NBER WORKING PAPER SERIES

DECENTRALIZATION THROUGH TOKENIZATION

Michael Sockin
Wei Xiong

Working Paper 29720
http://www.nber.org/papers/w29720

NATIONAL BUREAU OF ECONOMIC RESEARCH
1050 Massachusetts Avenue
Cambridge, MA 02138
February 2022

We thank Franklin Allen, Will Cong, Cam Harvey, Emiliano Pagnotta, Aleh Tsyvinski, Haoxiang Zhu, and participants of various seminars and conferences for helpful comments. We are particularly grateful to Bruno Biais, an Associate Editor, and three referees, whose highly constructive suggestions helped shape this paper. The views expressed herein are those of the authors and do not necessarily reflect the views of the National Bureau of Economic Research.

Decentralization Through Tokenization
Michael Sockin and Wei Xiong
NBER Working Paper No. 29720
February 2022
JEL No. G3

ABSTRACT

We examine decentralization of digital platforms through tokenization as an innovation to resolve the conflict between platforms and users. By delegating control to users, tokenization through utility tokens acts as a commitment device that prevents a platform from exploiting users. This commitment comes at the cost of not having an owner with an equity stake who, in conventional platforms, would subsidize participation to maximize the platform's network effect. This trade-off makes utility tokens a more appealing funding scheme than equity for platforms with weak fundamentals. The conflict reappears when non-users, such as token investors and validators, participate on the platform.

Michael Sockin
Department of Finance
UT Austin McCombs School of Business
Austin, TX 78712
michael.sockin@mccombs.utexas.edu

Wei Xiong
Princeton University
Department of Economics
Bendheim Center for Finance
Princeton, NJ 08450
and NBER
wxiong@princeton.edu

The proliferation of the digital economy and the recent rise of the fintech industry have led to two important trends. The first is that a sizable number of digital platforms have funded their development and operations through the issuance of cryptocurrencies or tokens. According to Allen, Gu and Jagtiani (2020), for instance, as of May 2020, 4,136 cryptocurrencies exist, not including many that have failed. Although rampant speculation and volatility are often observed in this asset class, its growing popularity raises important conceptual questions about the benefits and costs associated with the tokenization process. The second trend is the growing tension between digital platforms and their users as online platforms, such as Amazon, Google, and Facebook, become increasingly pervasive in our everyday lives. Their large networks of users not only facilitate monopoly power in pricing but also extensive access to users' private data.[1] These privileges are subject to misuse, as reflected by ongoing antitrust investigations into big-tech companies and the enactment of data privacy regulations in the European Union, the United States, and Japan. Such conflict between online platforms and their users represents a unique challenge to their design and raises questions about whether they could be disintermediated to protect consumers.

The success of Bitcoin, the first cryptocurrency to achieve unprecedented popularity across the world, was built largely on the notion that delegating the issuance of the cryptocurrency to pre-coded computer algorithms would free its users from potential abuses by central bankers, who control the supply of traditional fiat currencies and may increase it for their own interest at the expense of current holders. Since its inception, tokenization has continued to facilitate the decentralization of digital platforms in practice, in what are often referred to as Decentralized Autonomous Organizations (DAOs).[2] Filecoin, a platform that enables users to exchange secure data storage services, for instance, is governed by the Filecoin community who propose, discuss, and achieve consensus on Filecoin Improvement Protocols (FIPs). Tezos, a platform that facilitates peer-to-peer transactions and smart contracting, achieves governance through all users voting in two stages on updates proposed by

[1] There is extensive literature exploring how online platforms' extensive access to user data may allow them to price discriminate users, e.g., Taylor (2004), and take advantage of users' personal vulnerabilities such as weak self-control, e.g., Liu, Sockin and Xiong (2020).

[2] There is an inherent link between the promise of self-sovereignty and DAOs. Eric Voorhees, CEO of the ShapeShift trading platform that uses the FOX token, for instance, tweeted in his announcement of ShapeShift's impending decentralization: "Unorthodox, but it is the only way to maintain fidelity to the most important principles of crypto; specifically, self-sovereignty over money. [...] you may understand that the organizational format that succeeded during the Industrial Age may not be the optimal format for the digital age. There is a new kind of 'firm.' The decentralized autonomous organization." (https://twitter.com/ErikVoorhees/status/1415339998740508674?ref_src=twsrc%5Etfw)

developers who are compensated for their innovations in newly minted Tezos coins. There are also multi-purpose platforms, such as the decentralized finance (DeFi) platform MakerDAO and the decentralized organization manager platform Aragon, that issue governance tokens that confer control (but not cash flow) rights for voting on changes to the platform and its development.[3] The DeFi platform Kyber pays rewards in the native token KNC to users who participate in governance by staking their holdings. Furthermore, Harvey, Ramachandran and Santoro (2020) provide a roadmap for how crypto-based technologies can decentralize various aspects of the financial industry.

In this paper, we develop a model to examine tokenization as an innovative effort to resolve the tension between platforms and their users, similar to how corporate finance has developed governance tools to manage the classic tension between firm managers, who control the firm's operations, and firm owners, who own the firm's assets. Indeed, industry commentators have also highlighted the resolution of the principal-agent problem between a platform's stakeholders as a key motivation for DAOs.[4]

In what follows, we regard canonical tokens issued by a digital platform as an asset that conveys a right to the services of the platform and possible participation in its governance, but not necessarily cash flow rights. Such tokens are typically held by users who garner a convenience yield from participating on the platform, and include "payment" and "consumer" ("utility") tokens in the taxonomy of the Global Digital Finance (GDF).[5] In contrast, a security confers cash flow and potentially ownership rights, such as debt and equity, but not a right to services on the platform. Such securities are typically held by outside stakeholders, similar to how owners of Amazon or Apple stock need not buy products from Amazon or Apple. Thus, the key distinction between tokens and securities is that tokens are a claim to the platform's services while securities are a claim to its revenue.[6]

[3] With the announced dissolution of the Maker Foundation that currently stewards the platform, MakerDAO will be a completely decentralized platform by the end of 2021. As its CEO Rune Christensen writes in a blog, "Complete decentralization of Maker means that future development and operation of the Protocol and the DAO will be determined by thousands or perhaps millions of engaged, enthusiastic community members, all determined to extend the benefits of digital currency to people across the globe." (https://blog.makerdao.com/makerdao-has-come-full-circle/)

[4] For example, see the recent commentary by cointelegraph.com at https://cointelegraph.com/ethereum-for-beginners/what-is-a-decentralized-autonomous-organization-and-how-does-a-dao-work, and the discussion by JP Buntinx at https://vaultoro.com/what-is-a-decentralized-autonomous-organization-dao-and-why-does-it-matter/#h-exploring-the-principal-agent-problem.

[5] See "Code of Conduct: Taxonomy for Cryptographic Assets" at https://www.gdf.io/wp-content/uploads/2019/08/0010_GDF_Taxonomy-for-Cryptographic-Assets_Proof-V2-260719.pdf.

[6] Also note that some cryptographic assets, such as security tokens and "financial asset" tokens in the taxonomy of the GDF, are claims to cash flows but not services from a platform. As such, the SEC

Our key insight is that, although tokenization may protect users by shifting ownership and control of the platform to them from initial equity holders, this benefit comes at the expense of removing any owner who would subsidize user participation to maximize the platform's network effect. As network effects are essential for the success of online platforms, conventional platforms typically devote substantial resources to subsidize user participation to amass a large user base.[7] The equity holders of these platforms bear the costs of subsidizing user participation to maximize future advertising revenue, which increases with the size of the user base. Our model highlights the trade-off induced by decentralization between safeguarding users and subsidizing their participation in the presence of network effects.

Our model features an online platform that facilitates bilateral transactions among a pool of users. There are three dates. At time 0, the developer of the platform chooses to fund the platform by issuing either conventional equity or tokens. The choice of funding scheme also determines the control and ownership of the platform in the subsequent periods. At time 1, potential users choose whether to join the platform, subject to a personal cost of downloading the necessary software and becoming familiar with the platform's rules and user interface. After joining the platform, a user can benefit from matching with other users to make bilateral transactions at both times 1 and 2. We model a user's transaction need by his endowment in a consumption good and his preference of consuming his own good together with the goods of other users. As a result of this preference, users need to trade goods with each other, which can occur only on the platform. Consequently, there is a key network effect—each user's desire to join the platform grows with the number of other users on the platform and the size of their goods endowments.

We compare the conventional equity-based funding scheme, in which equity conveys both control and (residual) cash flow rights, with several token-based schemes. If the developer issues equity, it leads to a group of equity holders that is represented by an owner who takes ownership and control of the platform. The owner would choose to provide a subsidy at time 1 to attract the marginal user, whose own transaction need is relatively low and who is otherwise not incentivized to participate on the platform without the subsidy. The participation of the marginal user, however, makes it easier for other users to find transaction

ruled in 2017 that such cryptographic assets are securities as they confer an expectation of a return on investment through the efforts of others, according to the Howey test ("Blockchain and Cryptocurrency Regulation" at https://www.lw.com/thoughtLeadership/yellow-brick-road-for-consumer-tokens-path-to-sec-cftc-compliance.)

[7] Google and Facebook, for example, offer free search and social networking services to attract users.

partners and consequently maximizes the network effect. As the owner can profit from charging transaction fees that increase with the transaction surplus on the platform, it would internalize the participation cost of the marginal user by providing a subsidy to all users. Control of the platform, however, also allows the owner to exploit users at time 2 after the platform collects extensive data about them at time 1.

We consider a particular form of user exploitation—the owner may choose a subversive action (such as pursuing aggressive advertising strategies or selling user data to third parties, as is sometimes observed in practice), which benefits the owner at the expense of all users. Intuitively, the owner would choose this action only when the transaction fees from the platform fall below the gains from exploiting its users. Interestingly, while choosing this subversive action may benefit the owner ex post at time 2, the owner is strictly better off ex ante at time 1 if it can pre-commit to not taking such an action because anticipation of the owner's taking the subversive action discourages potential users from joining the platform initially, and this abandonment is magnified by the network effect. It is impossible to commit under the equity-based scheme, as the owner can always choose to reverse any previous commitment at time 2. This demand for commitment motivates tokenization.

Alternatively, the developer may adopt a token-based scheme. We focus on utility tokens because they represent the canonical form of tokens that entitile holders to services but not cash flows of the platform. To illustrate the key conceptual issues, we assume that the platform adopts a frictionless consensus protocol that confers voting rights to token holders, and we later examine the additional issues raised by protocols that require outside validators. Under this scheme, the owner sells tokens to users to participate on the platform instead of charging fees. By cashing out from issuing tokens to users who join the platform at time 1, the developer leaves control of the platform at times 1 and 2 to users through pre-coded algorithms, which can foster a commitment not to exploit users by requiring their consent. Although users, as holders of the tokens, may vote on changes to these algorithms, they would never agree to adopt an action that would hurt themselves. The lack of cash flow rights also discourages non-users from acquiring the tokens to seize control of the platform. This captures the key appeal of tokenization—giving ultimate control of the platform to users through decentralization. This benefit, however, comes at the cost of not having an owner with an equity stake who would subsidize user participation to maximize the platform's network effect.

Comparing utility tokens to equity leads to a sharp implication: utility tokens are more appealing for digital platforms with relatively weak demand fundamentals (i.e., aggregate transaction needs by users). Under the equity-based scheme, users' concerns about the owner subverting the platform are particularly high when the owner's transaction fees are low, which makes the commitment created by tokenization particularly valuable. Consistent with this observation, we show that for a given level of concern about user abuse, user participation, developer profit, and social surplus are all higher under the equity-based scheme when the platform fundamental is sufficiently high; for a given level of platform fundamental, in contrast, user participation, developer profit, and social surplus are all higher under the utility token-based scheme when the concern about user exploitation is sufficiently high.

We then consider two extensions of our model to illustrate the difficulty in overcoming the trade-off underlying decentralization when non-users also participate on the platform. First, we examine a hybrid scheme that allows the platform to collect transaction fees from users and pay out the fees to token holders as dividends. This scheme goes beyond the canonical tokens by giving token holders not only the right to make transactions but also the right to cash flows from the platform. At the risk of abusing our nomenclature, we call this hybrid cryptocurrency "equity tokens". Interestingly, we show that by extending the contract space, the equity token-based scheme is able to achieve the first-best outcome if the platform issues tokens only to users. As the platform collects more transaction fees from heavy users, the cash flows from the equity tokens serve as a subsidy from heavy to light users, which boosts user participation. Such cash flows, however, also incentivize investors who have no transaction need to acquire tokens as an investment, a phenomenon absent with utility tokens because they provide only transaction benefit to holders. The presence of investors diverts the subsidy away from users and thus harms their participation. More importantly, investors may even take a majority stake to seize control of the platform, which, as we show, occurs when the platform fundamental is sufficiently weak. The investors' concentration of control of the platform reintroduces the initial commitment problem that decentralization through tokenization aimed to overcome, as investors would choose the subversive action when transaction fees fall below the gain from selling user data. Allowing tokens to pay cash flows therefore leads to the converse of the key trade-off that we highlight—it helps to cross-subsidize user participation but at the expense of recreating the commitment problem.

Second, we introduce a frictional consensus protocol on the platform by assuming a group of decentralized validators compete for the right to record transactions on the blockchain in exchange for transaction fees. For example, a Proof-of-Work protocol requires miners to solve complex computational puzzles to add blocks to the blockchain, while a Proof-of-Stake protocol randomly allocates the right to add blocks among stakers based on their holdings. We formulate a general problem of using transaction fees as incentives to motivate the efforts of the validators to maintain the security of the blockchain. When the platform fundamental is strong and the transaction fees to the validators are sufficiently lucrative, they have strong incentives to compete for the transaction fees, making the blockchain robust to any outside attack. On the other hand, when the fundamental is weak and transaction fees fall below a threshold, the reduced incentives of the validators to compete make the blockchain vunerable to a "51% attack" by a rogue validator, leading to an outcome similar to the subversive action explored earlier. This result reveals that reliance on the validators to maintain the security of the blockchain in tokenization may reintroduce the commitment problem because the validators have interests divergent from the users.

Related Literature Our paper is related to the growing literature on initial coin offerings (ICOs) and their comparison to traditional financing schemes. Different from our focus on the conflict between platforms and users, many of these studies focus on the classic conflict induced by moral hazard between an entrepreneur and outside investors. Chod and Lyandres (2019) and Chod, Trichaskis and Yang (2019), for instance, show that utility token financing is preferable to equity in mitigating the underprovision of effort by an entrepreneur but leads to underinvestment and an underproduction of goods that are sold in advance. Catalini and Gans (2019) and Gan, Tsoukalas and Netessine (2020) compare utility tokens to revenue sharing and equity to profit sharing, with the former emphasizing that tokens facilitate competition and coordination among buyers and the latter emphasizing that equity is better in aligning the incentives of entrepreneurs and speculators. Malinova and Park (2018) find that tokens can finance a larger set of ventures in the presence of entrepreneurial moral hazard but are inferior to equity unless they are optimally designed to include revenue sharing. Gryglewicz, Mayer and Morrellec (2020) show that tokens are preferable to equity when financing needs and agency conflicts between the entrepreneur and outsiders are not severe. Other studies, such as Li and Mann (2017) and Bakos and Halaburda (2018), focus on the role of tokens in overcoming potential coordination failure among users.

Our analysis is also related to the literature on conflicts between a platform's owner and its users. Cong, Li and Wang (2020) investigate optimal platform financing of innovation by a firm that issues tokens to users, and how blockchain technology can foster commitment not to expropriate value through excessive seignorage. Similar to our analysis, Goldstein, Gupta and Sverchkov (2019) also emphasize that tokens can ease the tension between online platforms and customers, although their focus is on monopolistic price discrimination in which tokens unravel monopoly power by serving as durable goods. Mayer (2019) shows that conflicts of interest among the platform developer, users, and speculators interact through token liquidity on utility token platforms where the developer is subject to moral hazard and can sell its retained stake.

Our paper also contributes to the literature on the trade-offs of decentralizing digital platforms. Arruñada and Garicano (2018) explore how relational capital and the threat of hard forks on a decentralized platform can help resolve the "hold-up" problem in compensating content developers but at the cost of weakening coordination in the adoption of new innovations compared to a centralized platform. Cong and He (2019) investigate the trade-off of smart contracts on decentralized platforms in overcoming adverse selection while also facilitating oligopolistic collusion. Huberman, Leshno and Moallemi (2019) apply congestion pricing to find the optimal waiting fee structure under the Proof-of-Work consensus protocol and, in a similar spirit to our analysis, emphasize that decentralization prevents price discrimination by a monopolist but can lead to settlement delays. Tsoukalas and Falk (2020) argue that token-weighted voting among users on blockchain-based platforms is inefficient in aggregating information compared to centralized platforms. Choi and Park (2020) find that decentralization of information production can be socially costly because individual inspectors do not internalize the social benefit of their screening as would a monopolist in the context of academic journals. In contrast to these papers, we study how decentralization interacts with the financing of digital platforms and the trade-off between expropriating users and subsidizing their participation.

The rest of the paper is organized as follows. We introduce the model setting in Section 1 and describe the benchmark equity-based funding scheme in Section 2. We analyze the utility token-based scheme and the alternative equity token-based scheme in Section 3 and Section 4, respectively. Section 5 discusses issues related to the implementation of consensus protocols. Section 6 concludes the paper. We provide proofs to key propositions in the appendix and relegate omitted proofs of the other propositions to an online appendix.

1 The Model Setting

In this section, we present the model setting. There are three dates $t \in \{0, 1, 2\}$. For simplicity, we consider a generic platform, which facilitates bilateral transactions among a group of users. At $t = 0$, the developer of the platform chooses a scheme to fund the platform based on a prior belief about the platform's fundamental, which we will describe in more detail later. At $t = 1$, each potential user chooses whether to join the platform. After joining the platform, a user has the opportunity to randomly match with another user to make mutually beneficial transactions at $t = 1$ and $t = 2$, which can be viewed as the short run and the long run, respectively.

The developer of the platform needs to choose a funding scheme for the platform and we examine several alternative schemes. A key feature of our analysis is that the platform owner lacks commitment across the two periods and will not refrain from exploiting users at $t = 2$ after they have initially joined the platform at $t = 1$. This lack of commitment is a reasonable premise for several reasons. First, it is common for these digital platforms to update their terms of service, which gives them the flexibility to adopt strategies that benefit themselves at the expense of the users. Second, digital platforms collect large volumes of user data, which gives a platform the capacity to take advantage of its users by either selling the data to third parties or by pursuing aggressive advertising strategies. Specifically, we assume that the owner of the platform, which is only present under the equity-based scheme, can take a subverting action at $t = 2$ that monetizes users' private data. Anticipating the owner's lack of commitment may, in turn, affect the decisions of potential users to join the platform.

At $t = 1$, there is a continuum of potential users with a measure of one unit, indexed by $i \in [0, 1]$. These potential users need to transact goods with each other and can participate in two rounds of trading at $t = 1, 2$ on the platform. To join the platform, each user incurs a personal cost of $\kappa > 0$, which is related to setting up the necessary software and getting familiar with the institutional arrangements of the platform, and may need to pay an entry fee c to the platform. This entry fee may take different forms, depending on the platform's funding scheme, and can be positive or negative. As we will discuss, if the platform is funded by a token-based scheme, a user needs to pay the cost of acquiring a token to join the platform and consequently pay a positive fee. If instead the platform is funded by an equity-based scheme, the owner (i.e., equity holders of the platform) may choose to subsidize each user's initial participation by providing a subsidy, such as giving free digital services. In this case, a user incurs a negative entry fee. Those who do not join initially cannot participate on the platform in either round of trading. Let $X_i = 1$ if user i joins the platform, and $X_i = 0$ otherwise.

User i is endowed with a certain good, which is distinct from the goods of other users, and has a randomly matched trading partner, user j, in the general pool. Only if both i and j are on the platform can they trade their goods with each other at $t = 1$ and $t = 2$. After each round of transaction, user i has a Cobb-Douglas utility function over consumption of his own good and the good of user j according to

$$U_i\left(C_i, C_j\right) = \left(\frac{C_i}{1-\eta_c}\right)^{1-\eta_c}\left(\frac{C_j}{\eta_c}\right)^{\eta_c}, \tag{1}$$

where $\eta_c \in (0, 1)$ represents the weight in the Cobb-Douglas utility function on his consumption of his trading partner's good C_j , and $1 - \eta_c$ is the weight on consumption of his own good C_i. A higher η_c means a stronger complementarity between the consumption of the two goods. Both goods are needed for a user to derive utility from consumption. If one of them is not on the platform, there is no transaction, and each of them gets zero utility. This setting implies that each user cares about the pool of users on the platform, which determines the probability of matching with his trading partner.

User i has a goods endowment of e^{A_i}, which is equally divided across $t = 1$ and $t = 2$. A_i comprises a component A common to all users and an idiosyncratic component:

$$A_i = A + \tau_\varepsilon^{-1/2}\varepsilon_i,$$

with $\varepsilon_i \sim \mathcal{N}(0, 1)$ being normally distributed and independent across users and from A. The common component A represents the platform's demand fundamental, and it is publicly observed by all users and the developer only at $t = 1$. At $t = 0$, the developer has a normally distributed prior over A: $A \sim G\left(\bar{A}, \tau_A^{-1}\right)$ and chooses the platform's funding scheme based on this prior belief. We assume that $\int \varepsilon_i d\Phi\left(\varepsilon_i\right) = 0$ by the Strong Law of Large Numbers.

The aggregate endowment A is a key characteristic of the platform. A cleverly designed platform serves to amass users with strong needs to transact with each other. As we will show, a higher A leads to more users on the platform, which, in turn, implies a higher probability of each user completing transactions with another user; furthermore, each transaction gives greater surpluses to both parties. One can therefore view A as the demand fundamental of the platform.

When user i is paired with another user j on the platform, we assume that they simply swap their goods, with user i using $\eta_c e^{A_i}$ units of good i to exchange for $\eta_c e^{A_j}$ units of good j. Consequently, both users are able to consume both goods, with user i consuming

$$C_i(i) = (1-\eta_c)\, e^{A_i},\ C_j(i) = \eta_c e^{A_j}, \tag{2}$$

and user j consuming

$$C_i(j) = \eta_c e^{A_i},\ C_j(j) = (1-\eta_c)\, e^{A_j}. \tag{3}$$

We formally derive these consumption allocations between these two paired users in Appendix A through a microfounded trading mechanism between them. As each user receives half of his goods endowment in each period, this consumption is also equally divided across the two periods. We can use equation (1) to compute the utility surplus $U_{i,1}$ and $U_{i,2}$ of each user on both dates when the transactions happen.

