创业与管理学院

School of Entrepreneurship and Management

SHANGHAITECH SEM WORKING PAPER SERIES
No. 2020-010

An Impossible Trinity in Blockchain-based Transactions: Decentralization, Privacy, and Lower Transaction Costs

Soo Jin Kim

ShanghaiTech University

August 5, 2020

https://ssrn.com/abstract=3668057

School of Entrepreneurship and Management
ShanghaiTech University
http://sem.shanghaitech.edu.cn

An Impossible Trinity in Blockchain-based Transactions: Decentralization, Privacy, and Lower Transaction Costs

Soo Jin Kim*

August 5, 2020

Abstract

Decentralized blockchain-based transactions benefit users through their openness, transparency, and immutability, which may come at the expense of privacy concerns. This paper shows that if there is a dilemma between decentralization and privacy protection, such that a more decentralized system increases the risks of data leakage, allowing additional privacy protection within the blockchain network at a cost, such as hiring mixers, does not resolve the initial dichotomy. However, if non-protected users benefit from positive externalities from the additional protection provided to protected users, such that all users enjoy less privacy concerns with double protection, the dilemma of decentralization and privacy risks can be resolved, despite the higher transaction costs required. Thus, double privacy protection at a cost transforms the problem with a dilemma into one with a trilemma.

Keywords: Privacy, Decentralized Platform, Blockchain

JEL Classification Numbers: L10, L17, L86

*sjkim@shanghaitech.edu.cn; School of Entrepreneurship and Management, ShanghaiTech University, Room 436, 393 Middle Huaxia Road, Shanghai.

1 Introduction

A blockchain is a decentralized digital ledger that records a series of transaction data in its database called blocks. The blockchain system is decentralized in the sense that each economic agent has its own ledger, such that anyone in the network, without having centralized power, can validate whether a transaction request is authentic. The whole point of blockchain technology is decentralization, which can be achieved by having public blockchains. Public blockchains are permissionless systems by nature, in that no prior permission from the users' or miners' end is needed to use the service. Additionally, data recorded in public blockchain systems are transparently open to the public and are immutable, which means that everyone can see all the past transactions for anyone. The decentralization feature is inextricably linked with openness and transparency: to allow any user in a decentralized blockchain to check the validity of a transaction request, the system provides the user with an opportunity to look through the history of transactions. However, a decentralized blockchain with openness, transparency, and immutability, which creates trust among users even without a centralized authority, has some flaws: since any member of the public can access the historical data of transactions made in the platform, privacy is at risk. Although many people believe that records on blockchain are fully anonymized and seem to protect user privacy, users' transaction-related data are only pseudonymized and not perfectly anonymized. If attackers try to trace a user's history, it is technically possible that entire transaction histories will be leaked.

If users in a blockchain can be traced back and matched with their true identities, the blockchain system could violate privacy. Several studies show that Bitcoin users' private information can be obtained by linking their pseudonymized accounts with IP addresses or other external data such as cookies (e.g., Biryukov et al., 2014; Biryukov and Pustogarov, 2015; Goldfeder et al., 2017; Koshy et al., 2014). Other studies in computer science show that deanonymizing blockchain users' identities and tracing their true identities are feasible (e.g., Androulaki et al., 2013; Barcelo, 2007; Meiklejohn et al., 2013; Reid and Harrigan, 2013).

Indeed, putting privacy at risk in a transparent and open blockchain is more common and easy than one would think. To detect cyber-crimes using blockchain technology, the US government has developed a deanonymizing technique to uncover pseudonymized transaction

data.[1] The fact that the Internal Revenue Service (IRS) and the Federal Bureau of Investigation (FBI) have tracked Bitcoin transactions that were involved with money laundering and tax evasion and revealed the true identities of the users involved also shows that deanonymization in blockchain is doable. There are even companies that link identities to public blockchain addresses to track all Bitcoin activities, which is literally deanonymization.[2] In this regard, Catalini and Gans (2019) point out that users might need to take extra care to protect privacy because the entire transaction history under a pseudonymized identity can be read on the public blockchain if a user does not change the public address every time.[3]

As blockchain technology has been applied to a variety of fields, not only cryptocurrencies but also data storage and management, several plausible measures for additional privacy protection have been introduced. For public blockchains, such as Bitcoin and Ethereum, users can enhance their privacy by using a fresh address for each transaction. Alternatively, users can adopt an additional service such as a mixing service that collects multiple input addresses together and broadcasts with a time lag to obfuscate users' transactions. Some privacy-sensitive users might use a fully anonymous blockchain system with zero-knowledge cryptography, which allows one to verify transaction information without revealing additional personal data, such as Zcash. Although taking such additional actions somewhat resolves the conflict between decentralization and openness on the one hand and privacy protection on the other, it imposes an additional transaction cost on users, in either monetary or non-monetary terms: for example, using a mixing service is costly (e.g., SmartMix charges approximately 0.5% of the mix per output request) and using fresh addresses for each transaction can be labor intensive.

Concerning these points, one interesting question underlying blockchain technology is about an impossible trinity in blockchain-based transactions: it is impossible to simultaneously have (1) a perfectly decentralized platform, (2) privacy-enhancing transactions, and (3) lower transaction costs. Regarding this trilemma involving privacy concerns, several specific questions are

[1]Refer to https://thenextweb.com/hardfork/2018/12/04/us-government-cryptocurrency-forensics/ and https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts.

[2]Refer to https://ledgerops.com/blog/blockchains-arent-anonymous-but-they-can-be/05/01/2019 and https://hackernoon.com/privacy-on-the-blockchain-7549b50160ec.

[3]A recent Department of Justice (DoJ) report also states that individual blockchain users are likely to use the same public addresses multiple times for convenience, which eventually makes their transactions traceable. Refer to Criminal Complaint, USA v. Tibo Lousee, Klaus-Martin Frost, and Jonathan Kalla: https://www.justice.gov/opa/press-release/file/1159706/download.

raised in this paper. How does costly privacy protection affect the equilibrium size of blockchain users? Does allowing additional privacy protection at a cost always reduce the conflict between decentralization and privacy risks? When do we face this trilemma in a blockchain network?

As stated above, a perfectly decentralized blockchain system might put users' privacy at risk because of its open and transparent record-keeping system, which makes deanonymization feasible. If users choose a private blockchain in hopes of keeping the permissionless public from seeing their transaction histories even though they are pseudonymized, they end up having a less decentralized system. In this regard, I set up a theoretical model to show the trilemma in blockchain between decentralization, privacy protection, and lower transaction costs. The main player of the game is a unit mass continuum of users i who have a single transaction to complete. A user can complete a transaction using either a (public) blockchain (e.g., Bitcoin) or a centralized system (e.g., Paypal) as an outside option. Each user is heterogeneous with respect to privacy sensitivity. When using a blockchain, a user who is relatively privacy-sensitive might employ additional privacy-protecting technology such as a mixing service by incurring an additional transaction cost.

To model the relationship between decentralization and privacy in blockchain, I consider relevant metrics. First, I define the number of active addresses (or users) on the blockchain as decentralization metrics following Hinzen et al. (2019): I assume that the more active users there are with transactions in the system, the higher the proportion of the weights of miners with similar or equal power, which means more decentralization. As more transactions are settled, the blockchain accumulates more data, which means that more transparent data are open to the public. Depending on the types of privacy risks, having more open data availability on the blockchain can increase or decrease the privacy risks. That is, privacy risks are modeled as a function of the number of active users on the blockchain, i.e., decentralization metrics. Regarding individual-level privacy risks, i.e., personal data leakage, as several previous studies mention (e.g., Androulaki et al., 2013; De Filippi, 2016; Wang and Kogan, 2018), having more data means that there are more pieces of the puzzle, which are more easily fitted together, thereby allowing attackers to infer users' true identities. On the other hand, the risks could also decrease as more data are collected from a large number of users: it is easier for a user to hide himself in a crowd. To take every possible case into account, the model makes a flexible assumption about the functional form of the privacy risk: it can be either increasing

or decreasing in terms of decentralization metrics. Specifically, privacy risks that increase with the degree of decentralization of the blockchain reflect the dilemma between decentralization and privacy-enhancing transactions. The miner's strategy as well as the mixer's pricing game are abstracted from the main analysis.

First, I find that when additional privacy protection is available at a relatively low cost, more users choose blockchain over a centralized platform to settle transactions. However, if users have greater privacy concerns as the system becomes more decentralized, such that we face the dilemma between decentralization and privacy protection, allowing an additional privacy protection measure does not resolve the dilemma. In contrast, if there is no such dilemma in the first place, as with privacy risks decreasing in decentralization metrics, allowing additional privacy protection for individual users makes all users collectively better off by having a more decentralized and secure system if the cost is low enough that more users are attracted to blockchain.

