Self-Collateral and Crypto Run *

Wenjin Kang† Ke Tang‡ Yang You§ Jiaqing Zeng¶

October 5, 2023

Abstract

The sudden FTX collapse alerts that centralized cryptocurrency exchange can function as an unregulated crypto-bank. We build a crypto-run model highlighting that the fragility of crypto-exchange arises from its self-collateralness — FTX misappropriated its clients' funds to invest in the self-issued tokens FTT, whose value depends on the performance of the exchange itself. We find that a higher level of self-collateralness makes the crypto-run more likely to occur. Our model highlights a new degree of strategic complementarity — investors want to withdraw their funds from the exchange before other investors' withdrawals dampen the exchange's growth expectation and crash the token price. Unlike a bank run, suspension of convertibility alone is insufficient to prevent a crypto-run. A cryptocurrency custody mechanism can be considered to ensure the safety of clients' funds and avert such crises in the future.

Keywords: Cryptocurrency Exchanges; Self-collateralness; FTX Collapse; Global Game; Bank-run

JEL Classification: G23, G28, G33

---

*We are grateful for the comments and suggestions from Rose Lai, Taoxiong Liu, Xuewen Liu, Rachel Ma, Tony Qin, Zhen Sun, Jing Xie, Endong Yang, Jinqiang Yang, and the seminar participants at the University of Macau and Tsinghua University.

†University of Macau, Faculty of Business Administration, Macau, China; Email: wenjinkang@um.edu.mo.

‡Tsinghua University, Institute of Economics, China, Email: ketang@tsinghua.edu.cn

§The University of Hong Kong, Faculty of Business and Economics, Hong Kong, China. Email: yangyou@hku.hk

¶University of Macau, Faculty of Business Administration, Macau, China. Email: zengjq13@gmail.com.

1 Introduction

In recent years, the cryptocurrency market has experienced a dramatic surge in its trading activity – the total annual trading volume catapulted from merely 2.1 trillion dollars in 2017 to more than 100 trillion dollars in 2022.[1] Fueled by this exponential growth of cryptocurrency trading demand, many crypto-exchanges were founded and then aggressively expanded their business during this period in an unregulated manner. However, amid this rapid growth, scandals and frauds arose in terms of the operation of these cryptocurrency trading platforms. The most prominent example of such scandals is the sudden collapse of FTX, the world's second-largest crypto-exchange. The precipitous downfall of FTX highlights the risk of misappropriation of client funds and lack of transparency in the crypto-exchange's balance sheet. It has also garnered extensive coverage from global media and drawn a great amount of attention from investors and policymakers worldwide.[2]

For crypto-exchanges, token issuance is a common approach to raising capital by providing its investors specified benefits that depends on the performance of the exchange in the future. FTX issued its token FTT initially at $1 per token in 2019. As FTX rapidly expanded its business and gained more market shares, the FTT token price was traded as high as above $60. As of November 1, 2022, just before the collapse of FTX, the market price of FTT remained above $25. From November 2 to November 10, FTX experienced a dramatic fall from a multi-billion-dollar exchange to bankruptcy in just about one week time. The FTX crisis started with a CoinDesk news report on November 2, which suggested that Alameda Research, a hedge fund run by the same management team at FTX, held a tremendous amount of FTT tokens in its investment portfolio and had secretly borrowed billions of dollars from FTX clients' assets to finance these positions. In

[1] The data for this trading volume summary statistics comes from CoinMarketCap.

[2] The collapse of FTX has been widely reported in mainstream financial newspapers and magazines, such as Bloomberg, The Economist, Financial Times, Forbes, Wall Street Journal, etc. Janet Yellen, the current Treasury Secretary and the former Chair of the Federal Reserve, has suggested that the collapse of FTX can be regarded as the Lehman moment within the crypto market. The impact of FTX collapse on the stability of the global financial system has also been discussed in the Meeting of G20 Finance Ministers and Central Bank Governors in April 2023.

response to the report, FTX clients hurriedly withdrew their deposited funds from the exchange. On November 8, FTX suspended withdrawal requests, and the token price dropped to around $2. On November 10, FTX declared bankruptcy. The sudden collapse of FTX stands as one of the largest financial scandals, resulting in multi-billion-dollar losses for its clients and investors.

The collapse of FTX has unveiled two distinctive features that can be prevalent among other unregulated crypto-exchanges. First, FTX engaged in massive-scale misappropriation of client funds to finance Alameda's portfolio by adopting aggressive accounting and programming tactics.[3] The extensive misappropriation of client funds fundamentally transformed FTX from a crypto-exchange into a de-facto crypto-bank, with Alameda borrowing billions of dollars from FTX's clients to maintain its trading positions.[4] Consequently, the collapse of FTX shares some similarities with classical bank-run models (Diamond and Dybvig, 1983). Since the crypto-investment portfolio of Alameda/FTX heavily relies on the funds borrowed (or misappropriated) from its clients, we term this position as the *collateral portfolio* thereafter.

One reason for FTX to misappropriate the clients' funds to finance its investment portfolio is to boost the exchange-issued FTT token price. This leads to the second distinctive feature contributing to the FTX collapse, that is, the *self-collateralness* of FTX. The FTX's collateral portfolio includes a large portion of the FTT token.[5] As the token of FTX, the value of FTT is directly linked to FTX's performance as a cryptocurrency trading platform. When FTX clients lack confidence in the exchange's growth prospects and solvency, they are more likely to withdraw their funds from FTX, which in turn reduces the trading opportunities provided by the exchange and consequently

[3] According to the SEC investigation report, FTX had concealed the diversion of approximately $8 billion of clients' assets to Alameda without their consent. Furthermore, FTX provided undisclosed preferential treatment to Alameda on its trading platform, granting it a virtually unlimited "line of credit" funded by other FTX clients. This was facilitated by allowing a negative balance in Alameda's account on the FTX platform, and it is estimated that this privilege has provided Alameda access to tens of billions of dollars from FTX clients' funds without their awareness.

[4] Chiu and Wong (2023) argue that when FTX combined the token-issuing arm (the exchange itself) and the token-trading arm (Alameda) together into one crypto-conglomerate, it led to excessive leverage and created risks for the loans from its clients or outside of the platform.

[5] According to the report from Coindesk, right before the collapse of FTX, about 40% of Alameda's crypto-asset collateral portfolio is composed of the exchange's self-issued token FTT.

lowers the FTT token price (see Appendix Figure A1 for example). Therefore, when FTX uses the funds borrowed from its clients to support its position in the FTT token, this self-collateralness feature introduces a high level of instability— the withdrawal request from FTX clients not only tightens FTX's cash flow but also undermines the price of FTT token and hence the FTX's collateral portfolio value.[6] The self-collateralness feature distinctly differentiates our crypto-run model from the classical bank-run model.

We construct a model with the global-game technique to analyze how the self-collateralness of the crypto-exchange can influence the likelihood of the exchange's failure. Our model considers an exchange that misappropriates funds from its clients to finance its collateral portfolio, which includes a substantial portion of the exchange-issued token. For the exchange's clients who deposit their funds on the exchange, we name them as the *investors* on the exchange and assume that they receive noisy private signals about the exchange's growth prospects. The investors form expectations about the exchange's solvency and decide whether to withdraw their deposited funds from the exchange. The collapse of the crypto-exchange results from the coordination failure among investors, especially when they have concerns about the exchange's solvency. This is akin to the bank run modeled by Diamond and Dybvig (1983). More specifically, we introduce a noisy private signal, which coordinates agents' behaviors and transforms multiple equilibria into a unique equilibrium in our crypto-run model (see Carlsson and Van Damme (1993), Morris and Shin (1998)). We then solve the model by using the global-game technique. (e.g., Morris and Shin (2000), Rochet and Vives (2004), Goldstein and Pauzner (2005), Vives (2014), Liu (2016), Eisenbach (2017), Goldstein *et al.* (2022), Liu (2023), etc.)

Despite the similarities described above, we would like to highlight significant differences between our crypto-run model and traditional bank run models. In a bank run, the bank mainly faces

[6] In fact, one of the charges brought by the SEC against FTX is that it concealed the risk arising from FTX's exposure to Alameda's significant holdings of illiquid assets, such as FTX-affiliated tokens.

the liquidity mismatch risk. But in our crypto-run model, the crypto-exchange faces the risk that investors' withdrawal decisions can *alter* the fundamental value of the exchange, and therefore dampen the exchange's token price and its collateral portfolio value.[7] More specifically, if some investors perceive that the risk of exchange failure outweighs the trading benefit provided by the exchange, they will opt to withdraw. Such withdrawals reduce the trading opportunities on the exchange and, hence, a significant decline in the price of exchange tokens, which may encourage further additional withdrawals. Therefore, besides the typical bank-run-type strategic complementarity based on payoff externality, our model introduces a new degree of strategic complementarity that any given investor may want to withdraw from the exchange before other investors' withdrawal causes the exchange's token price drop and further devalues its collateral portfolio. This new strategic complementarity differentiates our crypto-run model from classical bank-run models.