As a benchmark for our analysis, we first characterize the first-best equilibrium that maximizes the utilitarian welfare of all users on the platform and a revenue-neutral scheme that implements it in the following proposition.

Proposition 1 *In the first-best equilibrium, if* $A \geq A_*^{FB} \equiv \log\kappa - \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\varepsilon^{-1}$*, all users participate on the platform, and a social planner can implement this outcome by imposing transaction fees proportional to users' transaction gain at a sufficiently high rate and redistributing the fees equally back to all users. If* $A < A_*^{FB}$*, then the platform shutters because the social surplus is negative.*

Proposition 1 illustrates a key network effect. In the first-best equilibrium, all users join the platform when the social surplus is positive, even though users with low endowments cannot cover their participation costs from their transaction gains, because their participation increases the transaction gains of other users. Thus, to implement this outcome, the social planner needs to cross-subsidize the participation of users with low endowments. A revenue-neutral scheme that accomplishes this is to impose a transaction fee proportional to each user's transaction gain and then equally redistribute the collected transaction fees back to the users. As users with high endowments have greater gains from transactions and therefore pay larger fees, the redistribution of the fees provides a cross-subsidy from users with high endowments to those with low endowments. A sufficiently high transaction fee can consequently ensure full user participation. With this benchmark in mind, we will examine several more practical schemes in the following sections.

2 The Equity-Based Scheme

We first examine the conventional equity-based scheme, which serves as a benchmark for other schemes. At $t = 0$, the developer may choose to set up a conventional equity-based scheme to fund the platform. Under this scheme, the developer issues equity, which is fully or partially sold to outside investors. The developer may also retain some of the equity shares. As it is not crucial to differentiate the heterogeneity between equity holders, we shall simply refer to them as the owner of the platform.

Owner choices The owner retains not only profit but also control of the platform. The profit motivates the owner to fully build up the platform's user base to maximize its network effect. Specifically, we allow the owner to provide an entry subsidy c (i.e., a negative entry fee) at $t = 1$ and then charge each user a fraction δ of his utility surplus $U_{i,t}$ from the transaction in each period $t = 1, 2$. We impose a cap on the entry subsidy:

$$c \geq -\alpha\kappa.$$

That is, the subsidy cannot be more than a fraction $\alpha \in (0, 1)$ of users' participation cost. As the platform has limited information about the potential users at entry, it cannot discriminate between legitimate users from the relevant pool and opportunistic individuals from outside the relevant pool, who have no intention to participate on the platform but join only to take advantage of the subsidy offered by the platform. Suppose that such opportunistic individuals incur a lower participation cost of $\alpha\kappa$. As a result, any subsidy above $\alpha\kappa$ will attract an arbitrarily large number of opportunistic individuals.

The owner's control of the platform also allows the owner to take a subverting action $s \in \{0, 1\}$ at $t = 2$. That is, if the owner chooses $s = 1$, this action benefits the owner by an amount proportional to the number of users on the platform, $\gamma \int_0^1 X_i di$, at the expense of the users. This action not only prevents any transaction on the platform, but also imposes a utility cost of $\gamma > \alpha\kappa$ on each user.[8] This action can be viewed as a wealth transfer between the owner and users. One can interpret this action as predatory behavior by the owner, such as the sale of user data to third parties that exploit vulnerable consumers susceptible to temptation goods (Liu, Sockin and Xiong (2020)).

[8] It is convenient, although not essential, to assume the platform collapses for users at date 2. What is needed is that the cost to users, γ, is sufficiently high.

The owner consequently chooses its fees at $t = 1$ to maximize its total expected profit:

$$\Pi^E = \sup_{\{c,\delta,s\}} E\left[\int_0^1 (c + \delta U_{i,1}) X_i di + \int_0^1 ((1-s)\,\delta U_{i,2} + s\gamma) X_i di \mid \mathcal{I}_1\right], \tag{4}$$

where $\mathcal{I}_1 = \{A\}$ is the owner's information set at $t = 1$. For simplicity, we constrain the owner to set the same entry fee c and transaction fee δ for all users, based only on the overall strength of the platform A, which is observed at $t = 1$.[9] The owner chooses its subversive action $s \in \{0, 1\}$ at $t = 2$ to maximize its profit:

$$s = \arg\max \int_0^1 (\delta U_{i,1} (1-s) + \gamma s) X_i di. \tag{5}$$

As the owner's profit is purely driven by the platform fundamental A, the owner's subversive action is also determined by A.

Anticipating the owner's subversive action for certain values of A, potential users are more reluctant to join the platform in this situation. As a result, the owner may prefer to commit to not subverting at $t = 1$ to maximize the user base. Such commitment, however, is not credible under the equity-based scheme. Even if the owner initially declares its commitment in the platform's charter at $t = 1$, nothing prevents the owner from changing the charter at $t = 2$, just as platforms regularly update their service agreements with users. As we will discuss later, a token-based scheme may allow the platform to commit to not take the subversive action if it assigns control of the platform to the users themselves.

User participation At $t = 1$, each user decides whether to join the platform. We assume that users have quasi-linear expected utility and incur a linear utility gain equal to the total fixed cost of participation $c + \kappa$ if they choose to join the platform at $t = 1$. Furthermore, each user needs to pay a fraction δ of his utility surplus $U_{i,t}$ from any transaction in each period as a variable fee to the platform and may suffer a loss of γ if the owner chooses the subversive action at $t = 2$. In summary, user i makes his participation decision according to

$$\max_{X_i \in \{0,1\}} E\left[(1-\delta)(U_{i,1} + (1-s) U_{i,2}) - \kappa - c - \gamma s \mid \mathcal{I}_i\right] X_i, \tag{6}$$

where $\mathcal{I}_i = \{A, A_i\}$ is the information set of user i at $t = 1$. Note that the expectation of the user's utility flow is with respect to the uncertainty associated with matching a transaction

[9] The platform may be able to impose transaction fees that are dependent on each user's transaction need. This flexibility allows the owner to extract more fees from the users, which, in turn, gives the owner an even greater incentive to subsidize user participation. As the owner already chooses the maximum subsidy in our current setting, however, this flexibility does not affect our qualitative comparison of the token-based and equity-based schemes. We prefer our conservative setting for its simplicity.

partner. By adopting a Cobb-Douglas utility function with quasi-linearity in wealth, users are risk neutral with respect to this uncertainty.

It then follows that user i's participation decision is given by

$$X_i = \begin{cases} 1 & \text{if } \; E\left[(1-\delta)\left(U_{i,1} + (1-s)\,U_{i,2}\right) - \kappa - c - \gamma s \mid \mathcal{I}_i\right] \geq 0 \\ 0 & \text{if } \; E\left[(1-\delta)\left(U_{i,1} + (1-s)\,U_{i,2}\right) - \kappa - c - \gamma s \mid \mathcal{I}_i\right] < 0 \end{cases} . \tag{7}$$

As the user's expected utility is monotonically increasing with his own endowment, regardless of other users' strategies, it is optimal for each user to use a cutoff strategy. This, in turn, leads to a cutoff equilibrium, in which only users with endowments above a critical level, $\hat{A}^E$, participate in the platform. This cutoff is eventually solved as a fixed point in the equilibrium to equate the fixed participation cost to the expected transaction utility of the marginal user from joining the platform. Given all users join the platform for whom $A_i \geq \hat{A}^E$, a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\left(A - \hat{A}^E\right)\right)$ of potential users join the platform.

Equilibrium Our model features a rational expectations cutoff equilibrium, which requires the following rational behavior of each user and the owner:

- Owner optimization: The owner chooses a two-part fee structure (c, δ) at $t = 1$ to maximize (4) and chooses its subversive action at $t = 2$ to maximize (5).
- User optimization: Each user chooses X_i at $t = 1$ to solve his maximization problem in (6) for whether to join the platform.

Proposition 2 summarizes the equilibrium under the equity-based scheme.

Proposition 2 *Under the equity-based funding scheme, there is a unique cutoff equilibrium with the following properties:*

1. *If $A > A_*^E$, where the threshold A_*^E is given by (31), the owner does not subvert the platform at $t = 2$, which in turn leads to the following outcomes at $t = 1$:*
   - *(a) The owner provides the maximum entry subsidy, $c = -\alpha\kappa$;*
   - *(b) The owner sets the transaction fee δ given by (28);*
   - *(c) Each user i adopts a cutoff strategy to join the platform if A_i is higher than $\hat{A}_{NS}^E$, where $\hat{A}_{NS}^E$ is decreasing in A and is the smaller root of (30).*

2. *If $A \in \left[A_{**}^{E}, A_{*}^{E}\right]$, where A_{**}^{E} is given by (33), the owner subverts the platform at $t = 2$, which leads to the following outcomes at $t = 1$:*

   (a) *The owner provides the maximum entry subsidy, $c = -\alpha\kappa$;*

   (b) *The owner sets the transaction fee δ given by (29);*

   (c) *Each user i follows a cutoff strategy to join the platform with the cutoff $\hat{A}_{SV}^{E}$, which is decreasing in A and is the smaller root of (32).*

3. *If $A < A_{**}^{E}$, the platform breaks down with no user participation at $t = 1$.*

Based on the realization of the demand fundamental A, there are three regions: 1) an equilibrium without subversion when A is higher than A_{*}^{E}; 2) an equilibrium with subversion when A is in an intermediate range $\left[A_{**}^{E}, A_{*}^{E}\right]$; and 3) the platform breaks down with no user participation if A is lower than A_{**}^{E}.

As more users join the platform, the greater user base on the platform creates more opportunities for each user to match with another user, which, in turn, generates more transaction fees for the owner. The equity cash flows give the owner the incentive to internalize the network effect and to subsidize the entry fee to maximize user participation. The owner therefore always chooses the maximum entry subsidy, $c = -\alpha\kappa$, to attract the marginal user. This is a key advantage of the conventional equity-based scheme. Nevertheless, the cap on the entry subsidy constrains user participation from reaching the first-best level shown in Proposition 1.

The equity ownership in the platform, however, also creates another problem—the owner may choose to exploit its control power by subverting the platform if the transaction fees are sufficiently low. That is, if the platform fundamental A is lower than a threshold A_{*}^{E}, the owner chooses the subversive action at $t = 2$, as described by the second case in Proposition 2. Anticipating the subversion and the resulting damage to the users, potential users are reluctant to join the platform at $t = 1$. Their reluctance forces the owner to reduce the transaction fee, and, despite the reduced fee, platform participation by the users is still lower than the level in the absence of the subversion. The following proposition establishes this effect induced by the owner's lack of commitment.

Proposition 3 *Under the equity-based scheme, when the subversion equilibrium occurs, that is, $A \in \left[A_{**}^{E}, A_{*}^{E}\right]$, user participation, owner profit, and social surplus all decrease with the degree of user abuse γ, while the boundary of platform breakdown A_{**}^{E} increases with γ.*

Proposition 3 illustrates that, in the absence of commitment, as γ grows, user participation, owner profit, and social surplus are all lower, and breakdown is more likely to occur. As such, subversion has a negative impact on the performance of the equity-based scheme. Essentially, the subversion induces another participation cost to users that increases with γ. The intuition for why subsidizing entry is optimal is therefore also the intuition for why owner profit is decreasing in γ. Because the total transaction surplus is greater than the product of the marginal surplus and the size of the user base due to the network effect, there are increasing returns to providing an entry subsidy, or, equivalently, decreasing returns to increasing participation costs. This proposition consequently highlights that, in the presence of the network effect, the lack of commitment is particularly damaging to platforms with relatively weak fundamentals.

3 Utility Tokens

The lack of commitment by the platform owner under the conventional equity-based scheme motivates decentralizing the platform as a DAO through tokenization. By giving control to users, tokenization enables users as a whole to protect themselves from non-users who would take the subversive action. We first consider a baseline token-based scheme motivated by utility tokens that are prevalent in practice. Specifically, this token-based scheme allows the developer to cash out by selling tokens to users at $t = 1$ and, furthermore, delegates the operations of the platform to pre-coded algorithms, which can be changed only by approval of the token holders. Under this scheme, a user needs to purchase a token to join the platform.[10] By acquiring a token at $t = 1$, a user obtains not only the privilege of transacting goods with other users on the platform but also the right to vote on issues related to the platform at $t = \{1, 2\}$. Consequently, a utility token conveys control rights to holders, but does not

[10] This assumption is consistent with the common practice on many utility token platforms that a user needs to hold tokens in his wallet to complete any bilateral transaction. There are, however, several subtle issues related to this assumption. First, a user may wait to buy a token until immediately before completing a transaction, assuming that market liquidity permits such a timely purchase. As all matched users need to make their transactions at the same time, each has to hold one token at the time of transaction. It follows that requiring each user to hold one token at the time of transaction, instead of when joining the platform, would lead to a quantitatively lower aggregate demand for the token, but would not qualitatively change the key insights of our model. Second, as each user has the need to make one transaction in each period in our model, no one would choose to purchase more than one token; as a result, those who join the platform would each buy one token. Finally, in practice, a user may need to make more than one transaction in a period and thus must hold more than one token. Allowing users to have different quantities of transaction needs again may quantitatively change the users' aggregate demand for the token, but not the qualitative implications of our analysis.

bestow cash flow rights to the platform's profits like equity. We assume that a majority is needed to pass any decision among the token holders and that this can be accomplished without conflicts among users. As the token holders would never agree to take the subversive action against themselves, this token-based scheme allows the platform to commit to not taking the subversive action.

This utility token-based scheme captures the notion of decentralization, which underlies many decentralized crypto-based platforms, such as Filecoin, Tezos, and Decred.[11] Decentralization leads not only to the commitment of not exploiting users but also to the absence of an owner with a stake in the platform's profit who has incentive to subsidize user participation. To the contrary, the marginal user under the token-based scheme needs to pay for the token at entry, in addition to the private participation cost. The lack of entry subsidy implies that the token-based scheme cannot accomplish the full user participation required by the first-best equilibrium. Instead, the token-based scheme serves as a compromise for platforms to pre-commit to not exploiting users.

It is important to note that in the absence of cash flow rights, there is no incentive for a non-user to acquire utility tokens in our setting. In a dynamic setting, speculative motives (i.e., expectation of future price appreciation) may also attract some non-users to hold utility tokens. Nevertheless, the convenience from using the platform's services is the main motive for holding utility tokens.[12] The simplicity of the utility token-based scheme makes it particularly appealing for highlighting the aforementioned trade-off introduced by

[11] While we focus on the archetypal utility token scheme, varying degrees of decentralization and tokenization exist in practice. CoinCheckup.com, for instance, classifies the governance structures of blockchain-based platforms into four categories, centralized-hierarchical, centralized-flat, semi-centralized, and decentralized, based on the extent to which a platform is governed by its community versus sponsoring organizations or key individuals. Such differences in governance structure have a material impact on a platform's performace as Chen, Pereira and Patel (2020), using this classification system, finds a U-shaped relation between the extent of a platform's decentralization and its market capitalization.

[12] In an earlier version, we examined a dynamic setting that allowed the retrading of tokens, as in Cong, Li and Wang (2021). Under rational expectations, although token price appreciation provides an additional source of return to owning tokens, it only defrays part of the effective cost of joining the platform. Therefore, even with retrade value, a buyer must still pay the token price and only recoups part of this investment through expected token price appreciation. Our key insight that tokenization leads to undersubsidization of the platform therefore remains valid even when the tokens have retrade value.

The issue becomes more nuanced when buyers have heterogeneous beliefs about future token price appreciation. Realistic short-sales constraints bias token buyers to be more optimistic, which may drive less optimistic users off the platform. Beyond hampering full user participation (i.e., the first-best outcome), optimistic token buyers may be non-users who treat tokens as an investment. As we discuss in Section 4 when tokens pay cash flows to holders, non-users induced by the cash flows to buy the tokens may re-create the commitment problem because they have divergent interests from users. This insight also applies when optimistic beliefs rather than cash flow payouts induce non-users to invest in the tokens.

decentralization. We will also examine a hybrid scheme that allows the platform to collect fees and pay out dividends to token holders in Section 4 and analyze issues introduced by implementing a consensus protocol in Section 5. In these alternative settings, cash flow rights may lead non-users, such as token investors and validators, to take control of the platform, which reintroduces the commitment problem.

Developer choice Under the token-based scheme, the developer has a simple choice at $t = 1$ of setting the token price P to maximize his revenue from the token issuance

$$\Pi^T = \max_P \int_0^1 P X_i \left(\mathcal{I}_i\right) di,$$

where the token price P adversely affects each user's decision to join the platform. The developer therefore faces a trade-off between a higher token price and a smaller user base.

User participation Similar to the equity-based scheme, each user chooses at $t = 1$ whether to join the platform by evaluating whether his expected transaction surplus with another matched user on the platform is sufficient to cover the costs of participation, which is now the fixed cost and the purchase of a token

$$\max_{X_i \in \{0,1\}} E\left[U_{i,1} + U_{i,2} - \kappa - P \mid \mathcal{I}_i\right] X_i.$$

Under the utility token-based scheme, a user does not face any subversion risk or transaction fees but needs to pay the token cost at entry.

Equilibrium The equilibrium under the utility token-based scheme is similarly defined as before, with the developer maximizing his revenue and each user making his optimal participation decision. We summarize the equilibrium in the following proposition.

Proposition 4 *Under the utility token-based funding scheme, the platform breaks down with no user participation if $A < A^T_{**}$, where A^T_{**} is given by (36), and there is a cutoff equilibrium with the following properties if $A \geq A^T_{**}$:*

1. *Each user i adopts a cutoff strategy in purchasing the token to join the platform*

$$X_i = \begin{cases} 1 & \text{if } \; A_i \geq \hat{A}^T \\ 0 & \text{if } \; A_i < \hat{A}^T \end{cases},$$

where $\hat{A}^T$ is given by the smaller root of (35).

2. *The token price P is given by*

$$P = e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z^T + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^T\right) - \kappa, \tag{8}$$

   where $z^T = \sqrt{\tau_\varepsilon}\left(\hat{A}^T - A\right)$.

As the decentralization instituted by the utility token-based scheme prevents the platform from taking the subversive action at $t = 2$, Proposition 4 confirms that there is no subversion equilibrium. Instead, there is a no-subversion equilibrium if the platform fundamental A is above an equilibrium cutoff A_{**}^T, below which the platform breaks down.

The token price P in (8) is determined by the willingness of the marginal user to participate in the platform. In contrast, the equity price under the equity-based scheme is determined by the transaction fee collected from the average user, who, by the nature of the network effect, benefits more from participation in the platform than the marginal user. This contrast has several important implications. First, token issuance is a less effective funding channel than equity issuance. Second, token prices have different determinants from equity prices and are particularly volatile because of the network effect of the platform.[13]

The following proposition compares performance of the token-based scheme along several dimensions to that of the equity-based scheme.

Proposition 5 *Compared to the equity-based scheme:*

1. *For a given level of γ, the utility token-based scheme leads to lower user participation, developer profit, and social surplus if the platform fundamental A is sufficiently high;*

2. *For a given level of A, the utility token-based scheme leads to higher user participation, developer profit, and social surplus if the degree of user abuse γ is sufficiently high.*

Proposition 5 reflects the trade-off induced by the decentralization of the utility token-based scheme. On one hand, the decentralization allows the platform to commit to not exploiting users. On the other hand, the decentralization also leads to the absence of any owner with the incentive to subsidize user participation and thus to maximize the network effect. The benefit of the decentralization is greater when the concern about the platform's

[13] We examine the dynamic properties of token prices, which are determined by the willingness of the marginal user to pay, in Sockin and Xiong (2020). These properties help explain patterns in token return predictability documented extensively by Liu and Tsyvinski (2019), Liu, Tsyvinski and Wu (2019), Hu, Parlour and Rajan (2018), Li and Yi (2018), and Shams (2019).

exploitation of users, as measured by the model parameter γ, is sufficiently high. In contrast, the benefit from having an owner to subsidize user participation and maximize the network effect is greater when the platform's fundamental is sufficiently strong and the concern about the platform's commitment problem is not severe.

Relating our model to DAOs, the importance of decentralization to DAO participants is evidenced by the explicit discussion of their governance structures in their advertising material and on their websites. Decred and MakerDAO, for instance, describe in great detail how token holders can engage in community discussions on recent proposals and vote on their implementation. The importance of subsidizing user participation to maximize the platform's network effect (e.g., Rochet and Tirole (2006)), however, makes tokenization particularly costly for DAOs. As there is no owner, such platforms often resort to seignorage to provide subsidies. Seignorage acts as a transfer from existing token holders through token inflation. Bitcoin, for instance, provided sizable block rewards that declined over time according to a predetermined schedule to foster early adoption by Proof of Work validators. ShapeShift engages in random "Rainfall" airdrops of FOX tokens to reward users for holding tokens and provides trading rebates. Such subsidization schemes are imperfect compared to the free or discounted services offered by centralized platforms such as Amazon and Google. In the next section, we examine a more direct scheme of subsidizing token holders through cash flows.

Choice between equity and utility tokens At $t = 0$, the developer chooses either the equity- or utility token-based scheme to fund the platform before the platform fundamental A becomes publicly observable at $t = 1$. Instead, the developer makes this choice based on his prior belief distribution about A, parameterized by the cumulative distribution function (CDF) $G(A)$. Given the trade-off introduced by the utility token-based scheme relative to the equity-based scheme, it is intuitive that the developer chooses the former when his prior is that A is weak, as formally established by the following proposition.

Proposition 6 *Consider two prior distributions about the platform fundamental, G and $\tilde{G}$, such that $G > \tilde{G}$ (in the sense of first-order stochastic dominance). Then, if the developer adopts the utility token-based scheme under G, it also adopts it under $\tilde{G}$, and the set of priors for which the developer chooses the utility token-based scheme is (weakly) increasing in γ. In the special case of a normal prior, $G\left(A\right) \sim \mathcal{N}\left(\bar{A}_G, \tau_A\right)$, the developer chooses the* *equity-based scheme if $\bar{A}_G \geq \bar{A}^c(\gamma)$ and the utility token-based scheme otherwise.*

Proposition 6 shows a sharp implication that the utility token-based scheme is more likely to be adopted by platforms with relatively weak fundamentals. The more weight that the developer's prior puts on lower realizations of the platform fundamental, the more likely it is to adopt the utility token-based scheme. This implication is consistent with the casual observation that many of the tokenized platforms in recent years tend to be in earlier stages than other traditional equity-based platforms.