Additional privacy protection employed by relatively privacy-sensitive users can have positive externalities for nonprotected groups of users. For instance, if some transaction counterparties adopt additional privacy protection, but the user does not doubly protect his/her own privacy, the amount of transaction data that is vulnerable to data leakage still decreases. When privacy risks increase in the decentralization metrics, allowing additional protection with positive externalities leads to a trilemma in blockchain: it can resolve the dilemma of decentralized or privacy protection only at a higher transaction cost.

I also compare the critical mass with and without additional privacy protection. The critical mass is the minimum number of users that the blockchain system must attain to reach a stable equilibrium number of users. Interestingly, even if additional protection increases the demand for blockchain, there is no guarantee that it is also easy to make the system successful with a lower critical mass. In other words, when a blockchain system implements additional privacy protection at a sufficiently low cost, this additional feature might require a greater initial burden with a higher critical mass to make the system stable. Whether an additional protection necessitates a smaller or larger critical mass depends on the effectiveness of the additional protection. If the blockchain platform provides highly effective privacy protection at a low cost, it can attract a large volume of users even with a small number of initial users: that is, a small critical mass is required for widespread adoption. However, if the privacy protection

it provides is not effective at reducing privacy costs, but still inexpensive, a larger critical mass is necessary to achieve widespread adoption in equilibrium. In this case, blockchain with additional protection requires a more serious initial effort to be successful even if it ultimately attracts more users to blockchain.

Previous Literature There have been a handful of previous studies on blockchain-related topics in economics. The stream of literature most closely related to my work includes research on how blockchain is related to trust and user privacy. Athey et al. (2017) show the privacy paradox using cryptocurrency experiments. Catalini and Gans (2019) mention that the pseudonymous nature of blockchain may allow a user's entire history of transactions to be disclosed to the public if s/he is ever tied to a specific public address in blockchain. Böhme et al. (2015) describe multiple aspects of Bitcoin and point out that significant privacy concerns remain in Bitcoin transactions. Franke et al. (2019) study the effects of privacy-preserving (private) blockchain on generating trustworthy information about firms fundamentals. Cong and He (2019) discuss many different forms of tradeoffs arising from decentralization, one of which is concern about decentralization and privacy. However, none of the abovementioned papers places a primary focus on the effect of blockchain on resolving or increasing users' privacy concerns, which I consider in this paper.

Outside of the field of economics, several works in the computer and information science literature address certain technical but practical questions, such as how privacy is at risk in blockchain (Böhme et al., 2015; Conti et al., 2017; De Filippi, 2016; Feng et al., 2018; Halpin and Piekarska, 2017; Hassan et al., 2019; Henry et al., 2018; Kshetri, 2018; Reid and Harrigan, 2013; Wang and Kogan, 2018; Zhang et al., 2019),[4] how to deanonymize users' identities in blockchain to link them to the true identities (Androulaki et al., 2013; Barcelo, 2007; Biryukov et al., 2014; Biryukov and Pustogarov, 2015; Goldfeder et al., 2017; Koshy et al., 2014; Meiklejohn et al., 2013; Reid and Harrigan, 2013), how to enhance user privacy in blockchain system (Bonneau et al., 2014; Fabian et al., 2018; Feng et al., 2019; Henry et al., 2018; Josh et al., 2018; Kshetri, 2018; Onik et al., 2019; Parizi et al., 2019), and how trust-free systems in blockchain reshape the problems of principal agency and information asymmetry (Hawlitschek et al., 2018; Mehrwald et al., 2019).[5] Specifically, Henry et al. (2018) mention that it is technically possible that if an

[4]For short articles, refer to https://www.technologyreview.com/s/608716/bitcoin-transactions-arent-as-anonymous-as-everyone-hoped/.

[5]In economics, Arruñada and Garicano (2018) study similar issues, focusing on the effect of blockchain on

attacker observes that a user receives money via cryptocurrency right before visiting a website, the attacker can suspect the linkage between the pseudonymized identity in blockchain and the true identity. Kshetri (2018) points out that if sellers access consumer blockchain-based transaction histories showing consumer spending patterns, they could use this information to increase prices.

Several studies also show that taking extra care to protect privacy still leaves a loophole. Androulaki et al. (2013) conduct an experiment showing that 40% of pseudonymized user profiles in the Bitcoin system are recovered even when each user uses a fresh address for each transaction. Al Jawaheri et al. (2019), Biryukov and Pustogarov (2015), Kappos et al. (2018), and Möser et al. (2018) show that adding anonymity to Bitcoin transactions through Tor or other technology with zero-knowledge proof still allows attackers to deanonymize users' identities.

In addition to those with a privacy-related focus, there are a few studies on the effect of blockchain on innovation and competition. Catalini et al. (2019) study how blockchain technology shapes innovation and competition in digital platforms. Allen et al. (2020) investigate the effect of blockchain on innovation policy. Several other papers study how to solve asymmetric information problems through trustless blockchain mechanisms (Arruñada and Garicano, 2018; Bakos and Halaburda, 2019; Berg et al., 2017).

Additionally, a few papers analyze trilemmas in blockchain systems, as in my paper. Abadi and Brunnermeier (2019) show that it is not possible to have a sustainable blockchain that is simultaneously self-sufficient, rent-free, and resource-efficient. Hinzen et al. (2019, 2020) show the trilemma of scalability, security, and decentralization in blockchain empirically and theoretically, respectively. In the computer science literature, Das et al. (2018) show the blockchain trilemma of strong anonymity, low bandwidth overhead, and low latency. However, my focus in this paper is a specific trilemma associated with individual-level privacy concerns in a blockchain system. Going one step further from the dilemma between decentralization/transparency and privacy, I take the possibility of improving privacy protections into consideration by incurring additional transaction costs.

In a broader sense, this paper is also relevant to other blockchain-related topics in economics. Given the relatively well-known dilemma between scalability and decentralization in blockchain,

the coordination problem.

some papers study how to improve efficiency in blockchain-based transactions without compromising their benefits. Ma et al. (2018) provide a theoretical foundation to show that free entry is the main cause of the Bitcoin payment system being resource-inefficient. Budish (2018) casts doubt on whether there is some other approach to generating anonymous and decentralized trust in a public ledger that is less economically constrained by the possibility of an attack. Sockin and Xiong (2018) show how to facilitate decentralized bilateral transactions by modeling a cryptocurrency as membership in a platform. Several papers set up a game-theoretic model to analyze strategies chosen by mixers and users (Aoyagi and Adachi, 2019; Arnosti and Weinberg, 2018; Mat et al., 2018; Liu et al., 2019; Biais et al., 2019; Carlsten et al., 2016; Iyidogan, 2019; Easley et al., 2019; Halaburda and Haeringer, 2019). Focusing on cryptocurrencies, there are a number of recent studies on broader questions, such as the existence and adoption of Bitcoin, the pricing of cryptocurrencies, and the impacts on fiat money (Athey et al., 2016; Chen et al., 2019; Cong et al., 2020a,b; Halaburda, 2018; Huberman et al., 2019; Schiling and Uhlig, 2018; Menuier and Zhao-Meunier, 2019). In contrast, I focus specifically on a relatively underexplored area: how the core of the blockchain system, which is decentralization, could place user privacy at risk and how this dilemma can be resolved by taking additional measures using a theoretical model in economics.

2 Background

A blockchain is a decentralized digital ledger that records a series of transaction data in its database called blocks. When a user places a transaction request, it is broadcast to a blockchain peer-to-peer network of nodes. The transaction information is verified by the nodes (i.e., miners) in the network and recorded in a new block, which is added to the blockchain. Miners receive rewards in cryptoassets based on the predetermined system. In the case of proof-of-work (PoW), the nodes (i.e., miners) need to verify the transaction information by solving very complicated math problems. In the case of proof-of-stake (PoS), a miner who owns more cryptoassets (i.e., coins), even with a simple computer, is more likely to be assigned as a validator.

There are multiple properties of blockchain technology. This paper focuses on the following three main properties: decentralization, openness and transparency (in terms of privacy protection), and no (or possibly small) transaction costs.

