Cryptocurrency, Delivery Lag, and Double Spending History

Kang, Kee-Youn

Yonsei University

6 May 2019

Cryptocurrency, Delivery Lag, and Double Spending History

Kee-Youn Kang*

Yonsei University

July 3, 2019

Abstract

We develop a general equilibrium model of cryptocurrency to study the optimal design of a cryptocurrency system. Agents trade cryptocurrency using digital wallets, and the cryptocurrency system provides verification of a digital wallet's history of double spending attempts. Delaying the delivery of goods until payment information is confirmed in the blockchain prevents double spending. However, double spending can be prevented without a delivery lag under some conditions if a wallet has a good reputation in terms of its history of double spending attempts. In particular, as the difficulty of mining work rises, the incentive to engage in double spending with a good wallet decreases. We study the optimal design of the cryptocurrency system in terms of the difficulty of mining work and the supply of cryptocurrency and evaluate the welfare gain that would be captured if the current Bitcoin system adopted the optimal cryptocurrency system.

J.E.L. Classification: D86, E40, E50, G10

Keywords: Blockchain, Cryptocurrency, Delivery lag, Double spending, Trade history

*Correspondence: School of Business, Yonsei University, 50 Yonsei-ro, Seodaemun-gu, Seoul 03722, South Korea, Email: keeyoun@yonsei.ac.kr.

1 Introduction

Blockchain-based cryptocurrencies (cryptocurrencies hereafter), in particular Bitcoin, have received much attention not only from the public but also from policy makers. A distinctive feature of cryptocurrencies is that their transactions are verified and recorded in a publicly shared ledger, called the blockchain, by anonymous groups of miners. A block is a set of information about cryptocurrency transactions, and the blockchain is a sequence of blocks in which each block depends on the previous block in time.[1] The verification and recording process, called the mining work, is costly, which makes it hard to rewrite the transaction history in the blockchain. Thus, a seller can discourage a buyer from double spending, i.e., using the same cryptocurrency more than once, by delivering goods only after payment information is recorded in the blockchain, as illustrated in Chiu and Koeppl (2017). However, the waiting time caused by a delivery lag is a nonpecuniary, but nonetheless, real cost and the slowness of cryptocurrency transactions has been criticized as an important factor that prevents cryptocurrencies, such as Bitcoin, from being widely used in retail payments (see Velde (2013), Lo and Wang (2014), and Baklanova et al. (2017)).[2]

The objective of this paper is to find an incentive mechanism to overcome double spending risk without a delivery lag, to study the optimal design of cryptocurrency systems, and to quantitatively evaluate the welfare gain from adopting the optimal cryptocurrency system in the current Bitcoin trading environment. For this purpose, we develop a general equilibrium model of a cryptocurrency by incorporating key features of cryptocurrencies and of the blockchain as a record keeping device for payments into the Lagos and Wright (2005) model. In the model, the cryptocurrency works as a medium of exchanges, and agents trade the cryptocurrency using their digital wallets. Specifically, if a buyer instructs his/her wallet to transfer the cryptocurrency to the seller's wallet,

[1] See Narayanan et al. (2016), Berentsen and Schar (2018) and Sanches (2018) for technical details on the block creation process and the Bitcoin transaction process.

[2] Under the current Bitcoin system, one needs to wait one hour on average for a transaction to be considered final. Although it may seem a rather brief delay by the standard of settlement in the mainstream financial system, it can be regarded as lengthy by those users who adopted Bitcoin for its promise of instantaneous settlement. In particular, one hour is a long time in the realm of retail transactions. To date, the uses of Bitcoin as a medium of exchange appear limited: it has been used as a means to transfer funds outside of traditional and regulated channels and, presumably, as a speculative investment opportunity.

this information is distributed to miners' "*Mempools*", which store all unconfirmed transactions. At this stage, the seller receives a message that the buyer sent the cryptocurrency to his/her wallet, but the currency does not belong to the seller yet.

The transaction by which the buyer cedes ownership of the cryptocurrency to the seller is validated only after the transaction information is recorded in the blockchain through the mining work. Miners create a block with transaction data in their Mempools by solving a computationally costly mathematical problem called proof of work (PoW) and append the new block to the blockchain. Thus, the blockchain records all past transaction information, which is publicly available. Because PoW is costly, a reward structure is needed for the mining work to take place, and the cryptocurrency system uses the supply of new cryptocurrency and transaction fees to generate rewards for the mining work.

A key feature of the cryptocurrency system in the model is that miners' Mempools contain information on all unconfirmed transaction instructions, which is in contrast to the current Bitcoin system.[3] Miners' Mempools are connected to each other to exchange the latest Mempool data and if two (or more) Mempools have different data, they are updated with the union of data in the two Mempools. All information in the Mempool of any miner is also open to the public. This structure implies that, combined with the fact that the blockchain records all past confirmed transactions, agents can verify the history of double spending attempts by any wallets. Thus, a digital wallet may obtain a good reputation if it has no history of double spending attacks for a sufficiently long period of time. As a result, there are two types of wallets: a wallet with a good reputation (good wallet) and a wallet without a good reputation (bad wallet).

In the model, if a buyer makes a payment through a bad digital wallet, a seller delivers goods only after payment information is recorded in the blockchain to prevent a double spending attack. The delayed consumption, however, leads the utility from consuming goods to be discounted by

[3]Under the current Bitcoin system, if a transaction instruction is not confirmed within a certain period, approximately seven days, then the transaction will eventually be rejected by the Bitcoin network and be deleted from the Mempool. If it is rejected, then the funds would remain at the bitcoin address they were sent from. Furthermore, when a new block is added to the blockchain, the Mempool removes all conflicting transactions as well as transactions contained in the new block.

the delivery lag discount factor. On the other hand, the seller may deliver goods immediately, before the payment information is recorded in the blockchain, if the payment is made through a good digital wallet as long as the cost of losing a good reputation of the wallet outweighs the short-run gain from double spending. In this case, the double spending incentive depends on the value of trading with a bad wallet because if the buyer loses a good wallet after committing double spending attacks, he/she must trade with a bad wallet from the next period onward.

In equilibrium, double spending does not occur, but depending on the degree of the double spending incentives, equilibrium can be one of three types: *delivery lag equilibrium, threat of double spending equilibrium, and no threat of double spending equilibrium.* First, in the delivery lag equilibrium, the value of trading with a bad wallet is sufficiently high that the cost of losing a good wallet is not high enough to prevent double spending attempts. Thus, a good reputation for a digital wallet does not expedite trading process, and sellers deliver goods only after payment information is recorded in the blockchain. Second, in the threat of double spending equilibrium, the cost of losing a good wallet due to double spending is high enough to incentivize agents to refrain from double spending. However, the binding incentive constraint that prevents double spending without a delivery lag restricts the volume of exchanges. Finally, in the no threat of double spending equilibrium, the cost of losing a good wallet is very high due to a sufficiently high utility loss from delivery lags, and hence agents have no incentive to double spend with a good wallet and sellers deliver goods without lags.

One of the key messages of our analysis is that the delivery lag discount factor, which is determined by the difficulty of the PoW, plays a critical role in determining the equilibrium type. Specifically, as the delivery of goods is delayed for a longer time, the delivery lag discount factor decreases and the value of trading with a bad wallet drops, which, in turn, reduces incentives to double spend with a good wallet. Thus, as the delivery lag discount factor decreases, the equilibrium type tends to change from the delivery lag equilibrium to the threat of double spending equilibrium and to the no threat of double spending equilibrium.

The delivery lag discount factor also affects economic activities such as trade volume and

mining work. First, in the delivery lag equilibrium, an increase in the delivery lag discount factor implies less utility loss from delayed consumption, and hence, the cryptocurrency trade volume rises. An increase in the trade volume of cryptocurrency implies an increase in transaction fees to miners, so the aggregate mining work increases. On the other hand, in the threat of double spending equilibrium, an increase in the delivery lag discount factor tightens the binding incentive constraint that prevents double spending, and the trade volume and mining work fall as a result. Finally, the delivery lag discount factor has no effect on allocations in the no threat of double spending equilibrium; economic activities are the same as in an economy where double spending is not a possibility.

We use the model to study the optimal design of the cryptocurrency system by determining the level of the delivery lag discount factor and the growth rate of the cryptocurrency. In the model, the cryptocurrency system determines the level of the delivery lag discount factor and the cryptocurrency growth rate by adjusting the difficulty of the PoW and the supply of new cryptocurrency to miners as a reward, respectively.

One result of the welfare analysis is that welfare increases with the quantity of goods traded although higher trade volume implies higher welfare cost from mining work. Thus, it is optimal to set the delivery lag discount factor sufficiently low that the no threat of double spending equilibrium is achieved whenever it is feasible because the trade volume is maximized in this equilibrium given other economic factors, such as the cryptocurrency growth rate. When the threat of double spending equilibrium is the only feasible equilibrium type, then it is optimal to minimize the delivery lag discount factor to maximize the trade volume. On the other hand, if only the delivery lag equilibrium is feasible equilibrium, then it is optimal to maximize the delivery lag discount factor to minimize the welfare loss from delivery lags. Finally, when the threat of double spending equilibrium and the delivery lag equilibrium are both feasible depending on the level of the delivery lag discount factor, then it is optimal either to minimize or to maximize the delivery lag discount factor.

In the model, an increase in the cryptocurrency growth rate has a direct negative effect on

welfare by raising the welfare loss from the mining work. Furthermore, in both the delivery lag and the no threat of double spending equilibria, an increase in the cryptocurrency growth rate has an indirect negative effect on welfare by reducing the trade volume. In the threat of double spending equilibrium, an increase in the cryptocurrency growth rate may raise the quantity of goods traded by relaxing the binding incentive constraint that prevents double spending without delivery lags, but our quantitative analysis shows that this positive effect on welfare is dominated by the negative effects from increased mining work. Thus, welfare decreases as the cryptocurrency growth rate increases in all types of equilibrium. However, welfare increases discontinuously when the economy switches from the delivery lag equilibrium to the threat of double spending equilibrium because welfare loss from delivery lags disappears abruptly. In this case, it could be optimal to set the cryptocurrency growth rate at the value where the change of equilibrium type occurs. However, if changing the cryptocurrency growth rate does not change the equilibrium type, it is optimal to minimize the cryptocurrency growth rate, which is the zero growth rate.

We then use the calibrated model to evaluate the current Bitcoin system, which does not support building a good reputation for digital wallets, so retail transactions have delivery lags in order to prevent double spending. We find that the welfare gain from eliminating delivery lags and double spending incentives is substantial: the welfare gain from switching from the delivery lag equilibrium, which is equivalent to equilibrium outcome under the current Bitcoin system, to the no threat of double spending equilibrium by setting the delivery lag discount factor sufficiently low is 0.744% of consumption. The calibrated model also shows that the economy can enjoy an additional welfare gain of 0.016% of consumption by optimally setting the Bitcoin growth rate.

Literature review The economic literature on cryptocurrencies is relatively thin, despite the recent rapid growth. A number of papers study the valuation and pricing of cryptocurrencies. Gandal and Halaburda (2014) empirically investigate network effects on competition among cryptocurrencies and on their relative valuations. Glaser et al. (2014) and Gandal et al. (2018) focus on the valuation and volatility of Bitcoin as a store of value, and not as a medium of exchange. Cong

et al. (2018) study the dynamic feedback between platform adoption and the responsiveness of the token price to expectations about future growth on the platform. Schilling and Uhlig (2018) and Choi and Rocheteau (2019) study cryptocurrency pricing in a monetary model where cryptocurrency can be held for a speculative motive.