What underlies Proposition 6 is a stark difference between the equity and the token price. In the absence of any subversion by the owner of the platform (as is the case in which A is sufficiently strong), the equity price under the equity-based scheme is determined by the aggregate transaction fees collected from all users of the platform. While the transaction surplus is heterogeneous across the pool of users, aggregate transaction fees are determined by the size of the user pool multiplied by the proportional fee collected from the average user. That is, the equity price is ultimately determined by the transaction surplus of the average user on the platform. In contrast, the token price under the utility token-based scheme is determined by the indifference condition of the platform's marginal user so that the token price is equal to the marginal user's transaction surplus. In the presence of the network effect, the transaction surplus of the marginal user is lower than that of the average user. This nature of the token price in the utility token-based scheme makes it less appealing for the developer to raise funding for the platform unless concerns about subversion are sufficiently severe; when such concerns are severe, however, the platform's profit is higher and breakdown occurs for a lower critical level of the fundamental under the utility token-based scheme.

The key prediction of Proposition 6 is that tokenization is appealing for platforms that have relatively weak fundamentals. Consistent with this observation, Howell et al. (2020), Benedetti and Kostovetsky (2018), and Fisch (2019) document skewed distributions for ICO proceeds in which relatively few ICOs have outsized successes while a significant number fail or raise only modest sums. Benedetti and Kostovetsky (2018) find similar evidence of such skewness when examining token returns prior to secondary market trading on an exchange.[14] One may also test our prediction more directly if one can measure the demand fundamental,

[14] Admittedly, fear of regulation and potential oversight by the SEC may have impacted the funding decision of entrepreneurs between equity and token financing during this period. While this may have dissuaded some entrepreneurs from issuing tokens, it is not clear that this would impact stronger or weaker projects differentially. In addition, such concerns are less likely to be relevant going forward as the cryptocurrency community continues to establish best practices for transparency of ICOs.

A, of a tokenized platform. Our theory suggests that total transaction fees, which are based on the average convenience yield of users, represent a reliable proxy. Given that many crypto token holders may own them to speculate rather than to use them, measuring platform performance by the number of users or unique wallets may be misleading.

4 Equity Tokens

Although the utility token-based scheme gives control of the platform to its users, it does not collect any transaction fees that could be used to cross-subsidize the participation of marginal users with the fees collected from heavy users. This additional cost of decentralization motivates hybrid schemes that combine features of equity and utility tokens. In this section, we consider such a hybrid scheme, which allows the platform to collect transaction fees from users and pay out the fees to token holders as dividends. A token therefore entitles its holder not only to the transaction service on the platform but also cash flow from the platform, which is typically associated with equity. Even though this hybrid scheme does not fall into our canonical definition of tokens, for ease of exposition we call this scheme equity tokens. It should be clear that this equity token-based scheme entails a more general contract space than the utility token-based scheme analyzed in the previous section.

The cash flows from the equity tokens provide a channel to subsidize marginal users. Such cash flows, however, may also incentivize non-users to acquire equity tokens as a financial investment. Given these two potential effects, we will examine how the equity token-based scheme may affect the platform in two steps. First, we analyze the case in which the owner issues equity tokens to users without the presence of any investors, who may acquire the tokens for investment motives. Interestingly, by cross-subsidizing marginal users, the equity token-based scheme is able to achieve the first-best outcome and allows the owner to extract the full transaction surplus through token sales. Next, we analyze another case in which the cash flows of equity tokens attract investors without any transaction need to acquire the tokens. Interestingly, the presence of investors re-creates the commitment problem as investors may choose to take the subversive action at the expense of users.

4.1 The Case Without Investors

Specifically, at $t = 1$, the developer of the platform issues equity tokens to users at a price of P and may also retain a stake of N tokens at a proportional cost, χN, which can be viewed as an opportunity cost with $\chi > 0$. The developer sets a transaction fee at $t = 0$, $\delta_T \geq 0$, to maximize its profits. That is, the developer maximizes its profits by setting a transaction fee rate δ_T, a token price P, and a retention policy of N tokens:

$$\Pi^{ET} = \max_{\delta_T, P, N} \int_0^1 P X_i(\mathcal{I}_i)\, di + \frac{N}{N + \int_0^1 X_i(\mathcal{I}_i)\, di} \int_0^1 \left(\delta_T U_{i,1} + (1-s)\, \delta_T U_{i,2} + s\gamma\right) X_i(\mathcal{I}_i)\, di - \chi N. \tag{9}$$

At $t = 2$, the token holders may vote by majority whether to revise the transaction fee and whether to take the subversive action to sell user data to third parties.

Interestingly, this equity token-based scheme is able to achieve the first-best outcome. The key mechanism is that the payout from the equity token can serve as a transfer from high-endowment users to low-endowment users, thus subsidizing the participation of low-endowment users, similar to the revenue-neutral scheme outlined in Proposition 1. Specifically, at $t = 1$ the developer chooses to set a transaction fee of 100% on the platform, and then at $t = 2$ it is also in the interest of most users to continue this transaction fee. A stark assumption of our setting is that the platform is unique in providing the matching service to users. As a result, even high-endowment users are willing to accept the high transaction fee to participate on the platform.[15] Through this transaction fee, the platform collects all the transaction surplus and redistributes the surplus among all users. As low-endowment users receive more in the token payout than they pay in transaction fees, this transfer helps to overcome the constraint imposed by the cap on the entry subsidy under the equity-based scheme.

This equity token-based scheme is able to achieve the first-best equilibrium outlined by Proposition 1: if the platform fundamental is higher than A_*^{FB}, there is full user participation on the platform and the developer is also able to extract the full transaction surplus through the token sale. If the platform fundamental is below the threshold, the platform breaks down as it does not lead to any social surplus. Proposition 7 summarizes the equilibrium in detail.

Proposition 7 *Under the equity token-based funding scheme, there is an unique equilibrium with the following properties:*

1. *If $A \geq A_*^{FB}$, where the threshold A_*^{FB} is given in Proposition 1, the platform achieves*

[15] It should be clear that relaxing this assumption would lead to a lower transaction fee and thus a smaller transfer from high-endowment users to low-endowment users. Nevertheless, the transfer helps to subsidize the participation of low-endowment users on the platform.

the first-best outcome with the developer earning the first-best social surplus as its revenue:

a. *At $t = 1$, the developer sets the token price as*

$$P = e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\epsilon^{-1}} - \kappa,$$

which is equal to the first-best social surplus, takes zero stake in the platform, $N = 0$, and sets the transaction fee $\delta_T = 100\%$;

b. *All users join the platform at $t = 1$;*

c. *At $t = 2$, the users maintain the transaction fee $\delta_T = 100\%$ by majority vote and will never choose the subversive action.*

2. If $A < A_*^{FB}$, the platform breaks down with no user participation at $t = 1$.

In the equilibrium described by Proposition 7, the developer pre-commits to not subverting the platform by not retaining any tokens; as such, it has no ability to subvert the platform at $t = 2$. In this setting, the lack of retention by developers represents a commitment device rather than a signal of moral hazard or the project's quality. Our analysis thus suggests that in the absence of investors, equity tokens can not only improve on traditional equity financing but also achieve the first-best outcome on the platform.

4.2 The Case With Investors

Until now, we have ignored an important issue that selling equity tokens that pay cash flows introduces, similar to equity, the incentive for non-users to acquire equity tokens as an investment. In contrast, there is no incentive to hoard utility tokens because they provide only transaction benefit and only one token is needed to participate on the platform. The presence of non-users to acquire a sufficient quantity of equity tokens may recreate the commitment problem, albeit through a modified form.

To illustrate this, we suppose that there is a large, risk-neutral outside investor who has no transaction benefit from the platform and can buy equity tokens to collect their dividends; as the investor does not use the platform, it does not incur the participation cost κ.[16] Thus,

[16] Although it is convenient for our analysis to assume that the investor is large, such an assumption is not necessary. Our key insight that the presence of investors reintroduces the commitment problem that utility tokens help to alleviate would remain valid even with a continuum of competitive investors.

at $t = 1$, the investor acquires n tokens to maximize

$$\Pi^I = \max_{n \geq 0} \frac{n}{n + N + \int_0^1 X_i(\mathcal{I}_i)\, di} \int_0^1 \left(\delta_T U_{i,1} + (1 - s_I)\,\delta_T U_{i,2} + s_I \gamma\right) X_i(\mathcal{I}_i)\, di - nP, \quad (10)$$

by taking as given the token price P, the transaction fee δ_T, and developer stake N, which are all chosen by the developer. Note that $\int_0^1 X_i(\mathcal{I}_i)\, di = \Phi\left(-z_I^{ET}\right)$ is the size of the user base. The token price P must be lower than the token's cash flows in order to subsidize the marginal user's participation cost. Thus, there is a positive gain for the investor to acquire the token. Furthermore, as $n/\left(n + N + \Phi\left(-z_I^{ET}\right)\right)$ is increasing and concave in n, the optimization program of the investor in (10) is concave in n.

At $t = 2$, the investor may vote to take a subversive action $s_I \in \{0, 1\}$ to sell user data to third parties if its share is sufficiently large. Such a decentralized governance mechanism of voting based on (staked) token holdings is consistent with current schemes implemented in practice, including those on MakerDao and Kyber. If it votes to sell user data, $s_I = 1$, the subversive action expropriates γ in value from each user at the cost of preventing all transactions on the platform at $t = 2$; as the investor does not use the platform for transactions, it is not harmed by this action. This revenue of γ is paid out as dividends to all token holders in lieu of transaction fees at $t = 2$. Because users lose their transaction benefit and recapture only a fraction of the revenue in dividends, they strictly lose from the sale of their data and thus will always vote against the subversive action.

Specifically, at $t = 2$, the investor receives a fraction $n/\left(n + N + \Phi\left(-z_I^{ET}\right)\right)$ of the platform's dividend, which is $\frac{1}{2}\delta_T U$, where U is the total transaction surplus, if it does not subvert the platform and $\gamma\Phi\left(-z_I^{ET}\right)$ if it does. It is therefore straightforward to see that the investor will want to subvert the platform if

$$\gamma\Phi\left(-z_I^{ET}\right) > \frac{1}{2}\delta_T U. \quad (11)$$

Thus, the presence of the investor may re-create the commitment problem.

The developer again maximizes its profit

$$\Pi_I^{ET} = \max_{P, \delta_T, N} P\left(n + \Phi\left(-z_I^{ET}\right)\right) + N \frac{\int_0^1 \left(\delta_T U_{i,1} + (1 - s_I)\,\delta_T U_{i,2} + s_I \gamma\right) X_i(\mathcal{I}_i)\, di}{N + n + \int_0^1 X_i(\mathcal{I}_i)\, di} - \chi N, \quad (12)$$

by taking the investor's stake n and subversion policy s_I as given. Like the equilibrium described in Proposition 7, we can show that the developer will not retain any tokens, that is $N = 0$. As a result, the investor will need a majority share of the tokens to vote against the users to subvert the platform.

For convenience, we express the token price as

$$P \equiv \frac{\frac{1}{2}\delta_T U + (1-s_I)\frac{1}{2}\delta_T U + s_I\gamma\Phi\left(-z_I^{ET}\right)}{n + N + \Phi\left(-z_I^{ET}\right)} - s_I\gamma + p_I^{ET},$$

which is the sum of the dividends paid by the token, the subversion cost imposed on the user, and a piece p_I^{ET}, which represents a price discount or premium for the marginal user. As the marginal user is indifferent between acquiring or not acquiring the token, p_I^{ET} is equal to the net of his expected transaction benefit and participation cost. In choosing the token price P to maximize its profit in (12), the developer needs to set a price discount $p_I^{ET} < 0$ to maximize user participation.

The developer, however, cannot distinguish the investor from users when selling tokens at $t = 1$. As a result, the investor may take a stake, which in turn diverts the subsidy away from platform users and thus harms user participation. Furthermore, the investor may even be incentivized to take a majority stake that gives it control of the platform. When this happens, the investor becomes the effective owner of the platform at $t = 2$ and would choose to take the subversive action if the condition in (11) is satisfied. Proposition 8 shows that this would happen when the platform fundamental, A, is sufficiently weak.

Proposition 8 *Under the equity token-based funding scheme with a large investor, there is an equilibrium with the following properties:*

1. *At $t = 1$, the developer retains zero tokens, $N = 0$, and sets the optimal transaction fee δ_T and token subsidy p_I^{ET} to satisfy (49) and (48), respectively;*

2. *The investor's optimal stake n is given by*

$$\frac{n}{\Phi\left(-z_I^{ET}\right)} = \sqrt{\frac{\frac{1}{2}\delta_T U + (1-s_I)\frac{1}{2}\delta_T U + s_I\gamma\Phi\left(-z_I^{ET}\right)}{P\Phi\left(-z_I^{ET}\right)}} - 1; \tag{13}$$

3. *The investor acquires a majority share of tokens and subverts the platform when the platform fundamental, A, is sufficiently weak;*

4. *The developer's profit, the token price, and user participation are lower than in the absence of the investor.*

Proposition 8 shows that while allowing for equity tokens to pay dividends can achieve the first-best outcome when only the developer and platform users are involved, the cash flows from equity tokens provide an incentive for an outside investor to buy tokens as an investment. Consequently, the commitment problem reappears. Specifically, when the platform fundamental is sufficiently weak, the investor takes a majority stake and chooses to subvert the platform.

Interestingly, the developer has incentive to pre-commit by not retaining tokens because subversion destroys its profit by lowering the token price and transaction fees. However, the lower token price induced by anticipation of subversion may reinforce the commitment problem of the investor because subversion reduces user participation and makes it even cheaper for the investor to acquire a majority stake of tokens.

Taken together, although allowing equity tokens to collect transaction fees helps to resolve the lack of subsidy of user participation, it re-creates the commitment problem by attracting token investors to take control of the platform in some states of the world. This outcome consequently highlights that the removal of cash flow rights from utility tokens is an important feature that ensures that users, and not outside stakeholders such as equity holders and equity-token investors whose presence would ultimately give rise to the commitment problem, control the platform.

The key shortcoming of equity tokens is that the platform's developer and pre-coded governance algorithms cannot distinguish between which token holders are users and which are investors. Governance protocols that weight user preferences by their (staked) holdings may be ineffective at resolving this issue because tokens also represent a speculative investment; as such, a token holder's stake need not correlate with his usage of the platform. A governance (and potentially consensus validation) mechanism that weighs stakeholders by their participation on the platform, i.e., Proof of Use, however, may be able to simultaneously accomplish subsidization of user participation with equity tokens while safeguarding users through decentralization. Because users are dispersed and can have multiple accounts or wallets, while investors can feign platform activity, overcoming such a severe asymmetric information problem would likely require either collecting vast amounts of token holder data or a sophisticated incentive compatible design of how to measure participation. Our analysis suggests that the fees paid by users to use the platform's services, which are relatively more costly for non-users to feign, may be an input to such a scheme, while also cautioning against the common practice of weighting stakeholders by their (staked) holdings, as is done on MakerDAO and Kyber.

5 Consensus Record Keeping

While we have assumed frictionless record keeping on the decentralized token platform in our analysis so far, tokenization in practice requires a consensus protocol to maintain the platform's blockchain. Implementation of such consensus protocol requires giving cash flow rights to a group of non-users as an incentive to validate transactions and defend the platform's security. Prominent examples of such protocols include Proof of Work, in which miners solve complex computational puzzles to add blocks to the blockchain in exchange for transaction fees and seignorage, and (delegated) Proof of Stake, in which stakers are randomly selected to add blocks based on their staked holdings in exchange for transaction fees. While such protocols have been implemented successfully in practice, they also introduce novel frictions that are absent on conventional platforms.[17] In this section, we highlight how such consensus protocols, by allocating cash flow rights and control rights to outside validators, may reintroduce issues of commitment.

We assume that the platform operates as in the baseline utility token setting, as outlined in Section 3, with users completing transactions at both dates and the developer selling tokens at $t = 1$. Users again self-select onto the platform based on a cutoff rule, joining if $A_i \geq \hat{A}_{TC}$, with $\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TC}\right)\right)$ users joining at $t = 1$. Now, however, transactions at each date must be completed by validators who charge transaction fees to maximize their revenue.

There is a pool of potential validators that each have a fixed cost of becoming a validator $\eta \geq 0$. Validator j records transactions on the platform's blockchain in exchange for transaction fees at date t, $\delta_{T,j}\frac{1}{2}U\left(\hat{A}_{TC}\right)$, where $\delta_{T,j}$ is set by each validator and $\frac{1}{2}U\left(\hat{A}_{TC}\right)$ is the total transaction surplus for the period given that users follow a cutoff policy with cutoff endowment $\hat{A}_{TC}$.[18] In addition to setting the transaction fee, validators compete for

[17] With Proof of Work, for instance, miners may have incentive to strategically attack the blockchain (e.g., Chiu and Koeppl (2017), Budish (2018), Pagnotta (2020)) or fork the blockchain (e.g., Biais et al. (2019), Saleh (2020)), and there are potential economic limits to the scope of its adoption because of congestion (e.g., Huberman et al. (2018), Easley, O'Hara and Basu (2019), Hinzen, Kose and Saleh (2020)) that have led to the use of off-chain transaction schemes (e.g., Bertucci (2020)). Furthermore, seignorage on the platform to pay miners acts as an inflation tax borne by users and other miners. As a permissioned blockchain, Proof of Stake suffers less from issues of security (e.g., Fanti, Kogan and Viswanath (2019b), Kose, Rivera and Saleh (2020)), but confronts concerns of scalability through the concentration of stake holdings via "richer gets richer" dynamics (e.g., Fanti, Kogan and Viswanath (2019a), Rosu and Saleh (2020)) and through delegation (e.g., Catalini, Jagadeesan and Kominers (2020)). Biais et al. (2018) develop a structural model of cryptocurrency pricing with transactional benefits and costs from hacking and estimate it with data on Bitcoin.

[18] In practice, record keepers choose which potential transactions to add to the next block based on the

transactions by exerting effort e_j at a linear proportional cost ξ. Their likelihood of completing transactions is given by their relative supply of effort $e_j / \left(e_j + \sum_{j' \neq j} e_{j'}\right)$. A validator that joins the platform decides its transaction fee and effort level at $t = 1$. As in practice, validators are decentralized and anonymous, and cannot collude. If no validators participate, the platform fails.

After paying the fixed cost to join the platform, with probability $\lambda \in (0, 1)$ one of the validators is randomly selected (with equal probability) to be a rogue validator.[19] Instead of validating any transactions, this rogue validator can prepare an attack on the platform's blockchain at $t = 1$ to expropriate a value of γ from each user and thus a total of $\gamma \Phi \left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TC}\right)\right)$ from all users at $t = 2$; if it does not attack, it participates in validating transactions on both dates with the other validators. The attack succeeds if the rogue validator at $t = 2$ supplies more effort than the other validators (i.e., at least $\sum_{j' \neq j} e_{j'}$), and, for simplicity, also destroys all transactions on the platform at $t = 2$. Such an attack, which is often called a "51% attack," could, for instance, be a "double spending" attack in which a validator creates false transactions and undoes legitimate ones to profit from the fraudulent behavior. It is profitable for a validator to attack if the net revenue from attacking is larger than honest validation of transactions. Users are aware whether there is a risk of a strategic attack when joining the platform.

Let M be the number of validators who join the platform in equilibrium so that users face an expected transaction fee:

$$\delta_T = \sum_{j=1}^{M} \delta_{T,j} e_j / \sum_{j'=1}^{M} e_{j'}. \tag{14}$$

Validator j solves the optimization program

$$\max \left\{ \left(1 - \lambda \frac{1}{M}\right) V_h + \lambda \frac{1}{M} V_a - \eta, 0 \right\}, \tag{15}$$

where V_h and V_a are the expected continuation values of an honest and a rogue validator,

fees proposed by the users submitting the transactions. We take a reduced-form approach to this complex auction process by assuming that the validators set the fees. We also abstract from seignorage block rewards in our static setting because there is no retrading, and consequently no retrade value, of tokens.

[19] We assume that no other validators can attack the blockchain because the payoffs to being the rogue versus an honest validator will generically differ in our static framework. In a dynamic version of our model, however, the continuation values among validators would ensure that all validators are indifferent to being the rogue or an honest validator at any point in time. For simplicity, we also ignore the possibility that several validators may form a pool, as discussed by Cong, He and Li (2018) and Lehar and Parlour (2020), to compete for transaction fees and even attack the blockchain.

respectively. In what follows, we construct a sequential Cournot-Nash equilibrium that is symmetric among honest validators.

This framework for validators is general enough to capture many of the trade-offs of two popular consensus protocols, Proof-of-Work and Proof-of-Stake. In Proof-of-Work, miners purchase specialized mining hardware and software to be able to mine cryptocurrencies. The computational power they supply to win the block reward and complete transactions from the mempool is based on how much electricity they allocate to their processors. In the context of our model, setting up a computer for mining represents the fixed cost, and the computational power and electricity costs represent the effort. Under the Proof-of-Stake protocol, a staker's stake is measured by how much cryptocurrency it has locked in an escrow account that has been inactive for a certain period of time. Stakers are assigned to complete transactions for fees based on their relative stakes, with larger stakes being awarded with more transactions. In the context of our model, the fixed cost represents the cost of setting up the necessary software and escrow account, and the effort represents the size of a validator's stake.

As our setting features strategic interaction among M large validators, there can exist many equilibria of this record keeping game. Recognizing that a comprehensive characterization of all possible equilibria is challenging and not the focus of our paper, we instead characterize two equilibria that illustrate our key conceptual insight: a "no attack" equilibrium in which there is no risk of a strategic attack, and a "mixed strategy attack" equilibrium in which the rogue and honest validators mix over a continuum of effort levels when attacking and defending the platform's blockchain, respectively. The following proposition characterizes these two equilibria.