2.1 Decentralization

When an economic agent wants to engage in an online transaction, say buying a computer online, s/he may need to take additional care to avoid consumer disputes because such online transactions have higher risks of security than offline transactions. To do so, the buyer can look up the sales histories of potential sellers, i.e., ledgers that contain a collection of records. The method of authenticating a ledger, thereby reaching a consensus about its current true state, can be either centralized or decentralized. If there are trusted intermediaries, such as governments, commercial banks, and ecommerce platforms, which certify the ledger and authenticate transactions between buyers and sellers, then the system is centralized. If instead each economic agent has its own ledger, such that anyone in a network, with no centralized power, can validate whether a transaction request is authentic, then the system is decentralized—each agent ends up having the same shared ledger in a distributed way. Blockchain is known as a decentralized digital ledger: it is trustless in the sense that it distributes trust among different agents in a network without having a central authority.

Such a blockchain can be either public (permissionless) or private (permissioned).[6] Although both types of system are decentralized, they are different in terms of accessibility. A public blockchain is completely open; therefore, no prior permission is needed to use the service. Bitcoin and Etherium are well-known examples of public blockchains. On the other hand, a private blockchain is a closed network in that a user needs to acquire permission to fully access the system. For the rest of the paper, I focus on a public blockchain that is more decentralized in nature with open accessibility.

2.2 Openness, Transparency, and Immutability (Privacy in Blockchain)

A transaction record in blockchain contains data on a pair of pseudonyms for the sender and receiver.[7] Such pseudonymized identities, also known as addresses (hashed public keys),[8] recorded in each block are open to the public, whereas the true identities of users (or private keys that are used to sign the transactions) are not available to the public. Pseudonymized data are

[6] Waelbroeck (2018) contains a helpful description of this aspect.

[7] Although there are other privacy-enhancing types of blockchain with full anonymity, such as Zcash, I focus on more common types of blockchain-based distributed ledgers with pseudonymity, such as Bitcoin.

[8] Throughout the paper, keys and addresses are used interchangeably.

open in the sense that everyone can access any information without permission and verify the transaction information; it is not only permissionless but also open-source. Additionally, everyone can see all the past transaction histories for anyone recorded in blockchain under public pseudonyms; thus, blockchain is transparent.

Related to these properties, it is debatable whether blockchain is a privacy-protecting or privacy-harming technology. Even if only the non-personally identifiable information behind public addresses is open to the public and the private keys are only visible to users themselves, it is technically possible to link multiple pseudonymized transactions recorded in the ledger in order to deanonymize data as long as a sufficient amount of data is available; in that sense, the data in blockchain are pseudonymous. If the users in blockchain can be traced back and matched with true identities, the blockchain system could invade privacy. That is, user privacy in blockchain is not guaranteed due to its transparency and openness.

2.3 (No) Transaction Costs in Blockchain

Technically, making a transaction in blockchain entails relatively low transaction costs. However, depending on what else the user demands, there could be additional costs per transaction. In this paper, I focus on such additional transaction costs spent to improve privacy in blockchain-based transactions. For instance, if users feel uneasy due to the blockchain's transparent system, they can implement additional measures to doubly protect their privacy. The simplest and easiest way of protecting privacy in blockchain is to use a fresh public address for each transaction, which can be overly burdensome, incurring nuisance costs. Additionally, users can hire *mixers* through mixing services, such as CoinJoin, to broadcast their transaction information on a delay by mixing it with other data. Then, it becomes more difficult to track down the personal information of an individual user by matching it with external data because a number of transactions are broadcast simultaneously, and this keeps attackers from identifying users' true identities; for example, SmartMix charges approximately 0.5% of the mix per output request. Alternatively, users can disguise their IP addresses by using a virtual private network to doubly protect their privacy. Recently, more privacy protecting models have been proposed that use zero-knowledge proof (e.g., Zcash or Monero), which allows one to verify transaction information without revealing additional personal data: however, it may take more

time to complete a transaction that requires more computing power.[9] In any case, such additional protection measures incur positive transaction costs, in either monetary terms (as in mixing services) or non-monetary terms such as nuisance costs or more time being required to complete a transaction (as in using fresh addresses or in Zcash).

3 Models

The main player of the game is a unit mass continuum of users $i \in [0,1]$ who have a single transaction to complete. A user can complete a transaction using either a (public) PoW blockchain such as Bitcoin or a centralized system such as Paypal as an outside option. When using a blockchain, a user might employ additional privacy-protection technology such as a mixing service. The miner's strategy as well as the mixer's pricing game are abstracted from the main analysis.

3.1 Blockchain Model

I first define three metrics for decentralization, privacy, and transaction costs to analyze how these three properties work together in a blockchain.

Decentralization Metrics If a blockchain network is decentralized, there is no single central entity that governs the verification process or access to information. Several previous studies employ different decentralization metrics. Gencer et al. (2018) measure the degree of decentralization using the distribution of mining power according to the ratio of main chain blocks generated by distinct entities; for instance, they show that the top four miners have more than 53% of the average mining power in Bitcoin. Similarly, Chu and Wang (2018) quantify decentralization by using the distribution of transactions contributed by different miners. In contrast, decentralization is measured by the number of functioning peers (i.e., nodes) in networks in Croman et al. (2016). Hinzen et al. (2019), following Cong et al. (2020a,b), measure decentralization in terms of the number of active addresses on the blockchain. I also define the degree of decentralization in a blockchain by the number of active users, denoted as $N \in [0,1]$,

[9]For example, completing a transaction using Bitcoin (known to be a less privacy protecting coin) takes 10 minutes on average, whereas doing so using Monero (known to be a more privacy protecting coin) takes 20 minutes. Refer to https://www.exodus.io/blog/monero-vs-bitcoin.

where each user is atomless; the total size of users is normalized to one. As in Hinzen et al. (2019), users (or addresses) are active if they engage in a transaction on a given day. I further assume that each user in a blockchain finishes a single transaction; thus, the number of active users can also be interpreted as the number of transactions in a blockchain. The underlying assumption here is that the more active users with transactions there are in the system, the higher the proportion of the weights of miners with similar or equal power, which means there is more decentralization.

Privacy Metrics A blockchain accumulates additional data every day. As more transparent data are made available to the public, privacy risks can either increase or decrease. Broadly speaking, there can be two different types of privacy risks: individual-level data leakage threats (user privacy concerns) and system-level security threats (system security concerns). Depending on how we define privacy and security risks, the overall privacy risks can increase or decrease with the degree of decentralization. Whereas most previous studies focus on the tradeoff between decentralization and systematic security, I focus on the individual-level privacy risks.

The overall individual-level privacy risks, which lead to pseudonymized data being matched with the true identities, in a blockchain network depend on the size of the network. Given that the number of active users or addresses reflects the size of the blockchain, I assume that the costs associated with privacy risks, denoted as $Q(N; s) \in (0, 1)$, are a function of N, the decentralization metric as measured by the number of active users, where s denotes the security system of the blockchain, which is assumed to be given exogenously, and $\frac{\partial Q(N;s)}{\partial s} < 0$; the more secure the system is, the less risky, in terms of data leakage, the blockchain system is.

Regarding the sign of $\frac{\partial Q(N;s)}{\partial N}$, individual-level identity leakage risks can either increase or decrease with the degree of decentralization, captured by N. On the one hand, having more data means that there are more pieces of the puzzle, which are more easily fitted together. That is, an attacker could obtain more pseudonymized transaction data about a user, which makes it easier to match the user to a real identity: in this regard, De Filippi (2016) notes that more information can be inferred if there are more transactions. Thus, more data may lead to more malicious attacks that trace past transactions to deanonymize users' identities: the risk of data leakage increases as the system becomes more decentralized; i.e., the more a user engages in blockchain-based transactions, the greater the risk that his/her true identity will be matched with pseudonymous information in the blockchain—i.e., $\frac{\partial Q(N;s)}{\partial N} > 0$.

On the other hand, having more information in the blockchain can also decrease identity leakage risk as the blockchain becomes more decentralized, i.e., the longer a chain is, the more difficult a privacy attack is: $\frac{\partial Q(N;s)}{\partial N} < 0$. This logic is reasonable in the sense that the existence of more transactions makes it more difficult for an attacker to discover specific transactions made by each user because it is easy to hide within a crowd consisting of a practically infinite number of transactions.[10] To accommodate all of the possibilities here, namely whether individual-level privacy risks are increasing in N (with $\frac{\partial Q(N;s)}{\partial N} > 0$) or decreasing in N (with $\frac{\partial Q(N;s)}{\partial N} < 0$), both cases are analyzed in Section 4.

Note that the privacy risks are affected not only by the number of personal transactions but also by the total number of transactions completed by all users in the blockchain. Such information externalities exist given that users interact with each other by trading in blockchains. For Bitcoin transactions, for instance, because users can be either senders or receivers of Bitcoin, transaction data might be revealed not only by the requests of a user but also by his/her counterparties' requests. Concerning this point, Androulaki et al. (2013) mention that as an attacker comes to know more addresses in a blockchain, s/he has a more complete view of the network. Similarly, Wang and Kogan (2018) state that the more users are added to a blockchain, the less confidential it is. In contrast, a blockchain with a small number of users is less likely to attract attackers, so the overall risks of data leakage are lower.