Our model analysis suggests that when the trader's private signal is precise enough, the unique equilibrium is that the investor chooses to withdraw early if and only if her signal is below a specific threshold value. The threshold value for the exchange client's private signal increases with the self-collateralness of the exchange. Therefore, a key finding of our model is that the crypto-run is more likely to occur if the self-collateral level is higher. In other words, when the exchange misappropriates a larger amount of its investors' funds and includes a higher proportion of its self-issued token in the collateral portfolio, the likelihood of the exchange failure is amplified.

Our paper contributes to the literature in the following ways. First, by building a crypto-run model augmented with the global-game technique, our paper is the first one that examines the role of self-collateralness in the sudden collapse of a major crypto-exchange such as FTX. This aligns with the growing body of recent literature on the potential instability of the cryptocurrency market.[8]

[7] As a contrast, it is unlikely that the bank depositors' withdrawal requests will substantially change the value of the houses that serve as the collateral for the bank's mortgage loans.

[8] More specifically, Klages-Mundt and Minca (2019) show that there can be a deleveraging spiral in the crypto market. Cong *et al.* (2021), Pagnotta (2022), and Sockin and Xiong (2023) show that the instability of token price is related to network effects among token users. Uhlig (2022) builds a dynamic model to study the crash of the stablecoin Luna.

Second, unlike the classical bank-run models that are mainly driven by liquidity mismatch, our crypto-run model highlights the risk that can arise from the crypto-exchange's self-collateralness feature and also the important role that the exchange platform growth expectation can play in the coordination failure. Our crypto-run model introduces a new degree of strategic complementarity based on the negative relationship between investors' withdrawal requests and the exchange's self-issued token price. Based on that, our model derives some interesting policy implications that differs from the bank run literature. For example, the suspension-of-convertibility policy alone cannot stop a crypto-run, and a custody mechanism should be considered to ensure the safety of clients' funds deposited on the exchange.

The paper is organized as follows. Section 2 provides a model setup. Section 3 characterizes the model equilibrium. Section 4 discusses the policy implications. Section 5 concludes our paper.

2 Model

2.1 Setup

We consider a discrete-time model with an infinite horizon. In a given period t, there are N_t investors on the crypto-exchange (i.e., the exchange's clients). These investors have deposited their funds in the exchange, one dollar each, to avail themselves of the cryptocurrency-market trading services provided by the exchange. The exchange uses a fraction m_t of its investors' funds to finance its own investment portfolio, which we will name as the *collateral portfolio* thereafter. Without loss of generality, we assume that, in the exchange's collateral portfolio, a subset θ_t is directed towards its self-issued tokens, and the rest portion is invested in stablecoins. Therefore, there is a total fraction of $\gamma_t = m_t\theta_t$ of investors' funds that are invested in the exchange-issued tokens. γ can be interpreted as the proxy for the self-collateralness of the exchange.

We assume that there is an exogenous growth rate g_t, for the number of investors on the ex-

Liu *et al.* (2023) use detailed data to show that investors' doubts about the system's sustainability lead to the Luna crash. Biais *et al.* (2023) show the existence of sunspot equilibria in Bitcoin pricing.

change from period t to period $t+1$. That is, there will be $N_t g_t$ new investors that are expected to arrive at the exchange at the beginning of period $t+1$.[9] We further assume that g_t follows a normal distribution, $g_t \sim N(\overline{g}, \tau_g^{-1})$. In period t, each investor observes a private noisy signal $x_{i,t}$ about g_t, that is, $x_{i,t} = g_t + \varepsilon_{i,t}$, with the error term $\varepsilon_{i,t} \sim N(0, \tau_\varepsilon^{-1})$. After observing $x_{i,t}$, the investor can decide whether to withdraw her fund from the exchange.[10] If the investor decides to withdraw in period t, she receives her one dollar back. On the other hand, if an investor chooses to keep her fund deposited on the exchange for another period (i.e., until period $t+1$) and the exchange does not fail at the beginning of period $t+1$, she will receive a convenience yield c_t, which represents the expected utility from the trading service provided by the exchange. However, if the investor chooses to keep her fund on the exchange and the exchange fails in period $t+1$, she will lose all her fund and receive zero convenience yield.[11]

Each investor will form her expectation about the probability of exchange failure, $q_{i,t}$, and choose to withdraw in period t if and only if she anticipates that $q_{i,t} - (1-q_{i,t})c_t > 0$. Thus, when the investor forms the assessment that the exchange failure probability $q_{i,t} > \frac{c_t}{1+c_t}$, she will withdraw in period t. Suppose there is a fraction l_t of investors who choose to withdraw and leave the exchange in period t ($0 \leq l_t \leq 1$). We assume that the exchange cannot fulfill its investors' withdrawals in period t by liquidating the exchange-issued tokens in its collateral portfolio.[12] Consequently, if $l_t > 1-\gamma_t$, the exchange does not have sufficient funds to meet investor demands. In such a scenario, we assume that the exchange chooses to borrow from an external creditor, for

[9]For the new investors, when they join the exchange, each of them will also deposit one dollar in the exchange.

[10]The global-game bank run models usually consider a private signal that can serve as the proxy for the fundamental of the bank. In our model, one of the most important determinants for the fundamental of the exchange is the number of investors on the exchange. Given that in period t, the number of investors N_t is already known at the beginning of the period, its (exogenous) growth rate g_t becomes the key driver for the number of investors in the future. Therefore, in our model, we assume that the private signal $x_{i,t}$ is about g_t, and it reflects the fundamental of the exchange — a higher private signal implies a lower probability of the exchange failure.

[11]The simplification refers to Rochet and Vives (2004). Our model's main results still hold if we assume that remaining investors lose a certain fraction of their funds in the exchange failure scenario.

[12]This assumption is based on the rationale that given that the exchange holds a significant amount of its own tokens in its collateral portfolio, when investors rush to withdraw their funds from the exchange, it is difficult for the exchange to sell its own tokens at a fair price within a short timeframe because of market illiquidity reasons.

example, a short-term lending facility, to meet investors' withdrawal demand. The exchange needs to repay these short-term borrowings by the time of the solvency test conducted at the beginning of the subsequent period.[13]

Whether the exchange fails in period $t+1$ depends on the solvency test conducted at the beginning of period $t+1$. This evaluation is based on whether the exchange's assets can cover its investors' withdrawal requests. More specifically, we assume that for all investors who stay in the exchange at the end of period t, the mass of which is $N_t(1-l_t)$, they need to submit withdrawal requests as a part of the exchange solvency test that will be conducted at the beginning of $t+1$.

(a) When $l_t \leq 1-\gamma_t$, the exchange does not need to borrow, the total assets of the exchange are $N_t(1-\gamma_t-l_t+g_t+\frac{P_{t+1}}{P_t}\gamma_t)$, and the withdrawal requests are $N_t(1-l_t)$, the exchange fails the solvency test if

$$\frac{P_{t+1}}{P_t}\gamma_t-\gamma_t+g_t<0. \tag{1}$$

(b) When $l_t>1-\gamma_t$, at the beginning of period $t+1$, the exchange needs to repay $N_t(l_t-1+\gamma_t)$, which is the amount of short-term borrowing from the external creditor in period t. The exchange also needs to satisfy the remaining investors' withdrawal requests $N_t(1-l_t)$. The exchange's assets are $N_t(g_t+\frac{P_{t+1}}{P_t}\gamma_t)$ at the beginning of period $t+1$. Therefore, the exchange's failure condition is also $\frac{P_{t+1}}{P_t}\gamma_t-\gamma_t+g_t<0$, as shown in the inequality equation (1) in this scenario.

Therefore, irrespective of whether the exchange needs to borrow in period t or not, its failure occurs when the inequality condition expressed in equation (1) is met. If the exchange survives the solvency test at the beginning of period $t+1$, investors cancel their withdrawal requests that are submitted at the end of period t, and the game continues. The model timeline is presented in the Appendix Figure A2. The number of investors staying on the exchange in period $t+1$ will be,

$$N_{t+1}=N_t(1+g_t-l_t). \tag{2}$$

[13]More specifically, we assume that in each period, once the exchange passes the solvency test at the beginning of this period, the external creditor is willing to provide a short-term loan at zero interest, which needs to be repaid at the beginning of the next period. Our model's main results still hold if the short-term loan has a non-zero interest rate.