Proposition 9 *When the platform fundamental, A, is sufficiently strong, that is, $A \geq A^*_{TC}$, there is an equilibrium with no attack and: 1) each validator chooses the same optimal transaction fee and effort:*

$$\begin{aligned}\delta_T &= -\frac{M}{\frac{\partial}{\partial \delta_T}\log U\left(\hat{A}_{TC}\left(\delta_T\right)\right)}, \\ e &= \frac{1}{\xi}\frac{M-1}{M^2}\delta_T U\left(\hat{A}_{TC}\left(\delta_T\right)\right);\end{aligned}$$

and 2) validators join the platform until $M = \max\left\{m : v_j\left(m\right) \geq \eta\right\}$, where $v_j\left(m\right)$ is given in (57). If $A \leq A^*_{TCS}$, there exists a mixed strategy attack equilibrium in which: 1) the transaction fee is

$$\delta_{TS} = -\frac{M-1}{\frac{\partial}{\partial \delta_{TS}}\log U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)};$$

and 2) the rogue validator mixes between a continuum of effort levels $e_a \in [\underline{e}_a, \bar{e}_a]$ and honest validators mix between levels $e \in [0, \bar{e}_h]$ according to the CDFs $1 - \pi_a(e_a)$ and $1 - \pi_h(e)$, respectively, as given by (68) and (71), and a strategic attack succeeds with probability

$$p_S = \frac{3}{4} \frac{\delta_{TS} U\left(\hat{A}_{TCS}(\delta_{TS})\right)}{\gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}(\delta_{TS})\right)\right)}.$$

Proposition 9 shows that across the two derived equilibria, the rogue validator has incentive to attack the blockchain when the platform fundamental, A, is relatively low. When A is low, validators earn less transaction fees and are thus less willing to exert high effort to defend the blockchain. For sufficiently low fees, they are willing to allow strategic attacks to succeed with a probability that is declining in their collective effort, which makes the platform vulnerable to an attack. To date, the cryptocurrencies that have suffered such attacks, including Feathercoin, Bitcoin Gold, ZenCash, Monacoin, and Verge (thrice), tend to have smaller market caps relative to Bitcoin, Ethereum, or Litecoin. Our analysis consequently reveals that giving control and cash flow rights to validators, as part of the tokenization scheme to decentralize the platform, can reintroduce the commitment problem because validators, such as miners and stakers, do not have their interests aligned with that of users.[20]

The impact of poor governance induced by consensus protocols on platform performance has been recognized in practice. For example, the payment platform Decred cites in its recent business brief the negative impact of user attrition from hard forks on a platform's network effect as rationale for building a strong decentralized governance system.[21] In this brief, the Decred team argues that Bitcoin is an example of a platform in which significant control has been consolidated by Proof of Work miners and its Core developers, leading to marginalization of other stakeholders, protracted disputes, and fissures in its community from hard forks. Decred has implemented a hybrid Proof of Work and Proof of Stake consensus protocol specifically to avoid centralization of the platform's governance among validators.[22]

[20] A related notion is the blockchain trilemma in Abadi and Brunnermeier (2019), which states that it is impossible for a digital record keeping system to simultaneously be resource efficient, self-sufficient, and rent-free.

[21] See the Business Brief of Decred at https://decred.org/brief/.

[22] On Decred, DCR token holders with a large enough stake vote on-chain and off-chain on changes to the platform by temporarily locking their tokens in a lottery ticketing system.

6 Conclusion

This paper develops a model to examine the decentralization of online platforms through tokenization as an innovation to resolve conflicts of interest between platforms and their users. By delegating control to users through a collection of pre-programmed smart contracts, tokenization acts as a commitment device that prevents a platform from exploiting its users. Our analysis highlights that this commitment comes at the cost of not having an owner with an equity stake who would subsidize user participation to maximize the platform's network effect. This cost is present even absent the frictions associated with implementing consensus protocols to accomplish this decentralization, although these frictions can reintroduce the conflict between users and validators. As such, decentralization through tokenization induces a fundamental trade-off between fostering commitment and subsidizing user participation. As a result, utility tokens may not always be better than equity for funding all platforms. Instead, utility tokens are more appealing for platforms with weak fundamentals because such platforms tend to have more severe concerns about user exploitation.

In addition to the archetypal utility token-based scheme, we also analyze a hybrid equity token-based scheme that allows the platform to collect transaction fees from users and pay them out to token holders as dividends. Interestingly, in the absence of investors who acquire tokens only as an investment, the equity token-based scheme is able to achieve the first-best equilibrium as the cash flows from the equity tokens boost user participation by acting as a subsidy from heavy to light users. Such cash flows, however, also incentivize investors without any transaction need to acquire tokens as an investment. The presence of investors diverts the subsidy away from users, which harms user participation. More importantly, investors may even take a majority stake to seize control of the platform when the platform fundamental is sufficiently weak. The investors' control of the platform consequently reintroduces the commitment problem that decentralization through tokenization aimed to overcome.

By comparing specific funding schemes, our analysis abstracts from the design of the optimal funding mechanism that resolves the conflict between a platform and its users. Such an exercise would need to be conducted within the context of an optimal implementation protocol for achieving consensus on the blockchain, an issue which is still unsettled in the literature and, as our analysis shows, may reintroduce the commitment problem.[23] Our work

[23] The optimal design, for instance, may involve a hybrid model of decentralization, such as in Cong, Li and Wang (2019), in which the platform's owner stewards the platform's operations and development through active token monetary policy.

nevertheless highlights a high-level trade-off that can inform such an optimal design, one that cannot be easily resolved with conventional arrangements for allocating control and cash flow rights. First, tokens are less efficient than equity in extracting value from a platform because token prices are based on the convenience yield of the marginal user, while equity is based on the average user through the platform's revenue from transaction fees. Second, although users will never act against their interests by undermining the platform, individually they do not have incentive to subsidize platform participation, despite that it is socially optimal. Third, if tokens carry cash flow in addition to control rights, users or outsiders may have incentive to centralize the platform by amassing tokens, which reintroduces the commitment problem, especially when the token price is low and the platform is vulnerable to subversion.

References

Abadi, Joseph and Markus Brunnermeier (2018), Blockchain Economics, Working Paper, Princeton University.

Allen, Franklin, Xian Gu, and Julapa Jagtiani (2020), A Survey of Fintech Research and Policy Discussion, Working Paper, Imperial College London.

Arruñada, Benito and Luis Garicano (2018), Blockchain: The Birth of Decentralized Governance, Working Paper, Pompeu Fabra University.

Bakos, Yannis and Hanna Halaburda (2018), The Role of Cryptographic Tokens and ICOs in Fostering Platform Adoption, Working Paper, NYU Stern.

Benedetti, Hugo, and Leonard Kostovetsky (2018), Digital Tulips? Returns to Investors in Initial Coin Offerings, Working Paper, ESE and Carroll School of Management.

Bertucci, Louis (2020), Incentives on the Lightning Network: A Blockchain-Based Payment Network, Working Paper, U.C. Berkeley Haas.

Bhambhwani, Siddharth, Stefanos Delikouras, and George Korniotis (2020), Blockchain Characteristics and the Cross-Section of Cryptocurrency Returns, Working Paper.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta (2019), The Blockchain Folk Theorem, *Review of Financial Studies* 32.5, 1662–1715.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, Catherine Casamatta, and Albert Menkveld (2018), Equilibrium Bitcoin Pricing, Working Paper.

Budish, Eric (2018), The Economic Limits of Bitcoin and the Blockchain, Working Paper, University of Chicago.

Catalini, Christian and Joshua S. Gans (2019), Initial Coin Offerings and the Value of Crypto Tokens, Working Paper, Calibra and Rotman School of Management.

Catalini, Christian, Ravi Jagadeesan, and Scott Duke Kominers (2020), Market Design for a Blockchain-Based Financial System, Working Paper, Calibra and Harvard.

Chen, Yan, Igor Pereira, and Pankaj C. Patel (2020), Decentralized Governance of Digital Platforms, *Journal of Management* 20, 1–33.

Chiu, Jonathan and Thorsten V. Koeppl (2017), The Economics of Cryptocurrencies—Bitcoin and Beyond, Working Paper, Victoria and Queen's University.

Chod, Jiri, and Evgeny Lyandres (2020), A Theory of ICOs: Diversification, Agency, and Information Asymmetry, *Management Science*, forthcoming.

Chod, Jiri, Nikolaos Trichakis, and S. Alex Yang (2019), Platform Tokenization: Financing, Governance, and Moral Hazard, Working Paper, Boston College.

Choi, Kyoung Jin and Jaevin Park (2020), Blockchain, Information Production, and Ownership Structure: The Case of a Decentralized Academic Journal, Working Paper, University of Calgary.

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

Cong, Lin William, Zhiguo He, and Jiasun Li (2018), Decentralized Mining in Centralized Pools, *Review of Financial Studies,* forthcoming.

Cong, Lin William, Ye Li, and Neng Wang (2021), Tokenomics: Dynamic Adoption and Valuation, *Review of Financial Studies* 34, 1105-1155.

Cong, Lin William, Ye Li, and Neng Wang (2020), Token-Based Platform Finance, Working Paper, *Journal of Financial Economics*, forthcoming.

Easley, David, Maurenn O'Hara, and Soumya Basu (2019), From Mining to Markets: The Evolution of Bitcoin Transaction Fees, *Journal of Financial Economics*, forthcoming.

Fanti, Giulia, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang (2019a), Compounding of Wealth in Proof-of-Stake Cryptocurrencies, In Ian Goldberg and Tyler Moore, editors, Financial Cryptography and Data Security, 42–61. Springer International Publishing.

Fanti, Giulia, Leonid Kogan, and Pramod Viswanath (2019b), Economics of Proof-of-Stake Payment Systems, Working Paper, ECE and MIT Sloan.

Fisch, Christian (2019), Initial Coin Offerings (ICOs) to Finance New Ventures, *Journal of Business Venturing*, forthcoming.

Gan, Jingxing (Rowena), Gerry Tsoukalas, Serguei Netessine (2020), Initial Coin Offerings, Speculation and Asset Tokenization, Working Paper, Wharton School.

Goldstein, Itay, Deeksha Gupta, and Ruslan Sverchkov (2019), Initial Coin Offerings As a Commitment to Competition, Working Paper, Wharton School.

Gryglewicz, Sebastian, Simon Mayer, and Erwan Morellec (2020), Optimal Financing with Tokens, Working Paper, Erasmus University Rotterdam and SFI.

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro (2020), DeFi and the Future of Finance, Working Paper, Duke.

Hinzen, Franz, John Kose, and Falad Saleh (2020), Bitcoin's Fatal Flaw: The Limited Adoption Problem, Working Paper, NYU Stern.

Howell, Sabrina T., Marina Niessner, and David Yermack (2020), Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales, *Review of Financial Studies* 33, 3925-3974.

Hu, Albert, Christine Parlour, and Uday Rajan (2018), Cryptocurrencies: Stylized Facts on a New Investible Instrument, Working Paper, UC Berkeley.

Huberman, Gur, Jacob Leshno, and Ciamac C. Moallemi (2019), An Economic Analysis of the Bitcoin Payment System, Working Paper, Columbia Business School.

Kose, John, Thomas Rivera, and Fahad Saleh (2020), Economic Implications of Scaling Blockchains: Why The Consensus Protocol Matters, Working Paper, NYU Stern.

Lehar, Alfred and Christine Parlour (2020), Miner Collusion and the BitCoin Protocol, Working Paper, UC Berkeley.

Li, Jiasun and William Mann (2017), Digital Tokens and Platform Building, Working Paper, George Mason University.

Li, Jiasun and William Mann (2019), Initial Coin Offerings: Current Research and Future Directions, Prepared for Palgrave-MacMillan Handbook of Alternative Finance.

Li, Jiasun, and Guanxi Yi (2018), Toward a Factor Structure in Crypto Asset Returns, Working Paper, Geroge Mason University.

Liu, Yukun and Aleh Tsyvinski (2019), Risks and Returns of Cryptocurrency, Working Paper, Yale University.

Liu, Yukun, Aleh Tsyvinski, and Xi Wu (2019), Common Risk Factors in Cryptocurrency, Working Paper, Yale University.

Liu, Zhuang, Michael Sockin, and Wei Xiong (2020), Data Privacy and Temptation, Working Paper, Princeton University.

Malinova, Katya and Andreas Park (2018), Tokenomics: When Tokens Beat Equity, Working Paper, University of Toronto.

Mayer, Simon (2019), Token-Based Platforms and Speculators, Working Paper, Erasmus University Rotterdam.

Pagnotta, Emiliano (2020), Bitcoin as Decentralized Money: Prices, Mining, and Network Security, *Review of Financial Studies,* forthcoming.

Rochet, Jean-Charles, and Jean Tirole (2006), Two-sided Markets: A Progress Report, *The RAND Journal of Economics* 37, 645–667.

Rosu, Ioanid and Fahad Saleh (2020), Evolution of Shares in a Proof-of-Stake Cryptocurrency, *Management Science*, forthcoming.

Saleh, Fahad, (2020), Blockchain Without Waste: Proof-of-Stake, *Review of Financial Studies*, forthcoming.

Shams, Amin (2019), What Drives the Covariation of Cryptocurrency Returns?, Working Paper, Ohio State University.

Sockin, Michael and Wei Xiong (2020), A Model of Cryptocurrencies, Working Paper, Princeton University and UT Austin.

Taylor, Curtis R. (2004), Consumer Privacy and the Market for Customer Information, *RAND Journal of Economics* 35, 631–650.

Tsoukalas, Gerry and Brett Hemenway Falk (2020), Token-Weighted Crowdsourcing, *Management Science*, forthcoming.

A Microfoundation of Goods Trading

In this Appendix, we microfound the goods trading between two users when they are matched on the platform at date t. As all objects are at date t, we omit time subscripts to economize on notation. We assume that user i maximizes its utility by choosing its consumption demand $\{C_i, C_j\}$ through trading with its trading partner user j subject to its budget constraint:

$$\begin{aligned} U_i &= \max_{\{C_i, C_j\}} U\left(C_i, C_j; \mathcal{N}\right) \\ &\quad \text{such that } \ p_i C_i + p_j C_j = p_i e^{A_i}, \end{aligned} \tag{16}$$

where p_i is the price of its good. Similarly, user j solves a symmetric optimization problem for its trading strategy. We also impose market clearing for each user's good between the two trading partners:

$$C_i\left(i\right) + C_i\left(j\right) = e^{A_i} \quad \text{and} \quad C_j\left(i\right) + C_j\left(j\right) = e^{A_j}.$$

Furthermore, we assume that users behave competitively and take the prices of their goods as given.

Proposition 10 *User i's optimal good consumption is*

$$C_i\left(i\right) = \left(1 - \eta_c\right) e^{A_i}, \ C_j\left(i\right) = \eta_c e^{A_j},$$

and the price of his good is

$$p_i = e^{\eta_c\left(A_j - A_i\right)}.$$

Furthermore, the expected utility benefit of user i at $t = 1$ is given by

$$E\left[U\left(C_i, C_j\right) \middle| \mathcal{I}_i\right] = e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - \hat{A}}{\tau_\varepsilon^{-1/2}}\right),$$

and the ex ante utility benefit of all users before observing their goods endowments is

$$U = e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}}\Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2}+\frac{A-\hat{A}}{\tau_\varepsilon^{-1/2}}\right)\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-\hat{A}}{\tau_\varepsilon^{-1/2}}\right).$$

Proposition 10 shows that each user spends a fraction $1-\eta_c$ of his endowment on consuming his own good $C_i\,(i)$ and a fraction η_c on the good of his trading partner $C_j\,(i)$. The price of each good is determined by its endowment relative to that of the other good. One user's good is more valuable when the other user has a greater endowment, and consequently each user needs to take into account the endowment of his trading partner when making his own decision. The proposition demonstrates that the expected utility of a user in the platform is determined by not only his own endowment e^{A_i} but also the endowments of other users. This latter component arises from the complementarity in the user's utility function.

B Proofs of Some Propositions

B.1 Proof of Proposition 1

We consider a social planner who maximizes the utilitarian social surplus on the platform, which is the sum of the total transaction benefit on both dates 1 and 2, net of the fixed costs paid by users to join the platform:

$$\begin{aligned} W &= \sup_{X_i\in\{0,1\}} E\left[\int_0^1 \left(U_{i,1}+U_{i,1}-\kappa\right)X_i di \mid \mathcal{I}_1\right] \\ &= \sup_{X_i\in\{0,1\}} E\left[\int_0^1 \left(e^{(1-\eta_c)A_i}E\left[e^{\eta_c A_j}\,|\mathcal{I}_i\right]-\kappa\right)X_i di \mid \mathcal{I}_1\right]. \qquad (17)\end{aligned}$$

Note that the transaction surplus on date 2 is the same as date 1 in the absence of subversion. It is obvious that, as the only heterogeneity among users is in their endowment, A_i, the planner would optimally follow a cutoff strategy, in which users with $A_i \geq A_W^*$, join the platform. Recognizing this, (17) reduces to

$$\begin{aligned} W \;=\; \sup_{A_W^*}\; & e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}}\Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right) \\ & -\kappa\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right),\end{aligned}$$

where the first term is the total surplus U derived in Proposition 10.

Notice that the derivative of W with respect to A_W^* is

$$\tau_\varepsilon^{-1/2}\frac{dW}{dA_W^*} = \kappa\phi\left(\frac{-A_W^*}{\tau_\varepsilon^{-1/2}}\right) - U\left(\frac{\phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left((1-\eta_c)\,\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}+\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}\right).$$

Notice that $U \geq \kappa\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)$, otherwise the total social surplus is negative. Thus,

$$\frac{\tau_\varepsilon^{-1/2}}{U}\frac{dW}{dA_W^*} < \frac{\phi\left(\frac{-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)} - \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon{}^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon{}^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)} - \frac{\phi\left(\eta_c\tau_\varepsilon{}^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)}{\Phi\left(\eta_c\tau_\varepsilon{}^{-1/2}+\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)} < 0,$$

because the hazard function for the normal distribution, $\frac{\phi(-z)}{\Phi(-z)}$, is increasing in z, which implies that both $\frac{\phi\left(\eta_c\tau_\varepsilon{}^{-1/2}-z_{NS}^E\right)}{\Phi\left(\eta_c\tau_\varepsilon{}^{-1/2}-z_{NS}^E\right)}$ and $\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{NS}^E\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{NS}^E\right)}$ are (weakly) greater than $\frac{\phi\left(-z_{NS}^E\right)}{\Phi\left(-z_{NS}^E\right)}$. As $\frac{\tau_\varepsilon^{-1/2}}{U}\frac{dW}{dA_W^*} < 0$, it follows that the optimal A_W^* is the corner solution $A_W^* = -\infty$, which implies full participation on the platform.

Suppose A is such that $e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}} \geq \kappa$, then our assumption that $U \geq \kappa\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)$ is satisfied to justify full participation on the platform. It follows that the planner can implement the first-best equilibrium by using a revenue-neutral scheme of subsidizing the marginal user with transaction fees collected from heavy users, that is, charging all users δU_i that are refunded as equal transfers of $\delta U/\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right)$ back to all users. As long as the fee δ is sufficiently high to ensure $\delta U/\Phi\left(\frac{A-A_W^*}{\tau_\varepsilon^{-1/2}}\right) > \kappa$, all users would participate on the platform.

If $e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}} < \kappa$, then $U < \kappa$, and the platform should shutter as the social surplus is negative.

B.2 Proof of Proposition 2

The expected utility of user i, who chooses to join the platform, to transacting with another user in each round is half of the following:

$$E\left[U_i\ |\mathcal{I}_i,\ A_i,\ \text{matching with user } j\right] = e^{(1-\eta_c)A_i}E\left[e^{\eta_c A_j}\ |\mathcal{I}_i\right],$$

which is monotonically increasing with the user's own endowment A_i. Note that $E\left[e^{\eta_c A_j} \mid \mathcal{I}_i\right]$ is independent of A_i but dependent on the strategies used by other users. It then follows that user i will follow a cutoff strategy that is monotonic in its own type A_i.

Suppose that every user follows a cutoff strategy with a threshold of $\hat{A}^E$. Then, in each round of transaction, the expected utility of user i from transacting with another user on the platform is half of the following:

$$E\left[U_i|\mathcal{I}_i\right] = e^{(1-\eta_c)A_i+\eta_c A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon{}^{-1/2}+\frac{A-\hat{A}^E}{\tau_\varepsilon{}^{-1/2}}\right). \tag{18}$$

B.2.1 Equilibrium at t = 2

We first examine the equilibrium at $t = 2$. In the absence of subversion, the owner charges a transaction fee δ to complete the transactions of users. Let

$$z^E = \sqrt{\tau_\varepsilon}\left(\hat{A}^E - A\right).$$

Note that the expected fraction of users that participate in the platform is

$$E\left[\int_{-\infty}^{\infty} X_i\left(\mathcal{I}_i\right) d\Phi\left(\varepsilon_i\right)|\mathcal{I}_t\right] = \Phi\left(\frac{A_1 - \hat{A}^E}{\tau_\varepsilon^{-1/2}}\right) = \Phi\left(-z^E\right).$$

The owner's profit at $t = 2$ is $\frac{1}{2}\delta U$, where U is the total trade surplus across the two periods, conditional on no subversion

$$U = e^{A+\frac{1}{2}\left((1-\eta_c)^2+\eta_c^2\right)\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z^E\right). \tag{19}$$

If the owner takes the subversive action, it earns revenue $\gamma\Phi\left(-z^E\right)$. Consequently, the owner takes the subversive action whenever

$$\gamma\Phi\left(-z^E\right) > \frac{1}{2}\delta U \tag{20}$$

and refrains from it otherwise. Consequently, the owner subverts at $t = 2$ whenever the average transaction surplus among users $\delta U/\Phi\left(-z^E\right)$ is sufficiently small. This subversion condition represents an incentive constraint for the platform owner in choosing its fees at $t = 1$, which in turn affects user participation. This condition is eventually determined by the platform fundamental A. Thus, we denote the owner's subversion policy at $t = 2$ by $s\left(A\right) \in \{0, 1\}$. As we will show later, the owner will ultimately choose subversion if the platform fundamental A falls below a certain level.

B.2.2 Optimal Fees at t = 1

We now analyze the equilibrium at $t = 1$. We first examine each user's participation choice and the owner's choices of entry and transaction fees by taking the value of A and the owner's subversion policy s as given.

Each user receives two rounds of transaction surplus, after the variable fee δ, if there is no subversion at $t = 2$ and only one round of transaction surplus, and $-\gamma$ otherwise. Given the expression for $E\left[U_{i,1} + U_{i,2} \mid \mathcal{I}_i, A_i = \hat{A}^E\right]$ from (18), the participation constraint for the marginal user with the cutoff endowment $\hat{A}^E$ is

$$\left(1 - \frac{1}{2}s\right)\left(1-\delta\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right) = \kappa + \gamma s + c. \tag{21}$$

The left-hand side is hump-shaped in z^E while the right-hand side has a fixed level at either $\kappa + c$ or $\kappa + \gamma + c$. The right-hand side is positive since $c \geq -\alpha\kappa$. This equation has zero or two solutions; when it has two solutions, one is a high cutoff and the other is low. Since user participation and platform revenue are always higher in the low cutoff equilibrium, the platform owner will always coordinate users on the low cutoff equilibrium.

