event of investment failure, investors must absorb significant financial losses, while the conventional firm incurs no loss due to limited liability. Moreover, excessive risk-taking enables the firm to dilute investors' share of financial income, as the higher return from a successful risky investment reduces each investor's share from c/S to c/R, where $c/S < c/R$.

Similarly, Lemma 1-(ii) implies that investors' share of the DeFi firm's investment returns increases with the repayment amount d. A high d discourages the DeFi firm from acting responsibly, as a larger portion of profits is allocated to investors. Consequently, the DeFi firm is more incentivized to shirk, prioritizing private benefits that remain inaccessible to investors, regardless of their investment share.

Our primary analysis examines how competition with the new DeFi firm affects the incumbent conventional firm's capital allocation decisions and risk-taking behavior. To emphasize the effects of borrowing competition, we adopt the following assumption.

Assumption 3. $\bar{c} \geq 1$.

If this assumption fails, the conventional firm will never manage its funds prudently in any equilibrium, regardless of the DeFi firm's entry into the financial market. Under this assumption, we obtain the following benchmark for the conventional firm's risk-taking behavior.

Theorem 1. *In the absence of the DeFi firm, the conventional firm offers a contract $c = 1$ and then prudently manages its asset risk.*

In the absence of the DeFi firm, the conventional firm holds full market power in raising funds from investors. In this scenario, the conventional firm leverages its monopoly advantage to manage asset risk prudently. The conventional firm's expected payoff per unit of funds is given by $\max\{q(R-c), S-c\}$, which leads the conventional firm to prefer minimizing the repayment obligation as much as possible. According to Assumption 3, the conventional firm chooses prudent risk management by minimizing borrowing costs through a repayment obligation of $c = 1 \leq \bar{c}$. This contract ensures investors break even, thereby incentivizing them to invest their funds in the conventional firm.[7]

Assumption 4. *$\bar{c} \neq p\bar{d}$.*

Finally, Assumption 4 ensures that our analysis excludes equilibria with complex structures that offer no additional economic insight. There are two possible scenarios for $\bar{c} > p\bar{d}$. In the first, I is small, so the DeFi firm's project is not profitable. In the second, β is large; that is, the project is profitable, but the severity of the moral hazard problem outweighs profitability. On the other hand, the case $\bar{c} > p\bar{d}$ suggests that the new DeFi sector does not contribute significantly to the economy nor holds a competitive advantage.

5 Coalition-Proof Equilibrium

In this section, we introduce the notion of equilibrium that we employ, called *coalition-proof equilibrium*, and then characterize it. We begin by introducing some useful notation. Define $V(d, \mu)$ as an investor's expected *revenue* from purchasing the DeFi firm's security, given that investors of total size μ also purchase it:

$$V(d, \mu) := \begin{cases} \mu kpd & \text{if } d > \bar{d}; \\ pd & \text{if } d \leq \bar{d}. \end{cases} \tag{3}$$

To understand (3), recall that the DeFi firm would shirk if $d > \bar{d}$. In this case, the DeFi-issued security yields revenue d with probability μk times p, where μk is the probability

[7] We emphasize that the main results of our analysis does not lose generality even without Assumption 3. Indeed, the opposite case $\bar{c} < 1$ merely leads to a boundary equillibrium outcome where the conventional firm always adopts the excessive risk-taking strategy.

that investors deter the DeFi firm's shirking through the blockchain-based monitoring, and p is the conditional probability that a positive return is generated under responsible investment. Thus, the expected revenue is μkpd when $d > \overline{d}$. On the other hand, if $d \leq \overline{d}$, the DeFi firm behaves for sure, and the expected revenue is pd.

Next, define $W(d, \mu)$ as the DeFi firm's expected payoff when it issues μ units of the security with the repayment term d:

$$W(d,\mu) := \begin{cases} \mu\left[\mu kp(I-d) + (1-\mu k)\beta\right] & \text{if } d > \overline{d}; \\ \mu p(I-d) & \text{if } d \leq \overline{d}. \end{cases} \tag{4}$$

To understand (4), recall again that the DeFi firm shirks if $d > \overline{d}$. In that case, shirking is detected and thus the DeFi firm earns $I - d$ as revenue *per unit of security issued* with probability μkp; shirking goes undetected and thus the DeFi firm obtains the private benefit β with probability $1 - \mu k$. If $d \leq \overline{d}$, the DeFi firm manages investment responsibly, and the expected revenue is $p(I - d)$ *per unit of security issued*.

Fix any candidate of equilibrium (μ^*, d^*, c^*), and consider the DeFi firm's deviation by issuing $\mu' \neq \mu^*$ units of securities with the repayment term d' such that $W(d^*, \mu^*) < W(d', \mu')$. That is, the deviation (d', μ') strictly improves the DeFi firm's payoff *if all these securities are purchased by investors.* However, the investors' payoff from purchasing the securities depends on how other investors respond to the DeFi firm's deviation (particularly when $d' > \overline{d}$). Thus, whether the deviation is indeed profitable for the DeFi firm hinges on how investors *coordinate* in the subgame.

We address this issue using the idea of coalition-proofness from the literature (Aumann, 1959; Bernheim, Peleg and Whinston, 1987).[8] Suppose that when the DeFi firm considers deviating, it can form a coalition with a subset of investors and ensure that coordination among them is resolved in its favor, subject to the investors' strict incentive compatibility. For example, the DeFi firm may deviate by offering (d', μ') and then forming a coalition of investors of measure μ' who purchase the security in the subgame, provided that doing so

[8]The difference between the notions of strong Nash equilibrium and coalition-proof equilibrium, proposed by Aumann (1959) and Bernheim, Peleg and Whinston (1987), respectively, is as follows. A strong Nash equilibrium requires stability against *every conceivable* coalitional deviation. In contrast, a coalition-proof equilibrium considers only *a subset of coalitional deviations* that are internally consistent; a valid coalitional deviation must be self-enforcing in the sense that no proper sub-coalition can reach a mutually beneficial agreement to deviate from the deviation, and furthermore, any potential deviation by a sub-coalition must also be evaluated by the same criterion, and so on. This distinction is inconsequential in our setting because, for any deviation (d', μ') by the DeFi firm, a sub-coalition of investors of measure $\mu'' < \mu'$ always yield weakly lower payoff than the original coalition of measure μ'.

yields the investors strictly higher profits than funding the conventional firm. In equilibrium, the DeFi firm should have no incentive to deviate in this manner. Formally, in addition to the usual requirement of a (subgame-perfect) equilibrium strategy profile, we impose coalition-proofness as defined below.

Definition 1. *(μ^*, d^*, c^*) is called coalition-proof if and only if there is no (d', μ') such that*

$$W(d', \mu') > W(d^*, \mu^*) \quad \text{and} \quad V(d', \mu') > U,$$

where $U = qc^*$ if $c^* > \bar{c}$, and $U = c^*$ if $c^* \leq \bar{c}$.

Now we are ready to define the coalition-proof equilibrium, which is a pure-strategy subgame-perfect equilibrium that integrates coalition-proofness and the tie-breaking rule (as discussed in Section 4).

Definition 2. *(μ^*, d^*, c^*) is called a* coalition-proof equilibrium *if and only if the following conditions hold.*

(i) Subgame-perfection: (μ^*, d^*, c^*) is a pure-strategy subgame-perfect equilibrium;

(ii) Coalition-proofness: (μ^*, d^*, c^*) is coalition-proof;

(iii) Tie-breaking: The DeFi firm behaves responsibly if and only if $d^* \leq \bar{d}$; the conventional firm manages its asset risk prudently if and only if $c^* \leq \bar{c}$.

We categorize equilibria into two distinct types. In the first type (Section 5.1), the DeFi firm shirks its project management responsibility because of an excessively high repayment obligation, i.e., $d^* > \bar{d}$. In the second type (Section 5.2), the DeFi firm behaves responsibly under a relatively low repayment obligation, i.e., $d^* \leq \bar{d}$. In the following analysis, we fully characterize these two types of equilibria, extract key economic insights, and discuss their policy implications.

5.1 When the DeFi Firm Shirks

In this section, we characterize equilibria in which the DeFi firm shirks in pursuit of private benefits. There are two possible cases: one in which the conventional firm prudently manages its asset risk, and another in which the conventional firm takes excessive risk.

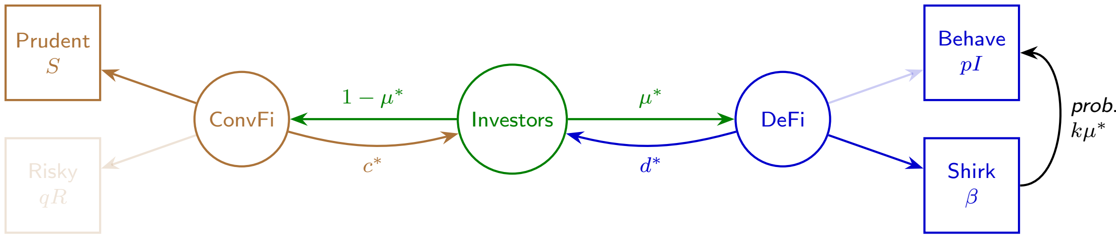

Figure 5 – PS Equilibrium: "ConvFi" stands for the conventional financial firm.

PS Equilibrium: Consider the first equilibrium type, referred to as the "PS" equilibrium, which denotes the strategy profile in which the conventional firm adopts "prudent" risk management, while the DeFi firm "shirks." According to Lemma 1, the conventional firm's equilibrium repayment obligation c^* must be sufficiently small ($c^* \leq \bar{c}$) to incentivize prudent risk management and achieve a higher NPV. Since the conventional firm's investments succeed with probability one, each investor earns a payoff of c^* from investing in the conventional firm. Figure 5 graphically illustrates the structure of PS equilibrium.

In contrast, the DeFi firm's repayment, d^*, must be sufficiently large ($d^* > \bar{d}$) for the DeFi firm to find it optimal to prioritize private benefits over responsible investment management. Since its investment management is subject to external monitoring, shirking is detected and corrected with probability $\mu^* k$. Consequently, each investor earns a payoff of $\mu^* kpd^*$ from holding the DeFi firm's security.

The DeFi firm's market share μ^* in the borrowing market is determined by its competitive advantage—specifically, its ability to offer investors a more attractive repayment structure compared to the conventional firm. In sum, the PS equilibrium is characterized as follows.

Theorem 2. *The PS equilibrium is characterized as follows:*

(i) $\mu^* = 0$ *or* 1 *in any PS equilibrium.*

(ii) *A PS equilibrium with* $\mu^* = 0$ *exists if and only if*

$$p\bar{d} \leq kpI \leq \bar{c}. \tag{5}$$

In equilibrium, the conventional firm offers $c^* = kpI$*, and the DeFi firm offers* $d^* = I$*.*

(iii) *A PS equilibrium with* $\mu^* = 1$ *exsits if and only if*

$$\bar{c} \geq qR \;\; \textit{and} \;\; p\bar{d} < \bar{c} \leq kpI. \tag{6}$$

In equilibrium, the conventional firm offers $c^* = \overline{c}$, and the DeFi firm offers $d^* = \frac{1}{kp}\overline{c}$.

Part (i) of Theorem 2 shows that only boundary outcomes exist in the PS equilibrium: all investors either invest in the conventional firm ($\mu^* = 0$) or fund the DeFi firm ($\mu^* = 1$). To understand why, suppose there exists a hypothetical interior equilibrium in which the DeFi firm raises funds of size $\mu^* \in (0, 1)$, and every investor earns $c^* = \mu^* kpd^*$ regardless of whether they finance the conventional or the DeFi firm. In such a scenario, the DeFi firm could profitably deviate by forming a blocking coalition with a subgroup of investors of size $\mu' \neq \mu^*$. If μ^* is relatively small, the DeFi firm could offer a repayment $d' \in \left(\overline{d}, d^*\right)$ and increase its fund size to $\mu' > \mu^*$, ensuring that each deviating investor earns a higher payoff than investing in the conventional firm, i.e., $\mu' kpd' > \mu^* kpd^* = c^*$. By doing so, however, the DeFi firm would incur a loss due to the increased precision of blockchain monitoring, since a larger number of investors ($\mu' k > \mu^* k$) reduces the likelihood of obtaining the private benefit from shirking. This loss is outweighed by the benefits of a lower borrowing cost ($d' < d^*$) with a larger investment size ($\mu' > \mu^*$). Conversely, if μ^* is relatively large, the DeFi firm could improve its payoff by offering a repayment $d' > d^*$ and reducing its fund size to $\mu' < \mu^*$. This deviation would guarantee a strictly higher payoff to all deviating investors. While this strategy increases the borrowing cost per unit of capital and reduces the investment size, it helps the DeFi firm secure a private benefit from shirking, since fewer participating investors reduce the precision of blockchain monitoring ($\mu' k < \mu^* k$). In sum, if $\mu^* \in (0, 1)$, the DeFi firm always has a profitable deviation, ruling out the existence of interior equilibrium outcomes.

Given that there are only two possible PS equilibria ($\mu^* = 0$ or $\mu^* = 1$), parts (ii) and (iii) of Theorem 2 provide the necessary and sufficient conditions for these outcomes. First, the PS equilibrium with $\mu^* = 0$ arises under condition (5). The inequality $kpI \leq \overline{c}$ allows the conventional firm to design a contract that outcompetes the DeFi firm in the borrowing market by offering $c^* = kpI$, which incentivizes itself to manage its asset risk prudently *ex post*. Under this condition, the DeFi firm is unable to finance its project because its equilibrium strategy $d^* > \overline{d}$ provides investors with a payoff no higher than $c^* = kpI$, the payoff they will earn from investing in the conventional firm. Furthermore, the DeFi firm cannot form a strictly mutually beneficial blocking coalition with any subgroup of investors. As discussed earlier, a security with any repayment $d' > \overline{d}$ cannot attract any single investor. Similarly, the inequality $p\overline{d} < \overline{c}$ in (5) implies $pd' \leq kpI = c^*$ for any $d' \leq \overline{d}$; that is, any deviation security offer that would induce the DeFi firm to behave responsibly *ex post* cannot guarantee a strictly higher payoff than c^* to any deviating investor.

The PS equilibrium with $\mu^* = 1$ arises when condition (6) is satisfied. First, the inequality $p\overline{d} < \overline{c}$ means that $\overline{d}$, the upper bound of the DeFi firm's repayment for behaving responsibly *ex post*, is sufficiently small. More precisely, we have $pd' \leq p\overline{d} < c^* = \overline{c}$, implying any security offer $d' \leq \overline{d}$ that induces the DeFi firm's responsible behavior cannot provide investors with a strictly higher payoff than the return from investing in the conventional firm. Hence, the DeFi firm must outbid the conventional firm by offering a shirk-inducing repayment $d^* > \overline{d}$. Indeed, the inequality $kpI \geq \overline{c}$ ensures that the DeFi firm can offer repayment $d^* \in (\overline{d}, I]$ to attract investors in the borrowing market: any repayment d' satisfying $kpd' \geq \overline{c}$ guarantees investors a higher payoff than investing in the conventional firm, given that the repayment from investing in the "prudent" asset is bounded above by $\overline{c}$. In sum, the DeFi firm wins the borrowing game by offering $d^* = \frac{1}{kp}\overline{c}$, which is feasible ($d^* \leq I$), provides investors with a strictly higher payoff than from investing in the conventional firm ($c^* \leq kpd^*$), and consistently incentivizes shirking *ex post* ($d^* > \overline{d}$). Finally, the inequality $qR \leq \overline{c}$ ensures that the conventional firm cannot profitably deviate from its equilibrium strategy $c^* = \overline{c}$. In fact, the only possible deviation left for the conventional firm would be to offer a higher repayment $c' > \overline{c}$, which would result in ex-post excessive risk-taking. However, the inequality $qR \leq kpd^* = \overline{c}$ implies that even such a deviation cannot provide investors with a strictly higher payoff than the security issued by the DeFi firm.

