Market Design with Blockchain Technology[*]

Katya Malinova[†] Andreas Park[‡]

First Version: February 2, 2016

This Version: July 26, 2017

Abstract

Blockchain or, more generally, distributed ledger technology allows to create a decentralized digital ledger of transactions and to share it among a network of computers. In this paper, we argue that the implementation of this technology in financial markets offers investors new options for managing the degree of transparency of their holdings and their trading intentions. We first identify two intrinsic features of a distributed ledger that impact the availability of these new options, namely the mapping between identifiers and end-investors and the degree of transparency of the ledger, and we then examine how the implementation design of these critical features affects investor trading behavior, trading costs, and investor welfare, in a theoretical model of intermediated and peer-to-peer trading. The most transparent setting yields the highest investor welfare, despite the risk of front-running. In the absence of full transparency, welfare is weakly higher if investors are allowed to split their holdings among many identifiers.

[*]We thank Thierry Foucault, Andrei Kirilenko, Christine Parlour, Ryan Riordan, Vincent van Kervel, Zhou Zhong and participants at the 2nd Women in Microstructure Meeting, the 2016 EFA, the P2P Financial Systems 2016, the 2016 NFA, the 2016 Imperial College London FinTech Conference, the 2016 NBER Microstructure Meeting, the 2016 Santiago Finance Workshop, Bank of Canada, the 2017 Finance Down Under Conference, and the 2017 Cambridge Center for Alternative Finance Annual Conference for insightful comments, as well as Stephen Bain from RBC Capital Markets, Jacob Farber and Tim Swanson from R3, Jeff Coleman from Ledgerlabs, and Rodrigo Sainz from Godzillion.io for inspiring and informative discussions on the topic. An earlier version of this paper was circulated as *Market Design for Trading with Blockchain Technology*.

[†]University of Toronto, Department of Economics, `katya.malinova@utoronto.ca`.

[‡]University of Toronto Mississauga, Department of Management, Institute of Management and Innovation, and Rotman School of Management, `andreas.park@rotman.utoronto.ca`.

"Blockchain" has been the buzz in the financial world since the second half of 2015. A common thread through most of the stories in the financial press is that blockchain technology is to transactions what the internet is to information. The internet, in essence, enables the direct, peer-to-peer digital transfer of information; blockchain technology does the same for transfers of value. All asset transfers require a mechanism to change the record of ownership. At present, most such records are kept in *centralized* ledgers that can only be accessed and modified by select, highly trusted parties; examples are bank accounts or central securities depositories such as those kept by the DTCC. In contrast, blockchain technology offers a consensus protocol to change records in *distributed* ledgers that can be accessed and modified by anyone and not just trusted intermediaries.

An intrinsic feature of a distributed ledger is that ownership records and transactions are possibly visible across a wide network with multiple parties. Since the availability of this information is a design choice, in particular for the private blockchains that will likely be the backbone of worldwide financial transactions in the years to come, it is critical to understand how this information impacts economic interactions.

Market participants often prefer privacy, even when full transparency may be socially desirable. Blockchain designers may choose to implement privacy in different ways, and the implementation choice will influence the nature of peer-to-peer interactions. A conservative option is to follow the current setup of centralized ledgers and to restrict the visibility of the distributed ledger to only those who verify and record changes. Such an arrangement does not require blockchain technology, and the impact of a distributed ledger will likely be limited; for instance, the technology may lower verification costs. Blockchain technology, however, offers a native option to implement privacy by allowing users to spread their activities across numerous digital identities.[1] This option gives rise

[1] A founder of the Ethereum Blockchain describes this option in great detail; see Buterin (2016).

to novel peer-to-peer interactions, which we examine in this paper.

We study the pros and cons of different transparency designs in a theoretical model of financial market trading. Transactions are recorded on a distributed ledger, and each transaction is attributed to identifiers for the buyer and seller, respectively. The design of the ledger's transparency determines whether investors can identify the holdings of other investors. We focus on the trading decision of an investor (e.g., an institution) that has to trade a large position. Trading in our model occurs repeatedly; each period one large investor experiences a liquidity shock. The liquidity-seeking investor can trade with small investors, who are costly to find, with intermediaries, who require compensation in exchange for taking a risky inventory,[2] and with another large investor, who may front-run. To prevent front-running, the liquidity-seeking trader may need to offer the liquidity-providing trader an incentive. By construction, the welfare optimum obtains when the large traders trade exclusively with each other.

We first establish the equilibrium behavior in a fully transparent setting, which serves as a benchmark. In this setting, large investors can identify one another, and there exists an equilibrium where they trade exclusively with each other. Furthermore, incentive payments are not necessary, provided that the interactions among large traders are sufficiently frequent. We then study two settings with reduced transparency, where investors can only see the holdings of the identifiers that they own. In the first setting, the ledger is not visible to investors, and each investor has a single ID. Identifiers are able to contact one another for peer-to-peer trading, but the IDs of large investors cannot be identified. In the second setting, investors have multiple IDs in the sense of "one share – one ID"; the system is set up so that IDs that belong to a single large investor cannot be identified, and an investor's total holdings cannot be inferred. This last setting

[2]We model the intermediated market in the tradition of Biais (1993).

is conceptually closest to a privacy protection solution that is technologically feasible with current public blockchains, as described by Buterin (2016). We assume that all the contacted IDs of a large investor take the same action: they all accept the offer to trade, or they all reject the offer to trade, or the liquidity-providing investor uses all the contacted IDs to front-run.

In both opaque settings, large investors trade peer-to-peer with small investors and they also trade in the intermediated market. In the single-ID setting, large investors find each other with zero probability. In the multi-ID setting large investors find each other with positive probability, and they contact a subset of each other's IDs. In this setting, they accept each other's offers and trade with each other in equilibrium, provided front-running is not too profitable; this is the case, for instance, when the intermediated market is sufficiently liquid or when interactions among the large investors are sufficiently frequent.

Lack of full transparency reduces welfare, because traders need to pay the intermediary for absorbing a risky position and they incur costs for dealing with small investors. Aggregate welfare is lowest when large investors do not trade with each other at all. When investors spread their trading activities across numerous IDs, they have more opportunities to source a suitable liquidity provider. We conclude that the multi-ID privacy solution, which is intrinsic to blockchain technology, improves welfare relative to the traditional approach of directly restricting the ledger's visibility.

I. Related Literature

In addition to contributing to the fast-growing literature on the implications of blockchain technology for financial markets, our paper relates to several strands of the

literature in market microstructure and market design.

Literature on Blockchain Technology. The academic literature on blockchain technology is small but growing. As of March 19, 2016, SSRN listed only 37 working papers that use the term "Blockchain", as of July 24, 2017, there are 222 papers. Harvey (2015) provides an overview of Bitcoin's technology. Cong, He, and Zheng (2017) study the impact of smart contracts (native to some Blockchains) and decentralized consensus on the competitive environment, focusing on the improved contractibility and enforceability potentially delivered by smart contracts. Catalini and Gans (2016) argue that the distributed ledgers lower verification costs and networking costs and can therefore facilitate innovation. Khapko and Zoican (2017) focus on the impact of faster settlement times afforded by the blockchain and describe how settlement times affect market makers' strategies. Yermack (2017) discusses the potential implications of blockchain-based trading on corporate governance. Brummer (2015) provides an overview of the effects of technological disruption on the regulation of financial markets. We contribute by examining the economic implications of transparency and different privacy options afforded by a distributed ledger, in the context of financial market trading.

Several papers study the organization and economics of verification and mining, focusing on the public blockchains. For instance, Evans (2014) discusses concerns with regards to the verification incentives and governance systems of public decentralized ledgers, which may render these less efficient than the existing systems. Kroll, Davey, and Felten (2013) propose to study mining as a coordination game; Biais, Bisiere, Bouvard, and Casamatta (2017) formally analyze the equilibrium strategies of rational, strategic miners in a dynamic coordination game, which admits forks on the equilibrium path; they argue that mining the longest chain is in line with the proposed Bitcoin implementation

is an equilibrium, and that it is not a unique outcome.

Differently to this line of work, we focus on the "end-users" of the technology and examine the impact of blockchain design on the decisions of network members who utilize the technology to facilitate value transfers rather than to obtain payoffs from mining. While the cost of transaction verification affects the decisions of these agents, the source of these costs and the specifics of transaction verification are not critical to our results; our findings remain applicable to private distributed ledgers where verification is performed by trusted parties, similarly to the current, centralized ledger system.