We can then apply the Implicit Function Theorem to recognize that

$$
\begin{aligned}
\frac{\partial z^E}{\partial A} &= -\frac{1}{(1-\eta_c)\,\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}} < 0, && (22)\\
\frac{\partial z^E}{\partial \delta} &= \frac{1}{1-\delta}\frac{1}{(1-\eta_c)\,\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}} > 0, && (23)\\
\frac{\partial z^E}{\partial c} &= \frac{1}{\left(1-\frac{1}{2}s\right)(1-\delta)\,e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\,\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}\\
&\quad \cdot\frac{1}{(1-\eta_c)\,\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}} > 0.
\end{aligned}
$$

The denominator of (22) is positive because it is on the left side of the hump. It then follows that

$$
\begin{aligned}
\frac{\partial z^E/\partial\delta}{\partial z^E/\partial c} &= \left(1-\frac{1}{2}s\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\,\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)\\
&= \left(1-\frac{1}{2}s\right)E\left[U_i \mid \mathcal{I}_i, A_i = \hat{A}^E\right]. && (24)
\end{aligned}
$$

We now consider the owner's objective at $t = 1$ in choosing its optimal fees:

$$
(\delta, c) \in \arg\sup_{\{\delta,c\}} V,
$$

where its total profit is

$$
V = \frac{1}{2}\delta U + c\Phi\left(-z^E\right) + \max\left\{\frac{1}{2}\delta U, \gamma\Phi\left(-z^E\right)\right\}.
$$

The first-order condition for δ is

$$
\frac{\partial V}{\partial \delta} = \left(1-\frac{1}{2}s\right)U + \left[\frac{1}{2}\delta\frac{\partial U}{\partial z^E} - c\phi\left(-z^E\right) + \frac{\partial \max\left\{\frac{1}{2}\delta U, \gamma\Phi\left(-z^E\right)\right\}}{\partial z^E}\right]\frac{\partial z^E}{\partial \delta} = 0.
$$

The first-order condition for c is

$$\begin{aligned}
\frac{\partial V}{\partial c} &= \Phi\left(-z^E\right) + \left[\frac{1}{2}\delta\frac{\partial U}{\partial z^E} - c\phi\left(-z^E\right) + \frac{\partial \max\left\{\frac{1}{2}\delta U, \gamma\Phi\left(-z^E\right)\right\}}{\partial z^E}\right]\frac{\partial z^E}{\partial c} \\
&= \Phi\left(-z^E\right) + \frac{\frac{\partial V}{\partial \delta} - \left(1-\frac{1}{2}s\right)U}{\frac{\partial z^E}{\partial \delta} / \frac{\partial z^E}{\partial c}} \\
&= \Phi\left(-z^E\right) - \frac{U}{E\left[U_i \mid \mathcal{I}_i, A_i = \hat{A}^E\right]}, \qquad (25)
\end{aligned}$$

where we have substituted (24) in the last step. Note that the utility of the marginal user $E\left[U_i \mid \mathcal{I}_i, A_i = \hat{A}^E\right]$ is lower than that of the average user. Thus,

$$\frac{\partial V}{\partial c} < \Phi\left(-z^E\right) - 1 < 0.$$

The owner is constrained in its choice of c and has to choose the lower bound at $c = -\alpha\kappa$.

Given this optimal c, equation (21) reduces to

$$\left(1 - s/2\right)\left(1-\delta\right)e^{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}z^E + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right) = \left(1-\alpha\right)\kappa + \gamma s, \qquad (26)$$

which identifies $\hat{A}^E$, the smaller root of the above equation when it exists. Comparing the two cases when $s = 0$ and $s = 1$ for a given level of A and δ, the effective cost to users of joining the platform is higher, leading to a higher participation threshold z^E. Consequently, the owner must charge a smaller δ to attract the same participation when subversion is anticipated. Notice from (21) that $\delta < 1$ since the right-hand side is always non-negative; users would never pay a cost for zero or negative benefit.

The first-order condition for δ when there is no subversion, given our expression for $\frac{\partial z^E}{\partial \delta}$ and $c = -\alpha\kappa$, becomes

$$\left(1-\delta\right)U + \frac{\delta\frac{\partial U}{\partial z^E} + \alpha\kappa\phi\left(-z^E\right)}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}} = 0, \qquad (27)$$

and, substituting for $\frac{\partial U}{\partial z^E}$, we arrive at

$$\delta = \frac{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)} + \frac{\alpha\kappa\phi\left(-z^E\right)}{U}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} + \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z^E\right)}}. \qquad (28)$$

When there is subversion, $s = 1$, then instead

$$\delta = \frac{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right)} - \frac{2\left(\gamma - \alpha\kappa\right)\phi\left(-z^E\right)}{U}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} + \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z^E\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z^E\right)}}. \qquad (29)$$

Since $\gamma > \alpha\kappa$, by comparing the third term in the numerators of both expressions, it is straightforward to see that δ is higher when there is no subversion for the same A and z^E.

In the next two subsections, we characterize the regions of the platform fundamental A, for which there is and there is no subversion under the optimal fees. We will also consider the possibility of the owner choosing a high fee level δ at $t = 1$ as a strategy to force no subversion at $t = 2$.

B.2.3 The No-Subversion Equilibrium at t = 1

We now analyze the equilibrium at $t = 1$ when the owner chooses no subversion $s = 0$ at $t = 2$. To avoid confusion, let z^E_{NS} be the equilibrium without subversion and z^E_{SV} be the equilibrium with subversion. We now characterize the domain of A for which a no-subversion equilibrium exists.

Substituting for δ in (28), when there is no subversion, the condition for z^E_{NS} in (26) becomes

$$\begin{aligned} & \frac{\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}+\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}-\alpha\kappa\frac{\phi\left(-z^E_{NS}\right)}{U}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}} e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E_{NS}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E_{NS}\right) \\ = \; & \left(1-\alpha\right)\kappa. \end{aligned} \tag{30}$$

The left-hand side of (30) is hump-shaped in z^E_{NS}. To see this, first note that, as $z^E_{NS} \to -\infty$, the left-hand side goes to 0. As $z^E_{NS} \to \infty$, since $e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E_{NS}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E_{NS}\right) \to 0$, by L'Hospital's rule and the Sandwich theorem, the left-hand side tends to

$$\begin{aligned} LHS \;\to\; & \lim_{z^E_{NS}\to\infty} 2e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E_{NS}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E_{NS}\right) \\ & -\frac{\alpha\kappa\phi\left(-z^E_{NS}\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E_{NS}-\frac{1}{2}(1-\eta_c)^2\tau_\varepsilon^{-1}}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)+\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)} \\ = \; & \lim_{z^E_{NS}\to\infty} -\frac{\alpha\kappa\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)+\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}\right)} \\ = \; & \lim_{z^E_{NS}\to\infty} \alpha\kappa\frac{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-z^E_{NS}}{z^E_{NS}} \\ = \; & -\alpha\kappa. \end{aligned}$$

As such, the left-hand side of (30) has finite limits in both tails. We next realize that the optimal δ is a (weakly) decreasing function of z^E_{NS}, $\frac{\partial\delta}{\partial z^E_{NS}} \leq 0$ since the marginal user has a lower endowment, so that $1-\delta$ is (weakly) increasing in z^E_{NS}. Consequently, as a product of a hump-shaped U and (weakly) increasing function $1-\delta$, the left-hand side is hump-shaped in z_{NS}^{E}. In addition, since $\delta > 0$, it follows that the left-hand side also has a finite upper bound. As such, there are either two or zero solutions to (30). When there are two solutions, the platform owner will always choose the low cutoff solution as it maximizes his revenue.

Notice next that increasing A raises the entire curve on the left-hand side of (30) since $\frac{e^{A}}{U}$ has no direct dependence on A. Since, in the low cutoff equilibrium, an upward shift in the left-hand side curve lowers the value of z_{NS}^{E} that intersects $(1-s)\,\kappa$, we have

$$\frac{dz_{NS}^{E}}{dA} < 0,$$

in the low cutoff equilibrium, where $\frac{dz_{NS}^{E}}{dA}$ is the total derivative of z_{NS}^{E} with respect to A.

Next, when the owner is deciding to subvert, the decision is determined by whether $\frac{1}{2}\delta U$ is greater or less than $\gamma\Phi\left(-z_{NS}^{E}\left(A\right)\right)$. Notice that

$$\begin{aligned}
&\frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right)\\
= \;& \frac{1}{\delta U}\frac{d\left(\delta U\right)}{dA} + \frac{\phi\left(-z_{NS}^{E}\right)}{\Phi\left(-z_{NS}^{E}\right)}\frac{dz_{NS}^{E}}{dA}\\
= \;& \frac{1}{\delta}\frac{d\delta}{dA} + 1 - \left(\frac{\phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2} - z_{NS}^{E}\right)}{\Phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2} - z_{NS}^{E}\right)} + \frac{\phi\left(\left(1-\eta_{c}\right)\tau_{\varepsilon}^{-1/2} - z_{NS}^{E}\right)}{\Phi\left(\left(1-\eta_{c}\right)\tau_{\varepsilon}^{-1/2} - z_{NS}^{E}\right)} - \frac{\phi\left(-z_{NS}^{E}\right)}{\Phi\left(-z_{NS}^{E}\right)}\right)\frac{dz_{NS}^{E}}{dA}.
\end{aligned}$$

where $\frac{dz_{NS}^{E}}{dA}$ is again the total derivative of z_{NS}^{E} with respect to A. Because the hazard function for the normal distribution, $\frac{\phi(-z)}{\Phi(-z)}$, is increasing in z, this implies that both $\frac{\phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}$ and $\frac{\phi\left((1-\eta_{c})\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left((1-\eta_{c})\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}$ are (weakly) greater than $\frac{\phi\left(-z_{NS}^{E}\right)}{\Phi\left(-z_{NS}^{E}\right)}$. This, and recalling that$\frac{dz_{NS}^{E}}{dA} < 0$ imply that

$$\frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right) > 1 + \frac{1}{\delta}\frac{d\delta}{dA}.$$

Since

$$\begin{aligned}
\frac{1}{\delta}\frac{d\delta}{dA} &= \frac{\partial\delta}{\partial A} + \frac{1}{\delta}\frac{\partial\delta}{\partial z_{NS}^{E}}\frac{\partial z_{NS}^{E}}{\partial A}\\
&= \frac{-\frac{\alpha\kappa\phi\left(-z_{NS}^{E}\right)}{U}}{\left(1-\eta_{c}\right)\tau_{\varepsilon}^{-1/2} - \frac{\phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left(\eta_{c}\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)} + \frac{\alpha\kappa\phi\left(-z_{NS}^{E}\right)}{U}} + \frac{1}{\delta}\frac{\partial\delta}{\partial z_{NS}^{E}}\frac{\partial z_{NS}^{E}}{\partial A},
\end{aligned}$$

one has that

$$\begin{aligned}\frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right) &> \frac{\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-\frac{\phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}}{\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-\frac{\phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}+\frac{\alpha\kappa\phi\left(-z_{NS}^{E}\right)}{U}}+\frac{1}{\delta}\frac{\partial\delta}{\partial z_{NS}^{E}}\frac{\partial z_{NS}^{E}}{\partial A}\\ &> \frac{1}{\delta}\frac{\partial\delta}{\partial z_{NS}^{E}}\frac{\partial z_{NS}^{E}}{\partial A},\end{aligned}$$

since $\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-\frac{\phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)}{\Phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{NS}^{E}\right)} \geq 0$ in the low cutoff equilibrium. As argued above, $\frac{\partial\delta}{\partial z_{NS}^{E}} \leq 0$. Since, in addition $\frac{dz_{NS}^{E}}{dA} < 0$, it follows that $\frac{\partial\delta}{\partial z_{NS}^{E}}\frac{\partial z_{NS}^{E}}{\partial A} > 0$. Therefore,

$$\frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right) > 0,$$

which implies

$$\frac{d}{dA}\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right) > 0.$$

Because there is no subversion when $\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)} \geq 2\gamma$, and subversion when $\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)} < 2\gamma$, it follows, since $\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}$ is increasing in A, that there exists a critical level A^* such that a no-subversion equilibrium exists if $A \geq A_*^E$, where the unique threshold A_*^E is defined by

$$\frac{\delta\left(A_*^E\right)U\left(A_*^E\right)}{\Phi\left(-z_{NS}^{E}\left(A_*^E\right)\right)} = 2\gamma. \tag{31}$$

This threshold represents the lowest A for which the owner maximizes his total revenue without subversion.

B.2.4 The Subversion Equilibrium at $\mathbf{t=1}$

We now analyze the equilibrium at $t=1$ when the owner chooses subversion $s=1$ at $t=2$. In this case, the condition for z_{SV}^{E} from (26) becomes

$$\begin{aligned}&\frac{\frac{1}{2}\frac{\phi\left(\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}{\Phi\left(\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}+\frac{1}{2}\frac{\phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}{\Phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}+\frac{\left(\gamma-\alpha\kappa\right)\phi\left(-z_{SV}^{E}\right)}{U}}{\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}+\frac{\phi\left(\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}{\Phi\left(\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right)}}e^{\left(1-\eta_c\right)\tau_{\varepsilon}^{-1/2}z_{SV}^{E}+A+\frac{1}{2}\eta_c^2\tau_{\varepsilon}^{-1}}\\ &\cdot\Phi\left(\eta_c\tau_{\varepsilon}^{-1/2}-z_{SV}^{E}\right) = \left(1-\alpha\right)\kappa+\gamma,\end{aligned} \tag{32}$$

where the $\frac{1}{2}$ arises since all $t=2$ transaction surplus is destroyed by the subversion. Similar to (30), as $z_{NS}^{E} \to -\infty$, then the left-hand side tends to 0, while, as $z_{NS}^{E} \to \infty$, the left-hand side tends to $\gamma - \alpha\kappa$. As such, the left-hand side is initially increasing in z_{SV}^{E}. This equation may have multiple solutions. As before, when this happens, the owner will choose the lowest cutoff, as it gives the highest user participation and revenue. Also similar to (30), an increase in A raises the left-hand side curve, which lowers the equilibrium z_{SV}^{E} in the lowest cutoff equilibrium. Consequently,

$$\frac{dz_{NS}^{E}}{dA} < 0,$$

which again is the total derivative of z_{NS}^{E} with respect to A. In addition, since an increase in z_{NS}^{E} lowers the endowment of the marginal agent, it follows that $\frac{\partial \delta}{\partial z_{NS}^{E}} \leq 0$.

We next establish the monotonicity of $\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}$ in A when $\delta > 0$. By similar arguments to the no-subversion equilibrium,

$$\begin{aligned}
& \frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{NS}^{E}\right)}\right) \\
= \quad & 1 + \frac{1}{\delta}\frac{d\delta}{dA} - \left(\frac{\phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} + \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} - \frac{\phi\left(-z_{SV}^{E}\right)}{\Phi\left(-z_{SV}^{E}\right)}\right)\frac{dz_{NS}^{E}}{dA} \\
> \quad & 1 + \frac{1}{\delta}\frac{d\delta}{dA}.
\end{aligned}$$

Since

$$\begin{aligned}
\frac{1}{\delta}\frac{d\delta}{dA} &= \frac{\partial \delta}{\partial A} + \frac{1}{\delta}\frac{\partial \delta}{\partial z_{SV}^{E}}\frac{\partial z_{SV}^{E}}{\partial A} \\
&= \frac{\frac{2(\gamma-\alpha\kappa)\phi\left(-z_{SV}^{E}\right)}{U}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} - \frac{2(\gamma-\alpha\kappa)\phi\left(-z_{SV}^{E}\right)}{U}} + \frac{1}{\delta}\frac{\partial \delta}{\partial z_{SV}^{E}}\frac{\partial z_{SV}^{E}}{\partial A},
\end{aligned}$$

it follows that

$$\begin{aligned}
& \frac{d}{dA}\log\left(\frac{\delta U}{\Phi\left(-z_{SV}^{E}\right)}\right) \\
> \quad & \frac{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} - \frac{2(\gamma-\alpha\kappa)\phi\left(-z_{SV}^{E}\right)}{U}} + \frac{1}{\delta}\frac{\partial \delta}{\partial z_{SV}^{E}}\frac{\partial z_{SV}^{E}}{\partial A} \\
> \quad & \frac{1}{\delta}\frac{\partial \delta}{\partial z_{SV}^{E}}\frac{\partial z_{SV}^{E}}{\partial A}.
\end{aligned}$$

As argued above, $\frac{\partial \delta}{\partial z_{SV}^{E}} \leq 0$. Since $\frac{dz_{NS}^{E}}{dA} < 0$, it follows that $\frac{\partial \delta}{\partial z_{SV}^{E}}\frac{\partial z_{SV}^{E}}{\partial A} > 0$. Therefore,

$$\frac{d}{dA}\left(\frac{\delta U}{\Phi\left(-z_{SV}^{E}\right)}\right) > 0.$$

Consequently, there exists a critical A^E_{*c} such that subversion occurs for $A \leq A^E_{*c}$, where A^E_{*c} satisfies

$$\frac{\delta U\left(A^E_{*c}\right)}{\Phi\left(-z^E_{SV}\left(A^E_{*c}\right)\right)} = 2\gamma.$$

Suppose now that for a given level of A, both a subversion and a no-subversion equilibrium exist, that is, solutions to both (30) and (32) exist. In the equilibrium without subversion

$$\frac{1}{2}\frac{\delta\left(z^E_{NS}\right)U\left(z^E_{NS}\right)}{\Phi\left(-z^E_{NS}\right)} \geq \gamma,$$

while in the equilibrium with subversion

$$\gamma \geq \frac{1}{2}\frac{\delta\left(z^E_{SV}\right)U\left(z^E_{SV}\right)}{\Phi\left(-z^E_{SV}\right)},$$

which implies that

$$\frac{\delta\left(z^E_{NS}\right)U\left(z^E_{NS}\right)}{\Phi\left(-z^E_{NS}\right)} \geq \frac{\delta\left(z^E_{SV}\right)U\left(z^E_{SV}\right)}{\Phi\left(-z^E_{SV}\right)}.$$

Since $\frac{\delta(z)U(z)}{\Phi(-z)}$ is monotonically decreasing in z, it follows that $z^E_{NS} \leq z^E_{SV}$, and user participation is higher in the equilibrium without subversion. It then follows that

$$\begin{aligned}\delta\left(z^E_{NS}\right)U\left(z^E_{NS}\right) - \Phi\left(-z^E_{NS}\right)\alpha\kappa &> \frac{1}{2}\delta\left(z^E_{NS}\right)U\left(z^E_{NS}\right) + \Phi\left(-z^E_{NS}\right)\gamma - \Phi\left(-z^E_{NS}\right)\alpha\kappa \\ &> \frac{1}{2}\delta\left(z^E_{SV}\right)U\left(z^E_{SV}\right) + \Phi\left(-z^E_{SV}\right)(\gamma - \alpha\kappa).\end{aligned}$$

As such, when both equilibria exist, the no-subversion equilibrium generates a higher profit for the owner. As such, the owner will choose not to subvert even when subverting is a sustainable action. Consequently, the cutoff A^E_* is the relevant cutoff for separating the equilibria with and without subversion.

Next, note that the left-hand side of (32), which we define as $LHS\left(z^E_{SV}\right)$, is hump-shaped in z^E_{SV}. Thus, it achieves its maximum at an interior point $\bar{z}(A) = \sup_z LHS(z)$. As this peak is increasing in A, it follows that there exists a critical A^E_{**}, such that

$$LHS\left(\bar{z}\left(A^E_{**}\right)\right) = (1-\alpha)\kappa + \gamma. \tag{33}$$

Thus, an equilibrium with subversion exists when $A \geq A^E_{**}$ and does not exist otherwise.

One may be concerned that the region $\left[A^E_{**}, A^E_*\right]$ may be an empty set for a certain value of γ. Suppose that this is the case. That is, as A decreases from ∞ to 0, the equilibrium shifts from a no-subversion equilibrium to no equilibrium at A^E_*. As the owner is willing to subsidize participation as long as there is a positive profit, it must be

$$V\left(A^E_*\right) = \delta U - \alpha\kappa\Phi\left(-z^E_{NS}\right) = 0,$$

which implies that $\delta U = \alpha\kappa\Phi\left(-z_{NS}^{E}\right)$. Because $\gamma > \alpha\kappa$, we have

$$\frac{1}{2}\delta U = \frac{1}{2}\alpha\kappa\Phi\left(-z_{NS}^{E}\right) < \gamma\Phi\left(-z_{NS}^{E}\right).$$

It follows that the owner is better off by taking the subversive action in this case. Thus, a subversion equilibrium exists. Thus, the region $\left[A_{**}^{E}, A_{*}^{E}\right]$ cannot be empty.

B.2.5 Forcing Equilibrium at $\mathbf{t = 1}$

One may argue that the owner may internalize his lack of commitment by treating the subversion condition as an incentive constraint. That is, the owner can avoid subverting the platform by imposing a constraint to prevent the subversion condition in (20) from being satisfied at $t = 2$. We now examine this possibility by constraining the owner's choice of δ at $t = 1$ such that $\frac{\delta U}{\Phi(-z^{E})} \geq 2\gamma$ (i.e., the owner will not choose subversion at $t = 2$). This condition imposes a lower bound on δ: $\delta \geq \underline{\delta} = \frac{2\gamma\Phi\left(-z^{E}\right)}{U}$.

Suppose that when this constraint is not imposed, there is a subversion equilibrium with δ_{SV} as the transaction fee and z_{SV}^{E} as the participation cutoff, and that when this constraint is imposed, there is a different forcing equilibrium with $\underline{\delta}$ as the transaction fee and $z_{forcing}^{E}$ as the participation cutoff. It is important to note that $\underline{\delta}$ is always in the owner's choice set. As such, it must give a lower profit to the owner than δ_{SV}. That is, $V\left(\underline{\delta}, z_{forcing}^{E}\right) < V\left(\delta_{SV}, z_{SV}^{E}\right)$, which implies that the forcing equilibrium is dominated by the subversion equilibrium if both exist and are different.

Furthermore, if a forcing equilibrium with $\underline{\delta}$ exists and if no subversion equilibrium exists, then the owner would choose $\underline{\delta}$ even without the constraint. Taken together, there is no need to separately consider the forcing equilibrium.

B.2.6 Equilibrium Uniqueness

As we discussed at the beginning of this proof, it is optimal for each user to adopt a cutoff strategy because his expected utility from joining the platform is monotonically increasing with his own good endowment. The uniqueness of the equilibrium follows directly from the platform owner's choice of the lowest cutoff and thus highest profit equilibrium, if there are multiple equilibria that are feasible.