Note that the PS equilibria arise when $\overline{c} > p\overline{d}$, that is, when the new DeFi industry offers relatively modest financial returns compared to the conventional financial sector and therefore does not dominate it in terms of profitability. In this case, the equilibrium crucially depends on the relative size between $\overline{c}$ and kpI. If $\overline{c}$ is relatively large as in (5), the conventional firm does not need to raise its repayment to win the borrowing game, obtaining full financing without making an excessively risky investment. However, if $\overline{c}$ is relatively small as in (6), the conventional firm cannot keep its borrowing rate low to preserve the ex-post incentive for prudent risk management. The DeFi firm then wins the borrowing competition by offering a higher repayment, even though this induces shirking *ex post*. Since k is substantially high ($k \geq \frac{1}{pI}\overline{c}$), investors are likely—but imperfectly—to prevent the DeFi firm from shirking in the ex-post project management using blockchain-based monitoring technology, and therefore purchase the DeFi firm's securities.

An important, and perhaps surprising, result is that investors' capital is inefficiently allocated to the DeFi firm's underperforming project when blockchain-based monitoring capabilities are substantially enhanced, i.e., as k increases. Specifically, all investors lend to the DeFi firm (i.e., $\mu^* = 1$) when the condition (6) is satisfied. In this PS equilibrium, the conventional firm, if funded, would manage its asset risk prudently, generating a net financial return of $S-1$. Furthermore, from Assumption 1, it follows that $S > \overline{c} = \frac{S-qR}{1-q}$, which in turn implies $S > pI - \beta$, since $\overline{c} > pI - \beta$ by (6). Since the maximum total surplus of the DeFi firm's investment is $pI - 1 - \beta$, the strict inequality $S > pI - \beta$ means that investors fund an underperforming project owned by the DeFi firm in equilibrium, particularly when $k \geq \frac{1}{pI}\overline{c}$ — i.e., the blockchain-based monitoring technology is highly developed.

How can this seemingly paradoxical outcome arise? The DeFi firm and the investors exploit enhanced blockchain-based monitoring capabilities to effectively *gamble* for higher, albeit riskier, private gains. First, each investor, rationally anticipating that other investors adopt the same strategy, bets on detecting the DeFi firm's misbehavior (shirking in project management) with a high probability, $k \geq \frac{1}{pI}\overline{c}$. Successful detection then rewards investors with a high expected repayment ($pd^* > \overline{c}$) as a "bounty." In contrast, the DeFi firm also capitalizes on the inherent imperfections of blockchain-based monitoring, betting on the likelihood of evading detection. This allows it to secure a private benefit β at the expense of investors' interests, with small but non-zero probability $1-k$.

These conflicting interests create allocational inefficiencies, as the DeFi firm and investors engage in a risky "catch-me-if-you-can" game. To win the competitive borrowing game, the DeFi firm offers disproportionately high repayments to attract funding, even though the conventional firm's underlying asset yields a higher net present value (NPV), i.e., $S-1 > pI-1-\beta$. However, the DeFi firm is relatively unconcerned about the resulting high borrowing cost: its primary objective is to extract private benefits by shirking, which materializes when investors fail to detect it. Investors also accept the DeFi firm's terms, motivated by the prospect of "catching" the shirking firm in the ex-post monitoring game. Consequently, the entry of the DeFi firm into the borrowing market can lead to inefficient *disintermediation*: the new-entrant DeFi firm captures a large share of funds from the incumbent financial service sector, yet undertakes an underperforming financial project with zero incentive to manage the funds responsibly.

However, disintermediation arises only when k is sufficiently large, i.e., when improvements in blockchain-based monitoring technology encourage investors to take risky bets on catching the DeFi firm's shirking. If k is relatively small, such a bet on winning the catch-me-if-you-can game becomes too risky. Thus, investors no longer finance the DeFi firm despite its hefty repayments. Instead, they invest in the conventional firm, even at a relatively low borrowing rate, and the conventional firm does not pay a risk premium because it prudently manages its asset risk under a low borrowing cost, thereby yielding a high NPV.

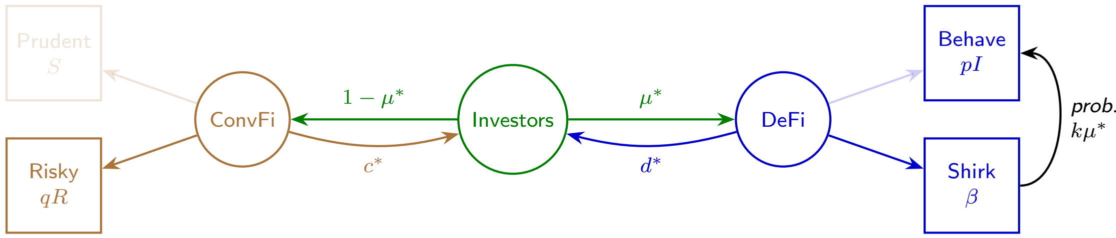

Figure 6 – RS Equilibrium: "ConvFi" stands for the conventional financial firm.

RS Equilbrium: We next analyze another equilibrium outcome, referred to as the "RS" equilibrium type, which stands for the strategy profile in which the conventional firm makes an excessively "risky" investment and the DeFi firm "shirks." Figure 6 depicts a stylized representation of RS equilibrium. The equilibrium strategy profile has the following features. First, by Lemma 1, the conventional firm offers a high repayment $c^* > \bar{c}$, and the DeFi firm also offers high repayment $d^* > \bar{d}$. Correspondingly, each investor gets a payoff qc^* from investing in the conventional firm, since the conventional firm's risky asset succeeds with probability q, while she gets a payoff $\mu^* kpd^*$ if she funds the DeFi firm.

Theorem 3. *The RS equilibrium is characterized as follows:*

(i) $\mu^* = 0$ *or* 1 *in any RS equilibrium.*

(ii) An RS equilibrium with $\mu^* = 0$ *exists if and only if*

$$p\bar{d} \leq kpI \leq qR \ \ \text{and} \ \ \bar{c} \leq kpI. \tag{7}$$

In equilibrium, the conventional firm offers $c^* = \frac{1}{q}kpI$*, and the DeFi firm offers* $d^* = I$*, respectively.*

(iii) An RS equilibrium with $\mu^* = 1$ *exists if and only if*

$$p\bar{d} \leq qR \leq kpI \ \ \text{and} \ \ \bar{c} \leq qR. \tag{8}$$

In equilibrium, the conventional firm offers $c^* = R$*, and the DeFi firm offers* $d^* = \frac{1}{kp}qR$*.*

Similar to the PS equilibrium, there are only boundary outcomes, where all investors either invest in the conventional firm ($\mu^* = 0$) or hold the DeFi firm's securities ($\mu^* = 1$).

The RS equilibrium with $\mu^* = 0$ exists if condition (7) is satisfied. First, the inequality $\bar{c} \leq kpI \leq qR$ means that the conventional firm cannot outbid the DeFi firm unless it promises an excessively large repayment $c^* > \bar{c}$, which induces the ex-post risky investment, given that the DeFi firm's equilibrium strategy $d^* = I > \overline{d}$ yields shirking. The same inequality also implies that the DeFi firm cannot win the borrowing game whether it offers to repay $d \leq \overline{d}$ or $d > \overline{d}$. Indeed, the DeFi firm's offer cannot provide a strictly higher payoff than the conventional firm's equilibrium strategy $c^* = \frac{1}{q}kpI > \bar{c}$, which yields an investor payoff $qc^* \geq kpI \geq p\overline{d}$. Furthermore, the inequality $p\overline{d} \leq kpI$ implies the DeFi firm must make a shirk-inducing offer $d^* = I > \overline{d}$ in the competitive borrowing market. Then, the conventional firm offers $c^* = \frac{1}{q}kpI$ to outbid the DeFi firm. Note that the conventional firm has no incentive to deviate by lowering its repayment obligation to any $c' < c^*$: after observing such a deviation, all investors ($\mu' = 1$) would switch to funding the DeFi firm to secure a strictly higher payoff $\mu' kpd^* = kpI > qc'$.

Furthermore, the RS equilibrium with $\mu^* = 1$ exists when condition (8) is satisfied. First, the inequality $qR \leq kpI$ implies that the DeFi firm can win the competitive borrowing game by offering $d^* = \frac{qR}{kp}$, given that the conventional firm competitively offers the investment contract with the highest possible repayment $c^* = R$. Next, the inequality $p\overline{d} < qR$ requires the DeFi firm to offer repayment $d^* > \overline{d}$ to win the borrowing game, ensuring that the DeFi firm shirks in project management after borrowing. Lastly, the inequality $qR \leq \bar{c}$ ensures that the conventional firm cannot profitably deviate from its equilibrium offer $c^* = R$. Specifically, any alternative offer $c' \in (\bar{c}, R)$ would fail to attract investors, as such an offer would provide a strictly lower payoff than the equilibrium offer ($qc' < qc^* = qR$). The other possible deviation is to offer $c' \leq \bar{c}$, which would incentivize the conventional firm to manage its risk prudently *ex post*. However, since $c' \leq qR = kpd^*$, such an offer would provide (weakly) lower payoffs than the DeFi firm's securities, making it uncompetitive in the borrowing market.

A couple of key insights emerge from Theorem 3. First, investors' behavior changes dramatically depending on the efficiency level of blockchain-based monitoring (k). If k is not sufficiently large, as in (7), all investors invest in the conventional firm. However, if k is sufficiently large enough, as in (8), all the investors instead invest in the DeFi firm. The underlying intuition mirrors that of the PS equilibrium. Investors prefer funding the DeFi firm, which, despite strong blockchain-based monitoring, generates a lower NPV than the conventional firm's risky asset ($pI - \beta - 1 < qR - 1$). Thus, blockchain-based monitoring exacerbates inefficiencies by reinforcing the "catch-me-if-you-can" dynamic observed in the PS equilibrium.

Furthermore, Theorem 3-(iii) highlights that competition harms investors when a high-risk DeFi firm enters the market with enhanced blockchain monitoring. That is, disintermedi-

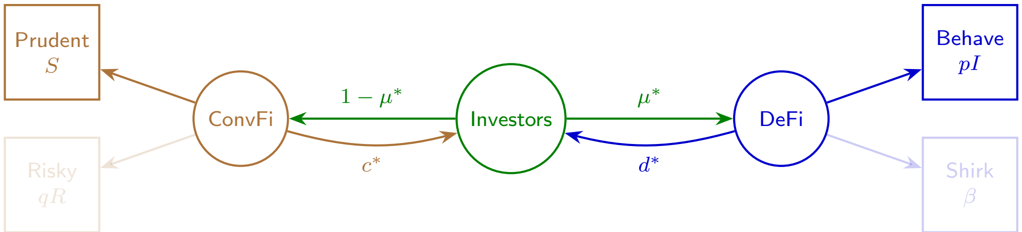

Figure 7 – PB Equilibrium: "ConvFi" stands for the conventional financial firm.

ation can arise in the RS equilibrium even when $\bar{c} > p\bar{d}$, provided that k is high and $\bar{c} \leq qR$. Absent the DeFi firm's entry with a sufficiently low $\bar{d}$ (i.e., $p\bar{d} < qR$), the conventional firm would adopt a prudent management strategy; but the presence of the DeFi competitor disrupts this efficient capital allocation in the conventional financial sector.

5.2 When the DeFi Firm Behaves

We now turn to the analysis of equilibria in which the DeFi firm behaves responsibly in project management after raising funds in the borrowing market. As discussed in Section 5.1, PS and RS equilibria, in which the DeFi firm shirks *ex post*, arise when blockchain-based monitoring capabilities are significantly enhanced, i.e., when k is sufficiently large. In this section, we identify the range of k that gives rise to equilibria distinct from the PS and RS types, thereby completing our analysis of the strategic interaction between the DeFi firm's *ex-post* project management decisions and the investors' monitoring abilities enabled by blockchain technology.

PB Equilibrium: We first analyze the equilibrium type, hereafter referred to as "PB," which stands for the equilibrium strategy profile that the conventional firm adopts the "prudent" risk management and the DeFi firm "behaves" responsibly in project management. Figure 7 graphically illustrates the stylized structure of PB equilibrium. According to Lemma 1, the conventional firm offers a contract with repayment $c^* \leq \bar{c}$, and the DeFi firm issues a security with repayment $d^* \leq \bar{d}$ in equilibrium. Furthermore, investors will get payoffs c^* and pd^* from financing the conventional firm and the DeFi firm, respectively. The PB equilibrium is characterized bythe following theorem.

Theorem 4. *The PB equilibrium is characterized as follows:*

(i) A PB equilibrium in which all investors invest in the conventional firm ($\mu^* = 0$) exists

if and only if

$$kpI \leq p\overline{d} < \overline{c}. \tag{9}$$

In equilibrium, the conventional firm offers $c^* = p\overline{d}$ *and the DeFi firm offers* $d^* = \overline{d}$.

(ii) *A PB equilibrium in which all investors hold the securities issued by the DeFi firm* ($\mu^* = 1$) *exists if and only if*

$$qR \leq \overline{c} < p\overline{d}. \tag{10}$$

In equilibrium, the conventional firm offers $c^* = \overline{c}$ *and the DeFi firm offers* $d^* = \frac{1}{p}\overline{c}$.

In the PB equilibrium with $\mu^* = 0$ described in Theorem 4-(i), the conventional firm outperforms the DeFi firm in securing funds from investors. To establish this equilibrium, the conventional firm should be able to offer larger repayment from its financial returns than the DeFi firm does. This competitive advantage is represented by the condition $p\overline{d} < \overline{c}$. By offering $c \in [p\overline{d}, \overline{c}]$, the conventional firm can attract all the investors and its profit is maximized at $c^* = p\overline{d}$. Indeed, $pd^* = p\overline{d}$ is the maximum payoff the DeFi firm can promise when behaving responsibly ($d \leq \overline{d}$). Furthermore, the DeFi firm cannot profitably deviate from its equilibrium strategy. The only possible deviation is to offer disproportionately high repayment $d' > \overline{d}$, which would induce the DeFi firm to shirk *ex post*. However, condition (9) implies that the DeFi firm cannot successfully raise funds with such a deviation; even with full investor participation, the payoff to investors from accepting $d' > \overline{d}$ is kpd', which falls short of $c^* = p\overline{d}$. Finally, the conventional firm has no incentive to deviate from offering $c^* = p\overline{d}$. Any repayment $c' < c^*$ will be rejected outright by investors. Moreover, the conventional firm's payoff under full financing, $\max\{S - c, q(S - c)\}$, decreases in c, so raising the repayment beyond c^* would only reduce its net financial payoff.