2.2 The Exchange-issued Token Price

We assume that the exchange-issued token each can be credited against one dollar of the transaction fee, and the token disappears after it is consumed. Investors can use the token as long as they can conduct transactions on the exchange trading platform. Suppose the probability of a transaction being conducted between two investors is $1-\alpha$. Hence, in period t, the probability for a specific investor to engage in trading with other investors on the exchange is $1-\alpha^{N_t-1}$. Following the token pricing formula in Rogoff and You (2023), the token price in period t is, [14]

$$P_t = \frac{\beta(1-\alpha^{N_t-1})}{1-\beta\alpha^{N_t-1}}. \tag{3}$$

Equation (3) suggests that the token price increases in the number of investors on the exchange.[15] Because the number of investors in period $t+1$ increases in g_t and decreases in l_t, the expected token price also increases in g_t and decreases in l_t. It implies that the token price is closely related with the fundamental value of the exchange trading platform. Once a large number of investors choose to leave the exchange, the exchange-issued token price will plummet.[16] Therefore, in our model, whether the exchange can pass the solvency test at the beginning of period $t+1$ is related to investors' actions in period t, since the exchange's own token price and hence its collateral portfolio value depend on the number of investors remaining on the exchange.

We denote $F(l_t, g_t, \gamma_t, N_t) = \frac{P_{t+1}(l_t, g_t, N_t)}{P_t(N_t)}\gamma_t - \gamma_t + g_t$ as the exchange failure condition. Since P_{t+1} is an increasing function of N_{t+1} and N_{t+1} increases in g_t and decreases in l_t, it is obvious to show that the exchange failure condition function $F(l_t, g_t, \gamma_t, N_t)$ is continuously increasing in g_t and decreasing in l_t. If $F(l_t, g_t, \gamma_t, N_t) < 0$, the exchange cannot pass the solvency test and fails.

[14] More specifically, our token pricing formula here follows the particular token price formula as shown in Section 4.2 (Page 983) of Rogoff and You (2023), which is $\beta p/[1-\beta(1-p)]$, with β as the discount factor. Here, we further assume that trading probability $p = 1-\alpha^{N_t-1}$ to obtain our token pricing formula in equation (3).

[15] In reality, holding the FTT token enables investors to enjoy a discount on their FTX trading commissions. We would like to mention that the details of the exchange-issued token pricing mechanism is not the main focus of this paper. Therefore, the token pricing equation in Rogoff and You (2023) is sufficient to capture the important observation that FTT token price decreases when there are less amount of investors that are expected to trade on the FTX exchange.

[16] This is exactly what happened to the FTT token price during the FTX collapse, as shown in the Appendix Figure A1.

3 Equilibrium

In this section, we analyze the exchange failure probability in the period $t+1$ given its conditions (i.e., l_t, g_t, γ_t, N_t) in period t. For ease of expression, we suppress the subscript t and use the notation of l, g, N, γ, and x_i as the private signal for g, in our model analysis in this section instead. If the exogenous growth rate g is common knowledge to the investors, there exist the following three possible equilibria.

(a) when the exchange is growing fast enough, that is, $g > \gamma$, the optimal strategy for any given investor is to keep her fund in the exchange in period t, regardless of the choices made by other investors. The exchange can always survive the solvency test in this scenario.

(b) When the exchange exogenous growth rate $g < 0$, the optimal strategy for all the investors is to withdraw from the exchange in period t. It is straightforward to show that when $g < 0$, $F(l, g, \gamma, N) < 0$,[17] and therefore the exchange always fails.

(c) When $0 \leq g \leq \gamma$, whether the exchange fails depends on the investors' withdrawal decisions in period t. In this scenario, when a specific investor expects that all other investors withdraw in period t, her optimal strategy is to withdraw in period t as well. Similarly, when she expects that all other investors keep their funds deposited in the exchange, her optimal strategy is not to withdraw in period t also. The coordination problem among investors is analogous to the bank run problem (Diamond and Dybvig, 1983). But the coordination failure operates differently in our crypto-run model; that is, the self-collateralness of the exchange links investors' actions to the value of its collateral portfolio, which leads to a new degree of strategic complementarity.

In our model, for a specific investor i, she can only observe her private signal x_i, and cannot observe other investors' private signals. Therefore, investor i needs to form an expectation about other investors' decision-making process, and her strategy profile is a function of her private signal

[17] When $g_t < 0$, we have that $P_{t+1} \leq P_t$, and hence $F(l_t, g_t, \gamma_t, N_t) = \frac{P_{t+1}}{P_t}\gamma_t - \gamma_t + g_t < 0$.

x_i. The game is a global game with a continuum of players and binary actions. The model equilibrium can be solved by referring to Rochet and Vives (2004) and Morris and Shin (2004). We first solve a "switching strategy" equilibria, in which investors withdraw their funds when their growth rate expectation is lower than a certain threshold, and keep their funds on the exchange when their growth rate expectation is higher than this threshold. Then, we further prove that the threshold equilibrium is the unique equilibrium as $\tau_\varepsilon \to \infty$.

When investor i observes the signal x_i, her posterior distribution of g is normal with mean $\xi_i = \frac{\tau_g \overline{g} + \tau_\varepsilon x_i}{\tau_g + \tau_\varepsilon}$ and precision $\tau_g + \tau_\varepsilon$. When investors use a switching strategy with a threshold level ξ, they choose to withdraw their funds if and only if the private signal x_i is lower than

$$x(\xi, \overline{g}) = \frac{\tau_g + \tau_\varepsilon}{\tau_\varepsilon}\xi - \frac{\tau_g}{\tau_\varepsilon}\overline{g}. \tag{4}$$

We denote ψ as the critical value g at which the exchange is on the margin of success and failure, that is, $F(l, \psi, \gamma, N) = 0$. Since an investor chooses to withdraw when her private signal is below the marginal signal $x(\xi, \overline{g})$, the fraction of investors who withdraw their funds equals

$$l(\xi, \overline{g}, \psi) = \Phi(\sqrt{\tau_\varepsilon}(x(\xi, \overline{g}) - \psi)), \tag{5}$$

where Φ is the cumulative distribution function of a standard normal distribution. Therefore,

$$F(l(\xi, \overline{g}, \psi), \psi, \gamma, N) = 0. \tag{6}$$

At the switching point ξ, investors are indifferent between withdrawing from and staying on the exchange. Since the conditional density over g is normal with mean ξ and precision $\tau_g + \tau_\varepsilon$, and the exchange fails with $g < \psi$, as far as the marginal investors are considered, the conditional probability of failure is $\Phi(\sqrt{\tau_g + \tau_\varepsilon}(\psi - \xi))$. The expected payoff of staying on the exchange is $[1 - \Phi(\sqrt{\tau_g + \tau_\varepsilon}(\psi - \xi))](1 + c)$, while the expected payoff of withdrawing is 1. The indifference condition is given by

$$[1 - \Phi(\sqrt{\tau_g + \tau_\varepsilon}(\psi - \xi))](1 + c) = 1. \tag{7}$$

Combining equations (6) and (7), we obtain the following equation, which solves ψ.

$$F(l(\psi - \frac{\Phi^{-1}(\frac{c}{1+c})}{\sqrt{\tau_g + \tau_\varepsilon}}, \overline{g}, \psi), \psi, \gamma, N) = 0. \tag{8}$$

When $\tau_\varepsilon \to \infty$, from equation (7), we have that $\lim_{\tau_\varepsilon \to \infty} \sqrt{\tau_\varepsilon}(\psi - \xi) = \Phi^{-1}(\frac{c}{1+c})$. Combined with equations (4) and (5), $\lim_{\tau_\varepsilon \to \infty} l = \Phi(-\Phi^{-1}(\frac{c}{1+c})) = \frac{1}{1+c}$. Equation (8) turns into

$$F(\frac{1}{1+c}, \psi, \gamma, N) = 0. \tag{9}$$

We can show that equation (9) has a unique solution. Then, we can prove that the switching strategy is the only strategy that survives the iterated deletion of dominated strategies. The proof methodology is analogous to Morris and Shin (2004) and Rochet and Vives (2004). The detailed proof is in the Appendix B. Therefore, we obtain Proposition 1 as below.

Proposition 1 *When $\tau_\varepsilon \to \infty$, the equilibrium is a unique equilibrium in which investors use a switching strategy around ξ, where $\xi = \psi$ satisfies equation* (9). *The switching strategy is the only strategy that survives the iterated deletion of dominated strategies.*

It is obvious that the probability for the exchange failure, $\Phi(\sqrt{\tau_g}(\psi - \overline{g}))$, increases in ψ. Hence, we can show in Proposition 2 that the exchange is more likely to fail with a higher degree of self-collateralness γ and fewer investors N on the exchange. The proof is in the Appendix B.

Proposition 2 *The probability of the exchange failure, $\Phi(\sqrt{\tau_g}(\psi - \overline{g}))$, is continuously increasing in the self-collateralness γ and decreasing in the number of investors N.*

To illustrate the impact of self-collateralness on the exchange failure probability, we provide simulation examples in the Appendix A. The Appendix Figure A3 shows that when the self-collateralness (γ on the x-axis) increases, the probability of exchange failure (on the y-axis) becomes higher. It suggests that a higher level of self-collateralness makes the crypto-run more likely to occur by exacerbating the reinforcement between the clients' withdrawal and the token price decline. Also, our simulations show that for the same level of self-collateralness, fewer investors on the exchange leads to a higher exchange-failure probability.