B.3 Proof of Proposition 4

We first examine the decision of a user to purchase the token. The expected utility of user i, who chooses to join the platform at $t = 1$ and then transact with another user at $t = 1$

and $t = 2$, is

$$E\left[U_{i,t}\ |\mathcal{I}_i,\ A_i,\ \text{matching with user } j\right] = \frac{1}{2} e^{(1-\eta_c)A_i} E\left[e^{\eta_c A_j}\ |\mathcal{I}_i\right],$$

which is monotonically increasing with the user's own endowment A_i. Note that $E\left[e^{\eta_c A_j} \mid \mathcal{I}_i\right]$ is independent of A_i but dependent on the strategies used by other users. It then follows that user i will adopt a cutoff strategy that is monotonic in his own type A_i.

Suppose that every user uses a cutoff strategy with a threshold of $\hat{A}^T$. Then, the expected utility of user i at $t \in \{1, 2\}$ is

$$E\left[U_{i,t}|\mathcal{I}\right] = \frac{1}{2} e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - \sqrt{\tau_\varepsilon}\left(\hat{A}^T - A\right)\right).$$

Since each user's endowment is the same in both periods, each user receives $E\left[U_i|\mathcal{I}\right] = E\left[U_{i,1} + U_{i,2}|\mathcal{I}\right]$ in total.

If a potential user does not join the platform, he saves the participation and token costs, $\kappa + P$. Consequently, we require that the expected utility of users from joining the platform at $t = 1$ exceeds $\kappa + P$. Consider a user with the critical endowment $A_i = \hat{A}^T$. His indifference condition to joining the platform is

$$E\left[U_{i,1} + U_{i,2}|\mathcal{I}, A_i = \hat{A}^T\right] = e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z^T + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^T\right) = \kappa + P, \tag{34}$$

where $z^T = \sqrt{\tau_\varepsilon}\left(\hat{A}^T - A\right)$.

Note, by the implicit function theorem, that

$$\frac{\partial z^T}{\partial P} = \frac{1}{\left(\left(1 - \eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^T\right)}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^T\right)}\right) e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z^T + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^T\right)} > 0$$

since the denominator is positive in the low cutoff equilibrium. As before, we assume that, if there are two solutions for z^T, the developer will coordinate users on the low cutoff (high price) equilibrium, as opposed to the high cutoff (low price) equilibrium, since both user participation and developer profit are higher in this equilibrium.

For any other user whose endowment satisfies $A_i > \hat{A}^T$, notice that

$$\begin{aligned}
E\left[U_{i,1} + U_{i,2}|\mathcal{I},\right] &= e^{(1-\eta_c)A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - \hat{A}^T}{\tau_\varepsilon^{-1/2}}\right) \\
&> e^{(1-\eta_c)\tau_\varepsilon^{-1/2} \hat{A}^T + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} + \frac{A - \hat{A}^T}{\tau_\varepsilon^{-1/2}}\right) \\
&= \kappa + P,
\end{aligned}$$

and consequently it is optimal for users to follow a cutoff strategy in which users with $A_i \geq \hat{A}^T$ join and users with $A_i < \hat{A}^T$ do not.

Since $A_i = A + \varepsilon_i$, it then follows that a fraction $\Phi\left(-\sqrt{\tau_\varepsilon}\left(\hat{A}^T - A\right)\right)$ of the users enter the platform, and a fraction $\Phi\left(\sqrt{\tau_\varepsilon}\left(\hat{A}^T - A\right)\right)$ choose not to participate. It is the integral over the idiosyncratic endowment of users ε_i that determines the fraction of potential users on the platform. The developer consequently maximizes

$$\Pi^T = P\Phi\left(-z^T\right),$$

which is the revenue from the sale of tokens, specifically, the price P multiplied by the quantity $\Phi\left(-z^T\right)$. The first-order condition with respect to the price, P, is

$$\Phi\left(-z^T\right) - P\phi\left(-z^T\right)\frac{\partial z^T}{\partial P}\begin{cases} = 0 \text{ if } P > 0 \\ < 0 \text{ if } P = 0 \end{cases}.$$

Substituting with $\frac{\partial z^T}{\partial P}$, an interior solution for the token price, when it exists, is given by

$$\begin{aligned} P \;=\; & \frac{\Phi\left(-z^T\right)}{\phi\left(-z^T\right)}\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right)}\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^T + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} \\ & \cdot\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right) \geq 0. \end{aligned}$$

Notice that the hazard rate $\phi\left(-z^T\right)/\Phi\left(-z^T\right)$ is increasing in z^T. As such, P decreases from ∞ to 0, at which point the non-negativity constraint imposes a critical $\bar{z}^T$ such that

$$\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - \bar{z}^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \bar{z}^T\right)} = \left(1-\eta_c\right)\tau_\varepsilon^{-1/2},$$

above which the token price is fixed at a corner solution of 0. This corner corresponds to the peak of the hump of $e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^T + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right)$.

Equating the two representations for P, we arrive at

$$\begin{aligned} & \left(1 - \frac{\Phi\left(-z^T\right)}{\phi\left(-z^T\right)}\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right)}\right)\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^T + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}} \\ & \cdot\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right) = \kappa, \end{aligned} \tag{35}$$

which identifies $z^T \leq \bar{z}^T$. The left-hand side of (35) is increasing from $-\infty$ to $\bar{z}^T$, with a peak at $\bar{z}^T$, while the RHS is fixed at κ. Suppose

$$e^{(1-\eta_c)\tau_\varepsilon^{-1/2}\bar{z}^T + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \bar{z}^T\right) \geq \kappa.$$

Then, there exists a cutoff equilibrium with the cutoff given by (35). If instead

$$e^{(1-\eta_c)\tau_\varepsilon^{-1/2}\bar{z}^T + A_1 + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \bar{z}^T\right) < \kappa,$$

then the LHS of (35) never intersects the RHS, and consequently, there is no equilibrium.

Note that the LHS of (35) is monotonically increasing in the platform fundamental A. As such, there exists a critical A_{**}^T such that

$$e^{(1-\eta_c)\tau_\varepsilon^{-1/2}\bar{z}^T\left(A_{**}^T\right) + A_{**}^T + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - \bar{z}^T\left(A_{**}^T\right)\right) = \kappa. \tag{36}$$

There exists an equilibrium with a non-negative profit for the developer if $A \geq A_{**}^T$ and such an equilibrium does not exist otherwise.

B.4 Proof of Proposition 6

We first consider the revenue-ranking across the equity and utility token-based schemes given the platform fundamental A. Recall that when there is no subversion, from Proposition 5, developer profit is higher under the equity-based scheme, $\Pi^E(A) \geq \Pi^T(A)$. From Proposition 2, subversion occurs for $A < A_*^E$, where A_*^E is given by (31). Therefore, if $A \geq A_*^E$, the developer's profit is higher on the equity platform.

Suppose $A < A_*^E$, so that there is subversion on the platform. If the degree of data abuse, that is, γ, is sufficiently high, then from Proposition 5, there exists an $A_T(\gamma)$ such that $\Pi^T(A) > \Pi^E(A)$ for $A < A_T(\gamma)$, and $\Pi^E(A) \geq \Pi^T(A)$ otherwise (this is just the dual to the statement that for a given A, there exists is a $\gamma(A)$ such that the statement holds).

In addition, from Proposition 5, user participation is (weakly) higher under the token-based scheme for $A < A_T(\gamma)$. This implies that the critical A below which the platform breaks down is also lower under the token-based platform. Consequently, for $A \geq A_T(\gamma)$, the developer's profit is higher under the equity-based scheme compared to the token-based scheme, and is lower otherwise.

Consider now the prior belief of the developer over A. The difference in expected profit of the platform under both arrangements is

$$E\left[\Pi^T - \Pi^E\right] = E\left[\left(\Pi^T - \Pi^E\right)\mathbf{1}_{\{A \geq A_T(\gamma)\}}\right] + E\left[\left(\Pi^T - \Pi^E\right)\mathbf{1}_{\{A < A_T(\gamma)\}}\right],$$

from which follows that

$$\begin{aligned} E\left[\Pi^T - \Pi^E\right] &= \Pr\left(A \geq A_T(\gamma)\right) E\left[\Pi^T - \Pi^E | A \geq A_T(\gamma)\right] \\ &\quad + \Pr\left(A < A_T(\gamma)\right) E\left[\Pi^T - \Pi | A < A_T(\gamma)\right], \end{aligned}$$

where $E\left[\Pi^T - \Pi | A \geq A_T(\gamma)\right] < 0$, since $E\left[\Pi^T - \Pi | A < A_T(\gamma)\right] > 0$. Consequently, the first term is negative while the second is positive.

We next recognize that $A_T(\gamma)$, and consequently the probability $\Pr(A < A_T(\gamma))$ is increasing in γ, because the more severe the temptation is to subvert the platform, the more difficult it is to operate without exploiting user data at $t = 2$. In addition, from Proposition 5, the owner's profit, conditional on subversion, is decreasing in γ.

Therefore if the prior belief, $G(A)$, puts sufficient weight on low A realizations, for which $\Pr(A < A_T(\gamma))$ is sufficiently large, then $E\left[\Pi^T\right] > E\left[\Pi^E\right]$. In contrast, if it puts sufficient weight on high A realizations, for which $\Pr(A < A_T(\gamma))$ is sufficiently small, then $E\left[\Pi^T\right] < E\left[\Pi^E\right]$. Furthermore, the set of measures for which $E\left[\Pi^T\right] > E\left[\Pi^E\right]$ is (weakly) increasing in γ.

Consequently, for two prior distributions, $G(A)$ and $\tilde{G}(A)$, if $\tilde{G} > G$ (in a first-order stochastic dominance sense), then if the developer adopts the token-based scheme under G, it will also adopt under $\tilde{G}$. Furthermore, the set of priors for which the developer will choose the token-based scheme is (weakly) increasing in γ.

In the special case of a normal prior with mean $\bar{A}$ and fixed precision τ_A, it follows from standard arguments that the developer's expected profit from the platform is a function of only $\bar{A}$ and τ_A, and is increasing in $\bar{A}$. Given our partition of the state space of A with $A_T(\gamma)$, there exists a prior mean, $\bar{A}^c$, such that the developer chooses the equity-based scheme if $\bar{A} \geq \bar{A}^c(\gamma)$ and the token-based scheme otherwise.

B.5 Proof of Proposition 7

We first conjecture that the token holders never subvert the platform and then confirm this conjecture at the end of the proof.

B.5.1 The No-Subversion Equilibrium

Let us conjecture that users follow a cutoff strategy to join the platform at $t = 1$ if $A_i \geq \hat{A}_{ET}$, and that users will vote by majority for 100% transaction fees at $t = 2$. Analogous to (34), the indifference condition for the marginal user to join the platform at $t = 1$ takes the form

$$(1-\delta_T)\, e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z^{ET} + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^{ET}\right) = \kappa + P - \frac{\delta_T U}{N + \Phi\left(-z^{ET}\right)}, \tag{37}$$

where $z^{ET} = \sqrt{\tau_\varepsilon}\left(\hat{A}^{ET} - A\right)$ and U is the total transaction surplus given in (19). We recognize from (19) that this total transaction surplus, U, is monotonically increasing in user participation (i.e., a lower $\hat{A}^{ET}$ or z^{ET}).

We define

$$p_{ET} \equiv P - \delta_T \frac{U}{N + \Phi\left(-z^{ET}\right)},$$

which is the effective cost for a user to join the platform by paying the token price and then receiving the dividend payout. Then, we can rewrite (37) as

$$(1-\delta_T)\, e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z^{ET} + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z^{ET}\right) = \kappa + p_{ET}, \tag{38}$$

and the objective of the developer in (9) as

$$\Pi^{ET} = \max_{\delta_T, p_{ET}, N} p_{ET} \Phi\left(-z^{ET}\right) + \delta_T U - \chi N, \tag{39}$$

subject to the indifference condition (38) of the marginal user.

From (39), it is apparent that the size of the developer's stake is irrelevant for the fraction of transaction fees the developer receives because it always recovers all transaction fees through the token price, P. As such, keeping a stake of N only incurs a proportional cost χN, which is minimized at $N = 0$; as such, the developer will choose to hold 0 tokens or no stake in the platform.

Notice now that (39) is essentially the same problem as that faced by the developer on the equity platform, (4), in the case of no subversion and with p_{ET} analogous to c. From analogous calculations to those underlying (25), the optimal choice of p_{ET} is the maximum possible subsidy, that is, $p_{ET} = -\kappa$, in which case all users join and $z^{ET} = -\infty$ and $U = e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\epsilon^{-1}}$. If all users participate, then it is trivial to see from (39) that the optimal transaction fee is $\delta_T = 1$, or 100% transaction fees.

With the equity platform, the subsidy c could not be lower than $-\alpha\kappa$ because of opportunistic individuals. Here, because the actual price users pay when they all participate when $\delta_T = 1$ is $P = e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\epsilon^{-1}} + p_{ET}$, the developer can choose $p_{ET} = -\kappa$ provided that $P = e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\epsilon^{-1}} - \kappa \geq 0$, or $A \geq \log \kappa - \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\varepsilon^{-1}$; if $P < 0$, in contrast, then the developer's profit, $\Pi^{ET} = P$, is negative, in which case the developer would not operate the platform. Choosing a zero stake, $N = 0$, also maximizes the value of dividends in the token price P, which helps facilitate subsidizing the platform through a token price discount.

Consequently, if $A \geq A_*^{FB} \equiv \log \kappa - \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\epsilon^{-1}$, then the optimal policy of the developer is to take a zero stake, $N = 0$, charge 100% transaction fees, and a token price equal to the total social surplus of the platform, $P = e^{A + \frac{1}{2}\left((1-\eta_c)^2 + \eta_c^2\right)\tau_\epsilon^{-1}} - \kappa$. Consequently, users follow a cutoff strategy at $t = 1$ as conjectured, albeit a trivial one in which all users participate (i.e., $A_i \geq -\infty$).

We now return to our assumption that users will vote by majority for 100% transaction fees at $t = 2$. It is straightforward to see that users at $t = 2$ will also follow a cutoff policy in voting for transaction fees. Those with relatively high endowments, A_i, will not want their endowment taxed $\delta_T U_{i,2}(A_i)$ to receive a smaller dividend, $\delta_T \int_{\hat{A}_{ET}}^{\infty} U_{i,2} \phi\left(\sqrt{\tau_\epsilon}(A - A_i)\right) di$, and consequently vote for zero transaction fees. In contrast, those with low endowments would vote for the net subsidy the dividend provides. Consequently, those whose endowment is such that $A_i > \hat{A}^1_{ET}$ will vote for zero transaction fees while those with $A_i \leq \hat{A}^1_{ET}$ will vote for a transaction fee such that the marginal user is indifferent, or

$$U_{i,2}\left(\hat{A}^1_{ET}\right) = \delta_T \frac{\int_{\hat{A}_{ET}}^{\infty} U_{i,2}\phi\left(\sqrt{\tau_\epsilon}\left(A - A_i\right)\right) di}{N + \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{ET}\right)\right)} + \left(1 - \delta_T\right) U_{i,2}\left(\hat{A}^1_{ET}\right),$$

from which follows that, substituting with (18), (19), and $N = 0$,

$$\exp\left(\left(1 - \eta_c\right)\hat{A}^1_{ET}\right) = E\left[\exp\left(\left(1 - \eta_c\right) A_i\right) \middle| A_i \geq \hat{A}_{ET}\right], \tag{40}$$

which uniquely determines the voting cutoff $\hat{A}^1_{ET}$. It is then trivial to see that the bloc that votes for transaction fees will vote to maintain 100% transaction fees, or $\delta_T = 1$. By Jensen's Inequality, (40) implies that $\hat{A}^1_{ET} \geq E\left[A_i \middle| A_i \geq \hat{A}_{ET}\right]$, and consequently the vote for maintaining 100% transaction fees always passes by majority.

If instead $A < A^{FB}_*$, then the developer cannot achieve the first-best equilibrium, and not all users participate. Notice that, when $A = A^{FB}_*$, the developer earns zero profit, that is, $\Pi^{ET} = P = 0$. As the profit on the platform, by the Envelope Theorem, is increasing in the platform fundamental, A, it follows that the developer's profit is (weakly) negative when $A \leq A^{FB}_*$, and the developer should shutter the platform.

Taken together, when the developer operates the platform, it achieves the first-best equilibrium and extracts the full social surplus, and consequently obtaining the maximum revenue, from the platform.

B.5.2 The Subversion Equilibrium

We now return to the issue of subversion by the controlling individual or group at $t = 2$. We first consider the case in which the developer does not retain a block of tokens and instead users own all of the tokens. It is easy to see that in this case none of the users would vote to take the subversive action because the action hurts every user by γ and cannot generate a higher payoff to compensate the user.

Then, we consider the case that the developer retains a block of tokens. It is clear that all users will vote against subverting the platform because they lose not only half their dividend from transaction fees but also the per-user cost of subversion, γ; as such, the developer must have at least a 50% stake to successfully subvert the platform.

Notice that the developer will subvert the platform at $t = 2$ if it has a stake of at least 50% and if the dividend per token is higher with subversion than from transaction fees

$$\frac{\gamma\Phi\left(-z^{ET}_{SV}\right)}{N + \Phi\left(-z^{ET}_{SV}\right)} \geq \frac{\delta^{SV}_T U}{N + \Phi\left(-z^{ET}_{SV}\right)},$$

where $z_{SV}^{ET} = \sqrt{\tau_\varepsilon}\left(\hat{A}_{SV}^{ET} - A\right)$ is the normalized cutoff with subversion, which reduces to whether γ is larger than the average transaction fee

$$\gamma \geq \frac{\delta_T^{SV} U}{\Phi\left(-z_{SV}^{ET}\right)}.$$

Analogous to (37), the marginal user's indifference condition with rational expectations, in anticipation of the subversion at $t = 2$, is given by

$$\left(1 - \delta_T^{SV}\right) \frac{1}{2} e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z_{SV}^{ET} + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{ET}\right) = \kappa + \gamma + P - \delta_T^{SV} \frac{\frac{1}{2}U + \gamma\Phi\left(-z_{SV}^{ET}\right)}{N + \Phi\left(-z_{SV}^{ET}\right)}, \tag{41}$$

where the key differences are the cost to each user from subversion γ and the modified dividend, which is the revenue from subversion at $t = 2$. We define

$$p_{ET}^{SV} \equiv P + \gamma - \delta_T^{SV} \frac{\frac{1}{2}U + \gamma\Phi\left(-z^{ET}\right)}{N + \Phi\left(-z^{ET}\right)}.$$

Then (41) can be rewritten as

$$\left(1 - \delta_T^{SV}\right) \frac{1}{2} e^{(1-\eta_c)\tau_\varepsilon^{-1/2} z_{SV}^{ET} + A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{ET}\right) = \kappa + p_{ET}^{SV}, \tag{42}$$

and the objective of the developer (9) when there is subversion is

$$\Pi_{SV}^{ET} = \max_{\delta_T, p_{ET}^{SV}, N} p_{ET}^{SV} \Phi\left(-z_{SV}^{ET}\right) + \delta_T^{SV} \frac{1}{2} U - \chi N, \tag{43}$$

subject to the indifference condition of the marginal user, (42).

Comparing (42) to (38), it is clear that users require more subsidization (a lower fixed fee p_{ET}^{SV} than p_{ET}) and a lower transaction fee (lower δ_T^{SV} than δ_T) to achieve the same level of participation because users only receive half their transaction benefit when there is subversion. In addition, the developer's profit (43) is strictly lower than (39) for the fixed fee ($p_{ET}^{SV} = p_{ET}$) and transaction fee ($\delta_T^{SV} = \delta_T$). This is because users require a discount to the token price that completely offsets the revenue extracted from subversion. As such, the developer earns less revenue for a given level of participation in the presence of subversion and would prefer not to subvert. It can commit to this by retaining a stake N smaller than 50% of outstanding tokens. As the optimal stake without subversion is zero, the developer will choose $N = 0$ to pre-commit to not subverting the platform at $t = 2$.

B.6 Proof of Proposition 8

B.6.1 The Developer

We again assume users follow a cutoff participation strategy and that the cutoff endowment of the marginal investor is $\hat{A}_I^{ET}$. The developer takes the optimal policies of the investor as given while internalizing the indifference condition for the marginal investor's participation, which is the analogue of (34):

$$\begin{aligned} P \;=\;& \frac{\frac{1}{2}\delta_T U + \frac{1}{2}\left(1-s_I\right)\delta_T U + s_I\gamma\Phi\left(-z_I^{ET}\right)}{n+N+\Phi\left(-z_I^{ET}\right)} - \kappa - s_I\gamma \\ &+ \left(1-\delta_T\right)\left(1-\frac{s_I}{2}\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z_I^{ET}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_I^{ET}\right), \end{aligned} \tag{44}$$

where the last term is the marginal user's transaction benefit. This equation implies a mapping between the token price and the marginal user z_I^{ET}. We define

$$P \equiv \frac{\frac{1}{2}\delta_T U + \left(1-s_I\right)\frac{1}{2}\delta_T U + s_I\gamma\Phi\left(-z_I^{ET}\right)}{n+N+\Phi\left(-z_I^{ET}\right)} + p_I^{ET} - s_I\gamma, \tag{45}$$

where p_I^{ET} is a residual component unrelated to the token cash flow. As the developer sets the token price, one may interpret p_I^{ET} as the markup charged by the developer. Then, (44) implies that p_I^{ET} is the marginal user's transaction benefit net of the participation cost:

$$p_I^{ET} = \left(1-\delta_T\right)\left(1-\frac{s_I}{2}\right)e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z_I^{ET}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_I^{ET}\right) - \kappa. \tag{46}$$

Thus, the objective of the developer reduces to

$$\Pi_I^{ET} = \max_{\delta_T,N,p_I^{ET}} p_I^{ET}\left(n+\Phi\left(-z_{SV}^{ET}\right)\right) + \delta_T\frac{1}{2}U + \left(1-s_I\right)\delta_T\frac{1}{2}U - s_I\gamma n - \chi N, \tag{47}$$

taking n and s_I as given. In particular, n is given by (46). Recall from the proof of Proposition 7 that the developer's revenue is strictly lower when there is subversion, that is, $s_I = 1$. By similar arguments to those in that proof, the developer retains a zero stake, $N = 0$, to avoid the proportional cost, χN, and to pre-commit not to subvert the platform itself.