There is another strand of literature that seeks to identify problems with cryptocurrencies and studies whether cryptocurrencies can function as a real currency. Böhme et al. (2015) discuss the cryptocurrency's potential to disrupt existing payment systems and perhaps even monetary systems. Yermack (2015) examines whether Bitcoin is a currency or not and concludes that Bitcoin appears to behave more like a speculative investment than a currency. Weber (2016) assesses the potential to create input and output legitimacy for Bitcoin as a payment system and as a monetary system in comparison to current practice. Kang and Lee (2019) study competition between central bank-issued money and cryptocurrency and study how monetary policy affects welfare and economic activities related to the use of cryptocurrency.

We depart from the abovementioned literature by studying the optimal design of the cryptocurrency system to improve the extent to which cryptocurrency can be used as a medium of exchange. In this sense, our paper complements previous studies that focus on the pricing of cryptocurrencies and that evaluate the current Bitcoin system as a representative cryptocurrency system.

The paper most closely related to ours is Chiu and Koeppl (2017), who incorporate the distinctive technical features of the Bitcoin system into Lagos and Wright (2005) model to understand how a cryptocurrency system affects the interactions among participants and double spending incentives and to study the optimal design of cryptocurrency systems. They show that Bitcoin can overcome double spending by relying on competition to update the blockchain and by delaying delivery of goods, but the reward scheme of the current Bitcoin system for mining work has an inefficient design. According to them, reducing transaction fees and controlling the new coin creation rate can decrease the welfare loss from 1.41% to 0.08%. They study the optimal design of the cryptocurrency system in terms of the cryptocurrency transaction fees and growth rate. In this paper, we take a step further and show that if the cryptocurrency system supports agents' ability to

verify a digital wallet's history of double spending attempts, then double spending can be prevented without lags in the delivery of goods, eliminating the welfare loss from late consumption.[4]

The fact that a good reputation for a digital wallet without a history of double spending attempts facilitates trade is echoed in related literature on debt contracts with limited commitment and credit histories. Kehoe and Levine (1993) and Azariadis and Kass (2013) study the condition under which the first best allocation is obtained in an economy with limited commitment. Azariadis (2014) and Carapella and Williamson (2015) study the role of preventive policies and government debt, respectively, in credit markets. Azariadis and Kass (2007) derive asset price fluctuation, Hellwig and Lorenzoni (2009) show that a model with borrowing constraints may generate bubbles, and Gu et al. (2013) show endogenous credit cycles in models of credit with limited commitment. Sanches and Williamson (2010) introduce credit with limited commitment into Lagos and Wright (2005) to study a set of frictions under which money and credit are both robust as a means of payment.

In the debt contract literature, however, an agent builds a good reputation and credit history by honoring his/her obligations, and there is a penalty on defaulters such as exclusion to future credit markets for a certain period of time. In our model, by contrast, the digital wallet, not the wallet holder, obtains a good reputation if it does not have the history of double spending attempts, and a seller may deliver goods immediately if payment is made from a wallet with a good reputation. This implies that an agent can still trade cryptocurrency using a new digital wallet that does not have a good reputation after committing double spending attacks, so there is no explicit penalty on double spenders such as exclusion from markets in our model. The only handicap is that the seller delivers goods only after payment information is recorded in the blockchain.

The rest of the paper is organized as follows. Section 2 presents the environment of the model, section 3 solves the economic agents' problems, and section 4 characterizes the equilibrium. In section 5, we conduct a welfare analysis and study the optimal cryptocurrency system. Section 6

[4]In their appendix, Chiu and Koeppl (2017) analyze conditions under which a Proof-of-Stake (PoS) protocol can support immediate settlement, although many fundamental issues of the PoS protocol, such as long range attacks for double spending and consensus problem due to a nothing-at-stake problem, need to be sorted out in their model, as pointed out in Chiu and Koeppl (2017). On the other hand, the long range attack and nothing-at-stake problem do not occur under the PoW protocol because of the enormous amount of computational power for those works.

concludes the paper. The omitted proofs are relegated to the Appendix.

2 Model of blockchain based cryptocurrency

The basic framework in the model is based on Lagos and Wright (2005), with heterogeneous agents similar to those in Lagos and Rocheteau (2005) and Rocheteau and Wright (2005). Time is indexed by $t = 0, 1, 2 \ldots$, and there are two sub-periods within each period; the centralized market (CM) followed by the decentralized market (DM). There is a continuum of buyers and sellers each with unit mass. Additionally, there are η number of miners. All agents live forever with the discount factor $\beta \in (0,1)$ across periods, and the instantaneous utility of each agent in period t is

$$\begin{aligned}
&\text{Buyers: } U_t(X_t, H_t, q_t, e_t^s) = X_t - H_t + \delta^N u(q_t) - e_t^s \\
&\text{Sellers: } U_t(X_t, H_t, h_t) = X_t - H_t - h_t \\
&\text{Miners: } U_t(X_t, H_t, e_t) = X_t - H_t - e_t.
\end{aligned}$$

Here, X_t and H_t are consumption and labor supply, respectively, in the CM, q_t is consumption in the DM, h_t is labor supply in the DM, and e_t is efforts to update the blockchain in the DM, i.e., appending a new block to the blockchain, which is called the mining work. Similarly, e_t^s is buyer's effort for secret mining that will be described in detail below. $N \in \{0,1\}$ is an indicator such that $N = 0$ if a buyer receives and consumes DM goods immediately and $N = 1$ if there is a delivery lag - time between the placement of an order for DM goods and their subsequent delivery - so the buyer consumes DM goods late. When a delivery lag occurs in the DM, there is a discount on the utility from consuming DM goods that is determined by the delivery lag discount factor $\delta \in [\beta, \overline{\delta}]$, where $\overline{\delta} < 1$, in the DM.

The utility function, $u(q)$, over the DM goods is a strictly increasing, strictly concave, and twice continuously differentiable function with $u(0) = 0, u'(0) = \infty$, $u'(\infty) = 0$, $-q\frac{u''(q)}{u'(q)} \geq 1$ for all $q > 0$, and the property that there is some $\widetilde{q}$ such that $u(\widetilde{q}) = \widetilde{q}$. The production technology for

consumption goods available to buyers, sellers, and miners allows the production of one unit of the perishable consumption good for each unit of labor supply in each sub-period, but miner's effort for mining work and buyer's effort for secret mining in the DM do not produce any consumption goods.

In the CM, there is a centralized Walrasian market in which all agents trade numeraire CM goods and assets. In the DM, there are bilateral meetings between buyers and sellers. We assume that a buyer makes a take-it-or-leave-it offer in a pairwise meeting in the DM. Ideally, a buyer would like to borrow output from a seller in the DM and repay the loan in the next CM. Such credit arrangements are ruled out here because agents are anonymous, buyers and sellers are assumed to distrust each other, and there is no device to record credit histories that allows the possibility of punishing someone who does not honor debt obligations. As a consequence, any trade between buyers and sellers in the DM must occur on a quid-pro-quo basis through the use of a medium of exchanges.

In this economy, there is a digital currency called cryptocurrency. Although it does not have any intrinsic values, it can potentially be used as a means of payment like government issued fiat money. Cryptocurrency is traded at the price of $\phi_t \geq 0$ in terms of CM goods in the CM in period t. The stock of cryptocurrency, denoted by M_t in period t, grows at the gross rate of γ, i.e., $M_{t+1} = \gamma M_t$, and newly created cryptocurrency is awarded to miners whose detailed information will be described later.

To use cryptocurrency as a means of payment, agents must have a digital wallet that allows them to store, send, and receive cryptocurrency. Each wallet has its own public key, which is referred to as a cryptocurrency address, and a cryptocurrency transaction takes place between two wallets, each identified by its cryptocurrency address. For example, a buyer transfers cryptocurrency from his/her digital wallet to the address of the seller's wallet. We assume that an agent can enter the DM with one digital wallet, but he/she can open additional wallets in the DM, holding multiple wallets temporarily. The maximum number of digital wallets that the agent can open additionally in the DM is $\overline{\tau} \in \mathbb{N}$. In the next CM, the agent must choose one of them and destroy

others.

To ensure that the transaction by which an agent cedes ownership of cryptocurrency to the other agent is validated, all transactions are recorded in a digital ledger, called the blockchain. More precisely, a block is a set of information on a transaction conducted between cryptocurrency users in a given period. The ledger consists of a chain of blocks that contains all the information recorded by miners starting from the first block, and hence the ledger is called the blockchain.

The blockchain is a decentralized ledger where anyone can publicly verify any transactions and the balance amount of all users. Specifically, the blockchain data are stored in miners' nodes which are a storage device, such as computers, laptops, or even bigger servers. Nodes form the infrastructure of the blockchain. All nodes on the blockchain system are connected to each other and they constantly exchange the latest blockchain data with each other so all nodes stay up to date.

Record keeping through the mining process The main threat to using cryptocurrency as a means of exchange is that it can be easily copied and reused for payment because it is simply a string of bits. Thus, there exists a double spending problem: for example, an agent can use the same cryptocurrency more than once. First, we assume that there is no double spending problem in the CM due to public monitoring, and any cryptocurrency transactions during the CM are automatically recorded in a new block and added to the blockchain, similar to Chiu and Koeppl (2017). However, a decentralized network of miners records cryptocurrency transactions in the DM and updates the blockchain.

Specifically, the following steps are taken to settle cryptocurrency transactions in the DM. Suppose that a buyer instructs his/her digital wallet to transfer cryptocurrency to the seller's wallet. Then, the information on payment instruction is distributed to "*Mempools*" of all miners. The Mempool is a device that stores all unconfirmed transactions between buyers and sellers in the DM until they are recorded in the blockchain. At this stage, the cryptocurrency does not belong to the seller even if the seller receives a message that the buyer sent the cryptocurrency to his/her wallet.

We assume that miner's Mempool is also publicly available, and hence any agents can see instruction information for all unconfirmed transactions in the Mempool of any miner. All Mempools are connected to each other to exchange the latest Mempool data with each other. In particular, if two (or more) miners have different Mempools, for example, due to a cyberattack to some Mempools, then miners update their Mempool with the union of data in all Mempools. Thus, Mempools store all unconfirmed transaction data unless a hacker attacks all Mempools and delete some unconfirmed transaction data at the same time, which occurs with the zero probability in the model economy.

The next step is moving transaction information from the Mempool to the blockchain. More precisely, each miner collects transaction data from his/her Mempool to create a block and add it to the blockchain, updating the blockchain. Once the transaction information is recorded in the blockchain, the transaction by which a buyer cedes ownership of cryptocurrency to a seller is validated. The seller receives a message confirming payment so that the seller can be sure that the cryptocurrency belongs to him/her.

However, to create a block with transaction data, miners must solve a mathematical problem. For example, let blockchain be x, let the proposed block be y, and let an arbitrary number be n. The goal is to find n such that the resulting hash function, $f(x,y,n)$, is less than a tolerance level ε. The hash function is deterministic but is so complex that the output seems random. Thus, the only reliable method of finding n is to try out many different values of n until the condition is satisfied. However, a proposed solution (x,y,n) can be easily verified just by inputting it into the hash function, $f(x,y,n)$. Furthermore, part of finding the solution n involves verifying that no cryptocurrency transacted in the proposed block has already been spent in the existing blockchain. Finding a solution n is called a proof-of-work (PoW) or mining.

A miner who finds a solution first broadcasts it to other miners, who verify it. Based on the block's legitimacy, miners can accept or reject the block. When a miner accepts the block, his/her node saves and stores the block on top of his/her own chain of exisiting blocks it already has stored. If more than half of miners accept the spread block and use it for the next block creation, then the

miner who made the new block successfully updates the blockchain. Once transaction information is recorded in the blockchain, transaction information is removed from Mempools of all miners. However, we assume that miners keep information on any transaction that is not incorporated into the blockchain in their Mempools.[5]

A miner cannot add his/her block if some of the transaction data in that block has already been added to the blockchain by other miners. Thus, miners must compete to solve mathematical problems and append their blocks to the blockchain first. Specifically, to find a solution to the mathematical problem in the mining process, a miner must expend his/her own effort e in the DM. In particular, the speed with which a solution is found for a mathematical problem increases with effort e. For example, a miner can increase the pace of mining work by investing in greater computing power. Thus, the probability of winning the competition increases with a miner's effort e relative to that of other miners.