Transaction Costs The model assumes that there is a transaction cost paid by users. In addition, I consider additional per-transaction costs for users to protect their privacy in hopes of further anonymizing their identities. For instance, if users hire mixers to make de-pseudonymization difficult, it incurs a cost of $c \in \mathbb{R}^+$ per transaction.

3.2 User's Utility Function

There is a unit mass continuum of users $i \in [0, 1]$. Each user i is heterogeneous with respect to privacy sensitivity, denoted as τ_i, which is distributed over $F[0, 1]$ with a density of f, where $F(0) = 0$ and $F(1) = 1$. User i becomes more privacy-sensitive as τ_i increases. Each user engages in a transaction on a given day. User i can use either a blockchain network or a well-established centralized alternative platform such as Paypal. The main driving factor that

[10] Refer to https://www.ibm.com/blogs/blockchain/2017/12/blockchain-security-what-keeps-your-transaction-data-safe/.

affects the user's choice is how effective a platform is in preserving privacy (or providing less risk). If the user chooses a blockchain (or a centralized platform), s/he is an active (or inactive) blockchain user. The total mass of active users is the demand for the blockchain network. The net utility for each user i of using the blockchain network is given as follows:

$$u_i = v \times N - \phi - (1 - \mathbb{1}_{i\in\mathcal{P}})\tau_i \times Q(N;s) - \mathbb{1}_{i\in\mathcal{P}}(\tau_i \times \psi Q(N;s) + c), \tag{1}$$

where v is the base utility of the blockchain and ϕ is a fee paid to a miner who successfully verifies and creates a block; the competition between miners with different computing powers is abstracted from the main analysis. The reward for miners given by the blockchain network is normalized to zero. The indicator function $\mathbb{1}_{i\in\mathcal{P}}$ is one if user i implements additional protection for his/her privacy and zero otherwise (i.e., if individual i does not protect his/her privacy, $i \in \mathcal{NP}$). Finally, $\psi \in (0,1)$ measures the amount of privacy-relevant cost savings obtained by implementing additional privacy protection, such as hiring mixers. The first term in the utility specification captures a positive network effect in the blockchain, in that the user's utility is higher if the system becomes more decentralized with a larger number of active users; Hinzen et al. (2019) show empirically that the demand is larger for a more decentralized blockchain.

The utility of an alternative centralized platform is normalized to zero. This implies that only users who sufficiently reduce privacy costs by using blockchain choose it over the alternative. The user knows that using an alternative centralized platform, such as Visa or Paypal, has both advantages and disadvantages. A traditional centralized platform with a greater market power usually charges higher usage fees, such as annual membership fees in the case of credit cards, whereas a blockchain platform charges a relatively lower price. In the model, this aspect is captured by ϕ: the average ϕ in the blockchain system is lower than that in a centralized outside option. However, users have formed trust in those centralized alternatives over a long period of time. Because of the positive network effects arising from this trust, using established services is more convenient; to date, sellers have been more accepting of traditional centralized payment methods than decentralized cryptocurrencies. This established trust is captured in the base utility v: the v of using a blockchain is lower than for the alternatives.

Given that there is a tradeoff between these two aspects, how much a transaction in the blockchain heightens or alleviates privacy concerns plays a critical role in adoption decisions. A centralized network faces a higher risk of single-point failure because only a centralized

authority, i.e., the company itself, has full information about the transaction histories of a specific user. A data breach following a single point failure, though unlikely to happen, seriously harms users' privacy. In terms of a network-wide single-point failure, blockchain networks are known to be safe because they are decentralized. This advantage of blockchain is reflected in s, which decreases the privacy risk $Q(N;s)$. Even for individual-level privacy risks, blockchains without single-point failure risks can better protect users' privacy by having only pseudonymized data. Nevertheless, their openness and transparency can disincentivize relatively privacy-sensitive users to adopt blockchain due to the fear that their true identities will be matched with pseudonyms. This reluctance is modeled as the privacy risk, $Q(N;s)$, which is a function of the total number of blockchain users N. For example, if $\frac{\partial Q(N;s)}{\partial N} > 0$, users are more likely to choose a centralized platform due to greater privacy concerns, as blockchain attracts more users with a growing number of transactions.[11] That is, if blockchain attracts many users with large N, although the users of blockchain enjoy a greater network benefit from more decentralization and relatively low usage fees, they face higher privacy-related costs. Each user makes an adoption decision by comparing the benefits and costs of using blockchain over a centralized platform.

For τ_i and $Q(N;s)$, this can also be interpreted as consumer i's risk aversion and the risk that keys will be lost or compromised. As Conti et al. (2017) explain, due to its decentralized feature, if a user loses the private key or the key is compromised by a hard drive crash or virus corruption, there is no way to recover all the Bitcoin in the wallet. Indeed, Krombholz et al. (2017) conduct a survey and show that 22% of Bitcoin users have lost money due to security breaches or lost keys. Assuming that the probability that a user loses his/her private key or the key is compromised is independent of how many transactions s/he makes (or is constant over time), s/he faces higher data security risks, which are irrevocable, the more cryptocurrency s/he has in a digital wallet. Given that more transactions in blockchain result in more cryptocurrency, a user faces higher data security risks as N increases; i.e., $\frac{\partial Q(N;s)}{\partial N} > 0$. In this scenario, τ_i indicates i's risk aversion when using a newly adopted decentralized blockchain-

[11] Even if N is sufficiently small, so is $Q(N;s)$, and blockchain users can face higher privacy risks in some cases because of the lack of prevalence. A small user base means that blockchain is not widely accepted by other transaction counterparties. Then, users are likely to convert blockchain-based cryptocurrencies into fiat money, such as US dollars, which ultimately reveals their blockchain addresses, thereby linking them to their true identities; Böhme et al. (2015) point out that blockchain-based transactions with pseudonymized data often reveal the true identities of users if funds are converted to fiat money.

based transaction without a trusted authority.

4 Equilibrium

In the game, user i first decides whether to use a blockchain to complete a transaction. Later, user i decides whether to hire a mixer to further de-pseudonymize his/her identity if such additional protection is feasible. I first investigate a game without any privacy protection as a benchmark and later look into what happens if privacy protection is allowed in the model. If no user employs additional privacy protection, the portion of users whose net utility from using the blockchain network is greater than zero is the total equilibrium number of blockchain users. That is, any user i whose $\tau_i \leq \frac{vN-\phi}{Q(N;s)} \equiv \bar{\tau}$ chooses a blockchain over the alternative. Proposition 1 summarizes this finding.

Proposition 1. *When an additional privacy-preserving means is not available, the equilibrium market share for the blockchain network, denoted as N^*, is implicitly determined by the following equation:*

$$N^* = F\left(\bar{\tau}\right), \tag{2}$$

where $\bar{\tau} = \frac{vN^*-\phi}{Q(N^*;s)}$.

Suppose now that a user i is allowed to employ additional privacy protection by hiring mixers at a cost of c. Given $\tau_i \sim F[0,1]$, relatively privacy-sensitive consumers with higher τ_i are more likely to hire mixers. For notational convenience, let $\mathcal{P}$ denote the privacy-protecting group that hires mixers, whereas $\mathcal{NP}$ denotes the non-protecting group. The threshold of τ, denoted τ^*, above which c is paid to mixers is derived as follows:

$$\tau^* = \frac{c}{(1-\psi)Q(N;s)}. \tag{3}$$

As above, users who are relatively privacy insensitive use blockchain. Since the privacy-protecting group of users is more privacy sensitive, a portion of $i \in \mathcal{P}$ does not choose to use blockchain for transactions due to having less trust in the system: a user $i \in \mathcal{P}$ whose $\tau_i \leq \frac{vN-\phi-c}{\psi Q(N;s)} \equiv \bar{\bar{\tau}}$ chooses blockchain over the alternative. The total equilibrium portion of participating users, denoted as $\widetilde{N^*}$, is derived in the following Proposition 2:

Proposition 2. *The total equilibrium portion of participating users, denoted as* $\widetilde{N^*}$*, is given by the solution* N *to the following equation:*

$$\widetilde{N^*} = F\left(\bar{\bar{\tau}}\right), \tag{4}$$

where $\bar{\bar{\tau}} = \frac{u\widetilde{N^*}-\phi-c}{\psi Q(\widetilde{N^*};s)}$.