Literature on Over-the-Counter Markets. Peer-to-peer trading has been extensively studied in the context of over-the-counter (OTC) markets. This literature started with Diamond (1982), Rubinstein and Wolinsky (1985), Gehrig (1993), and Yavas (1996), and it developed into a related strand on asset pricing in search-based models, e.g., Weill (2002), Duffie, Garleanu, and Pedersen (2005), Miao (2006), Vayanos and Wang (2007), Lester, Rocheteau, and Weill (2015), or Cujean and Praz (2015).

The multi-ID ownership that is native to public blockchains gives rise to new strategic considerations in peer-to-peer trading. For instance, sending two requests for quotes in a classic OTC market is synonymous with contacting two parties. In contrast, with multi-ID ownership the sender does not know whether two distinct recipient IDs belong to the same counterparty or to two different counterparties. Furthermore, an OTC dealer, upon receiving a request-for-quote typically does not know whether the sender has contacted other dealers. In contrast, a large investor who owns multiple IDs may be contacted multiple times and may therefore obtain additional insights (e.g, that the other side wants to trade a large quantity).

Our contribution is to identify the novel features of peer-to-peer interactions that

emerge when transactions are recorded on a distributed ledger, and we examine the economic impact of the relevant design choices.

Literature on Centralized vs. Decentralized Markets. Our model also touches upon the literature that compares centralized with decentralized markets. Pagano (1989) describes how the existence of multiple markets may lead, among other things, to fragmentation, where traders cluster according to the size of their desired transactions. Biais (1993) compares trading systems where quotes are collected and published centrally with fragmented, decentralized systems where deals are outcomes of bilateral negotiations.[3]

Our model implicitly combines a centralized, intermediated market with a decentralized, peer-to-peer market, and we do not study the pros and cons of either market in isolation. Instead, we assume that peer-to-peer trading, facilitated by the presence of a distributed ledger, is always available to investors, and that the intermediated market serves as an outside option and determines the peer-to-peer trading price. Our focus is on examining different decentralized, peer-to-peer arrangements that are enabled by different blockchain design choices, rather than on comparing the centralized vs. decentralized markets.

II. Model

Our model has three types of market participants: two large institutional investors, one of which is randomly hit by a liquidity shock and must trade a large quantity; a continuum of small investors that in aggregate have the capacity to absorb the institutional order; a group of risk-averse intermediaries that can absorb order flow for a fee. We allow investors to directly interact with each other, and they also have access to an

[3]See also De Frutos and Manzano (2002), or Yin (2005).

intermediated market.

The Asset has a fundamental value that is normally distributed with mean 0 and variance σ^2. Information regarding the distribution of the fundamental value is public knowledge. The asset is infinitely divisible.

Large Investors. There are two large, risk neutral investors. Each period, one of them is hit by a liquidity shock that requires them to trade a large quantity. We refer to this trader as the *liquidity demader*. To simplify the exposition, we assume that the large investor wants to buy, and we normalize the quantity to 1; the arguments are symmetric for a negative quantity. Investors discount future trading opportunities at rate $\delta < 1$. Each large investor has the capacity to absorb the other's shock without incurring a cost; and we refer to the large trader that is not hit by the liquidity shock as the *liquidity provider*.

Small Investors. There is a continuum of $1/\rho$ many small investors, who can trade unit quantities, with $\rho \leq 1/2$. Each period mass 2 of small investors are hit by liquidity shocks, mass 1 of them want to buy and mass 1 want to sell; the remaining small investors do not trade. We assume that small investors who are hit by liquidity shocks are willing to trade at any price that is at or better than what they can obtain from the intermediary at the time they agree to trade. Thus if a mass q of investors are approached with an offer to buy at or above the fair market price, mass ρq of them are willing to trade.

Intermediated Market. The model includes an intermediated market, where an investor is able to trade with risk-averse intermediaries who provide liquidity at a price. Following Biais (1993), an investor who wants to buy quantity q from intermediaries

who hold an aggregate inventory of I pays uniform price $p^{\mathsf{mm}}(I,q)$ per unit:

$$p^{\mathsf{mm}}(I,q) = \frac{\kappa\sigma^2}{N}(q-I) =: \frac{\ell}{2}(q-I), \tag{1}$$

where $\kappa > 0$ is an intermediary's risk aversion coefficient, N is the number of intermediaries in the market, and σ^2 is the variance of the fundamental value distribution. Parameter ℓ, defined by (1), signifies the liquidity or the price impact cost in the intermediated market. Appendix VII. provides the micro-foundation, in the tradition of Biais (1993), for the pricing equation (1). We assume that the intermediaries' aggregate inventories are zero at the beginning of the stage game, $I := \sum_{i=1}^{N} I_i = 0$.[4]

Timing. Trading is organized as an infinitely repeated game in discrete time. The stage game timing is as follows. At the beginning of each stage game, one of the large investors is randomly selected to be hit by a liquidity shock. This trader then approaches the other investors (small and/or large). The investors either accept the offer and the trade(s) occur, or they reject. The liquidity demander can contact the other investors only once; if necessary, he fills the remainder of his position in the intermediated market. Small traders who are hit by liquidity shocks and do not trade with the liquidity demander fill their positions in the intermediated market, after the large investor has traded. We assume that these remaining small investors all trade at the same time and that their trades in the intermediated market clear at the price $p^{\mathsf{mm}}(I,q)$, defined in (1), where q is the *net* amount demanded by these investors. This implies, in particular, that when large investors trade exclusively between each other, small investors trade in the intermediated market at the expected value of the asset.

[4]Loosely, we assume that between the arrivals of liquidity shocks for large investors, the intermediaries manage their inventories.

The intermediaries fill the large trader's request immediately upon receipt. We allow large investors to "front-run" each other in the sense that before responding to the liquidity demander's request, the liquidity provider can build up a position and make a counter-offer to the liquidity demander. A large investor that is being approached by the liquidity demander thus chooses between accepting the offer, rejecting the offer, or front-running and making a counter-offer.

Finally, we assume that trading offers are binding and cannot be withdrawn.

Direct Trading Costs. Direct trading costs in our model arise for two reasons. First, contacting mass q of small investors is *complex* (e.g., data processing, or keeping track of offers) and costs $C(q)$, where, for simplicity, $C(q) = \frac{c}{2}q^2$.

Second, transaction *validation* is costly. We assume, as with the Bitcoin and Ethereum blockchains, that costs accrue linearly based on the number of transactions, at a cost of γ per transaction, to be paid by the party that initiates a trade. These validation fees are paid to the underlying network, which we do not model explicitly.[5] If two parties trade mass q in a single trade, the costs are zero. If a trader initiates a trade with mass q of trader IDs or uses q IDs, costs are γq.

Indirect Trading Costs: Front-running. We model the indirect trading costs that arise from disclosing one's trading intent through the cost of front-running. When a liquidity demander contacts the liquidity provider, the liquidity demander may be front-run. We model the mechanics as follows. Suppose a large investor is contacted by the liquidity demander who wishes to buy a quantity q. If he chooses to front-run, this investor buys quantity q from the intermediary at a price and resells it to the liquidity demander at a higher price. We assume that the front-runner makes an "all-or-nothing"

[5]For Bitcoin or Ethereum transactions, "miners" receive a fee for each transaction that they verify. Analyzing the mechanics of transaction validation is outside the scope of this paper; see e.g., Biais, Bisiere, Bouvard, and Casamatta (2017) for a detailed study on the economics of mining.

offer to the liquidity demander for the quantity q, and that he charges the liquidity demander the minimum cost that the latter would incur to acquire q in the "public market" after front-runner has moved the price by purchasing q.[6]

Transparency of Ownership. Distributed ledger technology admits multiple levels of transparency about investors' holdings. In our benchmark setting, which we refer to as the *full transparency* setting, we assume that ownership is fully transparent in the sense that trader identifiers (IDs) that belong to large investors are publicly known. Since validation costs increase in the number of IDs, we assume that large investors concentrate their holdings under a single ID.

We then consider two settings with reduced transparency. In the first, investors concentrate their ownership under a single ID, as before, but an identifier's holdings and trades are not observable, and market participants cannot identify IDs that belong to large traders. We refer to this setting as the *single-ID opaque ownership* setting. In the second setting, each large investor owns a continuum 1 of IDs and equally disperses ownership over these IDs; in this setting, there are a total of of $\rho^{-1} + 1$ IDs. We assume that the system is set up in a way that investors cannot infer whether a given ID belongs to a small or to a large investor, and we refer to this setting as the *multi-ID opaque ownership* setting. As we explain in the introduction, the multi-ID opaque ownership setting corresponds to the solution that the Ethereum platform founders (see Buterin (2016)) describe as the simplest solution to achieve privacy in public blockchains.