The main implication derived from our crypto-run model is that, unlike a bank run, unregulated exchanges misappropriate clients' funds and expose investors to the risk of platform growth through the exchange-issued tokens (e.g., FTT for FTX). A lower growth expectation dampens the prospect of the exchange's solvency and incentivizes investors to withdraw from the exchange. As more investors share such concerns, their withdrawal requests further undermine the fundamental of the exchange, resulting in a sharp decline in the price of the exchange-issued tokens. This decreases the value of the collateral portfolio and makes the exchange less likely to survive the solvency test. Consequently, other investors are also more likely to consider further withdrawals. Therefore, our model highlights a new degree of strategic complementarity through the platform growth expectation, in addition to the payoff externality in a bank-run. More specifically, any given investor who receives a negative signal about the growth prospect may want to withdraw before other investors, and these withdrawal requests destroy the exchange's fundamental value. In the case of FTX collapse, the CoinDesk news on November 2 functioned as the initial negative signal, and panic investors coordinated on the equilibrium of submitting withdrawal requests. The investors' withdrawals and the consequently devaluation of FTT culminated in a solvency crisis and materialized financial instability driven by the unique self-collateralness feature of the crypto-exchange.

4 Regulation and Policy

Similar to a bank-run model, the investors' withdrawal, which stems from their apprehension regarding the exchange's solvency, is the primary source that drives the failure of a crypto-exchange. However, it's important to underline a key distinction between the bank-run model and our crypto-run model. In a bank-run model, the depositors' withdrawal only creates a liquidity mismatch but does not undermine the bank's long-term fundamentals. However, in our crypto-run model, the investors' withdrawal dampens the exchange's growth expectation, which in turn fundamentally devalues the exchange's self-issued token price and hence erodes its solvency due to the distinctive feature of self-collateralness. Based on this novel feature, our model yields several notably different policy implications that can be considered for the sake of crypto-exchange regulations.

4.1 Suspension of Convertibility

One policy implication drawn from the bank-run model is that the suspension of convertibility can effectively quell a bank run, since it alleviates the concerns among bank depositors that the withdrawals of other depositors might lead to bankruptcy and provides sufficient time for long-maturity loans to replenish liquidity. However, in our crypto-run model, suspending the convertibility alone is unlikely to stop the crypto-run. The withdrawals by investors in this context lower the fundamental value of the crypto-exchange as a trading platform, lead to the collapse of the exchange token price, and ultimately trigger insolvency as the exchange's liability outsizes its asset.

More specifically, suppose the exchange suspends its investors' withdrawal requests during period t. This suspension might enable the exchange to pass the solvency test at the beginning of period $t+1$ as investors are forced to stay within the exchange. However, as the game continues in period $t+1$, as long as the investors' signals remain below the threshold ξ as implied in our model (i.e., their pessimistic outlook on the exchange's future growth persists in the next period), they will still opt for withdrawals in period $t+1$. Therefore, the exchange cannot escape from an eventual failure unless it can restore it investors' confidence in its future growth during the suspension period. One feasible option to avert the collapse of FTX was an acquisition by another major crypto-exchange. The endorsement from the acquisition can stop investors from withdrawing their funds from FTX and encourage them to continue their cryptocurrency trading activity on the exchange trading platform. This would help keeping FTX solvent and boost the FTT token prices. As the FTT price rebounds, the crypto-run issue can be addressed endogenously, as FTX would be able to sell its FTT tokens at a more favorable price to satisfy its clients' withdrawal requests. Only through such a combination of both bailout measures and suspension-of-convertibility, the exchange can ensure its survival when confronted with the impending threat of a crypto-run.

4.2 Client's Fund Custodian

One key prediction in our model is that a higher level of self-collateralness (γ) leads to an increased probability of a crypto-run. To mitigate the risk of crypto-exchange failure, it is essential to reduce, or even eliminate the exchange's self-collateralness. One straightforward approach here is to engage a custodian and separate the banking functionality from the exchange. In this setup, investors would deposit and withdraw their fiat currency and cryptocurrencies through a third-party financial institution. The crypto-exchange would solely serve as a trading platform, refraining from any direct touch on investors' assets and effectively ensuring $\gamma = 0$.

In practice, policymakers have made some progress in making the custody of client funds an important rule for cryptocurrency exchanges to abide by. For example, the Hong Kong Securities and Futures Commission (SFC) announced *Licensing Handbook for Virtual Asset Trading Platform Operators* and required that a cryptocurrency exchange should only hold client assets through an associated entity that should not conduct any business other than that of receiving or holding client assets on behalf of the exchange according to the clause 3.2.22 in the SFC Licensing Handbook.[18]

5 Conclusion

We construct a crypto-run model that provides an intuitive explanation for the recent FTX collapse. Our model suggests that a high degree of self-collateralness in the FTX collateral portfolio plays a vital role in the sudden collapse of this world's second-largest crypto-exchange. We show that the exchange failure probability increases with the exchange's self-collateralness and decreases with the number of investors on the exchange platform. The policy implications that arise from our model suggest that suspension of convertibility alone cannot stop a crypto-run and custody of clients' funds can mitigate the risk of the crypto-run.

[18]For the sake of space, additional policy implication discussions about the technological challenge for the cryptocurrency custody mechanism and the deposit insurance scheme for investors' funds are included in the Appendix C.

References

Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. and Menkveld, A.J. (2023). 'Equilibrium bitcoin pricing', *The Journal of Finance*, vol. 78(2), pp. 967–1014.

Carlsson, H. and Van Damme, E. (1993). 'Global games and equilibrium selection', *Econometrica: Journal of the Econometric Society*, pp. 989–1018.

Chiu, J. and Wong, R. (2023). 'What is a crypto conglomerate like ftx? economics and regulations', *Economic Brief, Federal Reserve Bank of Richmond*.

Cong, L.W., Li, Y. and Wang, N. (2021). 'Tokenomics: dynamic adoption and valuation', *The Review of Financial Studies*, vol. 34(3), pp. 1105–1155.

Diamond, D.W. and Dybvig, P.H. (1983). 'Bank runs, deposit insurance, and liquidity', *Journal of Political Economy*, vol. 91(3), pp. 401–419.

Eisenbach, T.M. (2017). 'Rollover risk as market discipline: A two-sided inefficiency', *Journal of Financial Economics*, vol. 126(2), pp. 252–269.

Goldstein, I., Kopytov, A., Shen, L. and Xiang, H. (2022). 'Synchronicity and fragility', *Working Paper*.

Goldstein, I. and Pauzner, A. (2005). 'Demand–deposit contracts and the probability of bank runs', *the Journal of Finance*, vol. 60(3), pp. 1293–1327.

Klages-Mundt, A. and Minca, A. (2019). '(in) stability for the blockchain: Deleveraging spirals and stablecoin attacks', *arXiv preprint arXiv:1906.02152*.

Liu, J., Makarov, I. and Schoar, A. (2023). 'Anatomy of a run: the terra luna crash', *Working Paper*.

Liu, X. (2016). 'Interbank market freezes and creditor runs', *The Review of Financial Studies*, vol. 29(7), pp. 1860–1910.

Liu, X. (2023). 'A model of systemic bank runs', *The Journal of Finance*, vol. 78(2), pp. 731–793.

Morris, S. and Shin, H.S. (1998). 'Unique equilibrium in a model of self-fulfilling currency attacks', *American Economic Review*, pp. 587–597.

Morris, S. and Shin, H.S. (2000). 'Rethinking multiple equilibria in macroeconomic modeling', *NBER macroeconomics Annual*, vol. 15, pp. 139–161.

Morris, S. and Shin, H.S. (2004). 'Coordination risk and the price of debt', *European Economic Review*, vol. 48(1), pp. 133–153.

Pagnotta, E.S. (2022). 'Decentralizing money: Bitcoin prices and blockchain security', *The Review of Financial Studies*, vol. 35(2), pp. 866–907.

Rochet, J.C. and Vives, X. (2004). 'Coordination failures and the lender of last resort: was bagehot right after all?', *Journal of the European Economic Association*, vol. 2(6), pp. 1116–1147.

Rogoff, K. and You, Y. (2023). 'Redeemable platform currencies', *The Review of Economic Studies*, vol. 90(2), pp. 975–1008.

Sockin, M. and Xiong, W. (2023). 'A model of cryptocurrencies', *Management Science*.

Uhlig, H. (2022). 'A luna-tic stablecoin crash', *Working Paper*.

Vives, X. (2014). 'Strategic complementarity, fragility, and regulation', *The Review of Financial Studies*, vol. 27(12), pp. 3547–3592.

APPENDIX

Self-Collateral and Crypto-Run

Wenjin Kang, Ke Tang, Yang You and Jiaqing Zeng

October-2023

This Appendix includes three sections, that is, Appendix A, Appendix B, and Appendix C.

In Appendix A, we present a series of Appendix Figures as below.