In contrast, the PB equilibrium with $\mu^* = 1$ described in Theorem 4-(ii) arises when condition (10) is satisfied, i.e., the DeFi firm holds a stronger competitive advantage, $p\overline{d} > \overline{c}$. This inequality enables the DeFi firm to provide a larger expected payoff to investors than the conventional firm while maintaining its incentive for responsible behavior in project management. The DeFi firm outcompetes the conventional firm by offering d^* such that investors earn $pd^* = p\overline{d} > \overline{c} = c^*$, where $\overline{c}$ represents the maximum payoff the conventional firm can provide to investors while ensuring ex-post prudent risk management. Furthermore, neither firm can profitably deviate from their equilibrium strategies. The conventional firm

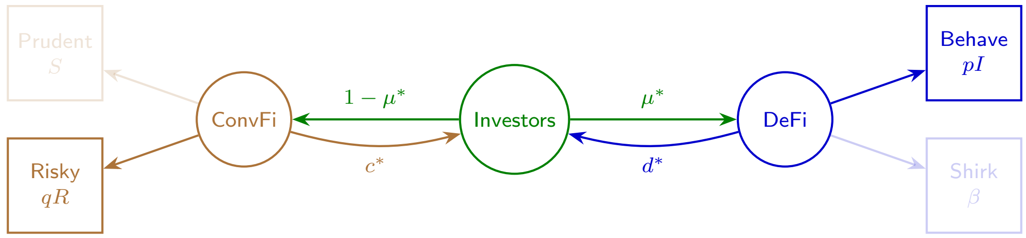

Figure 8 – RB Equilibrium: "ConvFi" stands for the conventional financial firm.

cannot attract investors by offering a contract with higher repayment $c' > c^* = \bar{c}$ because such an offer implies excessive financial risk and thus provides a strictly lower payoff than the DeFi firm's offer ($qc' \leq qR < p\bar{d}$). Similarly, the DeFi firm finds it unprofitable to deviate by increasing its repayment obligation to $d' > \bar{d}$. According to (2), such deviation would induce the DeFi firm to shirk *ex post*, yielding it either $\beta = p(I - \bar{d})$ if its shirking is not detected or $p(I - d') < p(I - \bar{d})$ if shirking is detected, while the net financial income from responsible behavior under $d^* \leq \bar{d}$ is $p(I - d^*) \geq p(I - \bar{d})$. Thus, pursuing private benefits from shirking cannot offset the increased borrowing cost. As a result, the DeFi firm will not excessively raise its repayment obligation beyond what is necessary.

A noteworthy implication of the PB equilibrium is that there is no risk-shifting when one borrower holds a sufficiently strong competitive advantage over its opponent to win the borrowing game without excessively increasing borrowing costs. Nevertheless, competition can lead to inefficiency due to capital misallocation when the DeFi firm wins the borrowing game. For instance, the PB equilibrium with $\mu^* = 1$ can exist even if $\bar{c} < p\bar{d} = pI - \beta < S$, meaning that investors fund the DeFi firm, even though it generates a strictly lower NPV than the conventional firm. This occurs because borrowers' competitive advantages in the borrowing market are only loosely aligned with their revenue structures (i.e., NPVs of their underlying assets). However, the structure of competition is primarily determined by cost structures—namely, how much borrowers can share their investment returns with investors without distorting their ex-post incentives for responsible risk management.

RB Equilibrium: We now analyze the last equilibrium outcome, referred to as "RB" type, which stands for the equilibrium strategy profile where the conventional firm makes a "risky" investment and the DeFi firm "behaves" responsibly in project management. Figure 8 depicts the structure of RB equilibrium. In this equilibrium, the conventional firm offers a contract with repayment $c^* > \bar{c}$ and the DeFi firm issues a security with repayment $d^* \leq \bar{d}$. An investor earns a payoff of qc^* if investing in the conventional firm and pd^* if funding the DeFi firm.

The RB equilibrium is characterized as follows.

Theorem 5. *The RB equilibrium is characterized as follows:*

(i) There exists an RB equilibrium where all investors invest in the conventional firm ($\mu^* = 0$) if and only if

$$\bar{c} < p\bar{d} < qR \ \ and \ \ k \leq \frac{p\bar{d}}{p\bar{d} + \beta}. \tag{11}$$

In equilibrium, the conventional firm offers $c^* = \frac{p\bar{d}}{q}$ and the DeFi firm offers $d^* = \bar{d}$.

(ii) There exists an RB equilibrium where investors with measure $\mu^* \in (0, 1)$ fund the DeFi firm if and only if

$$\bar{c} < p\bar{d} = qR \ \ and \ \ k \leq \max\left\{\frac{p\bar{d}}{p\bar{d} + \beta}, \frac{p\bar{d} - (1 - \mu^*)\beta}{p\bar{d}}\right\} \tag{12}$$

In equilibrium, the conventional firm offers $c^* = \frac{p\bar{d}}{q}$ and the DeFi firm offers $d^* = \bar{d}$.

(iii) There exists an RB equilibrium where all investors invest in the DeFi firm ($\mu^* = 1$) if and only if

$$\bar{c} \leq qR < p\bar{d}. \tag{13}$$

In equilibrium, the conventional firm offers $c^* = R$ and the DeFi firm offers $d^* = \frac{qR}{p}$.

The RB equilibrium with $\mu^* = 0$ in Theorem 5-(i) arises when condition (11) is satisfied. The first inequality implies that the conventional firm can design a contract $c^* \geq \frac{p\bar{d}}{q} > \bar{c}$ that delivers a higher payoff than the DeFi firm's offer ($qc^* \geq pd^*$), while also incentivizing the conventional firm to take excessive risk ($c^* > \bar{c}$). Furthermore, the same inequality ensures that the conventional firm cannot profitably deviate from its equilibrium strategy. Any deviation contract $c' \leq \bar{c}$, which induces the conventional firm to manage its risk prudently, cannot attract any investor since $c' < pd^*$. Likewise, any deviation offer $c' > \frac{p\bar{d}}{q}$ would only raise the conventional firm's borrowing cost without providing additional benefits.

Condition (11) also ensures that the DeFi firm has no opportunity for profitable deviation. First, any deviation offer $d' < \bar{d}$ cannot provide a strictly higher payoff to investors than the conventional firm's equilibrium offer, as investors would receive at most $pd' < p\bar{d} = qc^*$.

Likewise, any deviation with $d' > \overline{d}$ is unprofitable for the DeFi firm. To attract investors under full financing ($\mu' = 1$), the DeFi firm would need to offer repayment high enough to satisfy $kpd' > p\overline{d}$. However, when blockchain monitoring technology is weak (i.e., k is low), investors demand excessively high repayment d' due to the reduced likelihood of enforcing the DeFi firm's responsible behavior. Notably, under the weak monitoring conditions specified in (11), any shirk-inducing deviation remains unattractive, even if the DeFi firm promises to allocate its entire financial return to investors (i.e., $d' = I$). In other words, poor blockchain-based monitoring paradoxically reinforces the DeFi firm's ex-post responsible behavior. The same reasoning underlies the RB equilibrium with $\mu^* \in (0, 1)$ under condition (12) in Theorem 5-(ii).

Lastly, the RB equilibrium with $\mu^* = 1$ in Theorem 5-(iii) exists if and only if condition (13) is satisfied. Specifically, the DeFi firm can offer repayment $d^* \geq \frac{qR}{p}$ that provides investors with a payoff pd^* higher than the maximum payoff qR the conventional firm can deliver under ex-post excessive risk-taking. Conversely, the DeFi firm has no incentive to deviate from its equilibrium strategy, given that the conventional firm offers $c^* = R$. The only possible deviation would be $d' > \overline{d}$, which induces the DeFi firm to shirk *ex post*. However, the private benefit from shirking cannot offset the increased borrowing cost. Specifically, such a deviation would yield the DeFi firm either β or $p(I - d')$, both of which are strictly lower than $p(I - d^*) = p(I - \overline{d})$ from (2). Finally, the conventional firm cannot profitably deviate from offering the equilibrium repayment $c^* = R$. The only potentially profitable deviation would be to offer $c' \leq \overline{c}$ and manage the asset risk prudently. However, under (13), such a deviation would only provide investors with a payoff c', which is strictly lower than the payoff $pd^* = qR$ they obtain from funding the DeFi firm.

Regarding the conventional firm's competitive advantage, if the threshold value $\overline{c}$ is sufficiently high, the conventional firm can win the borrowing game without raising its repayment obligation beyond the level that preserves its incentive for prudent risk management. In this case, the conventional firm's optimal strategy is to offer $c^* \leq \overline{c}$ (Theorem 4-(i)). However, if $\overline{c}$ is relatively low, the conventional firm is forced to offer excessively high repayment $c^* > \overline{c}$ to outcompete the DeFi firm in the borrowing market. This high borrowing cost undermines the conventional firm's incentive for prudent risk management and leads to inefficiently excessive risk-shifting (Theorem 5-(i)).

Similarly, profitability of the DeFi firm's underlying asset significantly affects its ex-post incentive for responsible behavior. If the threshold value $\overline{d}$ is sufficiently high, the DeFi firm can sustain its incentive to behave responsibly even while offering a high repayment to compete for funding (Theorem 4-(ii) and Theorem 5-(iii)). On the other hand, if $\overline{d}$ is relatively low, the DeFi firm must promise a disproportionately high repayment to attract investors, which, in turn, induces it to shirk *ex post*.

However, offering high repayment alone cannot convince investors to fund the DeFi firm's project instead of investing in the conventional firm. If blockchain-based monitoring capabilities are weak, investors may prefer to allocate their wealth in the conventional firm unless they receive sufficient incentives to do otherwise. As highlighted in Theorem 2, investors might still choose to fund the DeFi firm—even when it is known to shirk *ex post*— because successfully "catching" the DeFi firm's misbehavior yields a highly rewarding payoff compared to the return from investing in the conventional firm. However, when monitoring capabilities are relatively weak, the potential gains from monitoring will diminish, making the conventional firm's offer a more attractive option for investors.

A weak blockchain-based monitoring system also discourages the DeFi firm from raising funds by offering excessively high repayment, which may induce shirking *ex post*. When the conventional firm holds a stronger competitive advantage over the behaving DeFi firm by taking excessive risk (i.e., $\bar{c} < p\bar{d} \leq qR$), the DeFi firm must promise a large repayment ($d > \bar{d}$) to attract investors. However, this strategy significantly undermines the DeFi firm's ex-ante profitability, as it will attempt to evade its repayment burden by shirking *ex post*, thereby lowering ex-ante expected investment returns. The only way to restore its *ex-ante* profitability is to guarantee responsible behavior with a high likelihood, which could be enforced through enhanced blockchain monitoring technology with a high k. Without improvements in monitoring, the DeFi firm will avoid financial losses from its ex-post misbehavior by offering a relatively low repayment, thereby splitting the investors' funds with the conventional firm.

5.3 Summary

In this section, we provide an overview of our analysis in Section 5.1 and 5.2. We interpret the equilibrium conditions in terms of the competitive advantages of the conventional and DeFi firms in the borrowing market. Specifically, we compare the sizes of $\bar{c}$ and $p\bar{d}$. Table 1 summarizes the types of coalition-proof equilibria along with their corresponding conditions.

- If the DeFi firm lacks a competitive advantage and operates with a weak blockchain-based monitoring system, the conventional firm attracts all investors (conditions (5), (7), and (9)).

Equilibrium Type	$\boldsymbol{\mu^*}$	Equilibrium Conditions	Equilibrium Offers	
			$\boldsymbol{c^*}$	$\boldsymbol{d^*}$
PS	$\mu^* = 0$	(5): $p\bar{d} \leq kpI \leq \bar{c}$	kpI	I
	$\mu^* = 1$	(6): $p\bar{d} < \bar{c} \leq kpI$, $qR \leq \bar{c}$	$\bar{c}$	$\frac{\bar{c}}{kp}$
RS	$\mu^* = 0$	(7): $p\bar{d} \leq kpI \leq qR$, $\bar{c} \leq kpI$	$\frac{1}{q}kpI$	I
	$\mu^* = 1$	(8): $p\bar{d} \leq qR \leq kpI$, $\bar{c} \leq qR$	R	$\frac{qR}{kp}$
PB	$\mu^* = 0$	(9): $kpI \leq p\bar{d} < \bar{c}$	$p\bar{d}$	$\bar{d}$
	$\mu^* = 1$	(10):$qR \leq \bar{c} < p\bar{d}$	$\bar{c}$	$\frac{\bar{d}}{p}$
RB	$\mu^* = 0$	(11): $\bar{c} < p\bar{d} < qR$, $k \leq \frac{p\bar{d}}{p\bar{d}+\beta}$	$\frac{p\bar{d}}{q}$	$\bar{d}$
	$0 < \mu^* < 1$	(12): $\bar{c} < p\bar{d} = qR$, $k \leq \left(\frac{p\bar{d}}{p\bar{d}+\beta}\right) \vee \left(\frac{p\bar{d}-(1-\mu^*)\beta}{p\bar{d}}\right)$	$\frac{p\bar{d}}{q}$	$\bar{d}$
	$\mu^* = 1$	(13): $\bar{c} \leq qR < p\bar{d}$	R	$\frac{qR}{p}$

Table 1 – Summary of Coalition-Proof Equilibria

- The conventional firm adopts a prudent risk-management strategy when its competitive advantage is sufficiently high (conditions (5) and (9)) but adopts excessive risk-taking if its competitive advantage is moderate (condition (7)).

■ If the DeFi firm lacks a competitive advantage but benefits from a strong blockchain-based monitoring system, it attracts all investors and then attempts to shirk (conditions (6) and (8)).

- These equilibria are characterized by the high-risk "catch-me-if-you-can" game and disintermediation in the conventional financial (banking) sector. In fact, competition harms investors: without the entry of the underperforming DeFi firm with enhanced blockchain-based collective monitoring technology, investors would allocate funds to the conventional firm, incentivizing it to manage risk prudently.

■ If the DeFi firm has a competitive advantage, it behaves responsibly (conditions (10) – (13)).

- If the competitive advantage is sufficiently high, i.e., $p\bar{d} > qR$, the DeFi firm attracts all investors (conditions (10) and (13)).

- If the DeFi firm's competitive advantage is not sufficiently high, i.e., $p\overline{d} < qR$, a weak blockchain-based monitoring system reinforces ex-post responsible behavior (condition (11)).[9] The indifference condition $p\overline{d} = qR$, as in (12), represents a special case where funds are divided between conventional and DeFi firms.

6 Shirking-Proof Equilibria

The main analysis of Section 5 is based on the refinement criterion of coalition-proofness under which the DeFi firm assumes that investors in the borrowing market will respond to its out-of-equilibrium, shirk-inducing offers in the most favorable way, maximizing its potential deviation payoff. This raises the question of whether the equilibrium outcomes in Section 5 remain robust under alternative refinements.

To address this question, we characterize all four equilibria under a new refinement criterion: *shirking-proofness*. We first formally define shirking-proofness as follows.

Definition 3. (μ^*, d^*, c^*) *is called shirking-proof if and only if there is no* (d', μ') *such that* $d' > \overline{d}$*, and*

$$W(d', 0) > W(d^*, \mu^*) \quad \textit{and} \quad V(d', 0) > U,$$

where $U = qc^*$ *if* $c^* > \overline{c}$ *and* $U = c^*$ *if* $c^* \leq \overline{c}$.