Given τ^*, $P(i \in \mathcal{NP}|i \in \mathcal{BC}) \equiv F(\tau^*)$, whereas $P(i \in \mathcal{P}|i \in \mathcal{BC}) \equiv F(\bar{\bar{\tau}}) - F(\tau^*)$, where $i \in \mathcal{BC}$ means that user i transacts via a blockchain network. That is, we have $\mathcal{P} \equiv \{\tau_i : \tau^* \leq \tau_i \leq \bar{\bar{\tau}}\}$ and $\mathcal{NP} \equiv \{\tau_i : \tau_i < \tau^*\}$.

By comparing the equilibrium portion of blockchain users with and without additional privacy protection, as in Propositions 1 and 2, I analyze how such additional privacy-preserving means affect the willingness to adopt blockchain technology. Before doing so, I make the following assumption:

Assumption 1. *The threshold for* τ*, either* $\bar{\tau}$ *or* $\bar{\bar{\tau}}$*, is sufficiently concave in* N*, which guarantees that* $F(\bar{\tau})$ *or* $F(\bar{\bar{\tau}})$ *is concave in* N*.*

Assumption 1 means that the marginal direct network effect of having more participating users diminishes.[12]

Assumption 2. $sgn\{\dot{N}\}$=$sgn\{F(\bar{\tau}) - N\}$=$sgn\{F(\bar{\bar{\tau}}) - N\}$*, where* $\dot{N}$ *is the change in* N*.*

Assumption 2 simply means that the demand for a blockchain system always adjusts smoothly toward a well-informed equilibrium, as similarly described in Evans and Schmalensee (2010). Consistent with the product diffusion models, this assumption implies that because it takes time for users to learn new technology, such as blockchain, due to imperfect information, a blockchain system can successfully launch its service, thereby driving a stable equilibrium number of users, only after a certain number of other users have already adopted blockchain: the specific number of users that triggers explosive growth of the blockchain system is called the critical mass. Thus, a critical mass point is an unstable equilibrium. If the system does not reach a critical mass, which can be represented by $F(\bar{\tau}) < N$ or $F(\bar{\bar{\tau}}) < N$, it ends up failing to attract any users, leading to $N = 0$. If the system does attain a critical mass, which can be represented by $F(\bar{\tau}) > N$ or $F(\bar{\bar{\tau}}) > N$, it will reach a higher stable equilibrium. Assuming that

[12]The concavity of $\bar{\tau}$ is guaranteed by $-QQ''(vN-\phi) < 2Q'[uQ-Q'(vN-\phi)]$, whereas that of $\bar{\bar{\tau}}$ is guaranteed by $-QQ''(vN-\phi-c) < 2Q'[uQ-Q'(vN-\phi-c)]$ where $Q' = \frac{\partial Q(N;s)}{\partial N}$ and $Q'' = \frac{\partial^2 Q(N;s)}{\partial N^2}$.

the origin (at which $N = 0$) is a locally stable equilibrium, a necessary and sufficient condition for a stable and positive equilibrium number of users is $f(\bar{\tau})\frac{\partial \bar{\tau}}{\partial N} < 1$ or $f(\bar{\bar{\tau}})\frac{\partial \bar{\bar{\tau}}}{\partial N} < 1$, which intuitively implies that network effects at the local level are not very large, so that the system is stabilized. For ease of discussion, I define stable and unstable equilibria as follows:

Definition 1. *The unstable and stable fixed points satisfying* $N = F(\bar{\tau})$ *or* $N = F(\bar{\bar{\tau}})$ *are defined respectively by:*

$$\begin{aligned} N_C &\equiv \inf\{N|F(\bar{\tau}) \leq N\}; \quad N^* \equiv \sup\{N|F(\bar{\tau}) \geq N\}. \\ \widetilde{N_C} &\equiv \inf\{N|F(\bar{\bar{\tau}}) \leq N\}; \quad \widetilde{N^*} \equiv \sup\{N|F(\bar{\bar{\tau}}) \geq N\}. \end{aligned} \tag{5}$$

That is, the equilibrium numbers of users shown in Propositions 1 and 2 are stable. A critical mass in either case, with or without additional protection, is defined as N_C or $\widetilde{N_C}$. For now, my focus is only on stable equilibria. I revisit the critical mass in Section 4.4.

From Equations (2) and (4), whether additional privacy protection at the cost of c expands or shrinks the total blockchain market size depends on the relative sizes of c and ψ: if the cost of protection c is relatively low compared with the benefit captured by a smaller ψ, more users choose blockchain over a centralized platform, which implies that $N^* < \widetilde{N^*}$. In other words, there exists a threshold for c, denoted as $\bar{c} \equiv (vN - \phi)(1 - \psi)$, below which it is guaranteed that $N^* < \widetilde{N^*}$ and above which the reverse occurs. Proposition 3 summarizes this finding.

Proposition 3. *If the cost of privacy protection is sufficiently low compared with any benefit of it, the equilibrium portion of blockchain users is larger with such protection than without it.*

4.1 Lower privacy risks as N increases

How the change in N caused by additional privacy protection, as shown in Proposition 3, affects privacy risks depends on whether such risks increase or decrease with N.

First, I focus on the case of $\frac{\partial Q}{\partial N} < 0$. Here, individual-level privacy becomes less vulnerable as the network size increases with N. As shown above, if the cost of double protection c is relatively low, marginally privacy-sensitive consumers who refuse to engage in blockchain-based transactions because of the privacy risks are more likely to switch and use a blockchain system if better protection is available at a low cost: $N^* < \widetilde{N^*}$. Here, additional privacy protection makes blockchain users collectively better off in that it leads to a more decentralized

system with less risk of being hacked. However, if the cost of protection is relatively high, allowing additional protection attracts fewer users to join blockchain-based transactions, and the equilibrium ends up being collectively worse: blockchain users face a higher risk of insecurity with a less decentralized system.

Proposition 4. *When a blockchain system is less vulnerable to malicious attacks as more information is recorded, as long as the cost of additional protection is sufficiently low, allowing additional privacy protections for individual users makes all users collectively better off by having a more decentralized and secure system.*

Per Proposition 4, if privacy risks are decreasing in the degree of decentralization, the blockchain system faces no dilemma between decentralization and privacy protection. Then, the only thing that matters for a successful system is to have sufficiently low-priced privacy protection available in the system.

4.2 Higher privacy risks as N increases

Now, I focus on the case of $\frac{\partial Q}{\partial N} > 0$. This case reflects the dilemma between decentralization and individual privacy risks. Per Proposition 3, if it is costly to adopt additional privacy protection, i.e., c is relatively high, the total number of blockchain users is smaller with additional protection than without it ($N^* > \widetilde{N^*}$). Then, there is less individual privacy risk when users' privacy is doubly protected. Although such additional protection guarantees more privacy-preserving transactions, it leads to a less centralized blockchain system. Thus, the dichotomy between decentralization and privacy protection is salient.

Similarly, if c is sufficiently low, more users employ blockchain-based transactions when additional protection is feasible ($N^* < \widetilde{N^*}$), which leads to a more decentralized system. However, this benefit of greater decentralization comes at the expense of greater privacy risks; there is still a dilemma. The intuition behind this unresolved dilemma is as follows: As users engage in more transactions in blockchain because they feel more secure by paying a small fee c to doubly protect their identities, they do not internalize any negative externalities that individual decisions can generate. If $\mathcal{P}$ is non-empty, such that the blockchain system is more decentralized, there are negative externalities toward $i \in \mathcal{NP}$ in terms of privacy risks due to

$Q(\widetilde{N^*}; s) > Q(N^*; s)$. Even if an additional protection reduces the privacy costs for participating users $i \in \mathcal{P}$ to $\psi Q(\widetilde{N^*}; s)$, this risk-reducing effect can be negligible because of the overall increase in Q, especially if $\psi Q(\widetilde{N^*}; s) \simeq Q(N^*; s)$. Thus, when aggregated by considering all externalities due to individual decisions, the equilibrium number of blockchain users is too large from society's perspective. Proposition 5 summarizes these findings.

Proposition 5. ***(Blockchain Dilemma)*** *When a user's true identity is more likely to be revealed as more information becomes available in the blockchain system, allowing an additional privacy protection measure does not resolve the dichotomy between decentralization and privacy protection in the blockchain.*

In other words, if users face greater privacy concerns as the system becomes more decentralized, we face the dilemma between decentralization and privacy protection. Moreover, allowing additional privacy protection does not resolve the dilemma. Given that an additional cost of c does not resolve the dichotomy in any way, the blockchain system does not experience any trilemma. As I will show in Section 4.3, the trilemma can be observed when additional privacy protection generates positive externalities.