Similar to the proof of Proposition 4, we can apply the implicit function theorem to (46) to find that

$$\frac{dz_I^{ET}}{d\delta_T} = \left(1-\frac{s_I}{2}\right)E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right]\frac{dz_I^{ET}}{dp_I^{ET}},$$

where $E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right]$ is the total transaction surplus of the marginal user, and express the first order condition for the optimal choice of p_I^{ET} as

$$\frac{n}{\Phi\left(-z_I^{ET}\right)} + 1 - \frac{U/\Phi\left(-z_I^{ET}\right)}{E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right]} \leq 0,\ (=\ if\ P > -\alpha\kappa) \tag{48}$$

and for δ_T as

$$\left(1-\frac{s_I}{2}\right)U + \left(\left(1-\frac{s_I}{2}\right)\delta_T\frac{dU}{dz_I^{ET}} - p_I^{ET}\phi\left(-z_I^{ET}\right)\right)\frac{dz_I^{ET}}{d\delta_T} = 0. \tag{49}$$

Without the investor (i.e., $n = 0$), because $U/\Phi\left(-z_I^{ET}\right) > E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right]$ the developer would choose the maximum subsidy and, as in Proposition 7, the developer would achieve the first-best outcome. The presence of the investor even without subversion, however, precludes the first-best subsidy, because the developer does not want to subsidize the investor (a less negative p_I^{ET}), and this reduces user participation. In addition, because p_I^{ET} is less negative and $\frac{dz_I^{ET}}{d\delta_T} > 0$, from (49) it also lowers the optimal transaction fee, δ_T. Because of the lower δ_T and user participation and a positive n, the average platform dividend $\delta_T U/\left(n + \Phi\left(-z_I^{ET}\right)\right)$ is also lower. As a result, the developer's revenue, the token price from (45), and user participation are all lower in the presence of the investor. As subversion further reduces developer revenue and user participation, these issues are exacerbated when the investor subverts the platform.

B.6.2 The Investor

The investor takes the token price, which the developer sets, as given. Working backward, if $n \geq \Phi\left(-z_I^{ET}\right)$, the investor has a large enough stake to subvert the platform at $t = 2$, and will do so if the dividend per token under subversion is higher than with transaction fees, or $s_I = 1$ when $\gamma\Phi\left(-z_I^{ET}\right) > \frac{1}{2}\delta_T U$.

We now consider the optimal stake of the investor, n, at $t = 1$. From the FOC of (10) for n when $N = 0$, the investor's optimal stake is

$$\frac{n}{\Phi\left(-z_I^{ET}\right)} \geq \sqrt{\frac{\frac{1}{2}\delta_T U + (1 - s_I)\frac{1}{2}\delta_T U + s_I\gamma\Phi\left(-z_I^{ET}\right)}{P\Phi\left(-z_I^{ET}\right)}} - 1, \ (= \text{ if } n > 0), \tag{50}$$

where $z_I^{ET} = \sqrt{\tau_\varepsilon}\left(\hat{A}_I^{ET} - A\right)$, and U is the total transaction surplus given in (19). Suppose $n = 0$. Then substituting with (45), (50) becomes

$$\frac{n}{\Phi\left(-z_I^{ET}\right)} \geq \sqrt{1 + \frac{s_I\gamma - p_I^{ET}}{P}} - 1, \ (= \text{ if } n > 0).$$

As $s_I\gamma \geq 0$ and the optimal p_I^{ET} is negative from (48) when $n = 0$, it follows that $\sqrt{1 + \frac{s_I\gamma - p_I^{ET}}{P}} > 1$, and $n > 0$. Consequently, it must be the case that $n > 0$.

It then follows that the optimal policy of the investor is unique and, because the investor's program is concave in n, the investor earns a positive profit from buying tokens.

B.6.3 Subversion

Suppose that there is subversion by the investor. This requires that $n \geq \Phi\left(-z_I^{ET}\right)$ and $\gamma\Phi\left(-z_I^{ET}\right) > \frac{1}{2}\delta_T U$ so that $s_I = 1$. Then, from (50) this imposes that

$$P < \frac{1}{8}\frac{\delta_T U}{\Phi\left(-z_I^{ET}\right)} + \frac{\gamma}{4}, \tag{51}$$

and substituting in (51) with our functional form for P, this implies

$$\frac{\frac{1}{2}\delta_T U + \gamma\Phi\left(-z_I^{ET}\right)}{n + \Phi\left(-z_I^{ET}\right)} + p_I^{ET} - \gamma < \frac{1}{8}\frac{\delta_T U}{\Phi\left(-z_I^{ET}\right)} + \frac{\gamma}{4},$$

which, because $n \geq \Phi\left(-z_I^{ET}\right)$, is satisfied if

$$p_I^{ET} < \frac{3}{4}\gamma - \frac{1}{8}\frac{\delta_T U}{\Phi\left(-z_I^{ET}\right)}. \tag{52}$$

Substituting p_I^{ET} with (46) and the definition of $E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right]$ into (52), we arrive at the sufficient condition:

$$\left(1-\delta_T\right) E\left[U|\mathcal{I}_i, A_i = \hat{A}_I^{ET}\right] < \frac{3}{2}\gamma + 2\kappa - \frac{1}{4}\frac{\delta_T U}{\Phi\left(-z_I^{ET}\right)}. \tag{53}$$

By the envelope theorem, average transaction fees $\frac{\delta_T U}{\Phi\left(-z_I^{ET}\right)}$ are increasing in the platform fundamental, A, from which follows $\gamma\Phi\left(-z_I^{ET}\right) > \frac{1}{2}\delta_T U$ is satisfied when A is sufficiently low. Similarly, the left-hand side of (53) is increasing in A while the right-hand side is decreasing in A; the condition is therefore slackened when A is low.

It follows that subversion occurs when the platform fundamental, A, is sufficiently weak.

Online Appendix of "Decentralization Through Tokenization"

Michael Sockin and Wei Xiong

In this online appendix, we provide proofs of propositions that are omitted from the main paper.

C Additional Proofs to Propositions

C.1 Proof of Proposition 3

First, we establish that the cutoff for the marginal user, z_{SV}^{E}, is decreasing with γ in the subversion equilibrium. Applying the implicit function theorem to (32), we have that

$$\frac{dz_{SV}^{E}}{d\gamma}=-\frac{\frac{\frac{\frac{\phi\left(-z_{SV}^{E}\right)}{U}e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z_{SV}^{E}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{(1-\eta_c)\tau_\varepsilon^{-1/2}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}}-1}{\frac{dLHS}{z_{SV}^{E}}},$$

where LHS is the left-hand side of (32). From the proof of Proposition 2, $\frac{dLHS}{z_{SV}^{E}}$ is positive in the lowest cutoff equilibrium. Furthermore, with some manipulation, one has that

$$\begin{aligned}
&\frac{\frac{\phi\left(-z_{SV}^{E}\right)}{U}e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z_{SV}^{E}+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}}-1\\
=\;&\frac{\frac{\phi\left(-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z_{SV}^{E}-\frac{1}{2}(1-\eta_c)^2\tau_\varepsilon^{-1}}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}}-1\\
=\;&\frac{\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}}{\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z_{SV}^{E}\right)}}-1<0.
\end{aligned}$$

Consequently, it follows that $\frac{dz_{SV}^{E}}{d\gamma}>0$.

Because z_{SV}^{E} is increasing in γ, it follows that the participation constraint for the marginal user is tightening in γ. As such, from (33), it follows that the critical A_{**}^{E} at which breakdown occurs with subversion is also increasing in γ.

Second, owner profit in the subversion equilibrium being decreasing in γ follows from the envelope condition that

$$\frac{dV}{d\gamma}=\left[\frac{1}{2}\delta\frac{\partial U}{\partial z_{SV}^{E}}-\left(\gamma-\alpha\kappa\right)\phi\left(-z_{SV}^{E}\right)\right]\frac{\partial z_{SV}^{E}}{\partial\gamma}+\Phi\left(-z_{SV}^{E}\right).$$

Applying the implicit function theorem to (26), it follows that

$$\frac{\partial z_{SV}^{E}}{\partial \gamma} = \frac{1}{\gamma} \frac{1}{\left(1-\eta_c\right) \tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}},$$

and, by using (23), we can express $\frac{\partial z_{SV}^{E}}{\partial \gamma}$ as

$$\frac{\partial z_{SV}^{E}}{\partial \gamma} = \frac{1-\delta}{\gamma} \frac{\partial z_{SV}^{E}}{\partial \delta} > 0.$$

Substituting this expression into $\frac{dV}{d\gamma}$, we arrive at

$$\frac{dV}{d\gamma} = \left[\frac{1}{2} \delta \frac{\partial U}{\partial z_{SV}^{E}} - \left(\gamma - \alpha\kappa\right) \phi\left(-z_{SV}^{E}\right)\right] \frac{\partial z_{SV}^{E}}{\partial \delta} \frac{1-\delta}{\gamma} + \Phi\left(-z_{SV}^{E}\right).$$

Substituting now the first-order necessary condition for the optimal choice of δ from (23) into $\frac{dV}{d\gamma}$, it follows that

$$\gamma \frac{dV}{d\gamma} = \gamma \Phi\left(-z_{SV}^{E}\right) - \frac{1}{2}\left(1-\delta\right) U.$$

Note that for all users that join the platform, it must be the case that

$$\frac{1}{2}\left(1-\delta\right) e^{\left(1-\eta_c\right) A_i + \eta_c A + \frac{1}{2}\eta_c^2 \tau_\varepsilon^{-1}} \Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right) \geq \left(1-\alpha\right)\kappa + \gamma,$$

which by integrating both sides against the population density of users, $\phi\left(\sqrt{\tau_\varepsilon}\left(A_i - A\right)\right)$ for $A_i \geq \hat{A}_{SV}^{E}$, we arrive at

$$\frac{1}{2}\left(1-\delta\right) U \geq \left(\left(1-\alpha\right)\kappa + \gamma\right) \Phi\left(-z_{SV}^{E}\right), \tag{54}$$

and therefore

$$\gamma \frac{dV}{d\gamma} \leq \gamma \Phi\left(-z_{SV}^{E}\right) - \left(\left(1-\alpha\right)\kappa + \gamma\right) \Phi\left(-z_{SV}^{E}\right) = -\left(1-\alpha\right)\kappa \Phi\left(-z_{SV}^{E}\right) < 0.$$

Therefore, $\frac{dV}{d\gamma} < 0$.

Finally, note that total social surplus with subversion is given by

$$U_0 = \frac{1}{2} U - \kappa \Phi\left(-z_{SV}^{E}\right),$$

since all surplus at $t = 2$ is destroyed by subversion. It is straightforward to verify that

$$\frac{2}{U} \frac{dU_0}{dz_{SV}^{E}} = \frac{2\kappa \Phi\left(-z_{SV}^{E}\right)}{U} \frac{\phi\left(-z_{SV}^{E}\right)}{\Phi\left(-z_{SV}^{E}\right)} - \frac{\phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} - \frac{\phi\left(\left(1-\eta_c\right) \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\left(1-\eta_c\right) \tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}.$$

When the social surplus is non-negative, it follows that $\frac{2\kappa\Phi\left(-z_{SV}^{E}\right)}{U} \leq 1$, and consequently

$$\frac{2}{U}\frac{dU_0}{dz_{SV}^{E}} < \frac{\phi\left(-z_{SV}^{E}\right)}{\Phi\left(-z_{SV}^{E}\right)} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} - \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z_{SV}^{E}\right)} < 0,$$

since the hazard function for the normal distribution, $\frac{\phi(-x)}{\Phi(-x)}$, is increasing in x. Consequently, when the social surplus is positive, it is increasing in user participation.

Note now from (54) that

$$\gamma\Phi\left(-z_{SV}^{E}\right) \leq \frac{1}{2}\left(1-\delta\right)U - \left(1-\alpha\right)\kappa\Phi\left(-z_{SV}^{E}\right),$$

from which it follows that

$$V = \frac{1}{2}\delta U + \left(\gamma - \alpha\kappa\right)\Phi\left(-z_{SV}^{E}\right) \leq \frac{1}{2}U - \kappa\Phi\left(-z_{SV}^{E}\right),$$

so that the owner's total profit is (weakly) less than the social surplus from the initial period. Consequently, subversion destroys the owner's profit at $t = 2$ and delivers, at best, the total surplus at date 1. Furthermore, if the social surplus is negative, then $V < 0$. Consequently, if the platform operates, it must be the case that $U_0 \geq 0$, and therefore the social surplus is decreasing in z_{SV}^{E}. As $\frac{dz_{SV}^{E}}{d\gamma} > 0$, it follows that the social surplus is also decreasing in γ.

C.2 Proof of Proposition 5

Our comparison of the two different platform funding schemes will eventually simplify to the observation that the token-based scheme represents a constrained revenue optimization (only a fixed fee) compared to the equity-based scheme. We begin with the first part of the proposition.

We begin with the case of no subversion under the equity-based scheme and compare user participation. Suppose that A is sufficiently high so that there is no subversion, $A \geq A_*^E$. We begin with user participation. We first recognize, from Proposition 2, that we can express (26) when there is no subversion as

$$e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^E + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^E\right) = \kappa + p,$$

where

$$p = \frac{\left(1-\alpha\right)\kappa}{1-\delta} - \kappa$$

is the implicit token price of participation on the platform. From Proposition 4, (8) reveals that

$$e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^T + A + \frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z^T\right) = \kappa + P.$$

Now consider a perturbation of the owner's profit on the token platform, Π^T, with respect to the participation cutoff z^T :

$$\begin{aligned}
&\frac{1}{\phi\left(-z^T\right)}\frac{d\Pi^T}{dz^T} \\
= &\frac{\Phi\left(-z^T\right)}{\phi\left(-z^T\right)}\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}\right) \\
&\cdot e^{(1-\eta_c)\tau_\varepsilon^{-1/2}z^T+A+\frac{1}{2}\eta_c^2\tau_\varepsilon^{-1}}\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)-P,
\end{aligned}$$

which at the equity-based scheme cutoff z^E where $P=p$ reduces to

$$\begin{aligned}
H\left(z^T\right) &= \frac{1-\delta}{\left(1-\alpha\right)\kappa\phi\left(-z^T\right)}\frac{dV^T}{dz^T}|_{z^T=z^E} \\
&= \frac{\Phi\left(-z^T\right)}{\phi\left(-z^T\right)}\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}\right)+\frac{\alpha-\delta}{1-\alpha},
\end{aligned}$$

where δ is given by Proposition 2. Substituting with the FOC for δ, (27), we recognize that

$$\frac{\alpha-\delta}{1-\alpha}=-1-\frac{\delta\left(\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^Y\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^Y\right)}\right)+\frac{\alpha\kappa\phi\left(-z^Y\right)}{U}}{\left(1-\alpha\right)\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^E\right)}\right)}<0$$

because $\delta>0$, we arrive at

$$\begin{aligned}
H\left(z^T\right) = &\frac{\Phi\left(-z^T\right)}{\phi\left(-z^T\right)}\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}\right)-1 \\
&-\frac{\delta\left(\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}+\frac{\phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^Y\right)}{\Phi\left((1-\eta_c)\tau_\varepsilon^{-1/2}-z^Y\right)}\right)+\frac{\alpha\kappa\phi\left(-z^Y\right)}{U}}{\left(1-\alpha\right)\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2}-\frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2}-z^T\right)}\right)}.
\end{aligned}$$

When $H>0$, then $z^T>z^E$, and participation is higher under the equity-based scheme, while when $H<0$, then $z^T<z^E$, and participation is higher under the token-based scheme. The first term of H is positive in the low cutoff equilibrium and strictly decreasing from $(\infty,0)$ for $P\geq 0$, while the third term is negative and decreasing in z^T. The LHS is then strictly decreasing in z^E from ∞ to a negative (potentially improper) limit, and there exists a unique z^{***} such that $H=0$. Furthermore, by the implicit function theorem, $\partial H/\partial A>0$ since δ, and consequently, the third term in H is decreasing in A, fixing z^T, that

$$\frac{dz^{**}}{dA}=-\frac{\partial H/\partial A}{\partial H/\partial z^T}>0.$$

Since the equilibrium z^E in Proposition 2 is decreasing in A, while z^{***} is increasing in A, it follows that there exists a critical A^{***} such that, for $A \geq A^{***}$, $z^E < z^{***}$, and consequently $H > 0$. As such, when $A \geq A^{***}$, $z^E \leq z^T$ and participation is higher under the equity-based scheme. In contrast, if $A < A^{***}$, then $z^E > z^{***}$, and $z^E > z^T$, so that participation is higher under the token-based scheme.

Therefore, when A is sufficiently high, $A \geq \max\left\{A_*^E, A^{***}\right\}$, user participation is higher under the equity-based scheme.

We next consider developer profit. Under the equity-based scheme when there is no subversion, the owner maximizes

$$\Pi^E = \sup_{\delta, c} \ \delta U + c\Phi\left(-z^E\right),$$

where U is the total transaction surplus. In contrast, under the token-based scheme the owner optimizes

$$\Pi^T = \sup_{P} \ P\Phi\left(-z^T\right).$$

Because the equity-based scheme can always choose $\delta = 0$ and $c = P$, it follows, by revealed preference, that the developer's profit must be (weakly) higher under the equity-based scheme. This inequality is strict once we recognize that the token price is equal to the transaction surplus of the marginal user minus the participation cost, while revenue scales with the total transaction surplus through the variable fee, δ.

Finally, we consider social surplus. Social surplus under the equity-based scheme without subversion and the token-based scheme are both given by

$$U_0 = U - \kappa\Phi\left(-z\right),$$

where z is z^E under the equity-based scheme and z^T under the token-based scheme. It is straightforward to see that

$$\begin{aligned}
\frac{1}{U}\frac{dU_0}{dz} &= \frac{\kappa\Phi\left(-z\right)}{U}\frac{\phi\left(-z\right)}{\Phi\left(-z\right)} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z\right)} - \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z\right)} \\
&< \frac{\phi\left(-z\right)}{\Phi\left(-z\right)} - \frac{\phi\left(\eta_c\tau_\varepsilon^{-1/2} - z\right)}{\Phi\left(\eta_c\tau_\varepsilon^{-1/2} - z\right)} - \frac{\phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z\right)}{\Phi\left(\left(1-\eta_c\right)\tau_\varepsilon^{-1/2} - z\right)} \\
&< 0,
\end{aligned}$$

since $U_0 \geq 0$ implies that $U > \kappa\Phi\left(-z^S\right)$ and the hazard function of the normal distribution $\frac{\phi(-x)}{\Phi(-x)}$ is increasing in x.

Note that $U_0 \geq 0$ under the equity-based scheme or else

$$0 > U - \kappa\Phi(-z) > \delta U - \kappa\Phi(-z) = \Pi^E,$$

and owner profits would be negative, which cannot be optimal because the owner can always choose not to launch the platform.

Similarly, integrating the participation constraint for users, (34), we also have that

$$U > (\kappa + P)\,\Phi\left(-z^T\right) > \kappa\Phi\left(-z^T\right),$$

as required. Consequently, $U_0 \geq 0$ and $\frac{dU_0}{dz} < 0$.

Because $\frac{dU_0}{dz} < 0$, the platform with higher participation has a larger social surplus. It then follows that, for $A \geq \max\left\{A_*^E, A^{***}\right\}$, the equity-based scheme also leads to a larger social surplus.

We now turn to the second part of the proposition. Notice that for $A < \max\left\{A_*^E, A^{***}\right\}$, the token-based scheme has higher user participation than the equity-based scheme without subversion. As subversion only lowers user participation from Proposition 3, it follows that user participation is higher with the token-based scheme for $A < \max\left\{A_*^E, A^{***}\right\}$.

With regard to social surplus, we recall from the arguments above that social surplus is increasing in user participation when the surplus is non-negative. From Proposition 3, social surplus is nonnegative when there is subversion, and from above it is non-negative on the token platform. As such, for $A < \max\left\{A_*^E, A^{***}\right\}$, social surplus is higher under the token-based scheme because user participation is higher than under the equity-based scheme.

Finally, we consider developer profits. Notice that the developer's profit is always higher with the equity than the token-based scheme in the absence of subversion. We therefore consider the case of subversion. From Proposition 3, developer profit is decreasing in γ. Further, the subversion threshold A_*^E is increasing in γ because being able to extract more from exploiting users makes subverting the platform more attractive. Consequently, for sufficiently large γ (that is, $\gamma > \gamma^*(A)$), $A < A_*^E$ and developer profit is higher under the token-based scheme.

C.3 Proof of Proposition 9

C.3.1 Equilibrium Without Strategic Attacks

We first consider the equilibrium when there is no strategic attack at $t = 2$. Recall that U is the total transaction surplus on the platform.

We begin with the continuation problem of validators who earn value, V_h, which solves

$$V_h = \sup_{\delta_{T,j}, e_j} \left\{ \frac{e_j}{e_j + \sum_{j' \neq j} e_{j'}} \delta_{T,j} U\left(\hat{A}_{TC}(\delta_T)\right) - \xi e_j \right\},$$

where again $U\left(\hat{A}_{TC}\left(\delta_T\right)\right) = \int_{\hat{A}_{TC}}^{\infty} U_i \phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TC}\left(\delta_T\right)\right)\right) di$ and δ_T is given in (14). The FOCs for the optimal fee and effort of each validator, $\delta_{T,j}$ and e_j, respectively, satisfy

$$\begin{aligned} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) + \frac{e_j}{e_j + \sum_{j' \neq j} e_{j'}} \delta_{T,j} \frac{\partial}{\partial \delta_T} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) &= 0, \\ \frac{\sum_{j' \neq j} e_{j'}}{\left(e_j + \sum_{j' \neq j} e_{j'}\right)^2} \delta_{T,j} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) + \frac{e_j}{e_j + \sum_{j' \neq j} e_{j'}} \delta_{T,j} \frac{\partial}{\partial \delta_T} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) \frac{\delta_{T,j} - \delta_T}{e_j + \sum_{j' \neq j} e_{j'}} - \xi &= 0. \end{aligned}$$

With some manipulation, we obtain

$$\begin{aligned} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) + \frac{e_j}{e_j + \sum_{j' \neq j} e_{j'}} \delta_{T,j} \frac{\partial}{\partial \delta_T} U\left(\hat{A}_{TC}\left(\delta_T\right)\right) &= 0, \\ \left(\delta_T - \frac{e_j}{e_j + \sum_{j' \neq j} e_{j'}} \delta_{T,j}\right) U\left(\hat{A}_{TC}\left(\delta_T\right)\right) - \xi \left(e_j + \sum_{j' \neq j} e_{j'}\right) &= 0. \end{aligned}$$

Similar to the case of utility tokens with token price P, the cutoff $\hat{A}_{TC}$ is again based on the indifference condition of the marginal user

$$\left(1 - \delta_T\right) E\left[U_i | \mathcal{I}, A_i = \hat{A}_{TC}\right] = \kappa + P,$$

although now there are transaction fees paid to validators. In a symmetric equilibrium, $\delta_{T,j} = \delta_T$ and $e_j = e$, and it follows that

$$\delta_T = -\frac{M}{\frac{\partial}{\partial \delta_T} \log U\left(\hat{A}_{TC}\left(\delta_T\right)\right)}, \tag{55}$$

$$e = \frac{M-1}{M^2} \frac{\delta_T U\left(\hat{A}_{TC}\left(\delta_T\right)\right)}{\xi}. \tag{56}$$

Notice that as $\delta_T \to 1$, $\hat{A}_{TC}\left(\delta_T\right) \to \infty$ (no user participation) because users get zero benefit from the platform. As a result, the denominator of δ_T in (55) diverges to $-\infty$, which would imply that $\delta_T \to 0$. As such, δ_T has an interior solution, $\delta_T \in (0, 1)$.