This refinement assumes that the DeFi firm believes that no investor will fund its project if it offers an out-of-equilibrium security with a shirk-inducing repayment (i.e., $d' > \overline{d}$). In other words, the DeFi firm adopts a pessimistic belief about out-of-equilibrium outcomes, assuming that any borrowing offer inferred to incentivize shirking *ex post* will be outright rejected in the financial market, yielding zero payoff. Unlike coalition-proofness refinement, shirking-proofness imposes stricter discipline on the DeFi firm's behavior. Specifically, anticipating that a shirk-inducing contract would result in zero funding, the DeFi firm is strongly discouraged from deviating and has an even greater incentive to adhere to its prescribed equilibrium strategy. In sum, the coalition-proofness refinement minimizes the DeFi firm's net gains from playing the prescribed equilibrium strategy, whereas the shirking-proofness refinement maximizes them.

Correspondingly, we define the shirking-proof equilibrium as follows.

[9] If the DeFi firm lacks sufficient competitive advantage but benefits from a strong monitoring system, this corresponds to condition (8).

Equilibrium Type	μ^*	Equilibrium Conditions	Equilibrium Offers	
			c^*	d^*
PS	$\mu^* = 0$	$p\overline{d} \leq kpI \leq \overline{c}$	kpI	I
	$\mu^* = 1$	$p\overline{d} < \overline{c} \leq kpI$, $qR \leq \overline{c}$	$\overline{c}$	$\frac{\overline{c}}{kp}$
RS	$\mu^* = 0$	$p\overline{d} \leq kpI \leq qR$, $\overline{c} \leq kpI$	$\frac{1}{q}kpI$	I
	$\mu^* > 0$	$p\overline{d} \leq qR \leq kpI$, $\overline{c} \leq qR$	R	$\frac{qR}{kp}$
PB	$\mu^* = 0$	$p\overline{d} \leq \overline{c}$	$p\overline{d}$	$\overline{d}$
	$\mu^* = 1$	$qR \leq \overline{c} < p\overline{d}$	$\overline{c}$	$\frac{\overline{d}}{p}$
RB	$\mu^* = 0$	$\overline{c} < p\overline{d} < qR$	$\frac{p\overline{d}}{q}$	$\overline{d}$
	$0 < \mu^* < 1$	$\overline{c} < p\overline{d} = qR$	$\frac{p\overline{d}}{q}$	$\overline{d}$
	$\mu^* = 1$	$\overline{c} \leq qR < p\overline{d}$	R	$\frac{qR}{p}$

Table 2 – Summary of Shirking-Proof Equilibria: we highlight the differences from Table 1 in red. All the others remain the same.

Definition 4. *(μ^*, d^*, c^*) is called a shirking-proof equilibrium if and only if the following properties hold.*

(i) Subgame-perfection: (μ^*, d^*, c^*) is a pure-strategy subgame-perfect equilibrium;

(ii) Shirking-proofness: (μ^*, d^*, c^*) is shirking-proof;

(iii) Tie-breaking: The DeFi firm behaves responsibly if and only if $d^* \leq \overline{d}$; the conventional firm prudently manages asset risks if and only if $c^* \leq \overline{c}$.

To assess the impact of equilibrium refinements on the DeFi firm's behavior, we characterize the four equilibria under the shirking-proofness refinement and compare them to those under the coalition-proof refinement. Table 2 summarizes the equilibria under shirking-proofness, with the full equilibrium analysis provided in Appendix F. A comparison between Table 1 and Table 2 highlights notable differences in the conditions on k required for equilibrium existence.

First, under the coalition-proofness refinement, k must be sufficiently small for PS, PB, and RB equilibria with $\mu^* < 1$ to exist. As shown in Table 1, coalition-proof equilibria require:

(i) $k \leq \frac{\overline{d}}{I}$ for the existence of a PB equilibrium with $\mu^* = 0$, and

(ii) $k \leq \left(\frac{p\overline{d}}{p\overline{d}+\beta}\right) \vee \left(\frac{p\overline{d}-(1-\mu^*)\beta}{p\overline{d}}\right)$ for the existence of an RB equilibrium with $\mu^* \in [0, 1)$.

When $\mu^* < 1$ in equilibrium, the DeFi firm may have an incentive to achieve full financing by offering an excessively high repayment (i.e., $d' \gg \overline{d}$) to investors while intending to extract private benefits from shirking. In the PB and RB equilibria under coalition-proofness, conditions (i) and (ii) ensure that such a deviation fails to attract investors away from the conventional firm's competitive offer. When blockchain-based monitoring is weak, any shirk-inducing offer becomes unappealing to investors because the probability of detecting shirking remains low despite the promise of excessively high repayment.

However, under shirking-proofness, these restrictions on k are no longer necessary for the PB and RB equilibria to exist (see conditions in red from Table 2). The DeFi firm anticipates that any deviation strategy with $d' > \overline{d}$ will fail to attract even a single investor, resulting in a zero payoff. Consequently, regardless of the value of k, the DeFi firm cannot profitably deviate by offering a shirk-inducing contract that departs from its equilibrium strategy. Likewise, the RS equilibrium with $\mu^* \in (0, 1)$ can exist under the shirking-proofness refinement. The DeFi firm expects that any deviation from its equilibrium offer strategy would fail to raise funds from investors, again leading to a zero payoff. Hence, the DeFi firm would rather divide the available outside capital with the conventional firm.

Another noteworthy feature is that k must be sufficiently high to sustain PS and RS equilibria with $\mu^* = 1$, regardless of the refinement invoked. This follows from the fact that investors' decision to fund the DeFi firm's investment occurs *on the equilibrium path*. Even if the DeFi firm is known to shirk *ex post*, investors will only choose to fund it in exchange for an excessively high repayment when blockchain-based monitoring is strong enough to enforce responsible behavior with high probability. Moreover, when blockchain technology is highly advanced, investors can fully coordinate their participation in blockchain monitoring, which further strengthens enforcement.

7 Policy Implications

7.1 Policy Levers and Their Effects (β and k)

We now examine the policy implications of our model, focusing on the two key levers that shape equilibrium outcomes in the presence of DeFi competition: moral hazard (β) and monitoring efficiency (k). The DeFi firm's competitive advantage is determined by $\overline{d} = I - \frac{\beta}{p}$, where I represents technological productivity and β captures the severity of moral hazard. A higher I or a lower β strengthens the DeFi firm's position in the borrowing market.

Our model suggests two broad policy objectives. The first is to mitigate moral hazard in the emerging DeFi sector (i.e., reducing β). Because market discipline in DeFi remains underdeveloped, policies that strengthen *fiduciary duties*—including the duty of loyalty, the duty of care, and meaningful disclosure requirements—are especially important. For example, allegations against Do Kwon related to the 2022 Terra–Luna collapse centered on breaches of such fiduciary responsibilities.

The second policy objective concerns enhancing monitoring capabilities (i.e., increasing k). Unlike interventions that directly reduce β, policies targeting k require more nuance. One potential avenue involves the adoption of central bank digital currencies (CBDCs). Even absent stricter regulation, integrating CBDCs into the financial system could improve investors' ability to detect misuse of funds. A DeFi ecosystem built on or interoperable with CBDCs would benefit from greater transparency in settlement and fund flows, making illicit activities more readily detectable (Gorton and Zhang, 2023; Rivadeneyra, Hendry and García, 2024).

However, stronger monitoring does not necessarily translate into more efficient capital allocation. When DeFi firms lack a competitive advantage, increasing k can strengthen investors' belief in their ability to "catch" shirking, thereby amplifying the speculative dynamics highlighted in our PS and RS equilibria with $\mu^* = 1$ (conditions (6) and (8)). In such cases, enhanced transparency may paradoxically encourage capital to flow toward underperforming or riskier DeFi projects, generating inefficient disintermediation from the conventional financial sector.

A notable development in this policy space is the GENIUS Act, the first federal legislation establishing a comprehensive regulatory framework for U.S. dollar-based stablecoins. The Act requires issuers to maintain fully backed one-to-one reserves, implements disclosure and technical compliance rules, and—most notably—prohibits stablecoins from paying interest to users.

Our analysis aligns closely with the logic behind the GENIUS Act. In particular, its interest ban directly addresses the incentive distortions we identify: namely, that strong monitoring capacity (k) can induce investors to rationally fund DeFi firms offering unsustainably high promised repayments. By removing yield incentives and strengthening compliance, the Act mitigates the capital misallocation and shirking that may arise absent prudential regulation.

While reducing moral hazard (lowering β) is essential, real-world regulation is neither uniform nor costless. Compliance burdens may reduce shirking incentives but simultaneously raise borrowing costs, potentially increasing the repayment that DeFi firms must offer investors. This introduces a policy trade-off: even as β falls, the cost-induced rise in F may reintroduce speculative dynamics. Extending the model to capture this dual role of regulation—both disciplining firms and reshaping cost structures—would be valuable for future policy design.

A second challenge arises from the global and borderless nature of DeFi. Jurisdictional arbitrage is pervasive: investors can easily shift funds to offshore or lightly regulated platforms, while domestic entities remain subject to stricter fiduciary rules. Variation in enforcement across jurisdictions—captured in our model as heterogeneity in β—can erode the stabilizing effects of any single regulator. This underscores the importance of cross-border coordination, especially in light of the emerging contrast between the EU's MiCA framework and the U.S. GENIUS Act. A natural extension is to introduce heterogeneous investors ("regulated" and "unregulated" types) to examine how uneven enforcement shapes equilibrium capital allocation.

Finally, beyond moral hazard, DeFi ecosystems face exogenous technological risks such as smart contract exploits, oracle manipulation, and MEV extraction. These risks, distinct from shirking, are outside the scope of our baseline model but significantly affect investor welfare. A richer framework incorporating a stochastic failure component could provide a more complete picture of capital misallocation. From a policy standpoint, mitigating these risks may require technical interventions—often described as *embedded supervision*—where regulatory rules are encoded directly into smart contracts, oracle systems, or stablecoin infrastructures themselves. Effective oversight may therefore depend not only on legal frameworks but also on the technical feasibility of embedding compliance into code.

7.2 Robustness of Policy Implications Under Different Refinements

We now examine how the previous policy insights change under the alternative refinement of shirking-proofness. As shown in Section 6, the welfare consequences of increasing monitoring efficiency (k) depend critically on beliefs about investor coordination.

Under coalition-proofness, investors are assumed to fully coordinate in monitoring the DeFi firm's behavior, even following unexpectedly generous repayment offers. This strong confidence in market discipline can induce the DeFi firm to offer excessively high, shirk-inducing repayment terms, triggering the "catch-me-if-you-can" dynamic described earlier. In contrast, the shirking-proofness refinement assumes the opposite: investors expect no coordination in monitoring once the DeFi firm deviates from equilibrium, causing any shirk-inducing deviation to fail.

This distinction yields important differences in policy implications. When $p\overline{d} < \overline{c} < S$, it is efficient for all capital to flow to the conventional firm, which prudently manages risk. Such outcomes occur in PS and PB equilibria with $\mu^* = 0$, but under coalition-proofness, they require k to remain below certain thresholds: $k \leq \overline{c}/(pI)$ in the PS equilibrium and $k \leq \overline{d}/I$ in the PB equilibrium ((5), (9) in Table 1). If investors have strong confidence in their ability to coordinate, the DeFi firm may profitably deviate by offering a high repayment, enticing investors into the catch-me-if-you-can game. This harms welfare both *ex ante* (misallocating capital to an inferior project) and *ex post* (failing to fully deter shirking).

Similarly, when $\overline{c} < p\overline{d} \leq qR$, it remains efficient for all capital to flow to the conventional firm—even if it takes excessive risk. This occurs in the RB equilibrium with $\mu^* < 1$, but again only when k is sufficiently low ((11), (12)). A high k encourages the DeFi firm to offer shirk-inducing repayments, anticipating that investors will accept them to exploit strong monitoring capabilities.

Under the shirking-proofness refinement, however, these concerns disappear. Investors refuse to monitor collectively when offered unexpectedly high repayments, causing any shirk-inducing deviation to fail. As a result, no restrictions on k are required to sustain PS or PB equilibria with $\mu^* = 0$ or RB equilibria with $\mu^* < 1$ (see Table 2).

Finally, regardless of refinement, increasing k may still lead to disintermediation if the DeFi sector is fundamentally less productive. In particular, the PS equilibrium with $\mu^* = 1$ and the PB equilibrium with $\mu^* > 0$ persist under the same conditions across refinements ((6), (8)). Thus, the risk that stronger monitoring induces speculative deviations—potentially intensified by CBDC-based transparency—remains a robust concern for regulators.

8 Conclusion

Our study demonstrates that improved monitoring through blockchain technology can contribute to the emergence of speculative equilibria. We also discuss the corresponding policy implications and hope our findings shed light on how to regulate financial markets when a new technology-driven competing industry emerges. In particular, by examining disintermediation risks associated with CBDC adoption and stablecoin regulation, our findings help inform policy discussions on maintaining financial stability amid technological disruption.

For the equilibrium analysis, we propose two equilibrium refinements: coalition-proofness and shirking-proofness. For each refinement, we examine in detail the conditions under which four different types of equilibria arise, including the catch-me-if-you-can scenario. We show that the gambling equilibrium can emerge when investors are equipped with strong monitoring capabilities, regardless of the refinement adopted. This finding underscores the robustness of our main results, as these refinements represent the two polar cases of investor confidence in the DeFi sector.

Our analysis thus highlights a broader lesson for both researchers and policymakers. The distinctive features of the blockchain-based monitoring mechanism differ fundamentally from conventional notions of transparency and can give rise to speculative equilibria even when transparency improves. This distinction carries direct regulatory implications: policies that focus narrowly on enhancing monitoring capacity, such as the introduction of CBDCs or stablecoin frameworks, may inadvertently destabilize capital allocation unless paired with fiduciary safeguards and cross-border coordination. By making this mechanism explicit, our study contributes not only to the theory of financial competition under new technologies but also to ongoing debates on how to design regulations that preserve the benefits of blockchain while mitigating its destabilizing risks.

References

Ahnert, Toni, Peter Hoffmann, and Cyril Monnet. 2025. "Payment and Privacy in the Digital Economy." *Journal of Financial Economics*, 169, 104050.

Allen, Franklin, and Douglas Gale. 2004. "Competition and Financial Stability." *Journal of Money, Credit and Banking*, 36(3): 453–480.

Allen, Franklin, Elena Carletti, and Robert Marquez. 2011. "The Value of Bank Capital and the Structure of the Banking Industry." *Review of Financial Studies*, 24(4): 983–1018.

Andolfatto, David. 2021. "Assessing the Impact of Central Bank Digital Currency on Private Banks." *Economic Journal*, 131(634): 525–540.

Aumann, Robert. 1959. "Acceptable Points in General Cooperative n-Person Games." In *Contributions to the Theory of Games IV*. Princeton University Press.

Beck, Thorsten, Asli Demirgüç-Kunt, and Ross Levine. 2006. "Bank Concentration, Competition, and Crises: First Results." *Journal of Banking and Finance*, 30(5): 1581–1603.