Equilibrium Concept. In each period, the liquidity demander wants to trade

[6]The advantage of our formulation is that the tension is created within the model. One can imagine other costs, for instance, investors may copy a competitor's portfolios and eliminate someone's comparative advantage; see Christoffersen, Danesh, and Musto (2015) who document that mutual funds often delay publishing their holding information in 13-F forms for as long as possible. Christoffersen et al. argue that mutual fund managers are mostly concerned about being front-run by competitors.Danesh (2015) provides a theoretical model in the tradition of Kyle (1985) to analyze front-running behavior.

$q = 1$, mass 1 of small investors want to buy and mass 1 want to sell. As a consequence, in our setup $q = 1$ would need to be traded with the intermediary — unless the liquidity demander can "tap into" the latent liquidity that can be provided by the other large trader. Any quantity that the large traders exchange with one another reduces the costs of an inefficient risk transfer that arise from trades with risk-averse intermediaries. In what follows, we search for equilibria in which large traders trade with each other. If large traders do not trade with each other, and instead trade with small investors, then some small investors will have to pay the intermediaries, which possibly redistributes welfare from small to large traders.

We examine the equilibria of the infinitely repeated stage game that can be sustained by so-called "trigger" strategies. That is, if any participant observes an "off-the-equilibrium-path" outcome, i.e., a deviation from an equilibrium strategy, then henceforth large investors follow a path of action in which no longer interact with one another. Examples for deviations that lead to "off-the-equilibrium-path" outcomes include a price other than the equilibrium price, a front-running by a liquidity provider, or trades by the liquidity demander with the intermediary or the small investors when the equilibrium strategy prescribes that large investors trade with each other.

III. Full Transparency Setting

We first describe the equilibrium behavior in the benchmark setting of full transparency where all trades are publicly observed, and trading identifiers that belong to large investors are publicly known.

In a stage game, the liquidity demander may choose to offer the other large investor a price concession or the liquidity demander may trade with the intermediary and the

continuum of small investors. The liquidity provider may choose to accept the offered price or he may front-run. We search for an equilibrium where large traders trade "peer-to-peer" in that sense that the liquidity demander makes an offer to the liquidity provider, for the full quantity demanded, and the latter accepts. In what follows, we refer to this type of equilibrium as "peer-to-peer."

Peer-to-Peer Trading Payoffs. After the liquidity demander is hit by a shock, he contacts the liquidity provider, and makes a take-it-or-leave it offer to trade at a price $p \geq 0$.[7] We further restrict attention to the case where the liquidity demander has full bargaining power, that is, if there are multiple feasible non-negative equilibrium prices, the smallest possible one obtains.

When offering the liquidity provider price p per unit and trading $q = 1$, in the absence of front-running, the liquidity demander pays p today. In the next period, with probability $1/2$, the trader receives another liquidity shock and has to pay p, and with probability $1/2$, the other trader receives a shock and the liquidity demander receives payment p. Taken together, the continuation payoff is 0, and the equilibrium payoff to the liquidity demander when the large traders trade peer-to-peer is $\Pi^*_{\mathsf{LD}}(p) = -p$.

The liquidity provider receives p today, and his equilibrium continuation payoff is the same as that of the liquidity demander, 0. Therefore, the liquidity provider's equilibrium payoff is $\Pi^*_{\mathsf{LP}}(p) = p$.

Deviation Payoffs. If the liquidity demander chooses to deviate, he approaches the continuum of small investors and the intermediaries. The following lemma describes the liquidity demander's optimal strategy and the payoff for this outside option. The lemma admits the possibility of the intermediaries having non-zero inventory, so that

[7]Negative equilibrium prices are, in principle, possible because liquidity providers may "pay it forward", meaning that they accept a low price today in return for getting a better price in the future when they are hit with a shock.

it also captures the liquidity demander's behavior in the event he is front-run by the liquidity provider. We also make the dependance on the probability of acceptance and the per-ID transaction cost explicit in this lemma, so that it continues to apply in the absence of full transparency.

Lemma 1 (Trading with the Continuum and Intermediaries)**:** *When trading with the intermediaries who hold an aggregate inventory of I and with the continuum of investors IDs that accept the offer with probability ρ, at cost γ per ID, the liquidity demander optimally approaches mass $\hat{x}(\gamma,\rho)$ of investor IDs with $p = p^{\mathsf{mm}}(I,0)$, and he obtains payoff $\hat{\pi}(\gamma,\rho,I)$:*

$$\hat{x}(\gamma,\rho) = \max\left\{0, \frac{\rho(\ell-\gamma)}{\ell\rho^2+c}\right\}, \tag{2}$$

$$\hat{\pi}(\gamma,\rho,I) = -\frac{1}{2}\frac{\ell c}{\ell\rho^2+c} - \frac{\gamma\rho^2}{2}\frac{2\ell-\gamma}{\ell\rho^2+c} + \frac{\ell}{2}I. \tag{3}$$

Proof. Since mass 1 of the ρ^{-1} small investors are interested in selling, each offer is accepted with probability ρ. Therefore when approaching measure x of small investors, the liquidity demander trades quantity ρx, at the price $p^{\mathsf{mm}}(I,0)$ per unit, and he additionally incurs complexity cost $C(x) = cx^2/2$ (for all offers) and validation cost $\gamma\rho x$ (for accepted offers). The liquidity demander then trades the remaining quantity $1-\rho x$ with the intermediaries at the price $p^{\mathsf{mm}}(I, 1-\rho x)$ per unit; in the single-ID setting, this transaction incurs zero validation costs. The continuation payoffs do not depend on the quantity x, and the liquidity demander chooses x to maximize his stage game payoff:

$$\max_x -\frac{c}{2}x^2 - \gamma\rho x - \rho x\frac{\ell}{2} \times (-I) - (1-\rho x)(1-\rho x - I) \times \frac{\ell}{2}. \tag{4}$$

Solving the optimization problem yields the optimal quantity as described in (2). The optimal quantity choice does not depend on the intermediaries inventory, and it is reduced by the validation cost. For large validation costs, $\gamma > \ell$, the large investor would not approach the continuum. The liquidity demander's payoff is found by substituting the expression for the optimal quantity $\hat{x}$ into the expected payoff expression (4). □

Under single-ID ownership, trading with an intermediary incurs zero validation costs, irrespective of the traded size, whereas trading with a continuum of small investors has a positive validation cost. As a consequence, when validation costs are too high, $\gamma > l$, the large liquidity demander never approaches small investors. Since the focus of our paper is on peer-to-peer trading, in what follows we assume that the per unit validation cost is bounded by twice the price impact of trading with an intermediary, so that the existence of a continuum of small investors is meaningful.

Assumption 1: *With single-ID ownership, validation costs satisfy* $\gamma < \ell$.

As a next step we compute the stage game deviation payoff to the liquidity provider, when he is offered to trade quantity q by the liquidity demander but chooses to front-run the liquidity demander.

Lemma 2 (Front-Running Profits)**:** *The stage payoff that the liquidity provider obtains by front-running is* $-\hat{\pi}(\rho, \gamma, 0)$.

Proof. To extract rents from the liquidity demander, the front-runner first accumulates a position of size 1 by trading with the intermediary. We assume that he is then able to resell this quantity to the liquidity demander at a price that equals the minimum possible price that the liquidity demander would need to pay to build this position on the open market (i.e., with the continuum of small investors and with the intermediaries). Front-

running is costly to the liquidity demander because the trade of the front-runner with the intermediaries would (i) move the public price, which the liquidity demander trades at with the small investors, and (ii) results in a positive inventory of the intermediaries, who then charge a higher price. The front-runner pays $\ell/2$ to build his position in the intermediated market. After being front-run, the liquidity demander solves the optimization problem as described in Lemma 1 for $I = -1$, and he earns $-\hat{\pi}(\rho, \gamma, -1)$ as defined in (3). The front-runner could then offer the liquidity demander quantity 1 at a price such that the liquidity demander's payoff remains that same, $\hat{\pi}(\rho, \gamma, -1)$. The front-runner's payoff is then $-\hat{\pi}(\rho, \gamma, -1) - \ell/2$, and the result of the Lemma obtains by equation (3), which defines the payoff function $\hat{\pi}$. □

In what follows, we use $\pi = \hat{\pi}(\rho, \gamma, 0)$ to denote the stage game payoff to the liquidity demander when he chooses to deviate and to trade with the intermediary and the continuum of small investors, instead of making an offer to the other large trader. Note that the payoff π is negative (it is costly for the liquidity demander to build a position), while the liquidity provider extracts a positive payoff of $-\pi$ by front-running.