4.3 Privacy Protection with Externalities

So far, I have assumed that additional privacy protection employed by relatively privacy-sensitive users (i.e., $i \in \mathcal{P}$) does not have any direct externalities for the non-protected group, $i \in \mathcal{NP}$: the privacy costs for only users $i \in \mathcal{P}$ are reduced to $\psi Q(N; s)$. However, there might be some cases in which the double protection given by $i \in \mathcal{P}$ has positive externalities, such that even the privacy costs for the non-protected group of users are reduced to some extent. Suppose that each user makes ten transactions through blockchain on a given day. If some transaction counterparties adopt additional privacy protection, whereas a certain user does not doubly protect his/her own privacy, the amount of his/her transaction data that is vulnerable to data leakage still decreases. In this sense, the additional privacy protection provided by a certain portion of users may have positive externalities for the overall network. To capture this aspect, I first assume that non-protected users $i \in \mathcal{NP}$ face a lower privacy cost of $\widehat{Q}(N; s)$, where $\widehat{Q}(N; s) < Q(N; s)$, which implies that $i \in \mathcal{NP}$ enjoys an indirect privacy cost reduction

if the portion of the protected group is positive. For protected users $i \in \mathcal{P}$, the privacy cost is $\psi\widehat{Q}(N;s)$. Note that if no user adopts additional protection, $\widehat{Q}(N;s) = Q(N;s)$.

First, if no additional privacy protection is available, the equilibrium portion of blockchain users is given by Equation (2) in Proposition 1, which is the same as in the case without externalities. If additional protection is available, the threshold for τ, denoted as τ_E^*, above which c is paid for double protection, is derived as $\tau_E^* = \frac{c}{(1-\psi)\widehat{Q}(N;s)}$, where the subscript E denotes the case with externalities. The equilibrium portion of blockchain users when privacy protection generates positive externalities is given as follows.

Proposition 6. *When privacy protection generates positive externalities, the total equilibrium portion of participating users, denoted as $\widetilde{N_E^*}$, is given by the solution N to the following equation:*

$$\widetilde{N_E^*} = F\left(\bar{\bar{\tau}}_E\right), \tag{6}$$

where $\bar{\bar{\tau}}_E = \frac{u\widetilde{N_E^*} - \phi - c}{\psi\widehat{Q}(\widetilde{N_E^*};s)}$.

Next, I compare the equilibrium $\widetilde{N_E^*}$ to N^* to see how allowing additional privacy protection with positive externalities affects the total blockchain market size and how it ultimately affects the overall privacy costs for all users. For the sake of discussion, I assume that the transaction cost c for double protection is sufficiently low—i.e., $c < \bar{c}$—to guarantee that double protection with positive externalities expands the blockchain market size in equilibrium; i.e., $N^* < \widetilde{N_E^*}$.[13]

First, I focus on the case in which the privacy risks increase with the size of the network, as in Section 4.2. If additional privacy protection expands the blockchain network, this leads to a more decentralized system, which benefits users. Previously, this has led to an unresolved dilemma because a more decentralized system makes individual users more vulnerable to the risks of data leakage. However, this dilemma can be resolved when double protection has positive externalities. Because the overall privacy risks $\widehat{Q}(N;s)$ are low with positive externalities, a blockchain with such externalities can be a more decentralized system with low privacy risks simultaneously. Specifically, there is a condition, $\widetilde{N_E^*} < \bar{N}$, which guarantees that the dilemma between decentralization and privacy protection is resolved, where $\bar{N} = \widehat{Q}^{-1}(Q(N^*;s))$.[14] However, such a dual benefit comes at the expense of higher transaction costs: the dilemma can be

[13] Note that even if $c > \bar{c} \equiv (vN - \phi)(1 - \psi)$, $N^* < \widetilde{N_E^*}$ is guaranteed as long as $(vN - \phi)(1 - \psi) < c < (vN - \phi)(1 - \psi\frac{\widehat{Q}(N;s)}{Q(N;s)})$.

[14] Given that $\widehat{Q}(N;s)$ is monotonically increasing (or decreasing), it is invertible.

resolved only if some portion of users pay c to doubly protect their privacy. In other words, there is a trilemma in the blockchain system: a blockchain system that is simultaneously more decentralized, more privacy-protecting, and less costly is impossible to implement. Proposition 7 summarizes these findings.

Proposition 7. ***(Blockchain Trilemma)*** *Suppose that the additional privacy protection employed by a portion of users lowers the overall privacy risks of a blockchain system. Allowing the additional protection leads to a trilemma in the blockchain: it can resolve the dilemma between decentralization and privacy protection only at a higher transaction cost.*

Now, I focus on the case in which the privacy risks decrease with the size of the network, as in Section 4.1. As above, suppose that the cost of additional privacy protection is sufficiently low ($c < \bar{c}$), which guarantees $N^* < \widetilde{N}_E^*$. Allowing double protection for some users ultimately leads to a much more favorable situation with positive externalities than without them. As in the case without positive externalities, double protection with them leads to a collectively better situation in terms of decentralization as well as privacy protection, while the effect of the privacy cost reduction is greater. Thus, the aggregate gains from additional privacy protection with positive externalities are increased.

Indeed, as long as the additional privacy protection implemented by some portion of users has positive externalities for other non-protected users, this resolves the dilemma between decentralization and privacy protection, despite the higher transaction costs. In other words, double privacy protection at a cost transforms the problem of the dilemma into that of the trilemma.

4.4 Critical Mass in Blockchain

Proposition 3 compares the equilibrium number of blockchain users with and without additional privacy protection. In addition to this equilibrium comparison, the critical mass that the blockchain system must attain to reach a stable set of users can be compared. Any new system with network effects among users, such as two-sided platforms, needs to have a certain number of users to sustain its business. If it does not attract enough users, it ends up going out of business. This minimum number of users that a system needs in order to attract more users

through network effects, thereby making its business successful via a virtuous cycle, is called a critical mass, denoted by N_C or $\widetilde{N_C}$, and is defined in Definition 1.

In this section, I examine how allowing additional protection changes the critical mass in a blockchain system. This problem is interesting to investigate given that even if additional protection increases the demand for blockchain, there is no guarantee that it will be easy to make a system successful with a lower critical mass. In other words, when a blockchain system implements additional privacy protection at a sufficiently low cost, this additional feature might require a greater initial burden with a higher critical mass to make the system stable. Whether it increases or decreases the critical mass depends on the relative privacy cost reduction effect from additional protection. To better focus on a blockchain with a trilemma, I restrict my attention to privacy risks increasing in N, i.e., $\frac{\partial Q(N;s)}{\partial N} > 0$, with relatively inexpensive privacy protection, i.e., $c < \bar{c}$.

4.4.1 More successful system with a smaller critical mass

I start by showing a graphical analysis of a numerical example. Figure 1 graphically compares how additional privacy protection expands the set of users in a blockchain system; i.e., $N^* < \widetilde{N^*}$ under the numerical assumptions of $\tau_i \sim U[0,1]$, $s = 1$, $Q(N) = \sqrt{N}$, $v = 1$, $\phi = \frac{1}{8}$, $\psi = \frac{1}{2}$, and $c = \frac{1}{70}$, which yields full adoption with additional privacy protection.

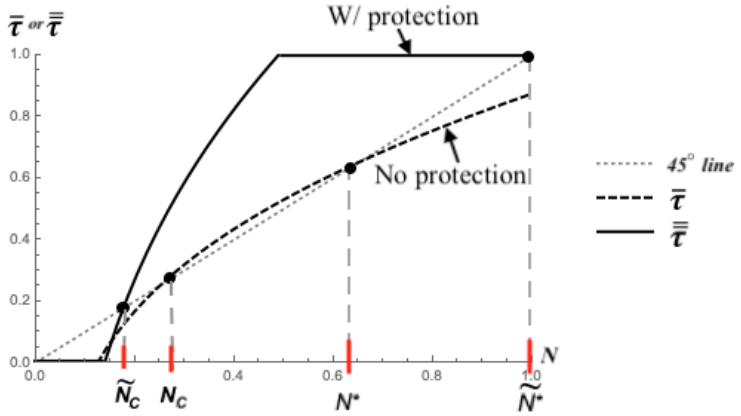

Figure 1: Equilibrium number of blockchain users when ψ is relatively small

Note that critical masses, denoted as $\widetilde{N_C}$ and N_C, with and without additional privacy protection, respectively, are saddle points, indicating unstable equilibria: by Assumption 2, if either $\bar{\tau}$ or $\bar{\bar{\tau}}$ is below the 45-degree line, N is decreasing. Thus, if the blockchain system

only has a number of users below point N_C or $\widetilde{N_C}$, it ends up failing to attract any users, thereby moving to the origin. However, if the system passes these points, it is led to a stable equilibrium number of users, either N^* or $\widetilde{N^*}$. This suggests that the unstable equilibrium points are critical masses. Comparing these critical masses shows that allowing additional privacy protection makes it easier for the blockchain system to successfully attain stable and large-scale adoption; given that $\widetilde{N_C}$ is smaller than N_C, a system that does not employ any additional privacy protection requires a more serious initial effort to stabilize in terms of the user base.