Berg, Tobias, Valentin Burg, Ana Gombovic, and Manju Puri. 2020. "On the Rise of FinTechs: Credit Scoring Using Digital Footprints." *Review of Financial Studies*, 33(7): 2845–2897.

Bernheim, B.Douglas, Bezalel Peleg, and Michael D Whinston. 1987. "Coalition-Proof Nash Equilibria I. Concepts." *Journal of Economic Theory*, 42(1): 1–12.

Boualam, Youness, and Peter Yoo. 2022. "Fintech Disruption, Banks, and Credit (Dis-)Intermediation: When Do Foes Become Friends?" *SSRN Working Paper*. Available at http://dx.doi.org/10.2139/ssrn.4001998.

Boyd, John H, and Gianni De Nicolo. 2005. "The Theory of Bank Risk Taking and Competition Revisited." *Journal of Finance*, 60(3): 1329–1343.

Broecker, Thorsten. 1990. "Credit-Worthiness Tests and Interbank Competition." *Econometrica*, 58(2): 429–452.

Brunnermeier, Markus, and Jennifer Payne. 2024. "FinTech Lending, Banking, and Information Portability." *Working Paper*.

Capponi, Agostino, and Ruizhe Jia. 2025. "Liquidity Provision on Blockchain-Based Decentralized Exchanges." *Review of Financial Studies*. forthcoming.

Choi, Kyoung Jin, and Keeyoung Rhee. 2025. "From the Fringe to the Core: Stablecoins and the Future of Banking Stability." Working Paper.

Choi, Kyoung Jin, Ryan Henry, Alfred Lehar, Joel Reardon, and Reihaneh Safavi-Naini. 2021. "A Proposal for a Canadian CBDC." *SSRN Working Paper*. Available at SSRN: https://ssrn.com/abstract=3786426orhttp://dx.doi.org/10.2139/ssrn.3786426.

Cong, Lin William, and Simon Mayer. 2025. "Strategic Digitization in Currency and Payment Competition." *Journal of Financial Economics*, 168, 104055.

Cong, Lin William, and Zhiguo He. 2019. "Blockchain Disruption and Smart Contracts." *Review of Financial Studies*, 32(5): 1754–1797.

Cong, Lin William, Yuanyu Qu, and Guojun Wang. 2025. "Blockchains for Environmental Monitoring: Theory and Empirical Evidence from China." *Review of Finance*. forthcoming.

Demirgüç-Kunt, Asli, and Harry Huizinga. 2004. "Market Discipline and Deposit Insurance." *Journal of Monetary Economics*, 51(2): 375–399.

Duflo, Esther, Michael Greenstone, Rohini Pande, and Nicholas Ryan. 2013. "Truth-Telling by Third-Party Auditors and the Response of Polluting Firms: Experimental Evidence from India." *Quarterly Journal of Economics*, 128(4): 1499–1545.

Egan, MArk, Ali Hortaçsu, and Gregor Matvos. 2017. "Deposit Competition and Financial Fragility: Evidence from the US Banking Sector." *American Economic Review*, 107(1): 169–216.

Fernandez-Villaverde, Jesus, Daniel Sanches, Linda Schilling, and Harald Uhlig. 2021. "Central Banking Digital Currency: Central Banking for All?" *Review of Economic Dynamics*, 41: 225–242.

Ferreira, Daniel, and Jin Li. 2025. "Governance and Management of Autonomous Organizations." *Working Paper*.

Flannery, Mark J. 1998. "Using Market Information in Prudential Bank Supervision: A Review of the US Empirical Evidence." *Journal of Money, Credit and Banking*, 30(3): 273–305.

Fuster, Andreas, Matthew Plosser, Philipp Schnabl, and James Vickery. 2019. “The Role of Technology in Mortgage Lending.” *Review of Financial Studies*, 32(5): 1854–1899.

Gorton, Gary B., and Jingyuan Y. Zhang. 2023. “Taming Wildcat Stablecoins.” *The University of Chicago Law Review*, 90(3): 910–971.

Greenstone, Michael, Guojun He, Ruixue Jia, and Tong Liu. 2022. “Can Technology Solve the Principal-Agent Problem? Evidence from China’s War on Air Pollution.” *American Economic Review: Insights*, 4(1): 54–70.

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro. 2021. *DeFi and the Future of Finance.* Wiley.

Hauswald, Robert, and Robert Marquez. 2003. “Information Technology and Financial Services Competition.” *Review of Financial Studies*, 16(3): 921–948.

He, Zhiguo, Jing Huang, and Jidong Zhou. 2023. “Open Banking: Credit Market Competition When Borrowers Own the Data.” *Journal of Financial Economics*, 147(2): 449–474.

Keeley, Michael C. 1990. “Deposit Insurance, Risk, and Market Power in Banking.” *American Economic Review*, 80(5): 1183–1200.

Keister, Todd, and Daniel Sanches. 2023. “Should Central Banks Issue Digital Currency?” *Review of Economic Studies*, 90(1): 404–431.

Kim, Young Sik, and Ohik Kwon. 2023. “Central Bank Digital Currency, Credit Supply, and Financial Stability.” *Journal of Money, Credit and Banking*, 55(1): 297–321.

Landsman, Wayne, Evgeny Lyandres, Edward Maydew, and Daniel Rabetti. 2025. “Auditing Smart Contracs.” Working Paper.

Malinova, Ksenia, and Andreas Park. 2023. “Tokenomics: When Tokens Beat Equity.” *Management Science*, 69(12): 6568–6586.

Martinez-Miera, David, and Rafael Repullo. 2010. “Does Competition Reduce the Risk of Bank Failure?” *Review of Financial Studies*, 23(10): 3638–3664.

Martinez Peria, Maria S., and Sergio L. Schmukler. 2001. “Do Depositors Punish Banks for Bad Behavior? Market Discipline, Deposit Insurance, and Banking Crises.” *Journal of Finance*, 56(3): 1029–1051.

Mazorra, B., M. Reynolds, and V. Daza. 2022. "Price of MEV: Towards a Game Theoretical Approach to MEV." *Proceedings of the 2022 ACM CCS Workshop on Decentralized Finance and Security*, 15–22.

Öz, Burak, Filip Rezabek, Jonas Gebele, Felix Hoops, and Florian Matthes. 2024. "A Study of Mev Extraction Techniques on a First-Come-First-Served Blockchain." *Proceedings of the 39th ACM/SIGAPP Symposium on Applied Computing*, 288–297.

Park, Andreas. 2025. "DeFi vs. TradFi: Convergence, Competition, and Fragility." Working Paper, University of Toronto.

Parlour, Christine, Uday Rajan, and Haoxiang Zhu. 2022. "When FinTech Competes for Payment Flows." *Review of Financial Studies*, 35(11): 4985–5024.

Repullo, Rafael. 2004. "Capital Requirements, Market Power, and Risk-Taking in Banking." *Journal of Financial Intermediation*, 13(2): 156–182.

Rivadeneyra, Francisco, Scott Hendry, and Maria García. 2024. "The Role of Public Money in the Digital Age." Bank of Canada Staff Discussion Paper 2024-11. Available at https://doi.org/10.34989/sdp-2024-11.

U.S. Senate. 2025. "Guarding and Enabling the Nation's Infrastructure Using Stablecoins (GENIUS) Act: Draft Bill Text." *U.S. Senate Banking, Housing, and Urban Affairs Committee.*

Vives, Xavier, and Zhiqiang Ye. 2025. "Information Technology and Lender Competition." *Journal of Financial Economics*, 163, 103957.

Whited, Toni M., Yufeng Wu, and Kairong Xiao. 2022. "Will Central Bank Digital Currency Disintermediate Banks?" *SSRN Working Paper*. Available at SSRN: https://ssrn.com/abstract=4091999.

Williamson, Stephen. 2022. "Central Bank Digital Currency: Welfare and Policy Implications." *Journal of Political Economy*, 130(11): 2829–2861.

Zou, Eric. 2021. "Unwatched Pollution: The Effect of Intermittent Monitoring on Air Quality." *American Economic Review*, 111(6): 2101–2136.

Appendix

A Preliminary Lemmas

Lemma A.1. *For any* (d, μ) *such that* $\overline{d} < d \leq I$ *and* $0 < \mu < 1$*, there exists* (d', μ') *such that (i)* $V(d', \mu') > V(d, \mu)$ *and (ii)* $W(d', \mu') > W(d, \mu)$*.*

Proof. Fix d and μ as stated in the lemma.

Step I: We first prove the lemma for the case $d = I$ and $\mu \in (0, 1)$. Because $d > \overline{d}$, we have $V(d, \mu) = \mu kpI$ and $W(d, \mu) = \mu[\mu pk(I-d) + (1-\mu k)\beta] = \mu(1-\mu k)\beta$, where the last equality holds because $d = I$ by construction. Now, consider (d', μ') where

$$d' = \min\{\mu kI(1+\epsilon), \overline{d}\} \leq \overline{d} \quad \text{and} \quad \mu' = 1.$$

where $\epsilon > 0$ is sufficiently small so that $\mu kI(1+\epsilon) < I$ and $\epsilon < (1-\mu)pI(1-\mu k)$. Note that $V(d', \mu') = pd' \geq \mu kpI(1+\epsilon) > V(d, \mu)$. Next, because $d' \leq \mu kI(1+\epsilon)$ and $d' \leq \overline{d}$,

$$W(d', \mu') = p(I - d') \geq pI(1 - \mu k(1+\epsilon)) > \mu(1-\mu k)pI \geq \mu(1-\mu k)\beta = W(d, \mu)$$

where the first strict inequality holds due to the assumption $\epsilon < (1-\mu)pI(1-\mu k)$, and the last strict inequality follows from the assumption $pI - 1 \geq \beta$.

Step II-(1): From now on, focus on the case $d \in (\overline{d}, I)$ and $\mu \in (0, 1)$. Define $d^\dagger(m) := \frac{V(d,\mu)}{mkp} = \frac{\mu}{m}F$ for any $m \in [0, 1]$. Let $m^* \in (\mu, 1)$ be the cutoff such that $\overline{d}(m^*) = \overline{d}$, and hence

$$\overline{d} < d^\dagger(m) \leq I \quad \Longleftrightarrow \quad \frac{d}{I}\mu \leq m < m^*. \tag{14}$$

Note that $\overline{d}(\mu) = d$ and $m^* > \mu$. Hence, $[0, \mu) \subsetneq [0, m^*)$ by construction.

Step II-(2): Pick any $\mu' \neq \mu$ such that $d\mu/I \leq \mu' < m^*$. We claim (a) $\overline{d} < d^\dagger(\mu') < I$, (b) $V(d^\dagger(\mu'), \mu') = V(d, \mu)$, and (c) $W(d^\dagger(\mu'), \mu') > W(d, \mu)$. The property (a) follows from (14). Next,

$$V(d^\dagger(\mu'), \mu) = k\mu' pd^\dagger(\mu') = k\mu' p\frac{\mu}{\mu'}d = k\mu pd = V(d, \mu)$$

and hence (b) follows. To prove (c), suppose for contradiction $W(d^\dagger(\mu'), \mu') \leq W(d, \mu)$ for any $\mu' \in [d\mu/I, m^*)$. By continuity, we also have $W(d^\dagger(\mu'), \mu') \leq W(d, \mu)$ for $\mu' = m^*$. Since

$d^\dagger(\mu) = d$,

$$W(d^\dagger(\mu), \mu) = W(d, \mu) \geq \max_{m \in [\mu d/I, m^*]} W(d^\dagger(m), m) \tag{15}$$

Due to the strict convexity of

$$W(d^\dagger(m), m) = m[mkp(I - d^\dagger(m)) + (1 - mk)\beta] = m[mk(pI - \beta) - U + \beta],$$

all solutions for the optimization problem in (15) must lie at a corner in the domain, implying $\mu = \mu d/I$ (recall $\mu < m^*$ by construction). This contradicts the hypothesis $d < I$.

Step II-(3): Pick any μ' that satisfies the properties (a)–(c) stated in Step II-(2). Also, pick a sufficiently small $\epsilon > 0$ such that $d' \equiv d^\dagger(\mu') + \epsilon < I$. We will prove that (d', μ') satisfies the properties (i) and (ii) stated in the lemma. First,

$$V(d', \mu') = V(d^\dagger(\mu') + \epsilon, \mu') > V(d^\dagger(\mu'), \mu') = V(d, \mu)$$

where the inequality holds because the mapping $\tilde{d} \mapsto V(\tilde{d}, \mu')$ is strictly increasing in $\tilde{d}$ over $(\overline{d}, I)$, and the last equality follows from the property (b) stated in Step II-(2). Next, $W(d^\dagger(\mu'), \mu') > W(d, \mu)$ by the property (c) stated in Step II-(2), and thus

$$W(d^\dagger(\mu'), \mu') > W(d', \mu') = W(d^\dagger(\mu') + \epsilon, \mu') > W(d, \mu)$$

provided that $\epsilon > 0$ is sufficiently small. *Q.E.D.*

Lemma 2. *$W(\overline{d}, 1) > W(d, \mu)$ for any $(d, \mu) \in (\overline{d}, I] \times [0, 1]$.*

Proof. Note that $W(\overline{d}, 1) = p(I - \overline{d}) = \beta$. On the other hand, for any $(d, \mu) \in (\overline{d}, I] \times [0, 1]$,

$$\begin{aligned} W(d, \mu) &= \mu[k\mu p(I - d) + (1 - \mu k)\beta] \\ &< \mu[k\mu p(I - \overline{d}) + (1 - \mu k)\beta] = \mu[k\mu\beta + (1 - \mu k)\beta] = \mu\beta \leq \beta. \end{aligned}$$

This completes the proof. *Q.E.D.*

B Proof of Theorem 2

In this section, we characterize the PS equilibrium. The incentive-compatibility for the project selection by the conventional firm and the DeFi firm requires

$$c^* \leq \bar{c} = \frac{S - qR}{1 - q} \quad \text{and} \quad d^* > \bar{d} = I - \frac{\beta}{p} \tag{16}$$

In this proof, let $W(d, \mu)$ and $V(d, \mu)$ respectively denote the DeFi firm's profit and each individual investor's expected revenue for the case that the DeFi firm attracts a fraction μ of investors with the repayment term d, as defined in (4) and (3).

In what follows, we will focus, without loss of generality, on equilibria such that, if the conventional firm deviates by offering $c' \neq c^*$, all investors coordinate to accept the DeFi firm 's offer d^* rather than c' if and only if

$$V(d^*, 1) = kpd^* \geq \begin{cases} c' & \text{if } c' \leq \bar{c}, \\ qc' & \text{if } c' > \bar{c}. \end{cases} \tag{17}$$

In other words, in the subgame that follows any deviation by the conventional firm, investors play the Nash equilibrium in which the conventional firm's final payoff is lower than in any other Nash equilibrium. This particular off-the-path play constitutes the most severe punishment for any deviation by the conventional firm, thereby allowing a PS equilibrium to be sustained for the widest set of parameters.

There are three possible cases with respect to the size of the securities that the DeFi firm issues in equilibrium: $\mu^* \in (0, 1)$, $\mu^* = 0$, and $\mu^* = 1$. However, we may exclude the case such that $\mu^* \in (0, 1)$ based on Lemma A.1.