Because miners create their own blocks and try to add their blocks to the blockchain, there are times when two (or more) miners, for example, add their blocks to the blockchain at the same time creating a split in the blockchain, which is called a fork. In this case, readers and writers of the blockchain (digital ledger) must reach a consensus about which state is considered as the valid state. We assume that agents coordinate on the longest chain of blocks as the valid state, as suggested in Nakamoto (2008) and we call the longest chain the consensus chain.[6] Blocks in the non-consensus chain are called orphaned blocks, and miners move transactions in orphaned blocks to their Mempools. Thus, any transactions in orphaned blocks that do not conflict with transactions in the (consensus) blockchain will be recorded in the blockchain later. However, a

[5]Under the current Bitcoin system, an unconfirmed transaction will eventually be accepted into a block by whichever miners mine the block, or the transaction will ultimately be rejected by the Bitcoin network after approximately seven days. If it eventually is rejected, then the funds would remain at the bitcoin address they were sent from. Furthermore, when a new block is added to the blockchain, the Mempool of the current Bitcoin system removes all conflicting transactions as well as transactions contained in the new block. In contrast to the current Bitcoin system, we assume that all unconfirmed transactions remain in the Mempool. On the other hand, we can also assume that information on all rejected transactions, such as transactions that conflict with the transaction history in the blockchain, is stored in an additional storage device, called the rejected pool. What we need for this study is for any transaction information that enters the cryptocurrency system to be stored in one of storage devices, such as the Mempool, the blockchain, and the rejected pool, of the cryptocurrency system.

[6]Biais et al. (2018) model the proof-of-work blockchain protocol as a stochastic game and show that mining the longest chain is a Markov perfect equilibrium, without forking.

conflicting transaction cannot be recorded in the blockchain and remains in the Mempool forever.

Finally, the block size limits the total number of transactions included in any block. For example, under the current Bitcoin system, a block can contain around 2,000 transactions at most if the size of each transaction record is, on average, 500 bytes. Given the fixed number of transaction in the DM, the block size determines the number of blocks mined in the DM. For simplicity, we assume that one block is mined in each DM, and when a fork occurs, the consensus chain is determined in the DM before a new block is added to the blockchain in the next CM. However, the number of blocks mined in the DM does not affect our analysis on equilibrium and welfare as long as the mining competition for each block is independent across blocks and the winners share the total reward in the DM.[7]

Rewards for mining work Because it is costly to perform mining work, a reward scheme is needed for mining to take place. In our model, such rewards are financed by transaction fees and the creation of new cryptocurrencies. First, agents must pay transaction fees to miners to purchase goods with cryptocurrency in the DM. We assume that transaction fees are proportional at the rate of $f > 0$ to the total amount of a cryptocurrency transaction.[8] Second, the miner also receives newly created (or supplied) cryptocurrency, S_t. The quantity of the new cryptocurrency, S_t, is determined by the growth rate, γ: $S_t = (\gamma - 1)M_t$. Because the reward cannot be negative, we assume that $\gamma \geq 1$.

Both transaction fees and newly created cryptocurrency are awarded to the winner of the mining competition for his/her successful mining work. Furthermore, we assume that miners accrue rewards for each block added to the tree only if the added block is on the consensus chain, i.e., the longest chain of blocks. Therefore, miners usually extend only the consensus chain, and readers of

[7]More precisely, the total reward for mining work is determined by the trade volume q and the growth rate of cryptocurrency γ as described in the subsection of "Rewards for mining work". As the number of blocks that are created in the DM increases, the reward and mining effort for each block decrease. However, the aggregate reward and mining effort for all blocks mined in the DM, which matter for equilibrium allocations and welfare, do not change.

[8]Under the current Bitcoin system, agents can determine transaction fees so that their transactions can be confirmed in the blockchain network as soon as possible. See Easley et al. (Forthcoming) for an analysis of transaction fees in Bitcoin based on the strategic interaction of users and miners. However, we assume that f is fixed because its level has remained stable at a low level since it was invented in 2009 (see Chiu and Koeppl (2017) and Kang and Lee (2019)). Furthermore, the cryptocurrency system can always determine the transaction fee rate.

the blockchain will act only in response to events on that chain.

Double spending strategy As explained above, the mining process verifies whether the cryptocurrency traded has been spent in the existing blockchain. Thus, the blockchain is dynamically consistent in the sense that current transactions are linked to transactions in all previous blocks. As a result, if an agent attempts to revoke a past transaction, he/she has to propose an alternative blockchain in which a particular transaction is removed and has to solve mathematical problems for each of the newly proposed blocks. Furthermore, for the proposed alternative blockchain to be the consensus chain, the agent must add his/her blocks to the alternative blockchain faster than all the other miners add their own blocks to the existing blockchain.

Consequently, it is very costly to rewrite the transaction history backward in reality. In particular, as the number of blocks in the blockchain following the block containing the buyer's payment information increases, double-spending becomes harder. To reflect this feature in a simple way, we assume that it is not possible in our model economy to revoke a transaction in the past recorded in the blockchain.[9]

Unfortunately, the blockchain system itself does not eliminate the threat of forward-looking double spending. Consider a trade in a DM meeting where a buyer purchases goods from a seller in exchange for cryptocurrency. The buyer instructs his/her digital wallet to transfer payment to the seller's digital wallet, while the seller simultaneously delivers goods. At this point, the digital wallet application adds the transaction instruction information to the Mempool and broadcasts a message to a large network of miners, announcing the proposed transaction between the buyer and the seller. We call this transaction an honest transaction.

However, the buyer can always secretly initiate an alternative transaction to undo the payment in which the funds are not transferred, committing a double spending attack. For example, the

[9]In the current Bitcoin system, a transaction record tends to be considered as 99.9% secured from backward looking double spending attacks if the transaction record is at least six blocks deep, i.e., when a block that contains a certain transaction record is followed by more than five blocks in the blockchain. However, this is a technical detail, and for our purpose, it is sufficient to assume that a transaction is safe from double spending attacks once a block containing that transaction is added to the blockchain.

buyer opens a new wallet in the DM temporarily and sends the same cryptocurrency to his/her new wallet. The information for this transaction instruction also enters the Mempool and is broadcast to the network of miners. We call this secret transaction a fraudulent transaction.

The honest and fraudulent transaction cannot be contained in the same block because the cryptocurrency is used twice. However, these two transactions can be contained in two separate blocks, and the final outcome of the transaction in the DM meeting depends on which block belongs to the consensus chain. If the block with the honest transaction is added to the blockchain first, then the seller receives the payment. On the other hand, if the block with the fraudulent transaction updates the blockchain first, then the buyer obtains goods without paying anything to the seller, so the double spending attempt succeeds. Finally, the two blocks can be added to the blockchain at the same time, generating a fork in the blockchain. In this case, the final outcome of the transaction in the DM meeting depends on which block belongs to the consensus chain. Figure 1 illustrates the case in which a double spending attack succeeds or fails.

In principle, the buyer can create $\tau \in \{1, \ldots, \overline{\tau}\}$ number of fraudulent transactions by opening τ number of digital wallets in the DM temporarily. Then, the number of all transactions, including honest and fraudulent transactions, submitted by the buyer is $\tau + 1$. We assume that when the buyer does not invest any effort to mine blocks with fraudulent transactions and mining work is performed by miners, the honest transaction and each fraudulent transaction are recorded in the consensus blockchain with the probability of $\frac{1}{\tau+1}$.

One may think alternative strategy for double spending. Specifically, the buyer may revoke the honest transaction by secretly mining a block that does not contain the honest transaction and attaching it to the consensus chain without creating the fraudulent transaction. In this case, the honest transaction is recorded in a orphaned block for a moment. However, the honest transaction does not conflict with previous transactions in the blockchain so it is a valid transaction. This implies that the honest transaction will be moved to the Mempool and be recorded in the consensus blockchain later so double spending fails. Therefore, the buyer must create fraudulent transactions for double spending.

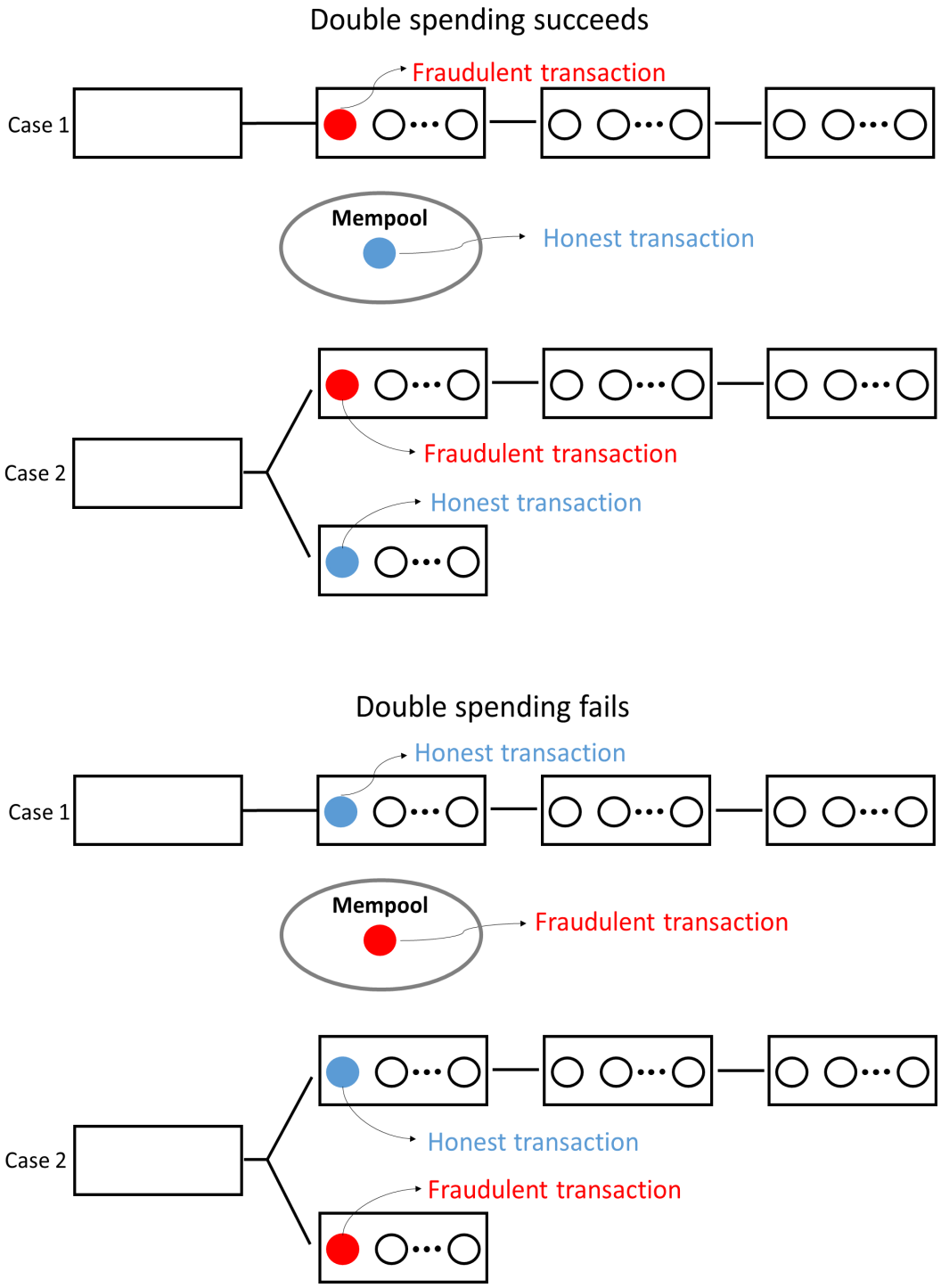

Figure 1: Double spending attack

Delivery lags to prevent double spending The seller can protect himself/herself against forward looking double spending attacks by holding up the delivery of goods until the payment information is incorporated into the consensus blockchain. This approach works because it is not possible to rewrite the transaction history backward and revoke a particular transaction in the blockchain.