After a deviation, either by the liquidity demander or by the liquidity provider, the trigger strategy would prescribe that the liquidity demander only traders with the intermediaries and the small investors. As a consequence, a large investor's stage game payoff will be π when he is hit by a liquidity shock and 0 otherwise. Each large trader experiences a liquidity shock with probability $1/2$ in each stage game, and a large trader's continuation value after a deviation is:

$$\frac{1}{2}\pi + \delta\frac{1}{2}\pi + \delta^2\frac{1}{2}\pi + \ldots = \frac{1}{2}\frac{1}{1-\delta}\,\pi. \tag{5}$$

Lemmas 1 and 2 together with equation (5) imply the following result.

Lemma 3 (Deviation Payoffs)**:** *The repeated game deviation payoffs that the liquidity demander and the liquidity provider achieve, respectively, by trading with the continuum of small investors and intermediaries and by front-running, are as follows:*

$$\pi^*_{\mathsf{LD}} = \pi\left(1 + \frac{1}{2}\frac{\delta}{1-\delta}\right), \text{ and } \quad \pi^*_{\mathsf{LP}} = \pi\left(-1 + \frac{1}{2}\frac{\delta}{1-\delta}\right). \tag{6}$$

Equilibrium Existence. It is always an equilibrium for the liquidity demander to approach only the continuum of small investors and the intermediaries, and for the liquidity provider to reject all offers. We ask whether there exists a "peer-to-peer" equilibrium where large investors trade with each other, so that the inefficient risk transfer to risk-averse intermediaries does not arise. For the large investors to trade with each other, there must exist a price p such that the equilibrium payoffs exceed the deviation payoff for both, the liquidity demander and the liquidity provider:

$$\Pi^*_{\mathsf{LD}}(p) \geq \pi^*_{\mathsf{LD}} \text{ and } \Pi^*_{\mathsf{LP}}(p) \geq \pi^*_{\mathsf{LP}}. \tag{7}$$

Proposition 1 (Peer-to-Peer Trading with Full Transparency)**:** *For all parametric configurations, there exists a price $p \geq 0$ such that the large investors trade with each other in equilibrium. For $\delta \geq 2/3$, the large investors trade with each other at $p = 0$.*

Proof. When the liquidity demander offers price p, the equilibrium payoff for the liquidity demander and the liquidity provider are $-p$ and p, respectively; their deviation payoffs are given by expressions (6). For the price p to be an equilibrium price, both inequalities

in (7) must hold. Expressing them in terms of p:

$$\pi\left(-1+\frac{1}{2}\frac{\delta}{1-\delta}\right) \leq p \leq -\pi\left(1+\frac{1}{2}\frac{\delta}{1-\delta}\right). \tag{8}$$

Since $\pi < 0$, the above inequalities are equivalent to:

$$1-\frac{1}{2}\frac{\delta}{1-\delta} \leq \frac{p}{-\pi} \leq 1+\frac{1}{2}\frac{\delta}{1-\delta}. \tag{9}$$

First, observe that the above relation always holds for $p = -\pi$, therefore large investors trading with each other is always an equilibrium. Second, for $\delta \geq 2/3$, $\frac{\delta}{2} > 1-\delta$, the left-hand side of the inequality in (9) is negative, and $p = 0$ satisfies the inequality. □

The inequality (9) illustrates, in particular, that the lowest non-negative price that the liquidity demander and the liquidity provider agree on is given by:

$$p = \max\left\{0, -\pi\left(1-\frac{1}{2}\frac{\delta}{1-\delta}\right)\right\}. \tag{10}$$

Since, by assumption, we allow the liquidity demander to choose his preferred price, expression (10) describes the equilibrium price in the full transparency setting.

IV. Opaque Single-ID Ownership

In the single-ID opaque ownership setting, the ledger designers require that investors concentrate their holdings under a single ID, and they do not allow investors to observe the ledger. In this setting, IDs of large investors cannot be identified, and therefore the liquidity demander is not able to contact the large liquidity provider directly. Since there is a continuum of traders (and therefore a continuum of IDs), the probability that the

liquidity demander contacts an ID that belongs to the other large investor when sending a trading request to the continuum is zero.

The liquidity demander's behavior in this setting is therefore captured by Lemma 1.

Proposition 2 (Single-ID Opaque Ownership)**:** *Liquidity demanders always split their position among small investors and intermediaries, as described in Lemma 1.*

The price impact cost l of trading in the intermediated market, defined by equation (1), increases with the intermediaries' risk aversion and the volatility of the asset value. Expression (2), which describes the quantity that the the liquidity demander trades with small investors, then yields the following corollary to Lemma 1:

Corollary 1: *In the single-ID opaque ownership setting, Iiquidity demanders trade more with small investors if intermediaries are more risk-averse or if fundamental risk increases, and they trade less with small investors if complexity costs or validation costs increase.*

V. Multi-ID Opaque Ownership

Multi-ID ownership allows traders to obfuscate the holdings of their IDs in public blockchains, following the mechanism described in Buterin (2016), even when the ledger designers do not mandate its opaqueness. We model this native way to achieve opaqueness on a distributed ledger by assuming that each large trader owns a continuum of trading identifiers ("one share, one ID"), and that the system has no memory after each round of trading – so that traders are not able to identify which IDs belong to large investors. Consequently, in this setting, the large liquidity demander is not able to contact exclusively the IDs that belong to the large liquidity provider, as the latter

IDs are indistinguishable from the IDs that belong to small investors. We search for an equilibrium in which the liquidity demander contacts the continuum of IDs and possibly the intermediary, offers *the continuum* a price concession, and the liquidity provider accepts the offer, where we only allow pure strategies in the sense that the public IDs that belong to the liquidity provider either all accept or all reject.

The Liquidity Demander's Choice. The liquidity demander is 's optimization problem is similar to that described in Lemma 1, with three crucial differences.

First, the probability of acceptance when contacting the continuum of IDs depends on whether the IDs that belong to the large liquidity provider accept or reject the offer. The mass of the continuum of traders that the liquidity demander is able to contact is $1+\rho^{-1}$, where mass 1 of IDs belong to the other large trader. If the liquidity provider accepts the offer, then when contacting mass x of IDs, the liquidity demander trades quantity $2\rho/(1+\rho)\times x$ with the continuum. If the liquidity provider rejects the offer, then the liquidity demander only trades with small investors, and by contacting mass x of IDs the liquidity demander trades quantity $\rho/(1+\rho)\times x$. In equilibrium, the probability of acceptance is either strictly larger than the probability ρ for the case of single-ID ownership or strictly smaller: $2\rho/(1+\rho) > \rho > \rho/(1+\rho)$.

Second, differently to the setup of Lemma 1, with multi-ID ownership the liquidity demander must always pay a validation fee of γ because the trader's holdings are dispersed and trading quantity 1 requires mass 1 transactions. The validation costs therefore do not affect the optimal quantity for the case of multi-ID ownership.

Third, when offering a price concession, this price cannot be paid exclusively to the large liquidity provider, because the liquidity demander cannot differentiate the IDs that belong to small investors from the liquidity provider's IDs. Consequently, in

contrast to the single-ID ownership case, transfers between the liquidity demander and the liquidity provider are not zero-sum among them: with non-zero price concession, the small investors necessarily capture some of this payment.

Denoting the probability of acceptance by the continuum of IDs by $\hat{\rho}$, when offering price p to the continuum at the beginning of a stage game ($I = 0$), the liquidity demander approaches mass x of IDs to maximize the following payoff:

$$\max_{x} -p \cdot x\hat{\rho} - \frac{c}{2}x^2 - \frac{\ell}{2}\left(1 - x\hat{\rho}\right)^2 - \gamma. \tag{11}$$

This maximization problem is similar to that in the single-ID case, described by equation (4), except that a per-unit transaction cost in this setting stems from a per-unit price concession p instead of the per-unit validation cost γ. The following Corollary to Lemma 1 summarizes the liquidity demander's optimal choice, described by (11):

Corollary 2: *When trading with the intermediaries and continuum of investor IDs at the beginning of a stage game, and given the price concession p and probability $\hat{\rho}$ of acceptance by the continuum, the liquidity demander optimally approaches mass $\hat{x}(p, \hat{\rho})$ of trader IDs, and he obtains payoff $\hat{\pi}(p, \hat{\rho}, 0)$.*

We restrict attention to prices such that trading with both the continuum and the intermediaries is cheaper than trading exclusively in the intermediated market.