Figure A1: FTX Asset Balances and FTT Token Prices from Oct-01 to Nov-10, 2022.

Figure A2: Model Timeline.

Figure A3: The Impact of the Exchange Self-collateralness on the Probability of Exchange Failure.

In Appendix B, we provide the proofs for Proposition 1 and Proposition 2 in our paper.

In Appendix C, we include additional policy implication discussions about the technological challenge for the cryptocurrency custody mechanism and the possibility of the deposit insurance scheme for investors' funds.

Appendix A: Appendix Figures

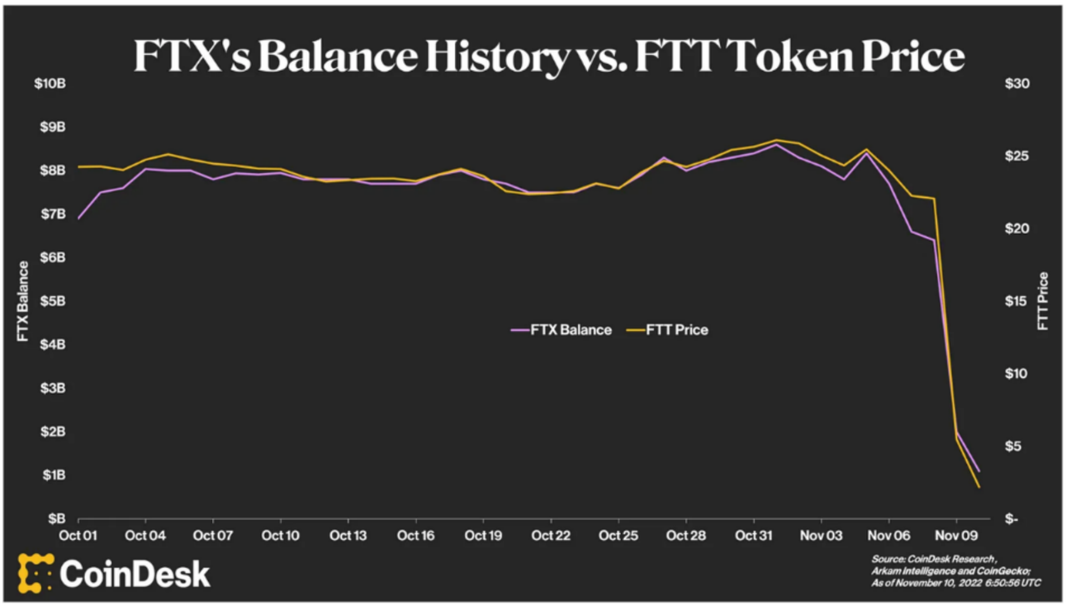

Figure A1: FTX Asset Balances and FTT Token Prices from Oct-01 to Nov-10, 2022.

This figure plots the time series of FTX asset balances (the left axis) and FTT token price (the right axis) during the period from October-01 to November-10, 2022. The FTX asset balance is the overall balance of digital assets deposited on the FTX trading platform. The figure shows that FTT token price and FTX assets balance co-move closely with each other.
(Source: Coindesk report at https://www.coindesk.com/markets/2022/11/10/ftx-balances-tumbled-87-in-5-days-in-epic-crypto-deposit-run-data-shows)

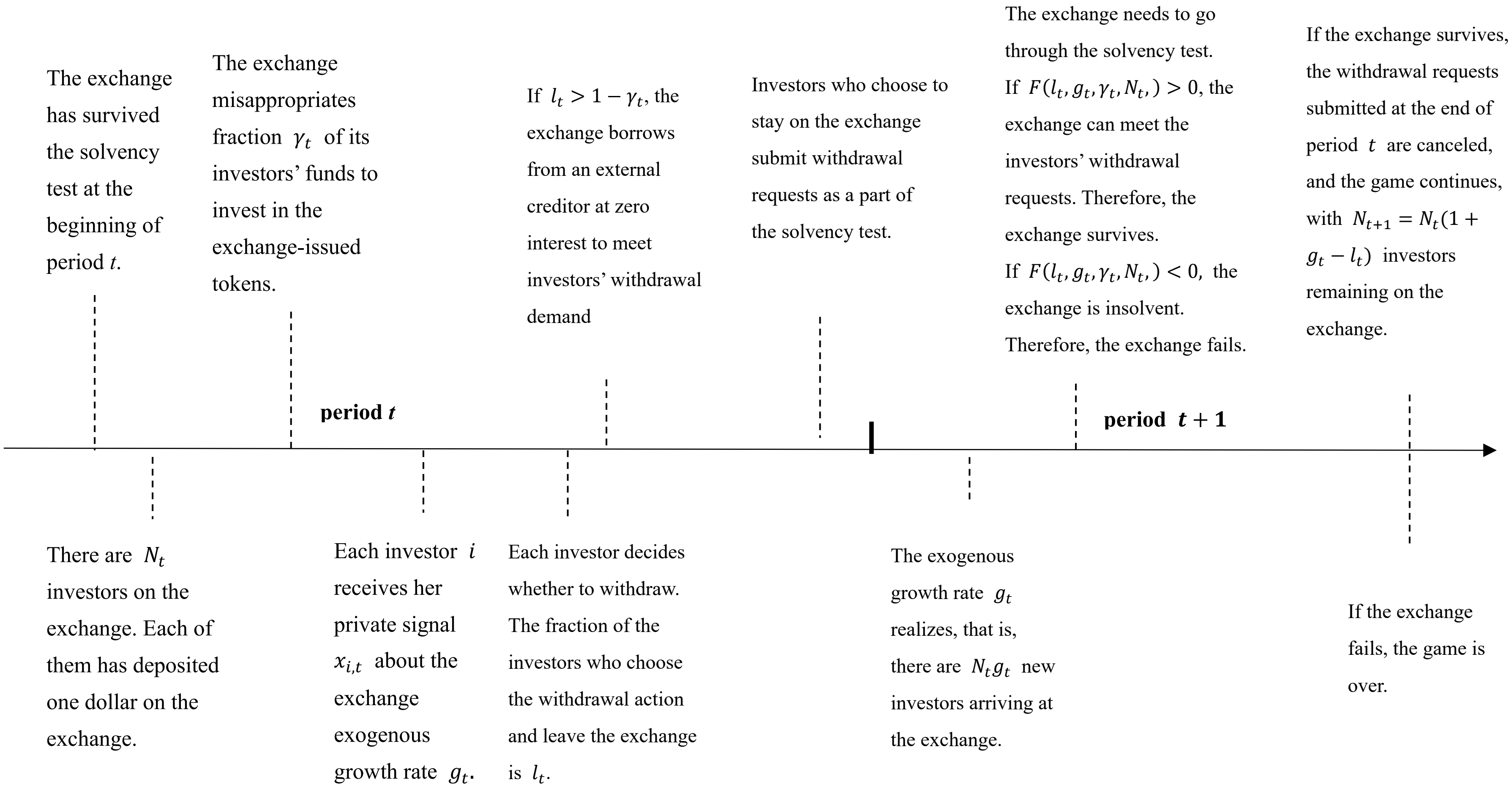

Figure A2: Model Timeline

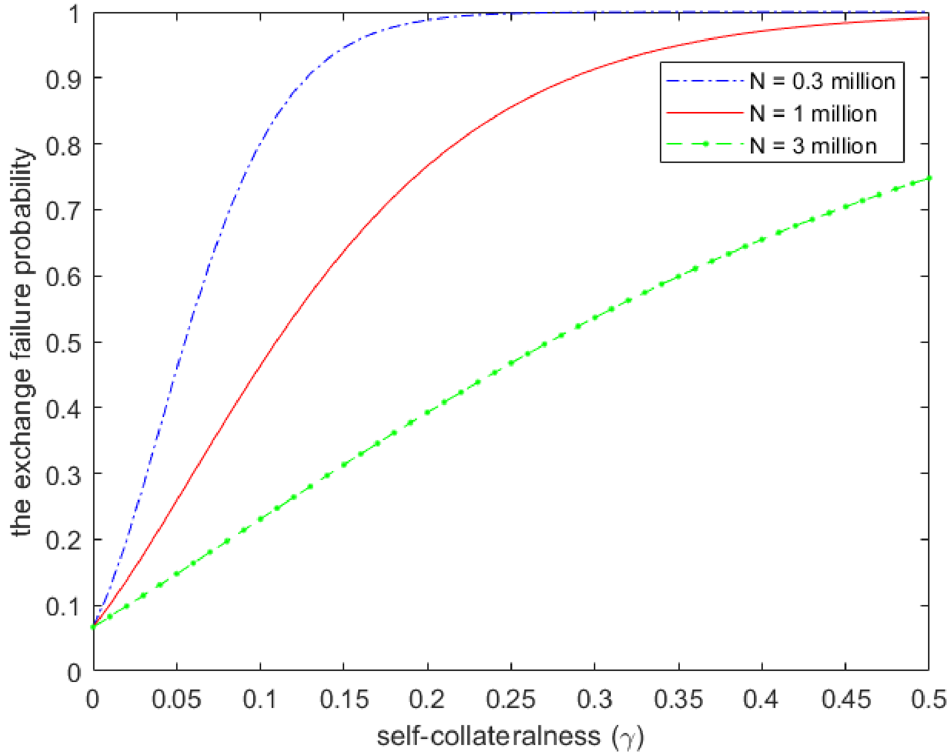

Figure A3: The Impact of the Exchange Self-collateralness on the Probability of Exchange Failure.