Specifically, we assume that a seller can commit to deliver goods but cannot commit to the timing of delivery: The seller can always choose whether to deliver goods immediately or not. For example, after receiving a message that a buyer sent the cryptocurrency to the seller's wallet, the seller will ultimately provide goods to the buyer as long as the seller receives the cryptocurrent, but the seller can deliver goods with a lag after the payment confirmation in the blockchain if he/she chooses. In particular, if the seller believes that there is a positive probability of double spending attacks, then he/she will deliver goods with a lag to prevent double spending attacks.

The problem of a delivery lag, however, is that the buyer has to wait for a certain amount of time before receiving goods, so the buyer can only consume the goods after a time lag. Because agents prefer early consumption, even within the subperiod, a delivery lag for the goods reduces the buyer's utility from the consumption of goods in the DM. To reflect this feature, we apply the delivery lag discount factor $\delta \in [\beta, \overline{\delta}]$ to buyer's utility in the DM. However, the seller may transfer goods immediately because this is always a feasible option. Thus, we introduce discounting as $\delta^N u(q)$, where $N = \{0,1\}$. If the seller delivers goods immediately, then there is no delivery lag and $N = 0$. On the other hand, if the seller waits until the payment information is incorporated into the blockchain, then $N = 1$, and the buyer consumes goods late.

The waiting time and the delivery lag discount factor δ depend on the difficulty of the mining process. As explained above, a miner has to find a particular number that makes the value of the hash function less than the tolerance level ε. As ε decreases, it becomes harder to find a solution to the mathematical problem, and it takes more time to add a new block to the blockchain and confirm cryptocurrency transactions. As a consequence, the time between the placement of an order for DM goods and their subsequent delivery increases, which implies a decrease in the delivery lag discount factor δ. Because consumption goods are perishable, delivery must occur within the

subperiod, which implies that $\delta \geq \beta$. Also, as explained in Velde (2013), to maintain the stability of a cryptocurrency (Bitcoin) system that is based on PoW, the mining process should not be easy, for example, to make backward looking double spending attacks costly.[10] This implies that it must take some time to perform mining work, and thus we introduce the upper bound on the delivery lag discount factor as $\delta \leq \overline{\delta} \in (\beta, 1)$.

In principle, the miner's effort level could also affect the level of the delivery lag discount factor δ. For instance, if miners use a super computer to find a solution to a mathematical problem, then they will find the solution quickly. However, the cryptocurrency system can determine the average time to solve a math problem by dynamically adjusting the tolerance level ε. For example, the current Bitcoin system is programmed to automatically adjust such that it takes approximately 10 minutes, on average, to mine a new block, even with advances in the computing technology to solve mathematical problems. For this reason, we assume that the aggregate mining efforts do not affect the delivery lag discount factor δ, and the system of cryptocurrency determines the level of the delivery lag discount factor δ by adjusting the tolerance level ε, i.e., the difficulty of the PoW.

Blockchain and Mempool as record keeping technologies and reputation As explained above, the blockchain is publicly available to all agents, which implies that every cryptocurrency transaction that has ever occurred in the history of the economy is publicly viewable. Thus, the blockchain allows anyone to trace the entire confirmed transaction history of a particular digital wallet. Furthermore, any information of transaction instruction that is not incorporated into the consensus blockchain remains in the Mempool, which is also publicly available.

This implies that a seller can see whether there was a double spending attempt from the buyer's digital wallet in the past. More precisely, if a buyer used the same cryptocurrency more than once in the DM meeting, there must be an honest transaction and fraudulent transactions. The information about these transactions is either in the blockchain or in the Mempool, and one of

[10]Specifically, a blockchain needs some time to propagate the latest block(s) to all nodes globally, in order for the blockchain to stay properly synchronized. If blocks are produced at an extremely fast pace, some nodes on the other side of the globe might not be able to catch up fast enough with the lates transaction data, and this may cause nodes to be no longer correctly aligned, leading to chain splits (forks), which is basically something a blockchain must avoid as much as possible in order to stay secure.

transaction information must be in the blockchain (see Figure 1). Thus, a seller can verify the history of double spending attempts by the buyer's wallet by looking at the blockchain and the Mempool.[11]

The above analysis implies that the cryptocurrency system allows agents to build the reputation of their wallets based on the history of double spending attempts. In particular, if there have been no double spending attempts from a particular wallet for a sufficiently long period of time, then the wallet may obtain a good reputation. Furthermore, a good reputation for a digital wallet may have its own value. For example, a seller might deliver goods to a buyer without a delivery lag if the buyer makes a payment from a digital wallet with a good reputation. We call a wallet with a good reputation a good wallet and a wallet without a good reputation a bad wallet. Although we divide wallets into good and bad, this does not mean that a good wallet must always be better than a bad wallet. There could be no economic differences between the two types of wallets in equilibrium.

However, a wallet does not contain any information about the identity of wallet holders, so agents are still anonymous in a trade. For example, an agent can destroy an old wallet after committing double spending attacks and open a new wallet with a new address to trade cryptocurrency whenever the agent wants. Furthermore, if this agent trades in an honest way for a sufficiently long time with the new wallet, then the wallet may build a good reputation.[12] To introduce this feature into the model, we assume that a new wallet obtains a good reputation with the probability $\rho \in [0,1]$, so it takes, on average, $\frac{1}{\rho}$ number of cryptocurrency transactions without double spending attempts in the DM for a new digital wallet to obtain a good reputation.

[11] In principle, a double spender can attack Mempools of miners to delet his/her transaction instructions for double spending. However, unless the double spender deletes the related information from all Mempools at the same time, this attack cannot succeed because Mempools are connected with each other and update unconfirmed transaction data with the union of data in all Mempools. Based on this rational, we assume that it is impossible to manipulate the history of double spending attempts.

[12] In reality, a reputation of a digital wallet must depend on many factors, such as the number of transactions, total transactions fees that a wallet paid for transactions in the past, and transaction patterns, etc. For example, if a reputation only depends on the number of transactions, then an agent can overstate the number of transactions by making a sufficient number of small transactions with very low transaction fees between his/her wallets. However, if a wallet needs to pay a sufficient amount of transaction fees, that is higher than the value of a good reputation, for past transactions in order to obtain a good reputation, then an agent has no incentives to make inside transactions among his/her wallets just to obtain a good reputation. Furthermore, a wallet must have a sufficiently long period of transaction history. For example, a large number of transactions without double spending attempts in a single day may not be enough to obtain a good reputation.

3 Economic agents' problem

In this section, we characterize the optimal behavior of each economic agent in stationary equilibria. By stationarity, we mean that all real quantities are constant over time, which implies that $\frac{\phi_t}{\phi_{t+1}} = \gamma$. In the following, variables with subscript +1 denote the next period's variables.

One important feature of the Lagos and Wright (2005) setup is that the value functions for economic agents at the beginning of the CM are linear in asset holdings, and the optimal decision of agents, such as the choice of asset portfolio, is independent of initial asset holdings. For example, let $V(m)$ denote the value function for an agent with m units of the cryptocurrency at the beginning of the CM. Then, because of quasi-linearity, the value function can be expressed as $V(m) = \phi m + V(0)$, which simplifies the analysis.

Furthermore, we focus on a stationary equilibrium with $\gamma \geq 1$, and thus $\gamma = \frac{\phi}{\phi_{+1}} > \beta$. This implies that no agents will carry cryptocurrency into the next CM because of the linearity of the value function with respect to the initial balance of the cryptocurrency at the beginning of the CM. For instance, a buyer will not bring more than the quantity of cryptocurrency necessary to buy certain amount of goods in the DM.

3.1 Miner's problem

Miners compete to update the blockchain with cryptocurrency transaction data in the DM by investing their own effort e in the DM. The probability that miner i will win the mining competition for updating the blockchain with a new block depends on his/her efforts e_i and the aggregate efforts of all miners, expressed as $\Lambda = \sum_{j=1}^{j=\eta} e_j$. Specifically, miner i will be the first one to solve the PoW and propose a new block with the probability $\frac{e_i}{\Lambda}$, as explained in Chiu and Koeppl (2017).[13] The difficulty of the PoW affects the expected time needed to solve the mathematical problem to mine a block, but it does not affect the probability of wining the mining competition (see Chiu and Koeppl (2017) for detailed information).

[13] See Chiu and Koeppl (2017) for a micro-foundation for this probability of winning.

By winning the competition in the DM, a miner can update the blockchain with his/her new block and receive R units of cryptocurrency as a reward that consists of transaction fees and newly created cryptocurrency. We assume that miners receive and consume this reward in the next CM. A miner i takes the choice of other miners as given and thus solves the following problem, by virtue of the quasi-linearity of preference in the DM:

$$\pi_i = \underset{e_i \geq 0}{Max} \left\{ \beta \phi_{+1} R \frac{e_i}{\sum_{j=1}^{j=\eta} e_j} - e_i \right\}, \tag{1}$$

which gives

$$\beta \phi_{+1} R \frac{\sum_{j \neq i} e_j}{\left\{ \sum_{j \neq i} e_j + e_i \right\}^2} = 1$$

as the first-order condition. Imposing symmetry $e_j = e$ for all $j = 1, \ldots \eta$, because all miners are homogeneous, we obtain

$$\beta \phi_{+1} R \frac{\eta - 1}{\eta^2 e} = 1$$

as the Nash equilibrium of the mining game. Then, the expected profit of a miner, given by (1) and the aggregate mining effort, Λ, are given as

$$\pi = \frac{\beta \phi_{+1} R}{\eta^2}$$
$$\Lambda = \eta e = \beta \phi_{+1} R \frac{\eta - 1}{\eta}.$$

In reality, anyone can be a miner if he/she installs a mining program on a computer to perform mining work. An estimate shows that there are likely to be over $1,000,000$ unique individuals mining Bitcoins in the world.[14] Thus, mining work is quite competitive, and to capture this fact, we let $\eta \to \infty$, which leads to the next lemma, whose proof is omitted.

Lemma 1 *As $\eta \to \infty$, each miner's effort, e, and the expected profit from mining work, π, converge*

[14] See Buy Bitcoin World (https://www.buybitcoinworldwide.com/how-many-bitcoins-are-there). In addition, according to blockchain.info, there are 14 mining pools that individually can account for at least 1% of the total computation power.

to zero, and the aggregate mining effort converges to the aggregate rewards for the mining work, i.e., $\Lambda \to \beta \phi_{+1} R$.

Note that competition dissipates the rent from mining, i.e., the expected profit from mining work is zero. Thus, buyers would not engage in mining work except for secret mining to double spend. We assume that $\eta \to \infty$ for the remainder of the paper.

3.2 Buyer's problem

Agents trade the cryptocurrency using their digital wallets. Depending on the transaction history of a wallet, there are two types of wallets indexed by j, where $j = g$ stands for a good wallet, i.e., a wallet with a good reputation due to no double spending attempts for a sufficient period of time, and $j = b$ stands for a bad wallet that has not established a good reputation. A good reputation for a wallet may have its own value to a buyer, as explained above; thus, we consider buyers' value with both types of wallets. Let $V^j(m)$ denote the value function for a buyer holding m units of cryptocurrency in the $j \in \{g, b\}$ type of wallet at the beginning of the CM.