Assumption 2: *With multi-ID ownership, the price concession satisfies $p < \ell$.*

Peer-to-Peer Equilibrium Payoffs. We search for a "peer-to-peer" equilibrium where large traders accept each other's offers and do not front-run each other. In this case, the liquidity demander's stage payoff is given by $\hat{\pi}(p, \hat{\rho}, 0)$, defined in (2), where the probability of acceptance is $\hat{\rho} = 2\rho/(1 + \rho) := \bar{\rho}$.

When the liquidity demander approaches a continuum of x, mass $x/(1+\rho^{-1}) \equiv x\bar{\rho}/2$ of the liquidity provider IDs receive the trading request. The liquidity provider's stage payoff, provided he accepts the offer, is $px\bar{\rho}/2$.

Since a large trader receives the liquidity shock with probability 1/2 in each period, the repeated game equilibrium payoffs to the liquidity demander and the liquidity provider, respectively, when they trade at price p are given by:

$$\Pi^{**}_{\mathsf{LD}}(p) = \hat{\pi}(p,\bar{\rho},0) + \frac{1}{2}\frac{\delta}{1-\delta}\left(\frac{p\bar{\rho}\hat{x}(p,\bar{\rho})}{2} + \hat{\pi}(p,\bar{\rho},0)\right) \tag{12}$$

$$\Pi^{**}_{\mathsf{LP}}(p) = \frac{p\bar{\rho}\hat{x}(p,\bar{\rho})}{2} + \frac{1}{2}\frac{\delta}{1-\delta}\left(\frac{p\bar{\rho}\hat{x}(p,\bar{\rho})}{2} + \hat{\pi}(p,\bar{\rho},0)\right) \tag{13}$$

Deviation Payoffs. The liquidity demander may deviate by offering a price or quantity that are different from those prescribed by the equilibrium strategy; either of these deviations is observable by the liquidity provider. In an equilibrium supported by the trigger punishment strategy, large trader IDs reject each other's offers after a deviation. Consequently, if a large trader deviates, the probability of acceptance by the continuum of IDs is $\hat{\rho} = \rho/(1+\rho) = \bar{\rho}/2 := \underline{\rho}$. Since the IDs that belong to small investors accept the offer with probability ρ, irrespective of the price concession, to maximize the stage payoff from the deviation, the liquidity demander offers zero price concession to the continuum, and he contacts mass $\hat{x}(0,\underline{\rho})$ of IDs. The liquidity provider rejects the offer, and he earns zero stage profits.

These deviation strategies constitute an equilibrium in a stage game. Given that the liquidity provider IDs reject the offers, approaching mass $\hat{x}(0,\underline{\rho})$ with $p = 0$ maximizes the liquidity demander's payoff. The liquidity provider earns zero profit by rejecting the offer, and he cannot earn positive profits by either accepting it, since $p = 0$, or by front-

running, since the liquidity demander fully fills his position with the small investors and the intermediaries before the liquidity provider is able to front-run.

Since a large trader receives the liquidity shock with probability 1/2 each period, the liquidity demander's repeated game payoff in the event of the deviation is given by:

$$\pi^{**}_{\mathsf{LD}} = \hat{\pi}(0, \underline{\rho}, 0) + \frac{1}{2}\frac{\delta}{1-\delta} \cdot \hat{\pi}(0, \underline{\rho}, 0). \tag{14}$$

The liquidity provider may deviate by front-running the liquidity demander for quantity $\hat{x}(p, \bar{\rho})\bar{\rho}/2$ (which equals the mass of contacted IDs that belong to the large liquidity provider). To build this position with the intermediary, the liquidity provider pays $\ell/2 \times (\hat{x}(p, \bar{\rho})\bar{\rho}/2)^2$ to the intermediary, and he additionally incurs validation costs of γ per unit. He then makes a counter-offer to the liquidity demander. Since the liquidity demander has already contacted the continuum, he can either accept the front-runner's counter-offer or purchase this quantity from the intermediated market at price $p^{\mathsf{mm}}(-\hat{x}(p, \bar{\rho})\bar{\rho}/2, \hat{x}(p, \bar{\rho})\bar{\rho}/2)$ per unit. The total cost of the latter purchase to the liquidity demander would be $\ell \times (\hat{x}(p, \bar{\rho})\bar{\rho}/2)^2$ plus the validation costs. The liquidity provider's counter-offer is such that the liquidity demander is indifferent between these two options, and the liquidity provider's stage payoff from front-running is:[8]

$$\pi_{\mathsf{fr}} = \ell \times \left(\frac{\bar{\rho}\hat{x}(p, \bar{\rho})}{2}\right)^2 - \frac{\ell}{2} \times \left(\frac{\bar{\rho}\hat{x}(p, \bar{\rho})}{2}\right)^2 - \frac{\gamma\bar{\rho}\hat{x}(p, \bar{\rho})}{2}. \tag{15}$$

Once the trigger strategy is invoked, the continuation payoff for the liquidity provider is the same as for the liquidity demander. Taken together, the payoff to the liquidity

[8]The front-runner extracts the maximum possible surplus, by assumption, and the payoff to him does not depend on who pays the validation costs for trades between the IDs of large investors after front-running.

provider if he deviates and front-runs is:

$$\pi^{**}_{\mathsf{LP}}(p) = \frac{\ell}{2} \times \left(\frac{\bar{\rho}\hat{x}(p,\bar{\rho})}{2} \right)^2 - \frac{\gamma\bar{\rho}\hat{x}(p,\bar{\rho})}{2} + \frac{1}{2}\frac{\delta}{1-\delta} \cdot \hat{\pi}(0,\underline{\rho},0). \tag{16}$$

Equilibrium Existence. As we discuss earlier in this section, there always exists an equilibrium where the large traders do not trade with each other. For an equilibrium where the liquidity demander and the liquidity provider trade with each other at price p, the following conditions must be satisfied:

$$\Pi^{**}_{\mathsf{LD}}(p) \geq \pi^{**}_{\mathsf{LD}} \text{ and } \Pi^{**}_{\mathsf{LP}}(p) \geq \pi^{**}_{\mathsf{LP}}(p). \tag{17}$$

We provide the following equilibrium characterization.

Proposition 3 (Peer-to-Peer Trading with Multi-ID Ownership)**:** *When the intermediated market is sufficiently liquid (ℓ is sufficiently small), or when the discount factor δ is sufficiently large (the future is important), or when validation cost γ is sufficiently high, there exists a "peer-to-peer trading" equilibrium where the large liquidity demander trades with the intermediaries, the continuum of small investors, and the liquidity provider at price $p = 0$.*

Proof. Using the definitions of $\bar{\rho}$ and $\underline{\rho}$ together with the explicit expressions (2)-(3) for $\hat{x}$ and $\hat{\pi}$, we can rewrite the future value in an equilibrium when the large traders trade with each other (from expressions (12)-(13)) as:

$$\frac{p\bar{\rho}\hat{x}(p,\bar{\rho})}{2} + \hat{\pi}(p,\bar{\rho},0) = -\frac{\ell}{2}\frac{p\bar{\rho}^2 + c}{\ell\bar{\rho}^2 + c}. \tag{18}$$

The payoff to the liquidity demander (12) when he offers price p and the large liquidity

provider accepts can then be expressed as

$$\Pi^{**}_{\mathsf{LD}}(p) = -\frac{\ell}{2} \times \frac{p\bar{\rho}^2 + c}{\ell\bar{\rho}^2 + c}\left(1 + \frac{1}{2}\frac{\delta}{1-\delta}\right) - \frac{p\bar{\rho}^2}{2}\frac{\ell - p}{\ell\bar{\rho}^2 + c}. \tag{19}$$

The liquidity demander's payoff when he offers the price $p = 0$ to the continuum and when the other large trader rejects is:

$$\pi^{**}_{\mathsf{LD}} = -\frac{\ell}{2} \times \frac{c}{\ell\underline{\rho}^2 + c}\left(1 + \frac{1}{2}\frac{\delta}{1-\delta}\right). \tag{20}$$

At $p = 0$, the payoff to the liquidity demander when the large traders trade with each other exceeds the payoff that obtains when they don't:

$$\Pi^{**}_{\mathsf{LD}}(0) - \pi^{**}_{\mathsf{LD}} = \frac{\ell}{2} \times \frac{c\ell(\bar{\rho}^2 - \underline{\rho}^2)}{(\ell\underline{\rho}^2 + c)(\ell\bar{\rho}^2 + c)} \times \left(1 + \frac{1}{2}\frac{\delta}{1-\delta}\right) > 0. \tag{21}$$

The liquidity demander does not have an incentive to deviate at $p = 0$.