In this figure, we assume $\alpha = 1 - 10^{-6}$, β = 0.98, g = 0.03, $1/\sqrt{\tau_g}$ = 0.02, c = 0.02 for the model simulation. The self-collateralness (γ) is defined as the proportion of investors' funds that are misappropriated by the exchange and then invested by the exchange in the exchange-issued token. The figure shows that the probability of exchange failure increases when the level of sell-collateralness of the exchange (γ) increases. Given the same γ, the probability of exchange failure becomes higher when there are a smaller number of investors on the exchange.

Appendix B: Proofs for Propositions.

To prove Proposition 1, we need to prove Lemma A.1. and Lemma A.2 first.

Suppose all other investors use switching strategy, the threshold of which is $\hat{\xi}$, the failure threshold ψ is determined by $F\left(l(\hat{\xi}, \bar{g}, \psi), \psi, \gamma, N\right) = 0$, which is expressed as

$$\frac{1-\alpha^{N\left(1+\psi-\phi\left(\sqrt{\tau_\epsilon}\left(\frac{\tau_g+\tau_\epsilon}{\tau_\epsilon}\hat{\xi}-\frac{\tau_g}{\tau_\epsilon}\bar{g}-\psi\right)\right)\right)-1}}{1-\beta\alpha^{N\left(1+\psi-\phi\left(\sqrt{\tau_\epsilon}\left(\frac{\tau_g+\tau_\epsilon}{\tau_\epsilon}\hat{\xi}-\frac{\tau_g}{\tau_\epsilon}\bar{g}-\psi\right)\right)\right)-1}} * \frac{1-\beta\alpha^{N-1}}{1-\alpha^{N-1}} * \gamma - \gamma + \psi = 0. \qquad (B.1)$$

Conditional on ξ, the posterior distribution of g is normal with mean ξ and variance $\frac{1}{\tau_g+\tau_\epsilon}$. Because the exchange fails when $g < \psi$, the probability of exchange failure is

$$P(\xi, \hat{\xi}) = \Phi\left(\sqrt{\tau_g+\tau_\epsilon}(\psi - \xi)\right). \qquad (B.2)$$

We use $u(\xi, \hat{\xi})$ to denote the investor *i*'s net expected payoff of keeping her fund on the exchange versus withdrawing conditional on the signal ξ when all other investors are using the switching strategy around some point $\hat{\xi}$. $u(\xi, \hat{\xi})$ is

$$u(\xi, \hat{\xi}) = \left(1 - P(\xi, \hat{\xi})\right) * (1 + c) - 1. \qquad (B.3)$$

$u(\xi, \hat{\xi})$ satisfies the following properties:

(1) **Monotonicity:** $u(\xi, \hat{\xi})$ is strictly increasing in ξ and is strictly decreasing in $\hat{\xi}$.

(2) **Continuity**: $u(\xi, \hat{\xi})$ is continuous in ξ and $\hat{\xi}$.

(3) **Full range**: For any $\hat{\xi} \in \mathbb{R} \cup \{-\infty, +\infty\}$, when $\xi \to -\infty$, $u(\xi, \hat{\xi}) \to -1$, when $\xi \to +\infty$, $u(\xi, \hat{\xi}) \to c$.

The following is the proof of these properties.

First, we prove the monotonicity of $u(\xi, \hat{\xi})$ respective to ξ and $\hat{\xi}$. Because $\frac{\partial P(\xi,\hat{\xi})}{\partial \xi} < 0$, we have that $\frac{\partial u(\xi,\hat{\xi})}{\partial \xi} = -\frac{\partial P(\xi,\hat{\xi})}{\partial \xi}(1+c) > 0$.

Since

$$\frac{\partial F\big(l(\hat{\xi},\bar{g},\psi),\psi,\gamma,N\big)}{\partial\psi}>0,\frac{\partial F\big(l(\hat{\xi},\bar{g},\psi),\psi,\gamma,N\big)}{\partial\hat{\xi}}<0, \qquad (B.4)$$

according to implicit function theorem, we obtain that,

$$\frac{\partial\psi}{\partial\hat{\xi}}=-\frac{\partial F\big(l(\hat{\xi},\bar{g},\psi),\psi,\gamma,N\big)}{\partial\hat{\xi}}\Big/\frac{\partial F\big(l(\hat{\xi},\bar{g},\psi),\psi,\gamma,N\big)}{\partial\psi}>0. \qquad (B.5)$$

$$\frac{\partial P(\xi,\hat{\xi})}{\partial\hat{\xi}}=\frac{\partial P(\xi,\hat{\xi})}{\partial\psi}\frac{\partial\psi}{\partial\hat{\xi}}>0. \qquad (B.6)$$

$$\frac{\partial u(\xi,\hat{\xi})}{\partial\hat{\xi}}=-\frac{\partial P(\xi,\hat{\xi})}{\partial\hat{\xi}}(1+c)<0. \qquad (B.7)$$

Therefore, monotonicity is proved.

Second, according to the function form, it is obvious to show that $u(\xi,\hat{\xi})$ is a continuous function in ξ and $\hat{\xi}$.

Third, for any $\hat{\xi}\in\mathbb{R}\cup\{-\infty,+\infty\}$, when $\xi\to-\infty, P(\xi,\hat{\xi})\to 1, u(\xi,\hat{\xi})\to -1$.

When $\xi\to+\infty, P(\xi,\hat{\xi})\to 0, u(\xi,\hat{\xi})\to c$.

Based on (1), (2) and (3), we have the following Lemma.

Lemma A.1. *Suppose there are two sequences of real numbers. The first are* $\underline{\xi}^1,\underline{\xi}^2,\dots,\underline{\xi}^k,\dots$, *which are the solutions of*

$u\left(\underline{\xi}^1,-\infty\right)=0,\ u\left(\underline{\xi}^2,\underline{\xi}^1\right)=0,\ \dots,\ u\left(\underline{\xi}^{k+1},\underline{\xi}^k\right)=0,\dots,$

The second are $\bar{\xi}^1,\bar{\xi}^2,\dots,\bar{\xi}^k,\dots$, *which are the solutions of*

$u(\bar{\xi}^1,+\infty)=0,\quad u(\bar{\xi}^2,\bar{\xi}^1)=0,\dots,u(\bar{\xi}^{k+1},\bar{\xi}^k)=0,\dots,$

And ξ *is the solution of* $u(\xi,\xi)=0$. *Then*

$$\underline{\xi}^1<\underline{\xi}^2<\cdots<\underline{\xi}^k<\cdots<\xi, \qquad (B.8)$$

$$\bar{\xi}^1>\bar{\xi}^2>\cdots>\bar{\xi}^k>\cdots>\xi. \qquad (B.9)$$

Moreover, if $\underline{\xi}$ *is the smallest solution to* $u(\xi,\xi)=0$, *and* $\bar{\xi}$ *is the largest solution* *to* $u(\xi,\xi)=0$. *We have* $\underline{\xi}=\lim_{k\to\infty}\underline{\xi}^k$ *and* $\bar{\xi}=\lim_{k\to\infty}\bar{\xi}^k$.