In the DM, a buyer makes an offer (q, d) to a seller. The terms of trade (q, d) specify that the buyer pays the seller d units of cryptocurrency and the seller delivers q units of DM goods.[15] We call an offer (q, d) double spending-proof if the buyer does not engage in double spending. In principle, a buyer can make an offer such that the buyer may attempt a double spending attack given terms of trade. However, if a buyer has an incentive to engage in double spending, then the seller will deliver goods after the payment confirmation in the blockchain because the timing of delivery, $N \in \{0, 1\}$, was not stipulated in the terms of trade. Thus, the buyer cannot engage in double spending. On the other hand, if the terms of trade in a DM meeting incentivize a buyer to not attempt double spending attacks even without delivery lags, then the offer is double spending proof and a seller would transfer goods immediately in the DM, i.e., $N = 0$. Thus, all offers in equilibrium are double spending-proof either because of delivery lags or because the buyer does not

[15] Note that the seller cannot commit to the timing of delivery, so the number of payment confirmation in the blockchain, $N = \{0, 1\}$, cannot be a part of the terms of trade.

have incentives to engage in double spending even without delivery lags, which is re-emphasized in the next proposition.[16]

Proposition 1 *In equilibrium, a buyer makes a double spending proof offer to a seller in the DM, so double spending does not occur.*

Proposition 1 allows us to focus on the double spending-proof equilibrium. Now consider the following trade in the DM to understand the double spending incentive structure when a seller delivers goods immediately. Given the result of proposition 1 and the assumption that a buyer makes a take-it-or-leave-it offer to a seller, a buyer can purchase q units of DM goods from a seller in exchange for $d = \frac{q}{\beta\phi_{+1}}$ units of cryptocurrency in the DM. Suppose that the seller delivers DM goods immediately without a delivery lag. In this case, the buyer can attempt a double spending attack to keep $\frac{q}{\beta\phi_{+1}}$ units of cryptocurrency in his/her wallet in the following way.

As explained above, the buyer creates $\tau \in \{1,\dots,\overline{\tau}\}$ number of fraudulent transactions in the DM to double spend the cryptocurrency. Fraudulent transactions can be recorded in the blockchain by miners or the buyer can also update the blockchain with fraudulent transactions by investing his/her own effort. Specifically, if the buyer exerts $e_{s,n} \geq 0$ units of effort to mine a secret block with the n^{th} fraudulent transaction where $n \in \{1,\dots,\tau\}$, the probability that the buyer updates the blockchain with one of his/her fraudulent transactions is given as

$$\widehat{\theta}(\overrightarrow{e_s}) = 1 - \left(1 - \frac{e_{s,1}}{\Lambda + e_s}\right) \cdots \left(1 - \frac{e_{s,\tau}}{\Lambda + e_s}\right),$$

where Λ is the aggregate mining efforts of all miners, $\overrightarrow{e_s} = [e_{s,1},\dots,e_{s,\tau}]$, and $e_s = \sum_{n=1}^{n=\tau} e_{s,n}$. With probability of $1 - \widehat{\theta}(\overrightarrow{e_s})$, the buyer does not update the blockchain with his/her fraudulent transactions. However, this does not yet mean the failure of the double spending attempt. A miner could update the blockchain with one of the fraudulent transactions, which occurs with probability

[16] If a seller can commit to the timing of delivery $N \in \{0,1\}$ so it can be a part of a contract, then the buyer may offer terms of trade that are not double spending-proof. For example, the seller will accept the offer and promise to deliver goods immediately even knowing that the buyer will attempt a double spending attack as long as the buyer also transfers a sufficient amount of cryptocurrency to the seller to compensate for the expected loss from the double spending attack.

$1-\left(1-\frac{1}{\tau+1}\right)^{\tau}$. Thus, the expected payoff from investing a profile of efforts $\overrightarrow{e_s}$ in secret mining is given as

$$\widehat{\theta}(\overrightarrow{e_s})[\beta\phi_{+1}R+q]+(1-\widehat{\theta}(\overrightarrow{e_s}))\left[1-\left(1-\frac{1}{\tau+1}\right)^{\tau}\right]q-e_s. \tag{2}$$

Note that if the buyer updates the blockchain, there is an extra return $\beta\phi_{+1}R$ from winning the mining competition. The next lemma describes the buyer's optimal choices of $(\tau,\overrightarrow{e_s})$ for secret mining, and the maximized expected payoff from double spending.

Lemma 2 *The buyer's optimal choices of the number of fraudulent transactions, τ, and effort $\overrightarrow{e_s}$ for secret mining are given as $\tau=\overline{\tau}$ and $\overrightarrow{e_s}$ is such that for any $\kappa\in\{1,\ldots,\tau\}$,*

$$e_{s,\kappa}=\sqrt{\left[\beta\phi_{+1}R+\left(1-\frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}}q\right]\beta\phi_{+1}R}-\beta\phi_{+1}R, \tag{3}$$

and $e_{s,n}=0$ for all $n\neq\kappa$. The expected payoff from double spending is given as

$$\left[\sqrt{\beta\phi_{+1}R+\left(1-\frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}}q}-\sqrt{\beta\phi_{+1}R}\right]^2+\left[1-\left(1-\frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}}\right]q. \tag{4}$$

Proof. See Appendix ■

Lemma 2 basically means that the buyer creates the maximum number of fraudulent transactions and invests effort to mine a single block with a fraudulent transaction. The intuition is as follows. First, as the number of fraudulent transactions rises, it is more likely that miners update the blockchain with one of fraudulent transactions. Thus, it is optimal for a double spender to create the maximum number of fraudulent transactions. Second, all fraudulent transactions conflict with each other, and hence only a single fraudulent transaction is recorded in the blockchain when double spending succeeds. Thus, if the buyer mines multiple blocks to update the blockchain with one of them, there is a competition among buyer's secret blocks. Then, the buyer can always increase the probability that he/she updates the blockchain by exerting the same level of mining effort only for mining a single block.

In reality, it does not take any cost to open digital wallets, which implies that there is no restriction on the number of fraudulent transactions that an agent can create for double spending. If there is no restriction on $\overline{\tau}$, the buyer would create infinite number of fraudulent transactions because the expected payoff from double spending (4) increases with $\overline{\tau}$. Thus, we assume that $\overline{\tau} \to \infty$ in the following analysis although the general setting can also be analyzed. Then, because $\lim_{\overline{\tau}\to\infty} \left(1 - \frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}} = \frac{1}{\exp(1)}$, we obtain the next lemma, whose proof is omitted.

Lemma 3 *As $\overline{\tau} \to \infty$, the buyer's expected payoff from double spending is given as*

$$\left[\sqrt{\beta\phi_{+1}R + \frac{q}{\exp(1)}} - \sqrt{\beta\phi_{+1}R}\right]^2 + \left[1 - \frac{1}{\exp(1)}\right] q. \tag{5}$$

Notice, from (5), that the buyer's expected payoff from secret mining is positive even though the expected profit of miners from mining work is zero because of competition as described in lemma 1. The expected payoff is positive because the buyer can keep $\frac{q}{\beta\phi_{+1}}$ units of cryptocurrency that were used for payment from secret mining in addition to rewards for successful mining work. Specifically, if $q = 0$, (5) becomes zero. Furthermore, the buyer's expected payoff from secret mining, (5), decreases with the real reward for the mining work, $\beta\phi_{+1}R$, because an increase in the real reward, $\beta\phi_{+1}R$, raises mining activities, which in turn, makes double spending harder to succeed.

However, if the buyer double spends the cryptocurrency, then he/she will start trading with a bad wallet from the next CM onward. Thus, the cost of double spending is given as $\beta\left[V^j(0) - V^b(0)\right]$ for $j = \{g, b\}$. Then, in a DM trade where a buyer exchanges $\frac{q}{\beta\phi_{+1}}$ units of cryptocurrency for q units of DM goods, if

$$\beta[V^j(0) - V^b(0)] \geq \left[\sqrt{\beta\phi_{+1}R + \frac{q}{\exp(1)}} - \sqrt{\beta\phi_{+1}R}\right]^2 + \left[1 - \frac{1}{\exp(1)}\right] q, \tag{6}$$

then the buyer does not attempt to double spend the cryptocurrency even though the seller transfers goods immediately without a delivery lag.

In the CM, an agent can always destroy an old wallet and open a new one if he/she wants. This implies that a good wallet cannot be worse than a bad wallet, and hence it must be $V^j(0) \geq V^b(0)$. Note that the necessary condition to satisfy the incentive constraint (6) is that $V^j(0) > V^b(0)$. Thus, if a buyer holds a bad wallet, i.e., $j = b$, then the incentive constraint (6) cannot hold. As a result, the buyer always has incentives to double spend. Knowing the buyer's double spending incentive, the seller delivers goods after confirming that the payment information has been incorporated into the blockchain to prevent double spending attacks. In summary, we have the following proposition, whose proof is omitted.

Proposition 2 *If a buyer makes a payment from a bad wallet in a DM meeting, a seller always delivers DM goods with a lag after the payment information is confirmed in the blockchain to prevent double spending attacks.*

Proposition 2 shows that there will be a delivery lag if a buyer makes a payment using a bad wallet. However, the result of proposition 2 also applies to an economy in which a wallet cannot reveal its history of double spending attempts. Suppose the cryptocurrency system does not allow a seller to verify the history of double spending attempts by the buyer's wallet. Then, a wallet cannot build a good reputation, so $j = b$ for all digital wallets. This implies that double spending incentives cannot be eliminated without holding up the delivery of goods, consistent with the result of Chiu and Koeppl (2017), in which a wallet cannot build a reputation based on its history of double spending attempts.

Given the result of proposition 2, a buyer holding a bad wallet optimally chooses terms of trade in the DM considering the delivery lag. Additionally, a bad wallet obtains a good reputation with probability ρ in the CM of the next period, as explained in the previous section. Thus, the value of a buyer entering the CM with m units of cryptocurrency in a bad wallet, $V^b(m)$, is given as

$$V^b(m) = \phi m + \underset{q \geq 0}{Max} \left\{ -\frac{\gamma(1+f)q}{\beta} + \delta u(q) + \beta \left[\rho V^g(0) + (1-\rho) V^b(0) \right] \right\}. \tag{7}$$

Now suppose a buyer has a good wallet in the DM. In this case, if a good reputation for the

wallet has its own value, i.e., $V^g(m) > V^b(m)$ for all $m \geq 0$, then the buyer may make an offer that satisfies the incentive constraint (6) to deter a seller from a delivery lag. In this case, the value function of buyers with a good wallet, $V^g(m)$, is given as

$$V^g(m) = \phi m + \underset{q \geq 0}{Max} \left\{ -\frac{\gamma(1+f)q}{\beta} + u(q) + \beta V^g(0) \right\} \tag{8}$$

subject to

$$\beta[V^g(0) - V^b(0)] \geq \left[\sqrt{\beta \phi_{+1} R + \frac{q}{\exp(1)}} - \sqrt{\beta \phi_{+1} R} \right]^2 + \left[1 - \frac{1}{\exp(1)} \right] q, \tag{9}$$

where (9) is the incentive constraint (6) for a buyer with a good wallet that prevents the buyer from engaging in double spending.

In contrast, if a good reputation for a wallet does not have its own value, then $V^g(m) = V^b(m)$, and thus the incentive constraint (9) cannot be satisfied. In this case, the buyer makes the same offer as that made by buyers holding a bad wallet, and sellers deliver DM goods only after payment information is confirmed in the blockchain. Thus, there is no economic difference between good wallets and bad wallets in this situation.

4 Equilibrium

Our definition of a stationary equilibrium is standard: given prices, all agents behave optimally, and all markets clear in equilibrium as described in the following definition.