The continuation utility of all validators is then

$$V_h = v_j\left(M\right) = \frac{\delta_T}{M^2} U\left(\hat{A}_{TC}\left(\delta_T\right)\right), \tag{57}$$

where $v_j\left(M\right)$ is a function of the number of validators M. From the outer optimization of (15), validators join the platform as long as $V_j \geq \eta$, from which follows that the number of validators M solves

$$M : \max\left\{m : v_j\left(m\right) \geq \eta\right\}. \tag{58}$$

As $v_j(m)$, given δ_T from (55), is decreasing in M, it follows that there is an interior choice of M.

From (56), the total effort supplied by the $M-1$ validators is

$$E_* = (M-1)\,e = \left(\frac{M-1}{M}\right)^2 \frac{\delta_T U\left(\hat{A}_{TC}(\delta_T)\right)}{\xi}. \tag{59}$$

Provided that the Hessian of the optimization program for validators is globally negative definite at a symmetric equilibrium, the optimal policies recovered from the FOCs are sufficient and constitute a symmetric Nash equilibrium.

Finally, we consider the incentives for the rogue validator to deviate from honest validating and engage in a strategic attack. Taking the strategies of the other $M-1$ validators as given, the rogue validator does not find it profitable to attack the blockchain if the net revenue from the attack is less than the net benefit from honest validating, $v_j(M)$, or

$$\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A-\hat{A}_{TC}\right)\right) - \xi\,(M-1)\,e \leq \frac{\delta_T}{M^2} U\left(\hat{A}_{TC}(\delta_T)\right). \tag{60}$$

Given (59), we can rewrite (60) as

$$\gamma \leq \frac{(M-1)^2+1}{M}\frac{\delta_T}{M} E\left[U_i(A_i)\,\middle|\,A_i \geq \hat{A}_{TC}(\delta_T)\right], \tag{61}$$

where $\frac{\delta_T}{M} E\left[U_i(A_i)\,\middle|\,A_i \geq \hat{A}_{TC}\right]$ is the average transaction fee. Notice that the average transaction fee $\frac{1}{M}\delta_T E\left[U_{i,2}(A_i)\,\middle|\,A_i \geq \hat{A}_{TC}\right]$ is increasing in the platform fundamental, A. Similarly, because $\frac{(M-1)^2+1}{M}$ is increasing in M for $M \geq 2$ and M is, in turn, increasing in A, it follows that the right-hand side of (61) is increasing in A. Consequently, by continuity, there exists a critical level of the platform fundamental, A^*_{TC}, such that the rogue validator does not have an incentive to deviate and attack the blockchain if $A \geq A^*_{TC}$.

As such, if $A \geq A^*_{TC}$, it is a Cournot-Nash equilibrium for all validators to choose their optimal policies according to (55), (56), and (58), and the rogue validator does attack the blockchain.

C.3.2 Equilibrium With Strategic Attacks

We now construct a Nash equilibrium with attack, which may occur when $A < A^*_{TC}$. In this equilibrium, the rogue validator attacks, and, if the attack is successful, the other $M-1$ validate to collect transaction fees only at $t=1$. We will search for an equilibrium in which the attacking validator and the honest validators follow mixed strategies over a potential continuum of effort levels and transaction fees. Let the user cutoff in this equilibrium be $\hat{A}_{TCS}$, for which we will later derive the identifying indifference condition.

For a given level of transaction fee δ_{TS} charged by all honest validators, let $1-\pi_a\left(e_a \mid \delta_{TS}\right)$ be the CDF that the rogue validator exerts effort less than or equal to $e_a=\sum_{j=1}^{M-1} e_{j'}$, with support $e_a \in \left[\underline{e}_a, \bar{e}_a\right]$. Similarly, let $1-\pi_h\left(e \mid \delta_{TS}\right)$ be the CDF that all honest validators exert a symmetric effort less than or equal to e with support $e_a \in \left[\underline{e}_h, \bar{e}_h\right]$.We will derive the effort intervals and show that all honest validators indeed choose the same level of transaction fee, δ_{TS}, and find it optimal to follow the coordinated effort level.

We proceed with the derivation of the equilibrium in four steps.

Step 1: Optimal Trasaction Fees and Effort of Honest Validators

When the rogue validator engages in a strategic attack, it does not participate in honest validation of transactions at either date. We again begin with the continuation problem of validators who earn value, V_h:

$$V_h=E\left[\sup_{\delta_{T,j}, e_j}\left\{\left(\frac{1}{2}+\frac{1-\pi_a}{2}\right) \frac{e_j}{e_j+\sum_{j' \neq j} e_{j'}} \delta_{T,j} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)-\xi e_j\right\}\left(1-\pi_h\left(e_j'\right)\right)\right],$$

where $1-\pi_a=1-\pi_a\left(\sum_{j=1}^{M-1} e_{j'}\right)$ is the probability the strategic attack fails, given the total effort of the honest validators $\sum_{j=1}^{M-1} e_{j'}$. The FOCs for the optimal transaction fee and effort, $\delta_{T,j}$ and e_j, respectively, are then

$$\begin{aligned} 0 &= 1+\frac{e_j}{e_j+\sum_{j' \neq j} e_{j'}} \delta_{T,j}\left(\frac{\partial}{\partial \delta_{TS}} \log U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)-\frac{\partial \log \pi_a}{\partial \delta_{TS}}\right), \quad (62)\\ 0 &= \frac{2-\pi_a}{2}\left(\delta_{TS}-\frac{e_j}{e_j+\sum_{j' \neq j} e_{j'}} \delta_{T,j}\right) U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)-\xi\left(e_j+\sum_{j' \neq j} e_{j'}\right) \\ & \quad -\frac{1}{2} \frac{\partial \pi_a}{\partial e_j} e_j \delta_{T,j} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right), \quad (63)\end{aligned}$$

where $U\left(\hat{A}_{TCS}\right)$ is the total transaction surplus when the user cutoff is $\hat{A}_{TCS}$. As the rogue validator mixes over a continuum of efforts with an atomistic probability on the interior of $\pi_a(e)$, $\pi_a(e)$ is differentiable so that a small change in effort by one honest validator does not change whether a strategic attack is successful. Imposing symmetry, that is, $\delta_{T,j}=\delta_{TS}$ and $e_j=e$, we can then rewrite the FOCs (62) and (63) as

$$1+\frac{1}{M-1} \delta_{TS}\left(\frac{\partial}{\partial \delta_{TS}} \log U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)-\frac{1}{2-\pi_a} \frac{\partial \pi_a}{\partial \delta_{TS}}\right) = 0, \quad (64)$$

$$\left(\frac{2-\pi_a}{2} \frac{M-2}{M-1}-\frac{1}{2} e \frac{\partial \pi_a}{\partial e_j}\right) \delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)-\xi(M-1) e = 0. \quad (65)$$

In addition, we require that honest validators are indifferent about mixing over different effort levels, $\left(\delta_{T,j}, e_j\right)$. Imposing symmetry among honest validators gives that $V_h^S\left(\delta_{TS}, e\right)=$

$V_h = v_h(A)$ for a certain function $v_h(A)$, which is independent of their effort:

$$V_h^S(\delta_{TS}, e) = \frac{2-\pi_a}{2}\frac{\delta_{TS}}{M-1}U\left(\hat{A}_{TCS}(\delta_{TS})\right) - \xi e = v_h(A). \tag{66}$$

This holds true if π_a satisfies

$$\pi_a = 2 - \frac{2}{\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right)}\left((M-1)v_h(A) + \xi e_a\right), \tag{67}$$

where again $e_a = (M-1)e$ for the rogue validator to overrun the honest validators.

Let us conjecture that $\frac{\partial \pi_a}{\partial \delta_{TS}} = 0$, so that $\pi_a = \pi_a(e_a)$. Then $\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right)$ is already optimized with respect to $\delta_{T,j}$ from the first order condition, and consequently it follows that $\frac{\partial \pi_a}{\partial \delta_{TS}} = 0$ by the envelope theorem. The optimal $\delta_{TS} = \delta_{T,j}$ from (64) is consequently the same as in the case without a strategic attack (when $e_j = e$)

$$\delta_{TS} = -\frac{M-1}{\frac{\partial}{\partial \delta_{TS}}\log U\left(\hat{A}_{TC}(\delta_{TS})\right)},$$

regardless of the effort that either honest validators or the rogue validator exert, which confirms the conjecture.

Imposing symmetry (i.e., $\delta_{T,j} = \delta_T$ and $e_j = e$) and substituting (67) into (65) lead to

$$\begin{aligned}&\left(\frac{2-\pi_a}{2}\left(\delta_{TS} - \frac{e_j}{e_j + \sum_{j'\neq j} e_{j'}}\delta_{T,j}\right) - \frac{1}{2}e_j\frac{\partial \pi_a}{\partial e_j}\delta_{T,j}\right)U\left(\hat{A}_{TC}(\delta_T)\right) - \xi\left(e_j + \sum_{j'\neq j} e_{j'}\right)\\ = \;& (M-2)v_h(A),\end{aligned}$$

which implies that honest validators are indifferent to any level of effort if $v_h(A) = 0$. Consequently, if $v_h(A) = 0$ in (67), then

$$\pi_a = 2 - \frac{2\xi e_a}{\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right)}, \tag{68}$$

and honest validators are indifferent to mixing over any level of effort.

We next derive the support of honest validator effort. Notice that if $\pi_a = 0$, then validators prevent a strategic attack with probability 1, so honest validators do not need to supply higher effort. Imposing $\pi_a > 0$ delivers the upper bound on rogue validator effort:

$$e_a \leq \bar{e}_a = \frac{\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right)}{\xi}.$$

Similarly, because $\pi_a \leq 1$, this imposes the lower limit on rogue validator effort:

$$e_a \geq \underline{e}_a = \frac{\delta_{TS} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)}{2\xi} = \frac{1}{2}\bar{e}_a.$$

Taken together, honest validators earn continuation utility $V_h^S = 0$, and the rogue validator mixes between effort levels $e_a \in [\underline{e}_a, \bar{e}_a]$ with CDF $1 - \pi_a(e_a)$.

Step 2: The Rogue Validator

The rogue validator maximizes the objective

$$V^a = \sup_{e_a} \left(1 - \pi_h\left(\frac{e_a}{M-1}\right)\right) \gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right) - \xi e_a,$$

where $1 - \pi_h\left(\frac{e_a}{M-1}\right)$ is the probability that the attacks succeeds, that is, honest validators exert collective effort less than e_a.

For the attacking validator to be indifferent to mixing, we require that its net profit be the same for all effort levels, that is, $V^a(e_a) = V^a(e_a') = v_a(A)$, or

$$\begin{aligned} & \left(1 - \pi_h\left(\frac{e_a}{M-1}\right)\right) \gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right) - \xi e_a \\ = & \left(1 - \pi_h\left(\frac{e_a'}{M-1}\right)\right) \gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right) - \xi e_a', \end{aligned}$$

from which it follows that

$$\frac{\pi_h\left(\frac{e_a'}{M-1}\right) - \pi_h\left(\frac{e_a}{M-1}\right)}{e_a' - e_a} = -\frac{\xi}{\gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)}.$$

By taking the limit as $e' \to e$, we obtain

$$\frac{d\pi_h(e)}{de} = -\frac{\xi(M-1)}{\gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)},$$

which, because $V^a(e_a) = v_a(A)$, has a solution:

$$\pi_h(e) = 1 - \frac{v_a(A) + \xi(M-1)e}{\gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)}. \tag{69}$$

For the rogue validator to be willing to mix with these probabilities, given $\pi_h(e)$, then playing $e_a = (M-1)e$ must be the best response. Notice that the FONC for the optimal e_a is

$$-\frac{d\pi_v\left(\frac{e_a}{M-1}\right)}{de_a} \gamma \Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right) - \xi = \xi - \xi = 0,$$

which confirms that exerting effort e_a is also a best-response when honest validators mix with probability function $\pi_h(e)$.

Notice from our solution for $\pi_a(e_a)$ that the rogue validator will never supply effort above $\bar{e}_a$. As such, honest validators will never supply effort above $\bar{e}_h = \frac{\bar{e}_a}{M-1}$, and that $\pi_v(\bar{e}_h) = 0$. Imposing $\pi_v(\bar{e}_h) = 0$ in (69) implies that

$$v_a(A) = \gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}(\delta_{TS})\right)\right) - \delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right), \tag{70}$$

and substituting (70) into (69), (69) reduces to

$$\pi_h(e) = \frac{\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right) - \xi(M-1)e}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}(\delta_{TS})\right)\right)}. \tag{71}$$

As the minimum effort the rogue validator will exert is $\frac{1}{2}\bar{e}_a$, it follows that $\underline{e}_h = \frac{1}{2}\frac{\bar{e}_a}{M-1}$, and there will be a masspoint at $\underline{e}_h$ with $\pi_0(\underline{e}_h) = \frac{\delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right)}{2\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A-\hat{A}_{TCS}(\delta_{TS})\right)\right)}$.

Given the mixing conditions and (70), the continuation utility for the rogue validator is

$$V_a^S = \gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}(\delta_{TS})\right)\right) - \delta_{TS}U\left(\hat{A}_{TCS}(\delta_{TS})\right), \tag{72}$$

which is non-negative assuming that a strategic attack at any level is expected to be profitable. Consequently, the rogue validator earns continuation utility V_a^S, and honest validators mix between effort levels $e_h \in \left[\frac{1}{2}\bar{e}_h, \bar{e}_h\right]$ with CDF $1 - \pi_h(e)$.

Step 3: The Number of Miners and Indifferent Condition of Marginal Users

In deciding whether to join the platform as a validator, each potential validator faces two possibilities: with probability λ, one of the validators becomes rogue and induces a risk of a strategic attack with the honest validators receiving a continuation utility of $V_h = 0$, while the rogue validator receiving V_a^S given in (72); with probability $1-\lambda$, there is no rogue validator and the equilibrium is the same as derived in Case 1 with all validators receiving V_h given in (57). The requirement that the expected continuation utility from validating exceed the fixed cost of joining the platform then imposes

$$M : \max\{m : w_j(m) \geq \eta\},$$

where given V_h and V_a^S in (66) and (72), respectively,

$$w_j(m) = (1-\lambda)V_h + \lambda\frac{1}{m}V_a^S, \tag{73}$$

which determines the number of validators that initially join the platform.

We next derive the indifference condition of the marginal user that determines the participation cutoff $\hat{A}_{TCS}$. Our characterization of the mixed strategy attack equilibrium implies an unconditional probability of a successful attack p_S that is given by

$$\begin{aligned}
p_S &= \pi_h\left(\underline{e}_h\right) + \int_{\underline{e}_h}^{\bar{e}_h} \pi_a\left(\left(M-1\right)e\right) d\left(1-\pi_h\left(e\right)\right) \\
&= \frac{\delta_{TS} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)}{2\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A-\hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)} \\
&\quad + \frac{2\xi\left(1-M\right)}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A-\hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)} \int_{\underline{e}_h}^{\bar{e}_h} \left(1-\frac{\xi\left(M-1\right)e}{\delta_{TS}U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)}\right) de \\
&= \frac{3}{4}\frac{\delta_{TS} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A-\hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)}. \qquad (74)
\end{aligned}$$

Notice that $p_S \in (0,1)$ provided that selling user data is more profitable than total transaction fees.

Given that users anticipate the mixing behavior of the validators, the indifference condition of the marginal user is then given by

$$\left(1-\delta_{TS}\right)\frac{2-p_S}{2}E\left[U_i|\mathcal{I}, A_i = \hat{A}_{TC}\right] = \kappa + p_S\gamma + P. \qquad (75)$$

Step 4: Optimality and Feasibility of a Strategic Attack

We next establish conditions under which a strategic attack by the rogue validator is more profitable than deviating and being an honest validator, that is, $V_a^S \geq V_h^{S\prime}$, where $V_h^{S\prime}$ is the continuation utility if there are instead M honest validators, taking the optimal policies of the other $M-1$ validators as given. The deviating rogue validator solves for a given level of effort supplied by the $M-1$ honest validators:

$$V_h^{S\prime}\left(e\right) = \sup_{\delta_{T,a}, e_a}\left\{\frac{e_a}{e_a+\left(M-1\right)e}\delta_{T,a}U\left(\hat{A}_{TC}\left(\delta_{TS}^{\prime}\right)\right) - \xi e_a\right\},$$

taking as given the symmetric effort and transaction fees, e and δ_{TS}, of the other $M-1$ validators. In the above, $\delta_{TS}^{\prime}$ is the actual transaction fee given that the rogue validator may choose a different one from the other $M-1$ validators, and $\delta_{T,a}$ and e_a are the best responses of the rogue validator when the honest validators play $\left(\delta_{TS}, e\right)$. From the objective, the rogue validator internalizes that there is zero probability of a strategic attack. Users now join following a cutoff strategy with cutoff endowment $\hat{A}_{TC}\left(\delta_{TS}^{\prime}\right)$, as they are competitive and anticipate the deviation by the rogue validator.

With some manipulation, the FOCs for the optimal transaction fee $\delta_{T,a}$ and effort e_a imply that

$$\begin{aligned}
\delta_{T,a} &= -\frac{e_a + (M-1)\,e}{e_a} \frac{1}{\frac{\partial}{\partial \delta'_{TS}} \log U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right)}, \\
e_a &= \frac{1}{\xi}\left(\delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right) + \frac{1}{\frac{\partial}{\partial \delta_{TS}} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right)}\right) - (M-1)\,e.
\end{aligned}$$

Substituting these optimal policies into the maximized objective function and taking expectations over the effort of the other honest validators, it follows that

$$\begin{aligned}
V_h^{S\prime} &= \xi\,(M-1)\left(\underline{e}_h \pi_h\left(\underline{e}_h\right) + \int_{\underline{e}_h}^{\bar{e}_h} e d\left(1 - \pi_h(e)\right)\right) - \delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right) \\
&= \frac{\left(\delta_{TS} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)^2}{4\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)} + \frac{\xi^2\,(M-1)^2}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)} \int_{\underline{e}_h}^{\bar{e}_h} ede - \delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right) \\
&= \frac{5}{8}\frac{\left(\delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)\right)^2}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)} - \delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right),
\end{aligned}$$

where we recognize that the mixing CDF $1 - \pi_h(e)$ and the maximum effort level $\bar{e}_h$ are their equilibrium values. It then follows that

$$\begin{aligned}
V_a - V_h^{S\prime} &= \gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right) - \delta_{TS} U\left(\hat{A}_{TCS}\left(\delta_{TS}\right)\right) \\
&\quad + \delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right) - \frac{5}{8}\frac{\left(\delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)\right)^2}{\gamma\Phi\left(\sqrt{\tau_\epsilon}\left(A - \hat{A}_{TCS}\left(\delta_{TS}\right)\right)\right)}. \qquad (76)
\end{aligned}$$

For (76) to be non-negative implies that

$$\begin{aligned}
\gamma &\geq \left(1 - \frac{\delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right)}{\delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)}\right) \delta_{TS} E\left[U_i\left(A_i\right) \middle| A_i \geq \hat{A}_{TCS}\left(\delta_{TS}\right)\right] \qquad (77) \\
&\quad + \frac{5}{8\gamma}\left(\delta_{TS} E\left[U_i\left(A_i\right) \middle| A_i \geq \hat{A}_{TCS}\left(\delta_{TS}\right)\right]\right)^2.
\end{aligned}$$

Notice that the total transaction fees are higher when the rogue validator deviates, or $\delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right) \geq \delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)$, because there is no strategic attack and because more users join the platform in anticipation of no attack (i.e., $\hat{A}_{TCS}\left(\delta_{TS}\right) \geq \hat{A}_{TCS}\left(\delta'_{TS}\right)$). This implies that $1 < \frac{\delta'_{TS} U\left(\hat{A}_{TC}\left(\delta'_{TS}\right)\right)}{\delta_{TS} U\left(\hat{A}_{TC}\left(\delta_{TS}\right)\right)}$. As a result, it is sufficient that

$$\gamma \geq \frac{5}{8\gamma}\left(\delta_{TS} E\left[U_i\left(A_i\right) \middle| A_i \geq \hat{A}_{TCS}\left(\delta_{TS}\right)\right]\right)^2,$$

or

$$\gamma \geq \sqrt{\frac{5}{8}}\delta_{TS}E\left[U_i\left(A_i\right)\middle|A_i \geq \hat{A}_{TCS}\left(\delta_{TS}\right)\right], \tag{78}$$

for (77) to be satisfied.

In addition, feasibility of a strategic attack equilibrium requires that $p_S \in (0,1)$, or else the equilibrium is degenerate. That $p_S > 0$ is trivial. Given our expression for p_S from (74), this also imposes that

$$\gamma \geq \frac{3}{4}\delta_{TS}E\left[U_i\left(A_i\right)\middle|A_i \geq \hat{A}_{TCS}\left(\delta_{TS}\right)\right]. \tag{79}$$

Because $\sqrt{\frac{5}{8}} > \frac{3}{4}$, it follows that it is sufficient that (77) is satisfied for (79) to be satisfied. Consequently, (77) is the binding constraint.

As the right-hand side of (77) is the average transaction fee, which is increasing in A by the envelope theorem, it follows that a mixed strategic attack equilibrium exists when A is sufficiently low. By continuity, there exists a critical A, A^*_{TCS}, such that a mixing strategic attack equilibrium exists if $A \leq A^*_{TCS}$. It then follows that the platform is susceptible to an attack when A is low and the platform is sufficiently weak.