Remark 1. *Allowing effective additional privacy protection in a blockchain system at a low cost implies that less serious initial effort is required to attain a critical mass that drives the system to stable and large-scale adoption by users.*

4.4.2 More successful system with a greater critical mass

I start by showing a graphical analysis of a numerical example. Figure 2 graphically compares how additional privacy protection expands the set of users in the blockchain system—i.e., $N^* < \widetilde{N^*}$—under the same numerical assumptions as in Section 4.4.1, except in the case of $\psi = 0.95$. In this case, ψ is close to one, which means that additional protection only reduces users' privacy concerns by a negligible amount.

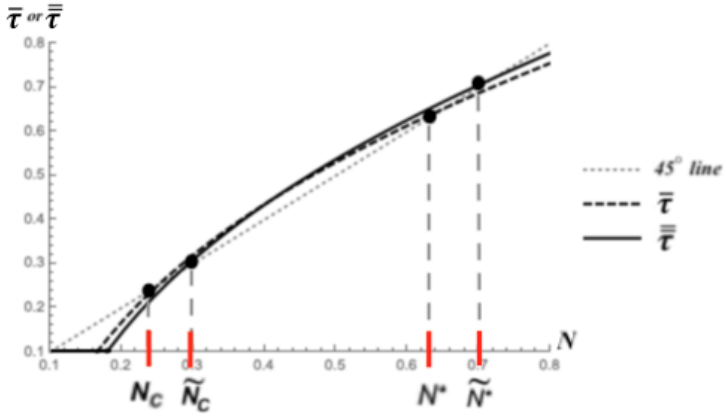

Figure 2: Equilibrium number of blockchain users when ψ is relatively large

Compared to Figure 1, the critical mass required for a blockchain without additional protection is much smaller than that with protection (i.e., $N_C < \widetilde{N_C}$), whereas allowing additional protection expands the total blockchain market size (i.e., $N^* < \widetilde{N^*}$). That is, unlike in Section

4.4.1, not allowing additional protection can mean that much less initial effort is required for the blockchain system to stabilize its demand. Per Proposition 3, the cost c of adopting additional protection needs to be sufficiently small—i.e., $c < \bar{c} \equiv (vN - \phi)(1 - \psi)$—to guarantee that $F(\bar{\tau}) < F(\bar{\bar{\tau}})$. Given v, ϕ, and ψ, if the user base N is very small, the threshold $\bar{c}$ decreases. Then, any cost c is likely to be higher than $\bar{c}$, which leads to $F(\bar{\tau}) > F(\bar{\bar{\tau}})$. In other words, when there are only a handful of users in the blockchain, even the privacy-sensitive group of users is less likely to adopt additional protection because it is not cost effective; the tendency for users to refuse more protection grows as ψ increases. Thus, when N is relatively small, a blockchain without additional protection can more easily reach a critical mass. After a sufficient number of users join, the situation is reversed, such that users find the additional protection cost effective, which ultimately yields a greater market share for a blockchain with protection.

Remark 2. *If additional privacy protection is not sufficiently effective at reducing privacy costs, allowing such protection in a blockchain system implies that a more serious initial effort is required to attain a critical mass that drives the system toward stable and large-scale adoption by users. Even if the required critical mass is greater, the blockchain with additional protection ultimately attains a larger market demand.*

Therefore, given that users are concerned about their privacy protection, the blockchain system can achieve widespread adoption in equilibrium even with less serious initial efforts by having relatively inexpensive but effective privacy protection.

5 Concluding Remarks

Decentralized blockchain-based transactions benefit users through openness, transparency, and immutability, which may come at the expense of heightened privacy concerns. This paper shows that if there is a dilemma between decentralization and privacy protection, such that a more decentralized system increases the risks of data leakage, then allowing methods of additional privacy protection within the blockchain network at a cost, such as hiring mixers, does not resolve the initial dichotomy. However, if there are positive externalities from privacy-protecting users who employ this additional protection to non-protected users, such that all users enjoy decreased privacy concerns with this double protection, then the dilemma between

decentralization and privacy risks can be resolved, despite the higher transaction cost to do so. Thus, double privacy protection at a cost transforms the problem of a dilemma into that of a trilemma.

References

[1] Abadi, J., Brunnermeier, M., (2019). Blockchain Economics. *Working Paper*.

[2] AI Jawaheri, H., AI Sabah, M., Boshmaf, Y., Erbad, A., (2020). Deanonymizing Tor Hidden Service Users through Bitcoin Transactions Analysis. *Computer & Security* Vol. 89.

[3] Allen, D.W.E., Berg, C., Markey-Towler, B., Novak, M., Potts, J., (2020). Blockchain and the Evolution of Institutional Technologies: Implications for Innovation Policy. *Research Policy* 49.

[4] Androulaki, E., O.Karame, G., Roeschlin, M., Scherer, T., Capkun, S., (2013). Evaluating User Privacy in Bitcoin. *Financial Cryptography and Data Security* pp. 34-51.

[5] Aoyagi, J., Adachi, D., (2019). Economic Implications of Blockchain Platforms. *Available at* https://ssrn.com/abstract=3132235.

[6] Arnosti, N., Weinberg, M., (2018). Bitcoin: A Natural Oligopoly. *Working Paper*.

[7] Arruñada, B., Garicano, L., (2018). Blockchain: The Birth of Decentralized Governance. *Available at* https://ssrn.com/abstract=3160070.

[8] Athey, S., Catalini, C., Tucker, C., (2017). The Digital Privacy Paradox: Small Money, Small Costs, Small Talk. *NBER Working Paper* No. 23488.

[9] Athey, S., Parashkevov, I., Sarukkai, V., Xia, J., (2016). Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. *SIEPR Working Paper* No. 17-033.

[10] Bakos, Y., Halaburda, H., (2019). The Role of Cryptographic Tokens and ICOs in Fostering Platform Adoption. *CESifo Working Paper* No. 7752.

[11] Barcelo, J., (2007). User Privacy in the Public Bitcoin Blockchain. *Journal of LaTeXClass Files* Vol.6, No.1.

[12] Berg, C., Davidson, S., Potts, J., (2017). Blockchains Industrialize Trust. *Available at* https://ssrn.com/abstract=3074070.

[13] Biais, B., Bisière, C., Bouvard, M., Casamatta, C., (2019). The Blockchain Folk Theorem. *The Review of Financial Studies* 32(5), pp. 1662-1715.

[14] Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J.A., Felten, E.W., (2014). Mixcoin: Anonymity for Bitcoin with Accountable Mixes. *Financial Cryptography and Data Security*, pp. 486-504.

[15] Biryukov, A., Khovratovich, D., Pustogarov, I., (2014). Deanonymisation of clients in Bitcoin P2P network. *in Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security* pp. 1529.

[16] Biryukov, A., Pustogarov, I., (2015). Bitcoin over Tor isn't a Good Idea. *Proceedings of the 2015 IEEE Symposium on Security and Privacy* pp. 122-134.

[17] Budish, E., (2018). The Economic Limits of Bitcoin and the Blockchain. *Working Paper.*

[18] Budish, E., (2018). The Economic Limits of Bitcoin and the Blockchain. *Working Paper.*

[19] Catalini, C., Gans, J.S., (2019). Some Simple Economics of the Blockchain. *Available at* https://ssrn.com/abstract=2874598.

[20] Chen, L., Cong, L.W., He, Z., (2019). A Brief Introduction to Blockchain Economics. *Available at* https://ssrn.com/abstract=3442691.

[21] Cong, L.W., He, Z., (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies*, Vol. 32, pp. 1754-1797.

[22] Cong, L.W., Li, Y., Wang, N., (2020a). Tokenomics: Dynamic Adoption and Valuation. *Becker Friedman Institute for Research in Economics Working Paper.*

[23] Cong, L.W., Li, Y., Wang, N., (2020b). Token-Based Platform Finance. *Fisher College of Business Working Paper Series WP 2019-28.*

[24] Conti, M., Kumar E. S., Lal, C., Ruj, S., (2017). A Survey on Security and Privacy Issues of Bitcoin. *IEEE Communications Surveys & Tutorials* vol. 20, no. 4, pp. 3416-3452.