Definition 1 *Given a system of cryptocurrency* $\{\delta, \gamma, f\}$ *and the probability that a new wallet obtains a good reputation* ρ*, a stationary cryptocurrency equilibrium is a list* $\{z, r, q, \{e_i\}_{i=1}^{\eta}, \Lambda\}$ *where* $z \equiv \phi M$ *and* $r \equiv \phi R$ *such that:*

1. *Given* $\{\delta, \gamma, f\}$*,* q *solves the buyer's problem.*
2. *Given* $\{\gamma, r, \{e_j\}_{j \neq i}\}$*,* e *solves the problem of miner* i *for all* $i = 1, \ldots \eta$

3. *Aggregate mining effort is the sum of mining effort of all miners as* $\Lambda = \eta e$
4. *Reward r is generated by* (γ, f) *and real cryptocurrency demand*
5. *The cryptocurrency market clears in the CM as*

$$z = \frac{\gamma(1+f)q}{\beta}. \tag{10}$$

The reward R for winning the mining competition is the sum of transaction fees and newly created cryptocurrency. First, the aggregate quantity of the new cryptocurrency, S, is determined by the growth rate γ as $S = (\gamma - 1)M$. Second, the aggregate transaction fees F depend on the aggregate quantity of cryptocurrency transactions, as $F = f\frac{q}{\beta\phi_{+1}}$ where $\frac{q}{\beta\phi_{+1}}$ is the quantity of cryptocurrency that buyers transfer to sellers in the DM given the quantity of DM goods, q, traded in equilibrium. Thus, the reward for the mining work is given as $R = (\gamma - 1)M + f\frac{q}{\beta\phi_{+1}}$. Then, using the market clearing condition (10) and the result of lemma 1, we obtain,

$$\Lambda = \beta\phi_{+1}R = [\gamma(1+f) - 1]q. \tag{11}$$

Therefore, all we need to do for equilibrium characterization is to analyze the equilibrium quantity of goods traded, q, in the *DM*, which can be obtained by solving the buyer's problem.

In equilibrium, double spending attempts do not occur. Thus, all buyers hold a good wallet, but a good reputation for the wallet may or may not have its own value. For the buyer's problem, there are three relevant cases in equilibrium depending on whether there is a delivery lag in the DM and whether the incentive constraint (9) that prevents double spending without the delivery lag binds.

1. (*Delivery lag equilibrium*) Sellers deliver goods in the DM after the payment information is confirmed in the blockchain, i.e., there is a delivery lag for DM goods.
2. (*Threat of double spending equilibrium*) There is no delivery lag for goods in the DM, and the incentive constraint (9) to prevent double spending binds.
3. (*No threat of double spending equilibrium*) There is no delivery lag for goods in the DM, and the incentive constraint (9) to prevent double spending does not bind.

To solve the buyer's problem and characterize equilibrium, we make the following definitions:

- The quantity of goods traded in the DM as

$$q_R^* \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\beta}\right) \tag{12}$$

$$q_R^{**} \equiv u'^{-1}\left(\frac{\gamma(1+f)+\omega\left[1-\beta(1-\rho)\right]}{\beta}\right), \tag{13}$$

where $\omega \equiv \left\{\sqrt{\gamma(1+f)-1+\frac{1}{\exp(1)}}-\sqrt{\gamma(1+f)-1}\right\}^2+1-\frac{1}{\exp(1)}$

- Functions of q and δ as

$$\Phi(q) \equiv -\frac{\gamma(1+f)+\omega\left[1-\beta(1-\rho)\right]}{\beta}q+u(q) \tag{14}$$

$$\Omega(\delta) \equiv -\frac{\gamma(1+f)}{\beta}\widehat{q}_N(\delta)+\delta u\left(\widehat{q}_N(\delta)\right), \tag{15}$$

where $\widehat{q}_N(\delta) \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$.

Given these definitions, the next proposition describes the quantity of goods, q, traded in the DM in each type of equilibrium.

Proposition 3 *In each type of equilibrium, the quantity of goods, q, traded in the DM is as follows:*

1. *In the delivery lag equilibrium,* $q=\widehat{q}_N(\delta) \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$.
2. *In the threat of double spending equilibrium,* $q=\widehat{q}_R(\delta)$ *where* $\widehat{q}_R(\delta)$ *is determined by* $\Phi(\widehat{q}_R(\delta))=\Omega(\delta)$ *with the property that* $\widehat{q}_R(\delta) \in [q_R^{**}, q_R^*)$.
3. *In the no threat of double spending equilibrium,* $q=q_R^*$.

Proof. See Appendix ■

In the delivery lag equilibrium, the double spending incentive is sufficiently high that a seller delivers goods only after payment information is incorporated into the blockchain to prevent double spending attempts. Thus, there is a delivery lag in the DM. A buyer chooses $q=\widehat{q}_N(\delta)$ to maximize the trade surplus in the problem (7).

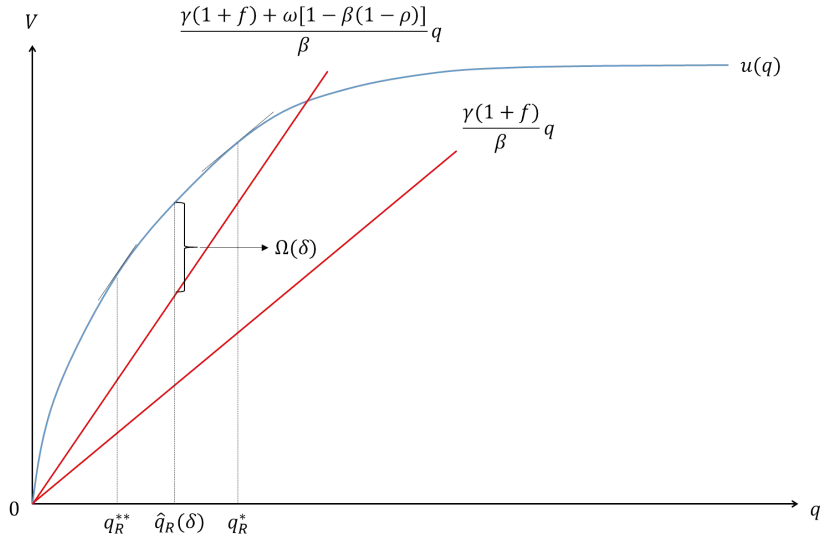

Figure 2: Trade volume q in the threat of double spending equilibrium

Next, in the threat of double spending equilibrium, a seller transfers goods to a buyer without a delivery lag in the DM and the buyer does not commit double spending in equilibrium. However, the incentive constraint (9) that prevents double spending without a delivery lag binds, and the binding incentive constraint (9) restricts the quantity of goods, q, traded in the DM. More precisely, substituting (7) with $q = \widehat{q}_N(\delta)$ in the delivery lag equilibrium, (8), and (11) into the binding incentive constraint (9) and using the definitions of $\Phi(q)$ and $\Omega(\delta)$ provided in (14) and (15), respectively, we obtain

$$\Phi(q) = \Omega(\delta), \tag{16}$$

which determines q given δ. Note from (13) and (14) that $\Phi(q)$ is maximized when $q = q_R^{**}$. Thus, if $\Phi(q_R^{**}) < \Omega(\delta)$, then there is no quantity of goods, q, traded in the DM that satisfies (16). When $\Phi(q_R^{**}) \geq \Omega(\delta)$, there are two values of q that satisfy (16), but only the q that is higher than q_R^{**} is the equilibrium quantity of goods traded because otherwise, the objective function (8) is not maximized. At the same time, q cannot be higher than q_R^* to have the binding incentive constraint (9). Figure 2 illustrates how the quantity of goods, q, traded in the threat of double spending equilibrium is determined.

Finally, in the no threat of double spending equilibrium, the cost of double spending, i.e., losing

a good wallet, is higher than the expected payoff from double spending. Thus, buyers do not have an incentive for double spending, and sellers deliver goods instantly without waiting until payment information is incorporated into the blockchain. The quantity of DM goods, q, traded is the same as that in an economy where double spending is not possible, and the buyer chooses $q = q_R^*$ to maximize the trade surplus in the problem (8).

We now characterize the necessary and sufficient condition for the existence of each type of equilibrium. For this purpose, we first define the cutoff levels of the delivery lag discount factor δ as follows:

$$\widetilde{\delta}_1 = \begin{cases} \Omega^{-1}\left(\Phi(q_R^*)\right) & \text{if } \Phi(q_R^*) \geq 0 \\ -\varepsilon_\delta & \text{if } \Phi(q_R^*) < 0 \end{cases} \tag{17}$$

$$\widetilde{\delta}_2 = \Omega^{-1}\left(\Phi(q_R^{**})\right), \tag{18}$$

where $\varepsilon_\delta > 0$ is a small number.

Proposition 4 *Given a set of parameters $\{\delta, \gamma, f, \rho\}$, there exists a unique stationary equilibrium as follows:*

1. *Suppose $\widetilde{\delta}_1 \geq \beta$. Then, (i) the no threat of double spending equilibrium exists for $\delta \in [\beta, \widetilde{\delta}_1]$, (ii) the threat of double spending equilibrium exists for $\delta \in (\widetilde{\delta}_1, \widetilde{\delta}_2]$, and (iii) the delivery lag equilibrium exists for $\delta \in (\widetilde{\delta}_2, \overline{\delta}]$.*
2. *Suppose $\widetilde{\delta}_1 < \beta \leq \widetilde{\delta}_2$. Then, (i) the threat of double spending equilibrium exists for $\delta \in [\beta, \widetilde{\delta}_2]$, and (ii) the delivery lag equilibrium exists for $\delta \in (\widetilde{\delta}_2, \overline{\delta}]$.*
3. *Suppose $\widetilde{\delta}_2 < \beta$. Then, the delivery lag equilibrium exists for $\delta \in [\beta, \overline{\delta}]$.*

Proof. See Appendix ■

Proposition 4 describes how the buyer's double spending incentives and the equilibrium type depend on the level of the delivery lag discount factor δ. As explained in proposition 2, a seller always delivers goods in the DM only after the payment information is incorporated into the blockchain if a buyer transfers cryptocurrency from a bad wallet to the seller. In this case, the

delivery lag discount factor δ affects the buyer's utility from consuming DM goods because of the delivery lag. Specifically, as δ falls, the trade surplus, $-\frac{\gamma(1+f)q}{\beta}+\delta u(q)$, decreases, and thus the value of trading with a bad wallet given in (7) decreases. Then, because the buyer loses the good wallet and will have to start trading with a bad wallet if he/she commits a double spending attack in the DM, the buyer has less of an incentive to double spend as δ decreases. Thus, as δ decreases, the equilibrium type tends to change from the delivery lag equilibrium to the threat of double spending equilibrium and to the no threat of double spending equilibrium.

Comparative statics Having characterized the existence of each equilibrium, we now discuss some comparative statics with respect to the set of parameters $\{\delta,\ \gamma,\ f,\ \rho\}$ on the quantity of goods, q, traded in the DM and the aggregate mining efforts Λ. In the model, the transaction fee rate f has exactly the same effects as the cryptocurrency growth rate γ. Thus, we do not analyze the effects of f explicitly in the following analysis.

In the delivery lag equilibrium, the marginal utility of the buyer in the DM increases as δ increases. Thus, the trade volume $q=\widehat{q}_N(\delta)$ and the aggregate mining effort, Λ, given by (11) increase with respect to δ. As a consequence, the value of trading with a bad wallet given in (7) increases. An increase in γ decreases q because it raises the holding cost of cryptocurrency across periods, which is the standard result in the money search framework.[17] Next, substituting $\widehat{q}_N(\delta)\equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$ into (11), we obtain $\Lambda=[\delta\beta u'(\widehat{q}_N(\delta))-1]\widehat{q}_N(\delta)$, which decreases with respect to $\widehat{q}_N(\delta)$, given the assumption on the utility function. Thus, the aggregate mining effort, Λ, increases with γ. This is because an increase in γ implies an increase in the reward for mining so miners invest more effort into winning the mining competition.