B.1 $\mu^* = 1$

We first investigate an equilibrium where all investors purchase the DeFi firm's securities (i.e., $\mu^* = 1$). We begin by investigating necessary properties that any such equilibrium (if any) needs to satisfy. In such an equilibrium, every investor weakly prefers purchasing the firm's security to investing in the conventional firm, i.e.,

$$kpd^* \geq \bar{c}. \tag{18}$$

If $kpd^* < \overline{c}$, the conventional firm can profitably deviate by offering $c' \in (kpd^*, \overline{c})$ that will attract all lenders. Note that d^* cannot exceed I, and thus, (18) also implies $kpI \geq \overline{c}$.

Note that $W(d, 1)$ decreases in d, and thus, we necessarily have $V(d', 1) \leq c^*$ for all $d' < d^*$; otherwise, the DeFi firm can increase its payoff by deviating to $d' < d^*$, which will still be accepted by all investors. This implies

$$V(\overline{d}, 1) = p\overline{d} \leq c^* \quad \text{and} \quad V(d^*, 1) = kpd^* \leq c^* \leq \overline{c}.$$

Furthermore, to make sure all investors prefer to purchase the DeFi firm's securities rather than invest in the conventional firm, we also need $kpd^* \geq c^*$. Finally, to make sure the conventional firm has no incentive to deviate, we must have $\overline{c} \geq qR$. Suppose this is not the case and the conventional firm deviates by offering $c' \in (\overline{c}/q, R)$. c' is larger than $\overline{c}$, and thus the conventional firm will make a risky investment once c' is accepted by an investor, in which case the investor would obtain a final expected revenue strictly larger than $qc' = \overline{c} > V(d^*, 1)$. Thus, the conventional firm's offer c' will be accepted by all investors and the conventional firm will obtain a strictly positive payoff.

Summing up, the following is the necessary condition for any PS equilibrium with $\mu^* = 1$ to exist, given the investors' off-the-path strategies as specified in the paragraph surrounding (17):

$$p\overline{d} = pI - \beta < c^* = \overline{c} = kpd^* \leq kpI \quad \text{and} \quad qR \leq \overline{c}. \tag{19}$$

Note that Assumption 4 implies that the first inequality in (19) holds strictly.

Now, we prove that there is a PS equilibrium such that $\mu^* = 1$ exists under the condition (19), by showing that both the DeFi firm and conventional firm have no incentive to deviate from d^* and c^* as characterized in (19). First, consider the DeFi firm's deviation to $(d', \mu') \neq (d^*, \mu^*)$. By Lemma A.1, we may focus on the deviations such that $\mu' = 1$ or $d' \leq \overline{d}$. For any (d', μ') such that $d' > \overline{d}$ and $\mu' = 1$, the condition $V(d', \mu') = k\mu' pd' \geq c^*$ requires $d' \geq c^*/(pk\mu') = d^*/\mu' = d^*$. However, any such (d', μ') would not be profitable for the DeFi firm because all investors would rather prefer to invest in the conventional firm and obtain c^*. Any (d', μ') such that $d' \leq \overline{d}$ is also not acceptable to the investors because $V(d', \mu') = pd' \leq p\overline{d} < c^*$ for any $\mu' \in [0, 1]$.

Finally, consider the conventional firm, who cannot benefit from deviating to $c' < c^* = \overline{c}$ as all such c' would be rejected by the investors for sure. For $c' > c^* = \overline{c}$ to be accepted, we must have $qc' \geq V(d^*, \mu^*) = kpd^* = \bar{c}$. However, for any such c', $q(R - c') \leq qR - \bar{c} \leq 0$, and thus any such deviations will not be profitable for the conventional firm.

B.2 $\mu^* = 0$

Let us characterize conditions for the existence of the safe-shirking equilibrium with $\mu^* = 0$, where the DeFi firm fails to raise capital and thus gets zero payoff. Given that $\mu^* = 0$, the DeFi firm's shirking behavior is never detected, and thus, any lender's payoff from accepting the DeFi firm's offer is zero on the equilibrium path. Note that the DeFi firm earns zero profit in this equilibrium.

First, we claim that

$$\max\{kpI, pI - \beta\} \leq \bar{c} = \frac{S - qR}{1 - q}. \tag{20}$$

is a necessary condition for the equilibrium of interest to exist. Note that all investors earn c^* in any PS equilibrium with $\mu^* = 0$. First, suppose for contradiction $kpI > \bar{c}$. Since $c^* \leq \bar{c}$ from (16), the DeFi firm can profitably deviate by offering (d', μ') such that $\mu' = 1$, $d' < I$ and $kpd' > \bar{c}$. If $d' > \bar{d}$, the investors' expected payoff from accepting (d', μ') is $V(d', \mu') = kpd' > \bar{c} \geq c^*$. If $d' \leq \bar{d}$, the investors would earn $V(d', \mu') = pd' > kpd' > \bar{c} \geq c^*$ by accepting (d', μ'). In both cases, $V(d', \mu') > c^*$, and thus all investors will accept the DeFi firm's offer, so the DeFi firm can get the payoff equal to either $p(I - d') > 0$ or $kp(I - d') + (1 - k)\beta > 0$. Next, suppose for contradiction $p\bar{d} = pI - \beta > \bar{c}$. Then, there exists a $d' \leq \bar{d}$ such that $V(d', \mu') = pd' > \bar{c} \geq c^*$ for any $\mu \in [0, 1]$. Therefore, the DeFi firm can profitably deviate by offering d' to attract all investors, yielding the DeFi firm a positive payoff.

Next, we claim that

$$pI - \beta = p\bar{d} \leq kpI = c^* \leq \bar{c} \quad \text{and} \quad d^* = I \tag{21}$$

are also necessary conditions for the equilibrium of interest to exist. First, suppose for contradiction $kpI < pI - \beta \leq \bar{c}$. The necessity of $c^* = kpI$ is straightforward. If $c^* < kpI$, the DeFi firm could attract all investors by offering $(d', \mu') = (I, 1)$ because $V(I, 1) = kpI > c^*$ and $W(I, 1) > 0$. If $c^* > kpI$, the conventional firm can increase its profit by deviating $c' \in (kpI, c^*)$, which will be still accepted by all investors because $c' < V(d^*, 1) \leq V(I, 1) = kpI$. Next, if $kpI = c^* < pI - \beta = p\bar{d} \leq \bar{c}$, again, the DeFi firm can attract all investors by offering $d' = \overline{d}$ because $V(\overline{d}, \mu') = p\overline{d} = pI - \beta > c^*$ for all $\mu' \in [0,1]$. This completes the proof of the necessity of the first condition in (21). Finally, the necessity of $d^* = I$ is also straightforward, because otherwise, the conventional firm can increase its profit by offering c' such that $c^* > c' \geq kpI > kpd^* = V(d^*, 1)$.

Next, we show that (21) is also a sufficient condition for a PS equilibrium with $\mu^* = 0$ to exist. Specifically, suppose that the conventional firm offers $c^* = kpI$, and the DeFi firm offers $d^* = I$, and all investors accept the conventional firm's offer (hence, $\mu^* = 0$). We first show that the DeFi firm cannot profitably deviate. Suppose the DeFi firm deviates by offering $d' < d^* = I$. If $d' \in (\overline{d}, d^*)$, the investors' payoff from accepting d' is at most kpd', but $kpd' < kpd^* = kpI \leq c^*$. Thus, the DeFi firm fails to attract any investors. If $d' \in [0, \overline{d}]$, $V(d', \mu) = pd' \leq p\overline{d} = pI - \beta \leq c^*$, and thus all investors weakly prefer to accept c^* rather than d'; thus, we can support the PS equilibrium by assuming that all investors would still accept c^* in this case.

We next show that it is optimal for the conventional firm to offer c^*. If the conventional firm deviates to $c' \in (c^*, \overline{c}]$, all investors will invest in the conventional firm, but the conventional firm will eventually earn less than the equilibrium profit. If the conventional firm offers $c' > \overline{c}$, the conventional firm's payoff from the deviation is bounded above by $q(R - \overline{c}) = \frac{q}{1-q}(R - S)$. However, since $c^* \leq \overline{c}$, equivalently, $\frac{q}{1-q}(R - S) \leq S - c^*$, the conventional firm never finds $c' > \overline{c}$ strictly profitable.

C Proof of Theorem 3

From the incentive-compatibility for the project selection by the DeFi and conventional firms, the necessary conditions for an RS equilibrium to exist are

$$d^* > \overline{d} = I - \frac{\beta}{p} \quad \text{and} \quad c^* > \overline{c} = \frac{S - qR}{1 - q} \tag{22}$$

In any RS equilibrium (if any), let $U^* = \max\{qc^*, V(d^*, \mu^*)\}$ denote each investor's pecuniary revenue in equilibrium, where μ^* denotes the total fraction of the DeFi firm's securities that the investors purchase, and V is as defined in (3). We will also adopt the definition of W, the DeFi firm's payoff, as defined in (4). By the same argument discussed in the proof of Theorem 2, we will focus, without loss of generality, on equilibria such that, if the conventional firm deviates by offering $c' \neq c^*$, all investors coordinate to accept the DeFi firm's offer d^* rather than c' if and only if (17) holds. Also, by Lemma A.1, we may focus on two cases, $\mu^* = 0$ and $\mu^* = 1$.

C.1 $\mu^* = 0$

We first show that an RS equilibrium such that $\mu^* = 0$ exists if and only if

$$p\overline{d} \leq kpI \leq qR \quad \text{and} \quad \overline{c} \leq kpI.$$

To prove the necessity, fix any RS equilibrium such that the DeFi firm offers $d^* > \overline{d}$, the conventional firm offers $c^* > \overline{c}$, and $\mu^* = 0$. In this equilibrium (if any), $U^* = \max\{qc^*, V(d^*, \mu^*)\} = qc^*$, and the DeFi firm and the conventional firm earn zero and $q(R - c^*)$, respectively, as their final payoffs.

We first consider an RS equilibrium (if any) such that $\mu^* = 0$. If such an equilibrium ever exists, we must have $U^* = qc^*$. The conventional and DeFi firms respectively earn $q(R - c^*) = qR - U^*$ and 0 as their final payoffs. The DeFi firm's deviation to a repayment lower than $\overline{F}$ is not profitable only if $p\overline{d} = pI - \beta \leq U^*$. On the other hand, the equilibrium is coalitional-proof only if

$$V(d, \mu) = \mu kpd \leq U^* = qc^* \quad \forall d > \overline{d} \quad \text{such that} \quad W(d, \mu) > 0. \tag{23}$$

In fact, $W(d, \mu) > 0$ whenever $\mu > 0$ and $d > \overline{d}$, and thus, the condition (23) is equivalent to $V(I, 1) = kpI \leq U^* = qc^*$. Summing up, the DeFi firm has no incentive to deviate from an RS equilibrium if and only if

$$pI - \beta \leq U^* = qc^* \quad \text{and} \quad kpI \leq U^* = qc^*. \tag{24}$$

Next, to deter the conventional firm's deviation to $c \in (\overline{c}, c^*)$, we need $U^* = qc^* \leq kpd^*$. On the other hand, to deter the conventional firm's deviation to $c \leq \overline{c}$, we need at least one of the following two inequalities to hold:

$$S - \overline{c} \leq qR - U^* \quad \text{or} \quad \overline{c} \leq kpd^*.$$

The first inequality is equivalent to $c^* \leq \overline{c}$, which contradicts the hypothesis that the conventional firm makes the risky management in equilibrium. Thus, in the end, the conventional firm's deviation is blocked only if

$$U^* = qc^* \leq kpd^* \quad \text{and} \quad \bar{c} \leq kpd^*. \tag{25}$$

Combining two necessity conditions (24) and (25), we obtain

$$\max\{p\bar{d}, kpI\} \leq U^* = qc^* \leq kpd^* \quad \text{and} \quad \bar{c} \leq kpd^*.$$

Note that c^* and d^* cannot be larger than R and I, respectively. Thus, the last condition holds only if $d^* = I$, and therefore, the following constitutes the necessity condition for an RS equilibrium with $\mu^* = 0$ to exist:

$$p\bar{d} \leq kpd^* = kpI = qc^* \leq qR \quad \text{and} \quad \bar{c} \leq kpI. \tag{26}$$

It is straightforward that (26) also constitutes a sufficient condition for an RS equilibrium with $d^* = I$, $c^* = (kpI)/q$, and $\mu^* = 0$ to exist. This completes the proof of Theorem 3-(i).

C.2 $\mu^* = 1$

Next, consider an RS equilibrium (if any) such that $\mu^* = 1$, and thus $U^* = V(d^*, \mu^*) = kpd^* \geq qc^*$, where qc^* is the investor's revenue from accepting the conventional firm's offer c^*. In such an RS equilibrium, if any, the conventional and the DeFi firms earn zero and $W(d^*, 1)$, respectively. We first derive necessary conditions that such an RS equilibrium must satisfy.

Consider the DeFi firm's incentive. d^* must be optimal for the DeFi firm among all d's such that $d > \bar{d}$ (i.e., d would induce the firm to shirk) and $V(d, 1) \geq qc^*$ (i.e., the investors are willing to accept d rather than the conventional firm's offer c^*). That is, d^* solves the following optimization problem:

$$\max_{d \in (\bar{d}, I]} W(d, 1) \;\; \text{subject to} \;\; V(d, 1) = kpd \geq qc^*. \tag{27}$$

Because the objective function decreases in d, we obtain (a) $kpI \geq qc^*$ (otherwise, no $d \in (\bar{d}, I]$ satisfies the constraint $kpd \geq qc^*$) and (b) $d^* = qc^*/(kp) > \bar{d}$ (otherwise, the optimization problem admits no solution). Next, suppose that the DeFi firm deviates from d^* to $d' \leq \bar{d}$, which will induce the firm to behave. If d' is accepted by all investors, the firm obtains

$p(I - d')$, where

$$p(I - d') \geq p(I - \overline{d}) = \beta > kp(I - d^*) + (1 - k)\beta = W(d^*, 1)$$

where the strict inequality holds because $p(I - d^*) < p(I - \overline{d}) = \beta$. Thus, to prevent the DeFi firm's deviation to $d' \leq \overline{d}$, we need to ensure that no investor is willing to accept any $d' \leq \overline{d}$. The investors' payoff from accepting $d' \leq \overline{d}$ is pd' while their payoff from accepting the conventional firm's c^* is qc^*. Thus, we must have $p\overline{d} \leq qc^*$. To sum up, the DeFi firm's incentive-compatibility in equilibrium requires

$$p\overline{d} \leq qc^* \leq kpI \text{ and } d^* = \frac{qc^*}{kp} > \overline{d}. \tag{28}$$

Next, consider the conventional firm's incentive. We claim that $c^* = R$ (i.e., the conventional firm must offer the highest c in equilibrium) in equilibrium. Otherwise, the conventional firm could attract a positive measure of investors and earn a positive revenue by offering $c' \in (c^*, R)$ instead of c^*. Finally, we also must have $\overline{c} \leq qR$; otherwise, the conventional firm can benefit by deviating from $c^* = R$ to $c' = \overline{c}$, which will attract all investors. Combining the necessary conditions $c^* = R$ and $\overline{c} \leq qR$ with (22) and (28), we obtain the following necessary conditions that any RS equilibrium with $\mu^* = 1$ should satisfy: $p\overline{d} \leq kpd^* = qc^* = qR \leq kpI$ and $\overline{c} \leq qR$.