Similarly to the computations for the liquidity demander, the payoff to the liquidity provider (13) when he is offered price p and accepts can be expressed as:

$$\Pi^{**}_{\mathsf{LP}}(p) = \frac{p\bar{\rho}^2}{2}\frac{\ell - p}{\ell\bar{\rho}^2 + c} - \frac{\ell}{2} \times \frac{p\bar{\rho}^2 + c}{\ell\bar{\rho}^2 + c} \times \left(\frac{1}{2}\frac{\delta}{1-\delta}\right). \tag{22}$$

The payoff to front-running is:

$$\pi^{**}_{\mathsf{LP}} = \frac{\bar{\rho}^2}{2}\frac{\ell - p}{\ell\bar{\rho}^2 + c} \times \left(\frac{\ell}{2}\frac{\bar{\rho}^2}{2}\frac{\ell - p}{\ell\bar{\rho}^2 + c} - \gamma\right) - \frac{\ell}{2} \times \frac{c}{\ell\underline{\rho}^2 + c} \times \left(\frac{1}{2}\frac{\delta}{1-\delta}\right). \tag{23}$$

The liquidity provider is willing to accept the price $p = 0$ when $\Pi^{**}_{\mathsf{LP}}(0) - \pi^{**}_{\mathsf{LP}} \geq 0$. Using expressions (22)-(23) and dividing both sides of this inequality by $\ell/2$, the liquidity

provider accepts $p = 0$ when:

$$\frac{\bar{\rho}^2}{\ell\bar{\rho}^2 + c} \times \left(\gamma - \frac{\ell^2}{2}\frac{\bar{\rho}^2}{2}\frac{1}{\ell\bar{\rho}^2 + c}\right) + \frac{c\ell(\bar{\rho}^2 - \underline{\rho}^2)}{(\ell\underline{\rho}^2 + c)(\ell\bar{\rho}^2 + c)} \times \frac{1}{2}\frac{\delta}{1-\delta} \geq 0. \tag{24}$$

Inequality (24) is satisfied, in particular, when $\ell \to 0$, $\delta \to 1$, or γ is sufficiently large. □

If the market is very liquid (ℓ small), then front-running is not profitable. Both the stage payoff to deviating and the future cost decline as the market is more liquid (ℓ declines), however, the costs decline proportional to ℓ^2 whereas the benefit declines at rate ℓ^3. When future interactions and payoffs are sufficiently important (δ is large), e.g., when investors interact sufficiently frequently, front-running can also be avoided because future benefits of being able to trade with the other large investor when hit by a liquidity shock outweigh the one-time profits that can be obtained by front-running. This latter result is a standard Folk Theorem. When validation costs are high, front-running itself becomes very costly, which reduces its benefit.

Finally, we illustrate that an equilibrium where large traders trade with each other does not always exist. Rearranging the payoff differences illustrates that the difference between the "peer-to-peer" equilibrium payoff and the deviation payoff are quadratic in the price concession, with the negative coefficient on p, for both the liquidity demander and the liquidity provider. For the liquidity demander, this difference is always positive at $p = 0$, and he therefore is always willing to offer a range of prices between 0 and a positive price P_{LD}, as an incentive for the large trader IDs to accept his offer in equilibrium. If the liquidity provider accepts $p = 0$, the "peer-to-peer" equilibrium exists. When he is only willing to accept a higher price, the equilibrium only exists if he the lowest price that he is willing to accept is below P_{LD}, the highest price that the liquidity demander is willing to offer. Inequality (24) illustrates that the liquidity provider front-

runs at $p = 0$ if, for instance, when both the discount rate δ and the validation cost γ are very low and the intermediated market is sufficiently illiquid (ℓ is high). We can show, by taking the derivative with respect to p of the payoff difference, that for sufficiently low values of δ, the payoff difference is increasing in p at $p = 0$, implying that the roots of the quadratic equation, if they exist, are both positive. Denoting these roots by p_{LP} and $P_{\mathsf{LP}} > p_{\mathsf{LP}}$, for the liquidity provider to not front-run, the price concession must be sufficiently large: $p \in [p_{\mathsf{LP}}, P_{\mathsf{LP}}]$.

The existence of a "peer-to-peer" equilibrium in this case depends on the relation between P_{LD}, the highest price that the liquidity demander is willing to offer, and p_{LP}, the lowest price that the liquidity provider is willing to accept.

Numerical Observation 1: *There exist parametric configurations such that a "peer-to-peer" equilibrium where large traders trade with each other does not exist in the multi-ID ownership setting.*

The above numerical observation obtains, for instance, by using the following set of parameters: $\delta = 1/100, \rho = 1/2, c = 1, \ell = 10, \gamma = 1/100$. Under these parameters,the liquidity demander is willing to offer at most $P_{\mathsf{LD}} = 1.64$, and the liquidity provider only accepts if p is between $p_{\mathsf{LP}} = 1.68$ and $P_{\mathsf{LP}} = 9.87$.

We further note that there also exist parametric configurations where the large traders do not trade with each other at $p = 0$, but they do trade at positive price concessions. For instance, lowering the illiquidity of the intermediated market in the preceding example to $\ell = 5$ leads to $P_{\mathsf{LD}} = 1.08$, $p_{\mathsf{LP}} = 0.72$, and $P_{\mathsf{LP}} = 4.94$. Under these parameters, large traders trade with each other for $p \in [0.72, 1.08]$.

Finally, our numerical results illustrate that private blockchain designers may be able to affect the type of equilibrium by adjusting the validation costs. For instance,

increasing the validation cost to $\gamma = 1/10$ in the original example reduces the liquidity provider's incentives to front-run and lowers the minimum price that he is willing to accept from $p_{\mathsf{LP}} = 1.68$ to $p_{\mathsf{LP}} = 1.60$, while leaving the maximum price that the liquidity demander is willing to pay unaffected at $P_{\mathsf{LD}} = 1.64$. Under these parameters, large traders are willing to trade with each other at $p \in [1.60, 1.64]$.

VI. Comparing Regimes

A. Welfare Comparison of ID Ownership Setting

The full transparency benchmark setting in our model is superior in terms of aggregate welfare, as there is no inefficient transfer of risk to the risk-averse intermediary and no complexity costs. We thus focus on comparing the two non-transparent regimes.

Welfare comparisons across the different designs require further assumptions on validation costs. To see why this is the case, observe that if, for instance, the per transaction cost is assumed to be the same for both the single-ID and the multi-ID setting, then the latter is mechanically more expensive in terms of validation costs, simply due to the larger number of IDs and therefore expected transactions. We believe that in practice validation costs will be part of the blockchain design, in particular, for private blockchains, and that they will be endogenous to the expected number of transactions and to the ownership ID design. The design of validation costs is outside the scope of this paper, and we henceforth make the simplifying assumption that $\gamma = 0$ when comparing the payoffs across the settings with different numbers of IDs.

There are two sources of welfare loss in our model. First, the liquidity demander incurs complexity costs when contacting the continuum. Second, if the liquidity demander fills part of his position with the risk averse intermediaries to fill part of his position,

there is an inefficient transfer of risk relative to the equilibrium where the large traders trade with each other. This cost is borne both, by the liquidity demander and by the small investors — in the absence of the large liquidity demander, the latter avoid this price impact cost since their net demand is zero. Finally, a price concession paid by the liquidity demander has no direct impact on welfare because the concessions are zero-sum among the traders.

In equilibrium, the only change from one period to the next pertains to which of the two large traders is hit by the liquidity shock, and it suffices to compare the welfare for the stage game.

Let x denote the mass of IDs that the liquidity demander contacts in equilibrium, and let $\hat{\rho}$ denote the probability of acceptance. The liquidity demander then trades $1 - \hat{\rho}x$ with the intermediaries. The amount that small investors must trade with the intermediaries depends on whether or not large traders trade with each other in equilibrium. By assumption, mass 1 of small investors want to buy and mass 1 want to sell each period. When the large traders do not trade with each other, either in the opaque single-ID setting or in the multi-ID setting when the liquidity provider IDs reject the offer, the liquidity demander's buys force the small investors to trade quantity $\hat{\rho}x$ with the intermediaries. When the large traders trade with each other in the multi-ID ownership setting, only half of the $\hat{\rho}x$ trades of the liquidity demander are with the small investors and the remaining traders are with IDs of the large liquidity provider. Consequently, the small investors demand net amount $\hat{\rho}x/2$ from the intermediaries.