[25] Chu, S., Wang, S., (2018). The Curses of Blockchain Decentralization. *arXiv:1810.02937v1.*

[26] Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxema, P., Shi, E., Sirer, E.G., Song, D., Wattenhofer, R., (2016). On Scaling Decentralized Blockchains. *Financial Cryptography and Data Security: FC 2016 International Workshops*, pp. 106-125.

[27] Das, D., Meiser, S., Mohammadi, E., Kate, A., (2018). Anonymity Trilemma: Strong Anonymity, Low Bandwidth Overhead, Low Latency - Choose Two. *2018 IEEE Symposium on Security and Privacy (SP).*

[28] De Filippi, P., (2016). The Interplay between Decentralization and Privacy: The Case of Blockchain Technologies. *Journal of Peer Production, Issue n.7: Alternative Internets.*

[29] Easley, D., O'Hara, M., Basu, S., (2019). From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics* 134, pp. 91-109.

[30] Evans, E.S., Schmalensee, R., (2010). Failure to Launch: Critical Mass in Platform Businesses. *Review of Network Economics* Vol. 9, Issue 4.

[31] Fabian, B., Ermakova, T., Krah, J., Lando, E., Ahrary, N., (2018). Adoption of Security and Privacy Measures in Bitcoin – Stated and Actual Behavior. *Available at* https://ssrn.com/abstract=3184130.

[32] Feng, T., Chen, X., Liu, C., Feng, X., (2019). Research on Privacy Enhancement Scheme of Blockchain Transactions. *Security Privacy* 89, pp. 1-13.

[33] Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., (2018). A Survey on Privacy Protection in Blockchain System. *Journal of Network and Computer Applications.*

[34] Franke, B., Gao, Q., Stenzel, A., (2019). Can You Trust the Blockchain? The (limited) Power of Peer-to-Peer Networks for Information Provision. *Working Paper.*

[35] Gencer, A.E., Basu, S., Eyal, I., van Renesse, R., Sirer, E.G., (2018). Decentralization in Bitcoin and Ethereum Networks. *Financial Cryptography and Data Security* pp. 439-457.

[36] Goldfeder, S., Kalodner, H., Reisman, D., Narayanan, A., (2018). When the Cookie Meets the Blockchain: Privacy Risks of Web Payments via Cryptocurrencies. *Proceedings on Privacy Enhancing Technologies* Vol. 2018, Issue 4, pp. 179-199.

[37] Halaburda, H., (2018). Blockchain Revolution Without the Blockchain. *Bank of Canada Staff Analytical Note* 2018-5.

[38] Halaburda, H., Haeringer, G., (2019). Bitcoin and Blockchain: What We Know and What Questions are Still Open. *NYU Stern School of Business; Baruch College Zicklin School of Business Research Paper* No. 2018-10-02.

[39] Halpin, H., Piekarska, M., (2017). Introduction to Security and Privacy on the Blockchain. *IEEE, Security and Privacy Workshops (EuroS&PW), IEEE European Symposium.*

[40] Hawlitschek, F., Notheisen, B., Teubner, T., (2018). The Limits of Trust-free Systems: A Literature Review on Blockchain Technology and Trust in the Sharing Economy. *Electronic Commerce Research and Applications* 29, pp. 50-63.

[41] Hassan, F., Ali, A., Latif, S., Qadir, J., Kanhere, S., Singh, J., Crowcroft, J., (2019). Blockchain And The Future of the Internet: A Comprehensive Review. *Working Paper.*

[42] Henry, R., Herzberg, A., Kate, A., (2018). Blockchain Access Privacy: Challenges and Directions. *The IEEE Computer and Reliability Societies.*

[43] Hinzen, F.J., Irresberger, F., John, K., Saleh, F., (2019). The Public Blockchain Ecosystem: An Empirical Analysis. *Working Paper.*

[44] Hinzen, F.J., John, K., Saleh, F., (2020). Bitcoins Fatal Flaw: The Limited Adoption Problem. *Working Paper.*

[45] Huberman, G., Leshno, J., Moallemi, C.C., (2019). An Economic Analysis of the Bitcoin Payment System. *Columbia Business School Research Paper* No. 17-92.

[46] Iyidogan, E., (2019). An Equilibrium Model of Blockchain-Based Cryptocurrencies. *Available at* https://ssrn.com/abstract=3152803.

[47] Joshi, A.P., Han, M., Wang, Y., (2018). A Survey on Security and Privacy Issues of Blockchain Technology. *American Institute of Mathematical Sciences* 1(2), pp. 121-147.

[48] Kappos, G., Yousaf, H., Maller, M., Meiklejohn, S., (2018). An Empirical Analysis of Anonymity in Zcash. *Proceedings of the 27th USENIX Security Symposium.*

[49] Koshy, P., Koshy, D., McDaniel, P., (2014). An Analysis of Anonymity in Bitcoin Using P2P Network Traffic. *Financial Cryptography and Data Security* pp. 469-485.

[50] Krombholz, K., Judmayer, A., Gusenbauer, M., Weippl, E., (2017). The Other Side of the Coin: User Experiences with Bitcoin Security and Privacy. *Financial Cryptography and Data Security* pp. 555-580.

[51] Kshetri, N., (2018). Cryptocurrencies: Transparency Versus Privacy. *Computer* 50(11), pp. 99-111.

[52] Liu, Z., Luong, N.C., Wang, W., Niyato, D., Wang, P., Liang, Y.C., Kim, D.I., (2019). A Survey on Applications of Game Theory in Blockchain. *arXiv preprint arXiv:1902.10865.*

[53] Ma, J., Tourky, R., Gans, J.S., (2018). Market Structure in Bitcoin Mining. *NBER Working Paper No. 24242.*

[54] Mehrwald, P., Treffers, T., Titze, M., Welpe, I.M., (2019). Application of Blockchain Technology in the Sharing Economy: A Model of Trust and Intermediation. *Proceedings of the 52nd Hawaii International Conference on System Sciences* .

[55] Meiklejohn, S., Pomarole, M., Jordan, G., Levchenko, K., McCory, D., Voelker, G.M., Savage, S., (2013). A Fistful of Bitcoins: Characterizing Payments Among Men with No Names. *Proceedings of the 2013 conference on Internet measurement conference - IMC '13, 2013, doi:10.1145/2504730.2504747*, pp. 127-140.

[56] Meunier, S., Zhao-Meunier, D., (2019). Bitcoin, Distributed Ledgers and the Theory of the Firm. *Available at* https://ssrn.com/abstract=3327971.

[57] Milgro, P., Roberts, J., (1994). Comparing Equilibria. *The American Economic Review* Vol. 84, No. 3, pp. 441-459.

[58] Möser, M., Soska, K., Heilman, E., Lee, K., Heffan, H., Srivastava, S., Hogan, K., Hennessey, J., Miller, A., Narayanan, A., Christin, N., (2018). An Empirical Analysis of Traceability in the Monero Blockchain. *Proceedings on Privacy Enhancing Technologies* pp. 1-22.

[59] Onik, M.M.H., Kim, C.S., Lee, N.Y., Yang, J., (2019). Privacy-aware Blockchain for Personal Data Sharing and Tracking. *Open Computer Science* 9, pp. 80-91.

[60] Parizi, R.M., Homayoun, S., Yazdinejad, A., Dehghantanha, A., Choo, K.K.R., (2019). Integrating Privacy Enhancing Techniques into Blockchains Using Sidechains. *Proceedings of the 32nd IEEE Canadian Conference on Electrical and Computer Engineering.*

[61] Reid, F., Harrigan, M., (2013). An Analysis of Anonymity in the Bitcoin System. *Security and Privacy in Social Networks.*

[62] Schiling, L., Uhlig, H., (2018). Some Simple Bitcoin Economics. *Working Paper.*

[63] Sockin, M., Xiong, W., (2018). A Model of Cryptocurrencies. *Working Paper.*

[64] Wang, Y., Kogan, A., (2018). Designing Privacy-Preserving Blockchain based Accounting Information Systems. *International Journal of Accounting Information Systems* 30, pp. 1-18.

[65] Waelbroeck, P., (2018). An Economic Analysis of Blockchains. *CESifo Working Paper No. 6893.*

[66] Zhang, R., Xue, R., Liu, L., (2019). Security and Privacy on Blockchain. *ACM Computing Surveys* Vol. 1, No. 1.