To sum up, any RS equilibrium must satisfy $d^* = qR/(kp)$ and c^*, which implies, combined with (22), the following necessary condition:

$$p\overline{d} \leq kpd^* = qc^* = qR \leq kpI \quad \text{and} \quad \overline{c} \leq qR. \tag{29}$$

This completes the proof of the first part of the theorem.

Finally, we show that both the DeFi and conventional firms have no incentive to deviate from the equilibrium strategies characterized in (29) (with $\mu^* = 1$). The conventional firm's incentive-compatibility is straightforward; hence, we focus on the DeFi firm. Suppose that the DeFi firm deviates by offering (d', μ') such that $d' \leq \overline{d}$. d' would induce the DeFi firm to deviate. Thus, the investors' revenue from accepting d' is $pd' \leq p\overline{d}$ and thus strictly less than qc^*, following from (29). Thus, any (d', μ') with $d' \leq \overline{d}$ yields the DeFi firm zero payoff only. Next, suppose that the DeFi firm deviates by offering (d', μ') such that $d' > \overline{d}$ and $d' \neq d^*$. (d', μ'), if accepted, the investors would earn $V(d', \mu') = k\mu pd'$; on the other hand, they could obtain qR by accepting the conventional firm's $c^* = R$. Thus, to ensure (d', μ') to be accepted, (d', μ') must satisfy the following condition: $k\mu' pd' \geq qR$. On the other hand, such a (d', μ') yields the DeFi firm

$$\begin{aligned} W(d', \mu') &= \mu'[k\mu' p(I - d') + (1 - k\mu')\beta)] \\ &\leq \mu'[k\mu' pI + (1 - k\mu')\beta - kpd^*] \\ &< \mu'[kpI + (1 - k)\beta - kpd^*] \\ &= \mu'[kp(I - d^*) + (1 - k)\beta] \\ &\leq kp(I - d^*) + (1 - k)\beta = W(d^*, 1), \end{aligned}$$

where the first and second inequalities respectively follow from $k\mu' pd' \geq qR = kpd^*$ and $pI > \beta$. Hence, the DeFi firm has no incentive to deviate to (d', μ') such that $d' > \overline{d}$. Finally, suppose that the DeFi firm deviates to (d', μ') such that $d' \leq \overline{d}$. If an investor accepts such (d', μ') she would earn a revenue of pd' ($d' \leq \overline{d}$ would induce the firm to behave). By (29), this payoff is less than qc^*. Thus, all investors have no incentive to accept (d', μ'), and hence the deviation yields the DeFi firm a payoff of zero. This proves that the DeFi firm has no incentive to deviate to any $(d', \mu') \neq (d^*, \mu^*)$.

D Proof of Theorem 4

We first discuss a set of necessary conditions that any PB equilibrium (if any) must satisfy. From the incentive-compatibility for the project selection by the DeFi and conventional firms, the necessary conditions for a PB equilibrium to exist are

$$d^* \leq \overline{d} = I - \frac{\beta}{p} \quad \text{and} \quad c^* \leq \overline{c} = \frac{S - qR}{1 - q} \tag{30}$$

In any PB equilibrium (if any), let $U^* = \max\{c^*, V(d^*, \mu^*)\} = \max\{c^*, pd^*\}$ denote each investor's pecuniary revenue in equilibrium, where μ^* denote the total fraction of the DeFi firm's securities that the investors purchase, and V is as defined in (3). We will also adopt the definition of W, the DeFi firm's payoff, as defined in (4). Recall that the DeFi and conventional firms compete in a Bertrand fashion. By the standard argument, U^*, c^* and d^*

must satisfy $U^* = c^* = pd^*$, and furthermore,

$$U^* = c^* = pd^* = \begin{cases} p\overline{d} & \text{if } \overline{c} > p\overline{d}, \\ \overline{c} & \text{if } \overline{c} < p\overline{d}. \end{cases} \tag{31}$$

in any PB equilibrium. In the former case $\overline{c} > p\overline{d}$, the conventional firm must attract the entire investor (i.e., $\mu^* = 0$) in equilibrium. In the latter case $\overline{c} < p\overline{d}$, the DeFi firm must attract the entire investors in equilibrium. It is immediate that μ^* must be either 0 or 1 in any PB equilibrium. Suppose not, i.e., $0 < \mu^* < 1$. Then, either the conventional firm (in the case $U^* = p\overline{d} > \overline{c}$) or the DeFi firm (in the case $U^* = \overline{c} > p\overline{d}$) increases its repayment term to attract the entire investors.

Now, we focus on the case $\overline{c} > p\overline{d}$ and investigate the condition under which a PB equilibrium such that $\mu^* = 0$ and $c^* = U^* = pd^* = p\overline{d}$ indeed exists. Note that the DeFi and conventional firms respectively earn 0 and $S - c^*$ in this kind of equilibrium. It is straightforward that the conventional firm has no incentive to deviate from $c^* = p\overline{d}$, given the DeFi firm's offer $d^* = \overline{d}$. Suppose that the DeFi firm deviates by offering (d', μ') where $d' > \overline{d}$. If (d', μ') is accepted by a fraction $\mu' > 0$ of the investors, the DeFi firm would shirk and earn a payoff of $W(d', \mu') = \mu'[\mu' kp(I - d') + (1 - \mu' k)\beta] > 0$. Thus, to prevent this kind of deviation, we must have

$$V(d', \mu') = kpd' \leq c^* = p\overline{d} \quad \forall d' > \overline{d} \qquad \Longleftrightarrow \qquad kpI \leq p\overline{d}$$

as a necessary condition for a PB equilibrium to exist. Next, consider the DeFi firm's deviation (d', μ') such that $d' \leq d^* = \overline{d}$, which would induce the DeFi firm to behave if accepted by investors. Note that $V(d', \mu') = pd' \leq p\overline{d} < U^* = c^*$; thus, (d', μ') is rejected by all investors, yielding the DeFi firm a payoff of zero. This proves that the DeFi firm has no incentive to deviate from the equilibrium strategy. In conclusion, a PB equilibrium with $\mu^* = 0$ exists if and only if $kpI < p\overline{d} < \overline{c}$, where the DeFi and conventional firms respectively offer $d^* = \overline{d}$ and $c^* = p\overline{d}$ in equilibrium.

Next, consider the other case $\overline{c} < p\overline{d}$. If a PB equilibrium exists in this case, we must have $\mu^* = 1$ and $c^* = U^* = pd^* = \overline{c}$. Suppose that the conventional firm deviates from c^* to c'. Any $c' < \overline{c}$ would not be profitable for the conventional firm because any such c' would be rejected by all investors for sure. Thus, let us focus on the case $c' > \overline{c}$. If c' is accepted by a fraction μ' of investors, the conventional firm would choose risky management and earn $\mu'(R - c')$. Thus, to prevent any such deviation, we must ensure that investors will not accept any $c' \in (\bar{c}, R)$, which is the case if and only if

$$qc' \leq U^* = \bar{c} \quad \forall c' \in (\bar{c}, R) \qquad \Longleftrightarrow \qquad qR \leq \bar{c}.$$

Now, suppose that the DeFi firm deviates by offering (d', μ'). Any (d', μ') with $d' < \overline{d}$ is clearly not acceptable to investors hence not profitable for the DeFi firm. Thus, we may focus on the case $d' > \overline{F}$. Note that (d', μ') is acceptable to investors only if $V(d', \mu') = kpd' \geq c^* = \bar{c}$. On the other hand, (d', μ') is profitable for the DeFi firm only if $W(d', \mu') > W(d^*, \mu^*)$. However,

$$W(d', \mu') = \mu'[k\mu' p(I - d') + (1 - k\mu')\beta] < \mu'[k\mu' p(I - \overline{d}) + (1 - k\mu')\beta] \leq \beta$$

while

$$W(d^*, \mu^*) = p(I - d^*) = pI - \bar{c} > pI - p\overline{d} = \beta \geq W(d', \mu').$$

This proves that the DeFi firm has no incentive to deviate from the equilibrium strategy. In conclusion, a PB equilibrium with $\mu^* = 1$ exists if and only if $qR \leq \bar{c} < p\overline{d}$, where the DeFi and conventional firms respectively offer $d^* = \bar{c}/p$ and $c^* = \bar{c}$ in equilibrium.

E Proof of Theorem 5

We first discuss a set of necessary conditions that any RB equilibrium (if any) must satisfy. From the incentive-compatibility for the project selection by the DeFi and conventional firms, the necessary conditions for a RB equilibrium to exist are

$$d^* \leq \overline{d} = I - \frac{\beta}{p} \quad \text{and} \quad c^* > \bar{c} = \frac{S - qR}{1 - q} \tag{32}$$

In any RB equilibrium (if any), let $U^* = \max\{qc^*, V(d^*, \mu^*)\} = \max\{qc^*, pd^*\}$ denote each investor's pecuniary revenue in equilibrium, where μ^* denotes the total fraction of the DeFi firm's securities that the investors purchase, and V is as defined in (3). We will also adopt the definition of W, the DeFi's payoff, as defined in (4). Recall that the DeFi and conventional firms compete in a Bertrand fashion. By the standard argument, U^*, d^* and c^* must satisfy

$U^* = qc^* = pd^*$, and furthermore,

$$U^* = qc^* = pd^* = \begin{cases} p\overline{d} & \text{if } qR \geq p\overline{d}, \\ qR & \text{iff } qR < p\overline{d} \end{cases} \quad \text{and} \quad \mu^* = \begin{cases} 0 & \text{iff } qR > p\overline{d}, \\ 1 & \text{iff } qR < p\overline{d} \end{cases} \tag{33}$$

and $\mu^* \in (0,1)$ if and only if $qR = p\overline{d}$. In what follows, we consider the following cases separately: (A) $qR < p\overline{d}$, (B) $qR > p\overline{d}$, and (C) $qR = p\overline{d}$.

Case A: First, suppose $qR < p\overline{d}$. In this case, in RB equilibrium (if any), the DeFi firm offers $d^* = qR/p < \overline{d}$ and attracts all investors (i.e., $\mu^* = 1$), and the conventional firm offers $c^* = R$. In addition, to prevent the conventional firm's deviation to c', we also must have $c' \leq pd^* = qR$ for all $c' \leq \overline{c}$; otherwise, the conventional firm can attract all investors and hence earn a positive payoff by deviating to $c' = \overline{c}$ and then making a prudent investment. From the observations so far, combined with (32), we obtain the following necessary condition for a RS equilibrium to exist:

$$\overline{c} \leq qc^* = qR = pd^* < p\overline{d} \quad \text{and} \quad \mu^* = 1. \tag{34}$$

Note that in any RS equilibrium characterized by (34) (if any), the conventional firm has no incentive to deviate to $c' \in (\overline{c}, R)$ as well, because all investors will strictly prefer purchasing the DeFi firm's security (which yields them a revenue of $V(d^*, \mu^*) = pd^* = qR$) than accepting c' (which yields them a revenue of $qc' < qR$).

Next, suppose (34) holds, and consider the DeFi firm's incentive-compatibility. Suppose that the DeFi firm deviates from d^* by offering (d', μ'). By Lemma 2, we may focus on the case $d' \leq \overline{d}$. But, $W(d', \mu') = \mu' p(I - d') \leq p(I - \overline{d}) < p(I - d^*) = W(d^*, \mu^*)$ where the strict inequality follows from $p\overline{d} > pd^*$ in (34). That is, the DeFi firm does not have any incentive to deviate from any RS equilibrium characterized by (34). This completes the proof of Theorem 5-(iii).

Case B: Next, suppose $qR > p\overline{d}$, and thus, $U^* = qB^* = pd^* = p\overline{d}$ (i.e., $d^* = \overline{d}$ and $c^* = p\overline{d}/q$) and $\mu^* = 0$ in any RB equilibrium (if any). Furthermore, the equilibrium payoffs are $q(R - c^*) = qR - p\overline{d}$ for the conventional firm and zero for the DeFi firm, respectively. To prevent the conventional firm's deviation from $c^* = p\overline{d}/q$ to $c' \leq \overline{c}$, we must have $p\overline{d} \geq \overline{c}$. If $p\overline{d} < \overline{c}$, the conventional firm may benefit by deviating from c^* to $c' = p\overline{d} + \epsilon \leq \overline{c}$, where $\epsilon > 0$ is small. Because $c' \leq \overline{c}$, c' would induce the conventional firm to make prudent investment and yield investors the revenue $c' = p\overline{d} + \epsilon > pd^*$; thus, c' would be accepted by all investors.

Furthermore, c' would yield the conventional firm the revenue $S - c' = S - p\overline{d} - \epsilon = S - qc^* > q(R - c^*)$, which is strictly larger than the conventional firm's equilibrium revenue. From this observation, combined with (32), we obtain the following necessary condition for the RS equilibrium to exist:

$$\overline{c} \leq qc^* = qR = pd^* = p\overline{d} < qR \text{ and } \mu^* = 0. \tag{35}$$

Note that in any RS equilibrium characterized by (35), the conventional firm has no incentive to deviate to $c' > \overline{c}$ because all of them would be rejected by all investors (when $c' \in (\overline{c}, c^*)$) or yield the conventional firm a strictly lower payoff than c^* (when $c' \in (c^*, R]$).

Next, suppose (35) holds, and consider the DeFi firm's incentive-compatibility. Suppose that the DeFi firm deviates from d^* by offering (d', μ'). Note that any $d' < d^* = \overline{d}$ would be rejected by all investors, as such an offer cannot yield investors a strictly higher payoff than $U^* = p\overline{d}$. Thus, we may focus on the case $d' > \overline{d}$. To prevent such deviation, we must make sure (d', μ') is rejected by investors for sure, which is the case if and only if $V(d', \mu') = k\mu' pd' \leq U^* = p\overline{d}$. This is the case for any (d', μ') with $d' > \overline{d}$ if and only if $kpI \leq p\overline{d} = p(I - \beta)$, or equivalently, $k \leq p\overline{d}/(p\overline{d} + \beta)$. In conclusion, the RS equilibrium exists if and only if

$$\overline{c} \leq qc^* = pd^* = p\overline{d} < qR,\ k \leq \frac{p\overline{d}}{p\overline{d} + \beta} \text{ and } \mu^* = 0. \tag{36}$$

Case C: Suppose $qR = p\overline{d}$, and thus, $U^* = qc^* = pd^* = p\overline{d} = qR$ (i.e., $d^* = \overline{d}$ and $c^* = p\overline{d}/q$) and $\mu^* \in (0, 1)$ in any RB equilibrium (if any). Furthermore, the equilibrium payoffs are $(1-\mu^*)q(R-c^*)$ for the conventional firm and $\mu^* p(I - \overline{d}) = \mu^*\beta$ for the DeFi firm, respectively. To prevent the conventional firm's deviation from $c^* = p\overline{d}/q$ to $c' \leq \overline{c}$, we must have $p\overline{d} \geq \overline{c}$. If $p\overline{d} < \overline{c}$, the conventional firm may benefit by deviating from c^* to $c' = p\overline{d} + \epsilon \leq \overline{c}$, where $\epsilon > 0$ is small. Because $c' \leq \overline{c}$, c' would induce the conventional firm to make prudent investment and yield investors the revenue $c' = p\overline{d} + \epsilon > pd^* = qc^* = U^*$; thus, c' would be accepted by all investors. Furthermore, c' would yield the conventional firm the payoff $S - c' = S - p\overline{d} - \epsilon = S - qc^* > (1-\mu^*)(qR - qc^*)$, which is strictly larger than the conventional firm's equilibrium revenue. From this observation, combined with (32), we obtain the following necessary condition for the RS equilibrium to exist:

$$\overline{c} \leq qc^* = pd^* = p\overline{d} = qR \quad \text{and} \quad \mu^* \in (0, 1). \tag{37}$$

Note that in any RS equilibrium characterized by (37), the conventional firm has no incentive to deviate to $c' > \bar{c}$ because all of them would be rejected by all investors (when $c' \in (\bar{c}, c^*)$) or yield the conventional firm a strictly lower payoff than c^* (when $c' \in (c^*, R]$).