By assumption, the liquidity demander acts first, and the intermediaries have inventory $I = 0$ at the beginning of a stage game. Therefore, when the small investors approach the intermediaries, their aggregate inventory is $I = -(1 - \hat{\rho}x)$. Denoting the

net demand by small investors by $y \in \{\hat{\rho}x/2, \hat{\rho}x\}$, per-stage aggregate investor welfare can then be expressed as:

$$W(x, y, \hat{\rho}) = -\frac{c}{2}\, x^2 - \frac{\ell}{2}(1 - \hat{\rho}x)^2 - \frac{\ell}{2}\, y\, (y + (1 - \hat{\rho}x)). \tag{25}$$

When the liquidity demander trades a larger quantity with the continuum, he incurs a larger complexity cost (the first term in (25)) and a smaller price impact cost of trading with the intermediaries (the second term), whereas small investors incur a larger price impact cost (the third term). Proposition 4 illustrates that these effects exactly offset each other in equilibria when the large traders do not trade with each other, and that the aggregate welfare in these equilibria only depends on the liquidity of the intermediated market but not on the complexity costs or the probability of acceptance by small investors.

Proposition 4: *Assume validation costs $\gamma = 0$. The aggregate welfare in an equilibrium of a multi-ID setting when the large traders do not trade is the same as that in an opaque single-ID setting: $W = -\ell/2$.*

Proof. When large traders do not trade with each other, small investors trade the net quantity $y = \hat{\rho}x$ with the intermediary. By Lemma 1 and Corollary 2, with zero validation cost $\gamma = 0$ and zero price concession $p = 0$, the optimal mass x of IDs that the large liquidity demander contacts is given by $x = \hat{x}(0, \hat{\rho}) = \hat{\rho}\ell/(\ell\hat{\rho}^2 + c)$. Substituting this expression into equation (25) and re-arranging delivers the constant welfare. □

We next compare the equilibrium of the opaque single-ID setting to the "peer-to-peer" equilibrium of the multi-ID ownership setting, where the large traders trade with each other. In the multi-ID ownership setting, the large buyer may need to pay the other

traders an incentive. This incentive is zero-sum among the large traders, but it affects how much the large trader seeks to trade with the continuum, and through this, it affects the complexity costs and the price impact costs. The following proposition illustrates that when large traders trade with each other in equilibrium in the multi-ID ownership setting, achieving opaqueness through this blockchain-native channel is welfare-superior to imposing an opaque single-ID regime.

Proposition 5: *Assume validation costs $\gamma = 0$. Assume further that model parameters are such that large traders trade with each other in the multi-ID ownership setting. Then welfare is higher in the multi-ID ownership setting than in the opaque, single-ID setting.*

Proof. In the multi-ID ownership setting, the acceptance probability is $\hat{\rho} = \bar{\rho} = 2\rho/(1+\rho)$ and the net demand by small investors in the intermediated market is $y = \hat{\rho}x/2 = \bar{\rho}\hat{x}(p,\bar{\rho})/2$, where function $\hat{x}$ is defined in (2). Welfare in the opaque single-ID ownership setting equals $-\ell/2$, by Proposition 4.

Substituting all the above expressions into (25) and rearranging, the difference between welfare in the multi-ID ownership setting where the large traders trade with each other and welfare in the opaque single-ID setting is positive:

$$W\left(\bar{\rho}, \hat{x}(p,\bar{\rho}), \frac{\bar{\rho}\hat{x}(p,\bar{\rho})}{2}\right) - \left(-\frac{\ell}{2}\right) = \frac{\bar{\rho}^2(l-p)}{8}\,\frac{(3\bar{\rho}^2\ell + 2c)(\ell+p) + 2cp}{(\bar{\rho}^2\ell + c)^2} > 0, \qquad (26)$$

where the inequality follows since we study equilibria with $p < \ell$, so that trading exclusively in the intermediated market is more expensive than trading with the continuum and the intermediaries. □

B. Payoffs to the Large Trader

Although a market designer's goal is maximizing aggregate welfare, it is also instructive to understand the payoffs of the large trader, for instance because these market participants may have lobbying power for market design. In the opaque single-ID setting, the large liquidity provider is contacted with probability zero, and the large trader's average stage payoff equals half the liquidity demander's payoff:

$$\bar{\pi}^* = \frac{\pi^*}{2} = -\frac{\ell}{4}\frac{c}{\ell\rho^2 + c}, \tag{27}$$

where, as before, we set $\gamma = 0$. In the multi-ID setting, the average stage payoff for a large trader can be expressed as:

$$\bar{\pi}^{**}(\hat{p}, \hat{\rho}) = \frac{1}{2}\left(\hat{\pi}(\hat{p}, \hat{\rho}) + \frac{\hat{p}\hat{\rho}\hat{x}(p, \hat{\rho})}{2}\right) = -\frac{\ell}{4}\frac{\hat{p}\hat{\rho}^2 + c}{\ell\hat{\rho}^2 + c}, \tag{28}$$

where $\hat{\rho} = \bar{\rho} = 2\rho/(1+\rho)$ and $\hat{p} = p$ when large traders trade with each other at price p, and $\hat{\rho} = \underline{\rho} = \bar{\rho}/2$ and $\hat{p} = 0$ when they do not trade with each other.

Comparing the average payoffs leads to the following proposition.

Proposition 6: *Assume $\gamma = 0$. Then the following relations hold for the average equilibrium stage payoffs of large traders.*

1. *When large traders do not trade with each other with multi-ID ownership, their equilibrium payoffs in this setting are lower than those the opaque single-ID setting.*

2. *When large traders trade with each other with multi-ID onwership at $p = 0$, their equilibrium payoffs in this setting dominate those in the opaque single-ID setting.*

Proof. When large traders do not trade with each other, they offer zero price concessions.

With $p = 0$, the average payoff for all the cases can then be expressed as $-\ell/2 \times c/(\ell\hat{\rho}^2 + c)$, where $\hat{\rho}$ is the relevant probability of acceptance. The payoff ranking follows directly from the relation of the probabilities of acceptance, with the highest payoff corresponding to the setting with the highest probability of acceptance. □

Since the aggregate welfare is constant when the large traders do not trade with each other (by Proposition 4), a corollary to Proposition 6 is that when the large traders do not trade with each other, small investors are *better off* with multi-ID ownership.

When large traders trade with each other at $p \geq 0$ in the multi-ID setting, their payments to each other are zero sum. However, the price concession affects the quantities that are traded in the continuum and in the intermediated market, with larger price concessions potentially leading to larger quantities traded in the intermediated markets and larger payouts to small investors. As a consequence, the average payoff for large traders in the multi-ID setting, $\bar{\pi}^{**}(p, \bar{\rho})$, decreases in p. This leads to the following observation:

Numerical Observation 2: *There exist parametric configurations such that large traders trade with each other at $p > 0$ in the multi-ID ownership setting, but their average equilibrium payoff in the opaque single-ID setting is higher: $\bar{\pi}^* > \bar{\pi}^{**}(p, \bar{\rho})$.*

The numerical observation obtains, for instance, by using the following set of parameters: $\delta = 2/3, \rho = 2/3, c = 4\ell/25$. Under these parameters, large traders trade with each other in the multi-ID setting for $p = \alpha\ell$, for all $\alpha \in [0, 1/5]$, yet the average payoff difference for the large traders between the multi-ID and opaque single-ID setting, $\bar{\pi}^{**}(p, \bar{\rho}) - \bar{\pi}^*$, changes sign from positive to negative as α increases from 0 to 1/5.

VII. Conclusion

At its core, the purpose of a primary financial market is to connect issuers and end-investors, and the purpose of a secondary financial market is to connect end-investors. Blockchain and distributive ledger technologies have the capacity to fundamentally change the interactions among market participants by eliminating intermediaries, which historically served as trusted parties to connect end-investors, and by replacing them with direct connections between end-investors. In this paper, we address several key market design questions that arise with the advent of this new technology.

First, distributed ledger technology allows for peer-to-peer interactions among anonymous identifiers, without the need for a trusted third party to verify the ownership of an identifier. The anonymity of identifiers raises questions with respect to their design and regulation; in particular, should the number of identifiers per investor be restricted? Second, the distributed nature of the ledger raises a question with respect to its transparency; in particular, should traders be permitted to see transactions of identifiers that they do not own? Third, blockchain transaction validation typically involves costs, raising the question of how these impact trading decisions.