In the threat of double spending equilibrium, the quantity of goods traded in the DM, given as $q=\widehat{q}_R(\delta)\in[q_R^{**},q_R^*)$, decreases with respect to δ as one can see from Figure 2, in contrast to the case of the delivery lag equilibrium. The intuition behind this result is in line with our earlier observation. An increase in δ raises the value of trading with a bad wallet as explained above,

[17] See Williamson and Wright (2010), Nosal and Rocheteau (2011), and Lagos et al. (2017) for detailed information on the money search framework.

	Delivery lag			Threat of double spending			No threat of double spending		
	δ	γ(or f)	ρ	δ	γ(or f)	ρ	δ	γ(or f)	ρ
q	$+$	$-$	$\cdot$	$-$	?	$-$	$\cdot$	$-$	$\cdot$
Λ	$+$	$+$	$\cdot$	$-$	?	$-$	$\cdot$	$+$	$\cdot$

Table 1: Effects of the delivery lag discount factor, cryptocurency growth rate, and the probability that a new wallet obtains a good reputation ρ

reducing the cost of losing a good wallet through double spending. This tightens the incentive constraint (9), and q decreases as a consequence. By the same rational, an increase in the probability ρ that a bad wallet obtains a good reputation also reduces the trade volume q because of its effects on the cost of losing a good wallet through double spending, and hence, double spending incentives.[18] The aggregate mining effort Λ given in (11) increases with q given (γ, f), and thus, it decreases with δ and ρ.

An increase in γ, in the threat of double spending equilibrium, has two counteracting effects on q. On the one hand, it means an increase in the cryptocurrency holding cost, which pushes down q. On the other hand, an increase in γ has a direct positive effect on the aggregate mining efforts Λ of miners as one can see from (11) by raising the reward for the mining work. This, in turn, makes double spending harder to succeed, and hence, an increase in γ relaxes the incentive constraint (9), which pushes up q. Which effect dominates the other, and hence the effects of γ on the quantity of goods, q, traded in the DM depend on the relative values of $\widehat{q}_R(\delta)$ and $\widehat{q}_N(\delta)$.[19] Similarly, it is not clear whether the aggregate mining effort, Λ, given in (11), increases or not as γ rises.

Finally, in the no threat of double spending equilibrium, the quantity of goods traded in the DM is q_R^* which only depends on γ (and f). Specifically, an increase in γ reduces the trade volume q_R^* because of the increased holding cost of cryptocurrency similar to the case in the delivery

[18] More precisely, $\frac{\partial \Phi(q)}{\partial \rho} < 0$ in (14). Note that $\Phi(q)$ decreases with $q \in [q_R^{**}, q_R^*]$, and thus, $\widehat{q}_R(\delta)$, defined by $\Phi(\widehat{q}_R(\delta)) = \Omega(\delta)$ with the property that $\widehat{q}_R(\delta) \geq q_R^{**}$, decreases with respect to ρ.

[19] From (14) - (16), we obtain

$$\frac{\partial \widehat{q}_R(\delta)}{\partial \gamma} = \frac{1+f}{\beta} \frac{\widehat{q}_R(\delta) - \widehat{q}_N(\delta)}{u'(\widehat{q}_R(\delta)) - \frac{\gamma(1+f)+\omega[1-\beta(1-\rho)]}{\beta}}.$$

Because the denominator is negative for all $\widehat{q}_R(\delta) \in [q_R^{**}, q_R^*)$, $\frac{\partial \widehat{q}_R(\delta)}{\partial \gamma} \gtreqless 0$ if and only if $\widehat{q}_N(\delta) \gtreqless \widehat{q}_R(\delta)$.

Figure 3: Quantity of goods q traded in the DM and the discount factor δ

lag equilibrium. Using the definition of q_R^* in (12), the aggregate mining effort is given as $\Lambda = [\beta u'(q_R^*) - 1]q_R^*$, which decreases with q_R^*. Therefore, Λ increases with γ, for the same reason as the case of delivery lag equilibrium. Table 1 summarizes the above analysis.

We close this section with the further analysis of δ. The delivery lag discount factor δ plays an important role in the model: It affects the equilibrium type through its effects on the double spending incentive, and δ also affects the quantity of goods, q, traded (and hence the aggregate mining effort Λ) except in the no threat of double spending equilibrium. To better understand the effects of the delivery lag discount factor δ, suppose $\beta < \widetilde{\delta}_1 < \widetilde{\delta}_2 < \overline{\delta}$. This implies that as δ increases from β to $\overline{\delta}$, the equilibrium type changes from the no threat of double spending equilibrium to the threat of double spending equilibrium and to the delivery lag equilibrium (see proposition 4). Then, by the definition of $\widetilde{\delta}_1 = \Omega^{-1}(\Phi(q_R^*))$ in (17) and $\widehat{q}_R(\delta)$ in proposition 3, we obtain $\lim_{\delta \to \widetilde{\delta}_1} \widehat{q}_R(\delta) = q_R^*$. Next, from (13) - (15), $\widetilde{\delta}_2 = \Omega^{-1}(\Phi(q_R^{**}))$ and $\widehat{q}_N(\delta) \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$, we obtain

$$-u'(q_R^{**})q_R^{**} + u(q_R^{**}) = \widetilde{\delta}_2 \left\{ -u'\left(\widehat{q}_N\left(\widetilde{\delta}_2\right)\right)\widehat{q}_N\left(\widetilde{\delta}_2\right) + u\left(\widehat{q}_N\left(\widetilde{\delta}_2\right)\right)\right\},$$

which implies $\widehat{q}_N(\widetilde{\delta}_2) > q_R^{**}$ because $\frac{\partial[-u'(q)q+u(q)]}{\partial q} > 0$. Thus, the quantity of goods, q, traded in the *DM* increases discontinuously when the economy switches from the threat of double spending equilibrium to the delivery lag equilibrium. Figure 3 describes the above analysis, and the effects of δ on the aggregate mining effort Λ given by (11) show a similar pattern.

5 Welfare analysis

To study the welfare implications of the model, we define the sum of expected utilities in a steady state equilibrium across agents as our welfare measure, which is given as

$$W = \delta^N u(q) - q - \Lambda. \tag{19}$$

Welfare consists of the gains from trade less mining costs which are equal to the aggregate rewards for mining work as we look at the case where $\eta \to \infty$. Next, substituting (11) into (19), we obtain

$$W = \delta^N u(q) - \gamma(1+f)q \tag{20}$$

as our welfare measure in equilibrium.

The probability that a bad wallet obtains a good reputation ρ are not under the control of the cryptocurrency system. It depends on a social agreement on the length of the period or number of transactions that a wallet must go through without double spending attempts to obtain a good reputation.[20] Similarly, the transaction fee rate, f, often depends on the behavior of cryptocurrency users and miners rather than on the protocol of the cryptocurrency system in reality. Furthermore, even though a cryptocurrency system determines the transaction fee rate f, a change in f technically has the same effect as changing γ in equilibrium.

However, the cryptocurrency system can determine the delivery lag discount factor, δ, by adjusting the level of difficulty with which a mathematical problem is solved to create a new block

[20] See footnote 12 for more discussion about the factors, in addition to the number of transactions, that need to be considered for designating a good reputation to a digital wallet.

and can determine the growth rate of cryptocurrency γ by changing the supply of new cryptocurrency provided to miners. Thus, in the following, we focus on the analysis of the effects of δ and γ on welfare to find their optimal levels.

5.1 Delivery lag discount factor δ and welfare

In this subsection, we study how the delivery lag discount factor δ affects welfare and what its optimal level is, denoted as δ^*, given other parameters (γ, f, ρ). To study the effects of δ on welfare, we first analyze the effects of trade volume q on weflare. The quantity of goods traded, q, has two conflicting effects on welfare. First, an increase in q raises the trade surplus in the DM, which pushes up welfare. On the other hand, higher trade volume means higher crtyprocurrency transaction fees, which raises the social cost from mining work due to increased competition. Combined together, the effects of q on welfare is not clear as one can see from (20). However, the next lemma shows that welfare increases with the trade volume, q, in equilibrium, which provides a useful intermediate step for welfare analysis.

Lemma 4 *Given a set of parameters $(\delta, \gamma, f, \rho)$, welfare increases with the quantity of goods, q, traded in the DM in equilibrium.*

Proof. See Appendix ■

Given the result of lemma 4, we can analyze how changing the delivery lag discount factor δ affects welfare in each type of equilibrium. First, in the delivery lag equilibrium, the trade volume $q = \widehat{q}_N(\delta)$ increases with δ. Furthermore, an increase in δ means less welfare loss from the discount on utility for the late consumption of goods due to delivery lags in the DM. Thus, welfare increases with δ in the delivery lag equilibrium. Second, in the threat of double spending equilibrium, the trade volume $q = \widehat{q}_R(\delta)$ decreases with δ, so welfare decreases with δ given the result of lemma 4. Finally, changing δ has no effects on the trade volume q and hence welfare in the no threat of double spending equilibrium. Based on the result of the above analysis, we obtain the next proposition which describes the optimal level of the delivery lag discount factor δ^* given

other parameters (γ, f, ρ).

Proposition 5 *Given (γ, f, ρ), the optimal delivery lag discount factor δ^* is as follows:*

1. *When $\beta \leq \widetilde{\delta}_1$, $\delta^* \in [\beta, \widetilde{\delta}_1]$.*
2. *When $\widetilde{\delta}_1 < \beta \leq \overline{\delta} < \widetilde{\delta}_2$, $\delta^* = \beta$.*
3. *When $\widetilde{\delta}_1 < \beta \leq \widetilde{\delta}_2 \leq \overline{\delta}$,*

$$\delta^* = \begin{cases} \beta & \text{if } u(\widehat{q}_R(\beta)) - \gamma(1+f)\widehat{q}_R(\beta) \geq \overline{\delta} u(\widehat{q}_N(\overline{\delta})) - \gamma(1+f)\widehat{q}_N(\overline{\delta}) \\ \overline{\delta} & \text{if } u(\widehat{q}_R(\beta)) - \gamma(1+f)\widehat{q}_R(\beta) < \overline{\delta} u(\widehat{q}_N(\overline{\delta})) - \gamma(1+f)\widehat{q}_N(\overline{\delta}) \end{cases}.$$

4. *When $\widetilde{\delta}_2 < \beta$, $\delta^* = \overline{\delta}$.*

Proof. See Appendix ■

The main implication of proposition 5 is as follows. In the no threat of double spending equilibrium, the economy achieves $q = q_R^*$, which is the highest trade volume attainable in the DM given a set of parameters (γ, f, ρ), and there is no welfare loss from delivery lags. Thus, welfare is maximized in the no threat of double spending equilibrium, and it is optimal to make the incentive constraint (9) slack by setting $\delta \in [\beta, \widetilde{\delta}_1]$ whenever feasible, which requires $\beta \leq \widetilde{\delta}_1$.

However, if $\widetilde{\delta}_1 < \beta$, the no threat of double spending equilibrium is not feasible, and the optimal delivery lag discount factor δ^* is either β or $\overline{\delta}$ because δ has different effects on welfare in the other two types of equilibria. First, if $\widetilde{\delta}_1 < \beta \leq \overline{\delta} < \widetilde{\delta}_2$, the threat of double spending equilibrium is the only feasible equilibrium, and hence it is optimal to minimize δ to maximize the trade volume. Second, if $\widetilde{\delta}_2 < \beta$, the only feasible equilibrium is the delivery lag equilibrium, and it is optimal to maximize δ to minimize the welfare loss from delivery lags. Finally, if $\widetilde{\delta}_1 < \beta \leq \widetilde{\delta}_2 \leq \overline{\delta}$, the threat of double spending equilibrium and the delivery lag equilibrium are both feasible depending on the level of δ, and it is optimal either to minimize or to maximize the delivery lag discount factor δ.