Next, suppose (35) holds, and consider the DeFi firm's incentive-compatibility. Suppose that the DeFi firm deviates from d^* by offering (d', μ'). Note that any $d' < d^* = \overline{F}$ would be rejected by all investors, as such an offer cannot provide investors a payoff higher than $U^* = p\bar{d}$. Furthermore, by Lemma A.1, we may focus on the case $\mu' = 1$ without loss. Thus, the DeFi firm has no incentive to deviate iff

$$\sup_{d' > \bar{d}: V(d',1) > p\bar{d}} W(d', 1) \leq W(\bar{d}, \mu^*) = \mu^* \beta \tag{38}$$

If $V(I, 1) = kpI \leq p\bar{d}$, or equivalently, if $k \leq p\bar{d}/(p\bar{d} + \beta)$, there is no $d' > \bar{d}$ such that $V(d', 1) > p\bar{d}$ and thus (38) holds trivially. Thus, focus on the case $k > p\bar{d}/(p\bar{d} + \beta)$. Because both $W(d', 1) = kp(I - d') + (1 - k)\beta$ and $V(d', 1) = kpd'$ are monotone in d', (38) is equivalent to

$$kp\left(I - \frac{\bar{d}}{k}\right) + (1 - k)\beta \leq \mu^* \beta \quad \iff \quad k \leq \frac{p\bar{d} - (1 - \mu^*)\beta}{p\bar{d}} = 1 - \frac{1 - \mu^*}{p\bar{d}}\beta.$$

Note that the upper bound $1 - [(1 - \mu^*)\beta/(p\bar{d})]$ is larger than $p\bar{d}/(p\bar{d} + \beta)$ if and only if $\mu^* > \beta/(p\overline{F} + \beta)$. Combining all these conditions, the DeFi firm has no incentive to deviate from the RS equilibrium strategy prescribed by (37) if and only if the following condition holds:

$$k \leq \kappa(\mu^*) := \begin{cases} \dfrac{p\bar{d}}{p\bar{d} + \beta} & \text{if } \mu^* \leq \dfrac{\beta}{p\bar{d} + \beta} \\ \dfrac{p\bar{d} - (1 - \mu^*)\beta}{p\bar{d}} & \text{if } \mu^* > \dfrac{\beta}{p\bar{d} + \beta} \end{cases}$$

Note that $\kappa(\mu^*)$ is continuous and (weakly) increasing in $\mu^* \in [0, 1]$. This completes the proof of Theorem 5-(iii).

F Shirking-Proof Equilibrium Characterization

We fully characterize all shirking-proof equilibria in Section 6. We omit the formal characterization of equilibria that yield the same outcomes as the coalition-proof equilibria, as they follow directly from the proofs of Theorem 2 – 5. Instead, as summarized in Table 2, we focus on RS equilibrium with $\mu^* > 0$, PB equilibrium with $\mu^* = 0$, and RB equilibrium with $\mu^* < 1$, which produce different outcomes from their coalition-proof counterparts.

F.1 RS equilibrium with $\mu^* > 0$

In RS equilibrium, we must have $c^* > \overline{c}$ and $d^* > \overline{d}$. Since the characterization of RS equilibrium with $\mu^* = 1$ directly follows from Theorem 3, we focus on the equilibria with $\mu^* \in (0, 1)$. In these cases, we must have $qc^* = \mu^* kpd^*$ ensuring that all investors are different between buying the DeFi firm's security and investing in the conventional firm. Therefore, we have $kpI \geq qd^*$ and $\frac{qd^*}{kp} = d^* > \overline{d}$. Furthermore, it follows directly from the proof of Theorem 3 that *(i)* $p\overline{d} \leq qc^*$ (to prevent the DeFi firm from deviating to behave-inducing offers) and *(ii)* $c^* = R$ and $\overline{c} < qR$ (to prevent the conventional firm from profitable deviation). Therefore, the necessary condition (8) for RS equilibrium with $\mu^* = 1$ under coalition-proofness must be satisfied for the existence of RS equilibrium with $\mu^* \in (0, 1)$ under shirking-proofness:

$$p\overline{d} < qR \leq kpI, \text{ and } \overline{c} \leq qR.$$

We next prove sufficiency. Fix any value of $\mu^* \in (0, 1)$. First, the conventional firm cannot attract any investor with any deviation offer $c' \neq c^* = R$: any $c' \in (\overline{c}, R)$ will yield $qc' < \mu^* kpd^*$; any $c' \leq \overline{c}$ will yield $c' \leq qc^* = qR$. Furthermore, the DeFi firm cannot profitably deviate from its equilibrium offer $d^* = \frac{qR}{kp}$: in shirking-proof equilibrium, any offer $d' > \overline{d}$ will yield $W(d', 0) = 0 < W(d^*, \mu^*) = \mu^*[\mu^* kp(I - d^*) + (1 - \mu^* k)\beta]$; any offer $d' \leq \overline{d}$ will be rejected outright by investors since $pd' \leq p\overline{d} < qR$. Therefore, it is optimal for both the conventional and DeFi firms to make the equilibrium offers $c^* = R$ and $d^* = \frac{qR}{kp}$, respectively. Lastly, since investors remain indifferent between investing in the conventional firm and funding the DeFi firm, it is weakly optimal for investors with measure μ^* to fund the DeFi firm, while the remaining investors find it optimal to invest in the conventional firm.

F.2 PB equilibrium with $\mu^* = 0$

The characterization of this equilibrium closely follows that under the coalition-proofness refinement stated in the proof of Theorem 4. Specifically, all necessary conditions remain unchanged except for $kpI \leq p\overline{d}$. Under coalition-proofness, this condition was required to ensure that the DeFi firm could not offer a strictly higher payoff to investors by deviating with $d' > \overline{d}$. However, in shirking-proof equilibrium, any such deviation is expected to be outright rejected, yielding $W(d', 0) = 0$. Consequently, offering $d' > \overline{d}$ cannot be a profitable deviation for the DeFi firm.

We now prove that PB equilibrium with $\mu^* = 0$ exists if $p\overline{d} < \overline{c}$. Recall that the conventional firm's offer must satisfy $c^* \leq \overline{c}$, while the DeFi firm's offer must satisfy $d^* \leq \overline{d}$. Given Bertrand competition in the borrowing market, the conventional firm's equilibrium strategy is $c^* = p\overline{d}$, and the DeFi firm's equilibrium strategy is $d^* = \overline{d}$.

- The optimality of the conventional firm's equilibrium strategy follows directly from the proof of Theorem 4.
- The strict suboptimality of the DeFi firm's deviation offer $d' < \overline{d}$ is also established in the proof of Theorem 4.
- Finally, the DeFi firm will never offer $d' > \overline{d}$, as such an offer is expected to yield $W(d', 0) = 0$ under the shirking-proofness refinement.

Finally, investors find it (weakly) optimal to invest in the conventional firm, completing the equilibrium characterization.

F.3 PB equilibrium with $\mu^* < 1$

The characterization of this equilibrium closely follows that under the coalition-proofness refinement stated in the proof of Theorem 4. Specifically, all necessary conditions remain unchanged except for $k \leq \left(\frac{p\overline{d}}{p\overline{d}+\beta}\right) \vee \left(\frac{p\overline{d}-(1-\mu^*)\beta}{p\overline{d}}\right)$. Under coalition-proofness, this condition was required to ensure that the DeFi firm could not offer a strictly higher payoff to investors by deviating with $d' > \overline{d}$. However, in shirking-proof equilibrium, any such deviation is expected to be outright rejected, yielding $W(d', 0) = 0$. Consequently, offering $d' > \overline{d}$ cannot be a profitable deviation for the DeFi firm.

We now prove that PB equilibrium with $\mu^* = 0$ exists if $\overline{c} < p\overline{d} < qR$ is satisfied and PB equilibrium with $\mu^* \in (0, 1)$ exists if $\overline{c} < p\overline{d} = qR$ is satisfied. Similar to the characterization of PB equilibrium with $\mu^* = 0$ in the previous section, the conventional firm's equilibrium strategy is $c^* = p\overline{d}$, and the DeFi firm's equilibrium strategy is $d^* = \overline{d}$. The optimality of these equilibrium strategies also directly follows from the above characterization of PB equilibrium with $\mu^* = 0$ in the previous section. Lastly, the optimality of investors' equilibrium funding strategies directly follows from the proof of Theorem 4.

G Example: the DAO decision making process

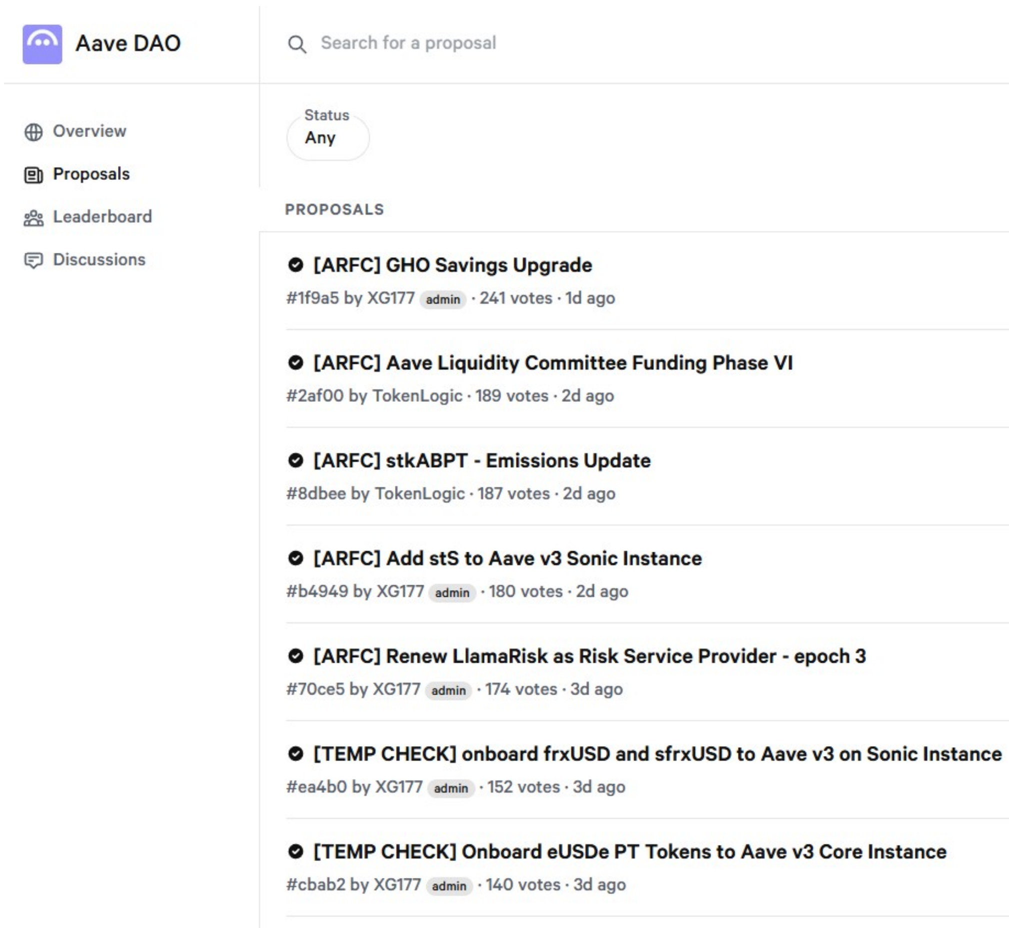

Figure 9 – Screenshot: a list of proposals in the Aave DAO (https://snapshot.box/#/s:aavedao.eth/proposals).

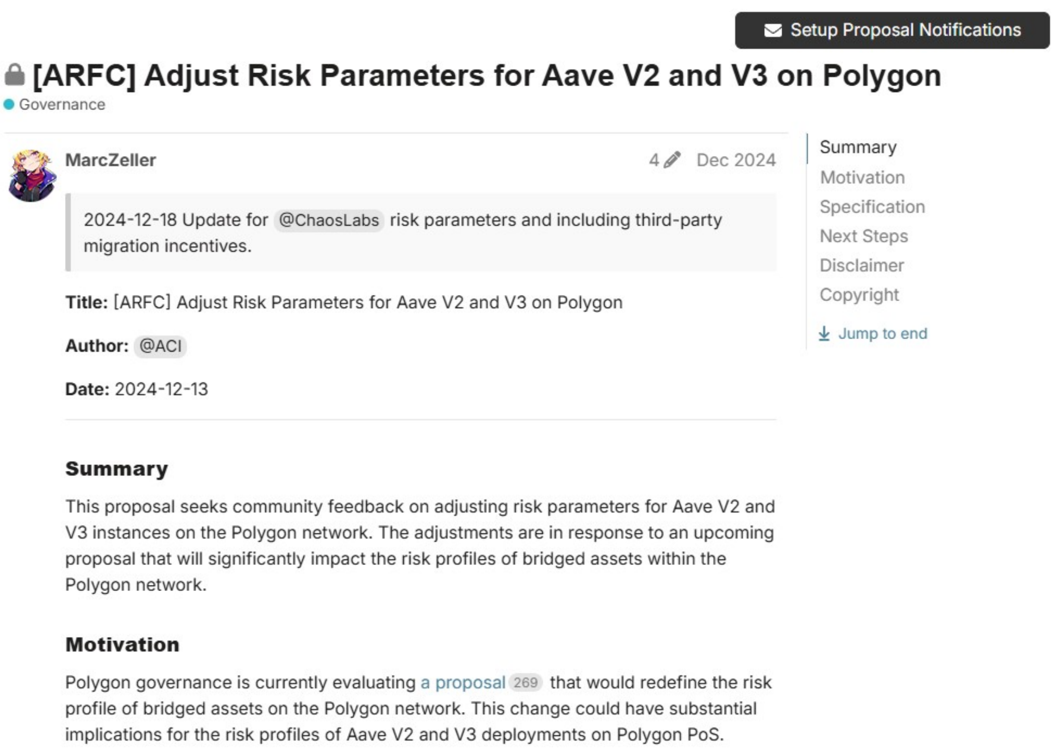

Figure 10 – Screenshot: a proposal in the Aave DAO titled "[ARFC] Adjust Risk Parameters for Aave V2 and V3" (Dec 2024). See https://governance.aave.com/t/arfc-adjust-risk-parameters-for-aave-v2-and-v3-on-polygon/20211/12 for the full proposal, including comments and discussions from developers and investors. The final voting result is available at https://app.aave.com/governance/v3/proposal/?proposalId=254.