Proof. Because $u\left(\underline{\xi}^1,-\infty\right)=0$, $u\left(\underline{\xi}^2,\underline{\xi}^1\right)=0$, $-\infty<\underline{\xi}^1$, according to the monotonicity of $u(\xi,\hat{\xi})$, we have that $\underline{\xi}^1<\underline{\xi}^2$. If $u\left(\underline{\xi}^k,\underline{\xi}^{k-1}\right)=0, u\left(\underline{\xi}^{k+1},\underline{\xi}^k\right)=0$, and $\underline{\xi}^{k-1}<\underline{\xi}^k$, monotonicity implies that $\underline{\xi}^k<\underline{\xi}^{k+1}$. Because $u\left(\underline{\xi}^{k+1},\underline{\xi}^k\right)=0$, $u(\xi,\xi)=0$, and $\underline{\xi}^k<\underline{\xi}^{k+1}$, we obtain that $\underline{\xi}^k<\xi$. Thus, $\underline{\xi}^1<\underline{\xi}^2<\cdots<\underline{\xi}^k<\cdots<\xi$. Analogously, we can prove that $\bar{\xi}^1>\bar{\xi}^2>\cdots>\bar{\xi}^k>\cdots>\xi$. If $\underline{\xi}$ is the smallest solution to $u(\xi,\xi)=0$, by (B.8) and monotonicity, $\underline{\xi}$ is the smallest upper bound for the sequence $\{\underline{\xi}^k\}$. Because $\{\underline{\xi}^k\}$ is increasing and bounded. We can get that $\underline{\xi}=\lim_{k\to\infty}\underline{\xi}^k$. According to (B.9), $\{\bar{\xi}^k\}$ is decreasing and bounded. If $\bar{\xi}$ is the largest solution to $u(\xi,\xi)=0$, $\bar{\xi}$ is the largest lower bound for sequence $\{\bar{\xi}^k\}$. $\bar{\xi}=\lim_{k\to\infty}\bar{\xi}^k$. Lemma A.1. is proved. □

Lemma A.2. *If* σ *is a strategy that survives k rounds of iterated deletion of dominated strategies, then*

$$\sigma=\begin{cases} withdraw, if\ \xi<\underline{\xi}^k, \\ stay, if\ \xi>\bar{\xi}^k. \end{cases} \tag{B.10}$$

Proof. We prove the Lemma by induction. We denote by σ^{-i} the strategy profile used by all other investors except *i*, and denote by $\tilde{u}(\xi,\sigma^{-i})$ the investor *i*'s expected payoff of keeping her fund on the exchange versus withdrawing conditional on the signal ξ when all others are using strategy σ^{-i}. The probability of exchange failure is maximized when all others withdraw from the exchange. and the probability of exchange failure is minimized when all others keep their funds on the exchange. Therefore,

$$u(\xi,+\infty)\le\tilde{u}(\xi,\sigma^{-i})\le u(\xi,-\infty). \tag{B.11}$$

When $\xi<\underline{\xi}^1$, we can get

$$\tilde{u}(\xi,\sigma^{-i})\le u(\xi,-\infty)< u\left(\underline{\xi}^1,-\infty\right)=0. \tag{B.12}$$

When $\xi < \underline{\xi}^1$, keeping funds in the exchange is strictly dominated by withdrawing from the exchange.
When $\xi > \bar{\xi}^1$, we can get

$$\tilde{u}\left(\xi, \sigma^{-i}\right) \geq u(\xi, +\infty) > u\left(\bar{\xi}^1, +\infty\right) = 0. \qquad (B.13)$$

When $\xi > \bar{\xi}^1$, withdrawing from the exchange is strictly dominated by keeping funds on the exchange.
Therefore, strategy σ^i survives the first round of deletion of dominated strategies,'

$$\sigma^i(\xi) = \begin{cases} withdraw, if\ \xi < \underline{\xi}^1, \\ stay, if\ \xi > \bar{\xi}^1. \end{cases} \qquad (B.14)$$

(B.14) shows that (B.10) holds when $k = 1$. Suppose (B.10) holds for k, if we prove that (B.10) holds for $k + 1$, the Lemma is proved.

We denote by U^k the set of strategies which satisfy (B.10) for k. We assume that a specific investor believes that others' strategy profile σ^{-i} consists of strategies drawn from U^k. When all others are using $\bar{\xi}^k$-trigger strategy, the expected payoff is the smallest. When all others are using $\underline{\xi}^k$-trigger strategy, the expected payoff is the largest. For any ξ, and any strategy profile σ^{-i} consisting of those drawn from U^k, we have that

$$u\left(\xi, \bar{\xi}^k\right) \leq \tilde{u}^i\left(\xi, \sigma^{-i}\right) \leq u\left(\xi, \underline{\xi}^k\right). \qquad (B.15)$$

If $\xi < \underline{\xi}^{k+1}$, according to monotonicity,

$$\tilde{u}^i\left(\xi, \sigma^{-i}\right) \leq u\left(\xi, \underline{\xi}^k\right) < u\left(\underline{\xi}^{k+1}, \underline{\xi}^k\right) = 0. \qquad (B.16)$$

When $\xi < \underline{\xi}^{k+1}$ and all others use strategy σ^{-i} drawn from U^k, keeping her fund in the exchange is strictly dominated by withdrawing from the exchange.
If $\xi > \bar{\xi}^{k+1}$,

$$\tilde{u}^i\left(\xi, \sigma^{-i}\right) \geq u\left(\xi, \bar{\xi}^k\right) > u\left(\bar{\xi}^{k+1}, \bar{\xi}^k\right) = 0. \qquad (B.17)$$

When $\xi > \bar{\xi}^{k+1}$ and all others use strategy σ^{-i} drawn from U^k, withdrawing from the exchange is strictly dominated by keeping her fund in the exchange. If strategy σ^i survives $k + 1$ rounds of deletion of dominated strategies, we have that

$$\sigma^i(\xi) = \begin{cases} withdraw, if\ \xi < \underline{\xi}^{k+1}, \\ stay, if\ \xi > \bar{\xi}^{k+1}. \end{cases} \qquad (B.18)$$

Lemma A.2. is proved. □

Based on Lemma A.1. and Lemma A.2., we can prove Proposition 1.

Proof of Proposition 1. First, we prove that as $\tau_\epsilon \to \infty$, there is one and only one ξ that satisfies $u(\xi,\xi) = 0$. From equation (B.2) and (B.3), $u(\xi,\xi) = 0$ is equivalent to

$$\sqrt{\tau_g + \tau_\epsilon}(\psi - \xi) = \Phi^{-1}\left(\frac{c}{1+c}\right), \qquad (B.19)$$

where ψ satisfies

$$\frac{1 - \alpha^{N\left(1+\psi-\phi\left(\sqrt{\tau_\epsilon}\left(\frac{\tau_g+\tau_\epsilon}{\tau_\epsilon}\xi - \frac{\tau_g}{\tau_\epsilon}\bar{g} - \psi\right)\right)\right)-1}}{1 - \beta\alpha^{N\left(1+\psi-\phi\left(\sqrt{\tau_\epsilon}\left(\frac{\tau_g+\tau_\epsilon}{\tau_\epsilon}\xi - \frac{\tau_g}{\tau_\epsilon}\bar{g} - \psi\right)\right)\right)-1}} * \frac{1 - \beta\alpha^{N-1}}{1 - \alpha^{N-1}} * \gamma - \gamma + \psi = 0. \qquad (B.20)$$

As $\tau_\epsilon \to \infty$, $\sqrt{\tau_\epsilon}(\psi - \xi) \to \Phi^{-1}\left(\frac{c}{1+c}\right)$, $\sqrt{\tau_\epsilon}\left(\frac{\tau_g+\tau_\epsilon}{\tau_\epsilon}\xi - \frac{\tau_g}{\tau_\epsilon}\bar{g} - \psi\right) \to -\Phi^{-1}\left(\frac{c}{1+c}\right)$. Combining (B.19) and (B.20), we have that

$$\frac{1 - \alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}}{1 - \beta\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}} * \frac{1 - \beta\alpha^{N-1}}{1 - \alpha^{N-1}} * \gamma - \gamma + \psi = 0. \qquad (B.21)$$

This is exactly $F\left(\frac{1}{1+c}, \psi, \gamma, N\right) = 0$. We need to prove that there is one and only one ψ that satisfies (B.21). Because $F\left(\frac{1}{1+c}, \psi, \gamma, N\right)$ is continuously increasing in ψ, and $F\left(\frac{1}{1+c}, 0, \gamma, N\right) < 0, F\left(\frac{1}{1+c}, \gamma, \gamma, N\right) > 0$, there is one and only one ψ that satisfies equation (B.21). As $\tau_\epsilon \to \infty, \xi \to \psi$. Therefore, there is one and only one ξ that satisfies $u(\xi,\xi) = 0$.

Second, we prove that if $u(\xi,\xi) = 0$, there is an equilibrium in which all investors withdraw if their signal is below ξ and keep their funds in the exchange if their signal is above ξ. Suppose others are using ξ −trigger strategy, because $u(\xi,\hat{\xi})$ is strictly increasing in ξ, if $\xi_1 < \xi < \xi_2$, we can have that

$$u(\xi_1,\xi) < u(\xi,\xi) = 0 < u(\xi_2,\xi). \qquad (B.22)$$

Therefore, ξ −trigger strategy is also the optimal strategy fore the specific investor. There is an equilibrium in which everyone uses switching strategy around ξ.

Finally, we show that if there is only one ξ that satisfies $u(\xi,\xi) = 0$, there is no other equilibrium in which the strategy that survives the iterated deletion of dominated strategies. From Lemma A.1., we can have that

$$\xi = \lim_{k\to\infty} \underline{\xi}^k = \lim_{k\to\infty} \bar{\xi}^k . \tag{B.23}$$

From Lemma A.2., we can prove that the ξ −trigger strategy is the only strategy that survives the iterated deletion of dominated strategies. Therefore, the threshold equilibrium is the unique equilibrium. □

Proof of Proposition 2.