We emphasize that the above three design choices become critical as soon as distributed ledgers are used, for instance, in clearing and settlement, and they must be considered carefully in debates about the roll-out of the technology and in market regulation. Our analysis focusses on the informational implications of the organization of distributed ledgers, and not on a specific blockchain validation protocol. We acknowledge that peer-to-peer trading does not require blockchain technology, and that our findings apply to trading arrangements that are not facilitated by it. We believe, however, that blockchain technology will enable the specific peer-to-peer trading features that we ex-

amine in this paper. First, the possibility to digitally and anonymously transfer value will expand the scope of peer-to-peer trading, in particular, by extending the option to small, retail investors. Second, the usage of numerous digital IDs to achieve privacy, which we focus on in this paper, is native to public blockchains. Our contribution is to identify the new strategic considerations that arise in anonymous peer-to-peer trading with numerous IDs and to highlight the implications of the related ledger design choices.

In our framework, by design, the optimal system is a private blockchain that offers full transparency and mandates a single, unique ID per user. Our focus is on the role of privacy implementation, and we compare two fully opaque systems. The first is a private blockchain that achieves investor privacy by restricting the ledger visibility to the trusted parties who verify transactions; similarly to the current setup with centralized ledgers. The second is a blockchain, which can be public or private, where users obfuscate their holdings and behavior by using numerous digital IDs; similarly to what is technologically feasible in public, inherently transparent blockchains. Our analysis illustrates that the implementation of privacy on a distributed ledger has economic implications beyond simply reducing the level of transparency; between the two fully opaque setups, the blockchain-native solution of multiple IDs is superior in terms of welfare.

Finally, our findings in this paper are most applicable to trading securities such as bonds, where most costs arise from finding liquidity rather than from being adversely selected by insiders. Arguably, bonds and also derivatives are the natural candidates for the first implementation of distributed-ledger-based trading, because digital versions of these instruments can take advantage of smart contract features, e.g. by automating coupon payments. Our analysis therefore is well-positioned as a starting point for a debate on the market design with these new technologies. We illustrate that transparency

of a distributed ledger and its design of privacy options play a critical role, even in the absence of asymmetric information, and we leave an analysis on the role of asymmetric information in blockchain design for future work.

REFERENCES

Biais, Bruno, 1993, Price formation and equilibrium liquidity in fragmented and centralized markets, *The Journal of Finance* 48, 157–185.

——— , Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, 2017, Blockchain folk theorem, Working paper Universite Toulouse.

Brummer, Chris, 2015, Disruptive technology and securities regulation, *Fordham Law Review* forthcoming.

Buterin, Vitalik, 2016, Ethereum: Platform review, opportunities and challenges for private and consortium blockchains, Discussion paper, Ethereum Foundation http://www.r3cev.com/s/Ethereum_Paper-97k4.pdf.

Catalini, Christian, and Joshua S Gans, 2016, Some simple economics of the blockchain, Discussion paper National Bureau of Economic Research.

Christoffersen, Susan Kerr, Erfan Danesh, and David K. Musto, 2015, Why do institutions delay reporting their shareholdings? Evidence from form 13f, Working Paper No. 2661535 Rotman School of Management Working Paper.

Cong, Lin William, Zhiguo He, and Jingtao Zheng, 2017, Blockchain disruption and smart contracts, Working paper University of Chicago.

Cujean, Julien, and Remy Praz, 2015, Asymmetric information and inventory concerns in over-the-counter markets, *Working Paper*.

Danesh, Erfan, 2015, Strategic trading and delayed disclosure by informed traders, Working paper Rotman School of Management, University of Toronto.

De Frutos, M. Ángeles, and Carolina Manzano, 2002, Risk aversion, transparency, and market performance, *The Journal of Finance* 57, 959–984.

Diamond, Peter A, 1982, Aggregate Demand Management in Search Equilibrium, *Journal of Political Economy* 90, 881–94.

Duffie, Darrell, Nicolae Garleanu, and Lasse Heje Pedersen, 2005, Over-the-counter markets, *Econometrica* 73, 1815–1847.

Evans, David S., 2014, Economic aspects of bitcoin and other decentralized public-ledger currency platforms, Discussion Paper, No. 685 University of Chicago Coase-Sandor Institute for Law & Economics Research Paper.

Gehrig, Thomas, 1993, Intermediation in search markets, *Journal of Economics & Management Strategy* 2, 97–120.

Harvey, Campbell R., 2015, Cryptofinance, Working paper Fuqua School of Business.

Khapko, Mariana, and Marius Zoican, 2017, Smart settlement, Working paper University of Toronto.

Kroll, Joshua, Ian Davey, and Edward Felten, 2013, The economics of bitcoin mining or bitcoin in the presence of adversaries, *Proceedings of WEIS*.

Kyle, Albert S., 1985, Continuous auctions and insider trading, *Econometrica* 53, 1315–1336.

Lester, Benjamin, Guillaume Rocheteau, and Pierre-Olivier Weill, 2015, Competing for order flow in otc markets, *Journal of Money, Credit and Banking* 47, 77–126.

Miao, Jianjun, 2006, A search model of centralized and decentralized trade, *Review of Economic Dynamics* 9, 68 – 92.

Pagano, Marco, 1989, Trading volume and asset liquidity, *The Quarterly Journal of Economics* 104, 255–274.

Rubinstein, Ariel, and Asher Wolinsky, 1985, Equilibrium in a market with sequential bargaining, *Econometrica* 53, 1133–1150.

Vayanos, Dimitri, and Tan Wang, 2007, Search and endogenous concentration of liquidity in asset markets, *Journal of Economic Theory* 136, 66 – 104.

Weill, Pierre-Olivier, 2002, The liquidity premium in a dynamic bargaining market, Working paper Stanford University.

Yavas, Abdullah, 1996, Search and Trading in Intermediated Markets, *Journal of Economics & Management Strategy* 5, 195–216.

Yermack, David, 2017, Corporate governance and blockchains, *Review of Finance* 21, 7.

Yin, Xiangkang, 2005, A comparison of centralized and fragmented markets with costly search, *The Journal of Finance* 60, 1567–1590.

Appendix: The Intermediated Market

We assume that there are $N > 0$ intermediaries. When asked to sell quantity q (i.e., when an investor wants to buy q units), each intermediary maximizes their expected utility by selling $q_i(p)$; in equilibrium the price clears the market so that $\sum_{i=1}^{N} q_i(p) = q$. At the beginning of each stage game, intermediaries hold no inventory. An intermediary may hold a position when contacted by a front-runner, as a consequence of an earlier trade with the liquidity demander. He also holds a position when approached by the liquidity demander who has been front-run by the liquidity provider. We derive the price in the intermediated market, assuming that an intermediary holds a position I_i.

With negative exponential (i.e., CARA) utility of wealth w, $u(w) = -e^{-\kappa w}$, where $w = -(v-p)q_i + I_i \cdot v$ and v denotes the asset value, the intermediary chooses quantity q_i given price p, in order to maximize his expected utility, $\max_{q_i} \mathsf{E}U[-(v-p)q_i(p) + I_i \times v]$. For CARA-normal frameworks, this task reduces to maximizing the certainty equivalent for each price p:

$$\max_{q_i}[I_i \times V - (V-p)q_i] - \frac{\kappa}{2}\sigma^2[-q_i + I_i]^2,$$

where V denotes the expected value of the asset; in the main text, we assume $V = 0$. The maximization problem results in the following first order condition:

$$V - p - \kappa\sigma^2 \times I_i + \kappa\sigma^2 q_i = 0.$$

Solving this equation for q_i yields the demand schedule

$$q_i(p) = -\frac{V-p}{\kappa\sigma^2} + I_i.$$

The market clearing condition

$$\sum_{i=1}^{N} q_i(p) = q$$

implies, substituting for q_i, and simplifying, that

$$\sum_{i=1}^{N} \left(-\frac{V-p}{\kappa\sigma^2} + I_i \right) = q \quad \Leftrightarrow \quad p^{\mathsf{mm}}(I,q) = V + \frac{\kappa\sigma^2}{N}\,(-I+q), \tag{29}$$

where I denotes the combined inventory of the intermediaries: $I = \sum_{i=1}^{N} I_i$. We further simplify the exposition by defining the (il-)liquidity factor ℓ as follows

$$\ell := \frac{2\kappa\sigma^2}{N}.$$

Price changes in this model occur for two reasons: changes in the fundamental, and trades due to liquidity shocks. When an investor approaches the intermediaries who hold total inventory I in order to buy q units, and the investor's payoff is

$$\pi^{\mathsf{mm}}(I,q) = q \times (V - p^{\mathsf{mm}}(I,q)) = -\frac{\ell}{2}\,q(q-I).$$