The token price is an increasing function of the number of investors on the exchange. $\frac{\partial P_t}{\partial N} = \frac{-\log(\alpha)\alpha^{N-1}(1-\beta)}{(1-\beta\alpha^{N-1})^2} > 0$. Since $F\left(\frac{1}{1+c}, \psi, \gamma, N\right) = \frac{1-\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}}{1-\beta\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}} * \frac{1-\beta\alpha^{N-1}}{1-\alpha^{N-1}} *$ $\gamma - \gamma + \psi,$ we can obtain that

$$\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial \psi} = \frac{\partial P_{t+1}}{\partial \psi}\frac{1}{P_t}\gamma + 1 > 0. \tag{B.24}$$

If $\psi > \frac{1}{1+c}$, which means $N\left(1+\psi-\frac{1}{1+c}\right) > N,$ as the price is increasing in the number of investors, we obtain that $\frac{P_{t+1}}{P_t} > 1.$ Therefore, $F\left(\frac{1}{1+c}, \psi, \gamma, N\right) > 0.$

If $\psi < 0,$ $\frac{P_{t+1}}{P_t} < 1.$ We can get $F\left(\frac{1}{1+c}, \psi, \gamma, N\right) < 0.$ Therefore, $F\left(\frac{1}{1+c}, \psi, \gamma, N\right) =$ 0 means that $0 < \psi < \frac{1}{1+c},$ which means $1 + \psi - \frac{1}{1+c} < 1.$ The number of investors on the exchange decreases. Therefore, $\frac{1-\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}}{1-\beta\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}} < \frac{1-\alpha^{N-1}}{1-\beta\alpha^{N-1}}.$ The derivative of $F\left(\frac{1}{1+c}, \psi, \gamma, N\right)$ with respect to $\gamma,$

$$\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial \gamma} = \frac{1-\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}}{1-\beta\alpha^{N\left(1+\psi-\frac{1}{1+c}\right)-1}} * \frac{1-\beta\alpha^{N-1}}{1-\alpha^{N-1}} - 1 < 0, \tag{B.25}$$

According to implicit function theorem,

$$\frac{\partial \psi}{\partial \gamma} = -\frac{\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial \gamma}}{\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial \psi}} > 0, \tag{B.26}$$

Because $\Phi(\sqrt{\tau_g}(\psi - \bar{g}))$ continuously increases in $\psi,$ we obtain that $\Phi(\sqrt{\tau_g}(\psi - \bar{g}))$ continuously increases in $\gamma.$ Therefore, we have proved that the probability of exchange failure is an increasing function of the exchange's self-collateralness γ.

Next, we prove that the probability of exchange failure is a decreasing function of the number of investors N. We first prove that when $0<\alpha<1, 0<\beta<1$, $N\left(1+\psi-\frac{1}{1+c}\right)-1>0$, $F\left(\frac{1}{1+c},\psi,\gamma,N\right)$ is increasing in N. Here $0<\alpha<1$ and $0<\beta<1$ are obvious in our model setup. The inequality $N\left(1+\psi-\frac{1}{1+c}\right)-1>0$ is a mathematical precondition that ensures there are at least more than one investors on the exchange in period $t+1$, so that there exist opportunities that trading can occur among different investors on the exchange trading platform.

For simplification, we denote by $d=1+\psi-\frac{1}{1+c}$. $0<d<1$. We denote by $f(N)=\frac{1-\alpha^{Nd-1}}{1-\beta\alpha^{Nd-1}}*\frac{1-\beta\alpha^{N-1}}{1-\alpha^{N-1}}$. To prove $F\left(\frac{1}{1+c},\psi,\gamma,N\right)$ is increasing in N, we just prove that $f(N)$ is increasing in N.

$$f(N)=1-\frac{(1-\beta)(\alpha^{Nd-1}-\alpha^{N-1})}{(1-\beta\alpha^{Nd-1})(1-\alpha^{N-1})}. \qquad (B.27)$$

It is obvious that $\frac{1}{(1-\beta\alpha^{Nd-1})}$ is decreasing in N. The sufficient condition to guarantee that $f(N)$ is increasing in N is $g(N)=\frac{\alpha^{Nd-1}-\alpha^{N-1}}{1-\alpha^{N-1}}$ and $g'(N)<0$.

As $g(N)=1-\frac{1-\alpha^{Nd-1}}{1-\alpha^{N-1}}$, we denote $h(N)=\frac{1-\alpha^{Nd-1}}{1-\alpha^{N-1}}$.

We then need to prove that $h'(N)>0$.

$$h'(N)=\frac{-\mathrm{d}*\log\alpha*\alpha^{Nd-1}(1-\alpha^{N-1})+\log\alpha*\alpha^{N-1}*(1-\alpha^{Nd-1})}{(1-\alpha^{N-1})^2} \qquad (B.28)$$

$$h'(N)>0 \iff d*\alpha^{Nd-1}+(1-d)\alpha^{Nd-1+N-1}>\alpha^{N-1}. \qquad (B.29)$$

We know that α^x is convex, according to Jensen's inequality, we get

$$d*\alpha^{Nd-1}+(1-d)\alpha^{Nd-1+N-1}\geq\alpha^{d*(Nd-1)+(1-d)*(Nd-1+N-1)}=\alpha^{N+d-2}$$
$$=\alpha^{N-1}*\alpha^{d-1}>\alpha^{N-1}.$$

Therefore, $g'(N)<0$ is proved. It means that when $N>\frac{1}{1+\psi-\frac{1}{1+c}}$, $F\left(\frac{1}{1+c},\psi,\gamma,N\right)$ is increasing in N. According to implicit function theorem,

$$\frac{\partial \psi}{\partial N} = -\frac{\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial N}}{\frac{\partial F\left(\frac{1}{1+c}, \psi, \gamma, N\right)}{\partial \psi}} < 0. \qquad (B.30)$$

Because $\Phi(\sqrt{\tau_g}(\psi - \bar{g}))$ continuously increases in ψ, we obtain that the exchange-failure probability $\Phi(\sqrt{\tau_g}(\psi - \bar{g}))$ continuously decreases in N. □

Appendix C: Additional Policy Implications.

C.1. *The Technological Challenge for the Cryptocurrency Custody Mechanism.*

There are significant technological challenges about how to implement an effective custody of clients' crypto-assets in practice. The reality is that very few reputable traditional banks or financial institutions can provide custodian services under the changing regulatory environment for cryptocurrencies. The blockchain technology grants full control rights of assets to crypto-wallet owners who possess the private keys. If the exchange controls private keys, we further need to audit these custodian wallets and make sure that the exchange cannot swap its clients' crypto-assets into other types of cryptocurrencies without the clients' consent. On the other hand, if a custodian agency manages the private keys, it must bear the burden of handling deposit and withdrawal requests for a very large number of different cryptocurrencies. Furthermore, the custodian may also need to pay gas fees and address additional cybersecurity hacking risks. The sophistication and operation costs are much higher than the custodian service with a conventional bank account -- that is why traditional banks exhibit great hesitance to provide crypto custodian services. One possibility is to let an insurance company provide at least some coverage for the potential loss in the crypto wallets and hence guarantee the exchange's solvency. For example, Hashkey Exchange, a licensed Hong Kong crypto-exchange, collaborates with OneDegree (an insurance provider for digital assets) to obtain crypto wallet insurance.

C.2. *Deposit Insurance for Investors' Funds*

Another commonly-used policy tool to prevent a bank run is deposit insurance. In the context of a crypto-run, introducing a similar insurance policy for the investors' funds deposited in the exchange can serve as a theoretically effective approach to prevent a crypto-run. If investors can be assured that, regardless of the exchange's solvency status, they are always able to receive their deposited assets back, they will choose to keep their funds in the exchange because they can enjoy the additional convenience yield from the exchange-provided trading service. Consequently, the deposit insurance can address the risk that investors' withdrawals make the exchange insolvent and hence prevent a crypto-run.

Despite the theoretical merits described above, a more important question is who should provide the insurance for the investors on the crypto-exchange in practice. Should a private insurance company assume this role, the insurance premiums could become prohibitively expensive. This predicament arises because private insurers often lack the means to effectively monitor the exchange's business operations, which leaves them unable to prevent potential misappropriations of investors' funds by the exchange. Consequently, this exposes the private insurer to significant moral hazard issues. Facing the dilemma, the private insurance company may be compelled to demand exorbitant premiums to offset such risk, and this will make the private investor-insurance scheme practically infeasible.

In contrast, a public deposit insurance scheme provided by the government may have the virtue that the insurance premium can be reduced by implementing effective oversight of the crypto-exchange. For instance, if a regulator can monitor the exchange's operations, audit its financial statements, and hold exchange operators accountable for any misconduct, the moral hazard concerns in insurance provision can be significantly mitigated. This enables more affordable insurance costs for exchange and ultimately lowers the overall expenses incurred by crypto-investors. The example of public insurance scheme illustrated here suggests that well-designed regulatory guidance can actually benefit regulated crypto-exchanges by preventing crypto-run and enabling them to provide a low-cost and safe trading venue for crypto-investors.