5.2 Cryptocurrency growth rate γ and welfare

We now study how the cryptocurrency growth rate γ affects welfare and the optimal growth rate of cryptocurrency γ^*, given other parameter values (δ, f, ρ). Note, from (20), that an increase in γ has a direct negative effect on welfare by increasing the aggregate mining efforts. Thus, whenever an increase in γ reduces the quantity of goods, q, traded in the DM, welfare definitely decreases. This implies that as γ increases, welfare decreases in the delivery lag and no threat of double spending equilibria because q in both equilibrium types decreases with γ. Similarly, if q falls when γ rises in the threat of double spending equilibrium, welfare decreases. However, q may increase in response to an increase in γ in the threat of double spending equilibrium, and in this case, it is not clear whether welfare increases or decreases in response to an increase in γ.

Furthermore, an increase in γ could change the equilibrium type by affecting $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$, defined in (17) and (18), respectively. In particular, when the equilibrium type changes between the delivery lag and threat of double spending equilibria, allocations and the existence of a delivery lag change abruptly, as explained above, which may change welfare discontinuously. Thus, to understand the optimal growth rate of cryptocurrency γ^*, we also need to understand how changing γ affects the equilibrium type in addition to understanding how γ affects welfare in each equilibrium type.

For this purpose, we conduct numerical exercises with the buyer's utility function in the DM as $u(q) = A\frac{(q+\xi)^{1-\alpha}-\xi^{1-\alpha}}{1-\alpha}$ where $A > 0$, $\alpha > 1$, and $\xi \approx 0$. The length of the time period is a day, and we set $\beta = 0.97^{1/365}$ with an annual discount factor of 0.97, so the annual real interest rate on an illiquid bond is 3.1%. The estimates for the curvature of $u(q)$ vary widely, and we use $\alpha = 1.2$, which is within the range of previous studies, and we set $A = 0.001$. We choose $f = 0.0007$, which is the average ratio of the transaction fees to the Bitcoin transaction volume for the period from 2016 to 2017.[21] We set $\rho = 0.0083$, so it takes 120 days (or 120 number of honest transactions) on average for a bad wallet to obtain a good reputation.[22] Finally, we use $\delta = \beta^{1/24}$, which implies

[21] Source for Bitcoin data: blockchain.info

[22] There is no data to discipline the probability ρ, and there is no reason to set $\rho = 0.0083$. We choose $\rho = 0.0083$ to show that welfare can be maximized when the equilibrium type changes from the delivery lag to the threat of double

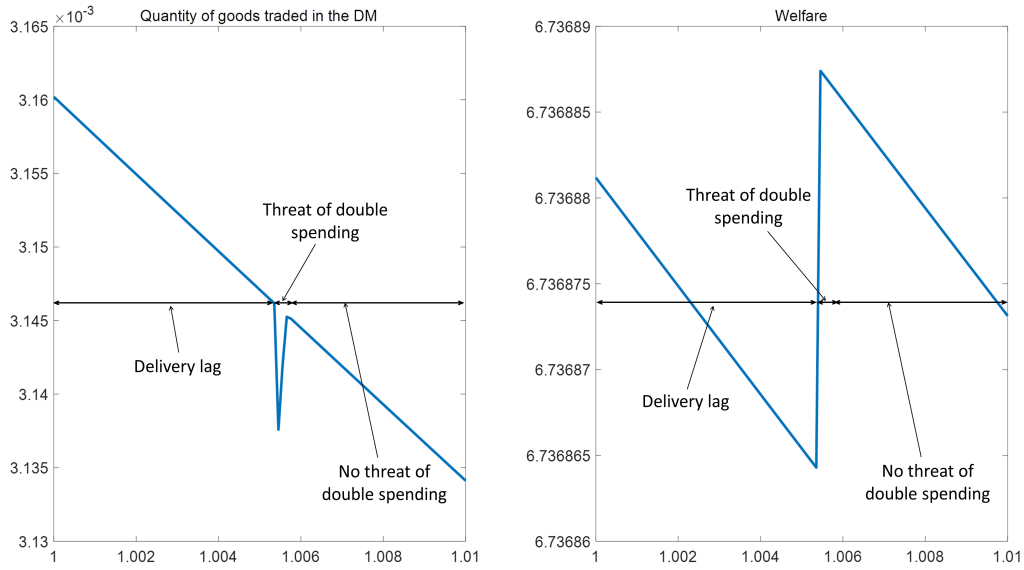

Figure 4: Effects of cryptocurrency growth

that it takes an hour on average for a transaction to be fully confirmed in the blockchain and hence the average waiting time before receiving goods in the DM in the delivery lag equilibrium is an hour.[23]

Figure 4 shows how welfare responds to a change in the growth rate of cryptocurrency γ when γ changes from 1 to 1.01. We also describe the effects of γ on the aggregate quantity of goods, q, traded in the DM to better understand the mechanism through which γ affects welfare. As explained above, q and welfare decrease as γ rises in the delivery lag and no threat of double spending equilibria. In the threat of double spending equilibrium, q increases as γ increases because the effects of relaxing the double spending incentive by making double spending attempts harder to succeed dominate the effects of reducing the trading volume by raising the holding cost of cryptocurrency across periods. However, an increase in γ induces more mining work, and thus welfare decreases due to increased welfare loss from mining work, although an increase in γ raises q in

spending equilibrium as described in Figure 4. If we set $\rho \leq 0.007$, for example, the no threat of double spending equilibrium exists for all $\gamma \geq 1$, and welfare decreases with γ. However, the probability ρ quantitatively affects real allocations only in the threat of double spending equilibrium. Thus, the main results such as the welfare gain from adopting the optimal cryptocurrency system eliminating delivery lags in the current Bitcoin trading environment do not hinge on the value of ρ.

[23] Under the current Bitcoin system, it takes 60 minutes on average for a transaction to be almost 99.9% secured against double spending risk (see Baklanova et al. (2017) and Kang and Lee (2019)).

this case. Combining these results together, welfare decreases as γ rises in all types of equilibria, as shown in Figure 4.

However, as γ increases, the equilibrium type also changes: from the delivery lag to the threat of double spending and then to the no threat of double spending equilibrium. As explained in the previous section, an increase in γ reduces the expected payoff from double spending by increasing the aggregate mining effort Λ of miners. Thus, an increase in γ relaxes the incentive constraint (9), changing the equilibrium type toward an equilibrium with a lower double spending incentive.

In particular, when the equilibrium type changes from the delivery lag to the threat of double spending equilibrium, the discount on the utility from consuming goods late in the DM due to the delivery lag disappears abruptly. Thus, welfare spikes and is maximized at that point, and thus the optimal growth rate of cryptocurrency, γ^*, is the value of γ that changes the equilibrium type from the delivery lag to the threat of double spending as one can see in Figure 4. However, these results depend on other parameter values, in particular, the delivery lag discount factor δ and the probability ρ. For example, if $\delta = \beta^{1/12}$ or $\rho \leq 0.007$, then the no threat of double spending equilibrium exists for all $\gamma \geq 1$, and welfare strictly decreases with γ so $\gamma^* = 1$. In this case, welfare is maximized for all (δ, γ).

We close this section with an evaluation of the current Bitcoin system. The current Bitcoin system provides limited support for digital wallets building a good reputation.[24] Thus, it is recommended the goods in retail transactions be delivered after Bitcoin payments are fully confirmed in the blockchain, which is equivalent to the delivery lag equilibrium in our model (see Baklanova et al. (2017) and Chiu and Koeppl (2017)). Furthermore, the average annual growth rate for the period from 2016 to 2017 is 5.7%, which is inefficiently set based on our welfare analysis.

To evaluate the efficiency of the current Bitcoin system, we compare welfare in the delivery lag

[24]Under the currency Bitcoin system, if an agent instructs a transfer of Bitcoin to other agents, then the transaction information enters to the Mempool. However, if a sufficiently long time passes, such as one week, for example, without the transaction information being recorded in the blockchain, then that transaction information disappears from the Mempool. Thus, agents may not be able to track the full transaction instruction history of a particular digital wallet. Furthermore, we need an application that can effectively verify the double spending history of a digital wallet because it is hard to track all transaction history of a particular wallet by looking at the blockchain and Mempool manually although it is technically feasible.

equilibrium with $\gamma = 1.057^{1/365}$ to welfare when (δ, γ) is set optimally. We measure the welfare gain as the fraction of additional consumption that the economy needs so that agents are indifferent between the current Bitcoin system and the optimal cryptocurrency system. Our calibrated model shows that the economy achieves the no threat of double spending equilibrium with $\gamma = 1$ by setting $\delta = \beta^{1/12}$ and suggests that the welfare gain from adopting the optimal design of Bitcoin system is 0.76% of consumption in terms of the consumption equivalent measure. In particular, the major portion of the welfare gain comes from eliminating the delivery lag. Specifically, when the cryptocurrency growth rate is inefficiently set to $\gamma = 1.057^{1/365}$, the welfare gain from switching the equilibrium type from the delivery lag to the no threat of double spending equilibrium by setting $\delta = \beta^{1/2}$ is 0.744% of consumption. The economy can enjoy an additional welfare gain of 0.016% of consumption by setting γ optimally, i.e., $\gamma = 1$.

6 Conclusion

In this paper, we constructed a search theoretic model of cryptocurrency based on blockchain technology to study the optimal design of the cryptocurrency system. The inherent threat to cryptocurrency as a medium of exchange is double spending risk due to its digital nature. Current cryptocurrency systems, such as the Bitcoin system, overcomes double spending risk by relying on costly mining work and delaying the delivery of goods.

We find that if the cryptocurrency system supports agents checking the history of double spending attempts for any digital wallet used to trade cryptocurrency, then double spending can be prevented without delivery lags. Specifically, as long as the loss of losing a good wallet, or a good reputation based on the history of double spending attempts, outweighs the short-run gain from double spending, an agent will not commit double spending with a good wallet. Thus, the agent can receive goods immediately if he/she made the payment from a good wallet. We have shown that double spending incentives critically depend on the level of difficulty of the mining work, which determines the wait time before receiving goods when the delivery of goods is delayed until

payment information is recorded in the blockchain. We conduct a welfare analysis to study the optimal design of the cryptocurrency system in terms of the level of difficulty of mining work and the cryptocurrency growth rate, and use our model to quantitatively assess the current Bitcoin system and evaluate the welfare gain from adopting the optimal cryptocurrency system.

Acknowledgments. I have benefited from discussion with Yongsung Chang, Jonathan Chiu, Inkee Jang, Young Sik Kim, Seungduck Lee, Christopher Waller, Stephen Williamson, and Menghan Xu as well as with all seminar participants at Korea University, Seoul National University, and Xiamen University. This work was supported (in part) by the Yonsei University Research Fund of 2019-22-0117.

References

AZARIADIS, C. (2014): "Credit Policy in times of Financial Distress," *Journal of Macroeconomics*, 39, 337–345.

AZARIADIS, C. AND L. KASS (2007): "Asset price fluctuations without aggregate shocks," *Journal of Economic Theory*, 136, 126–143.

——— (2013): "Endogenous credit limits with small default costs," *Journal of Economic Theory*, 148, 806–824.

BAKLANOVA, V., C. CAGLIO, M. CIPRIANI, AND A. COPELAND (2017): "Beyond the doomsday economics of "proof-of-work" in cryptocurrencies," Federal Reserve Bank of New York Staff Reports 758.

BERENTSEN, A. AND F. SCHAR (2018): "A Short Introduction to the World of Cryptocurrencies," *Federal Reserve Bank of St. Louis Review*, 100, 1–16.

BIAIS, B., C. BISIERE, M. BOUVARD, AND C. CASAMATTA (2018): "The blockchain folk theorem," Working paper.

BÖHME, R., N. CHRISTIN, B. EDELMAN, AND T. MOORE (2015): "Bitcoin: Economics, Technology, and Governance," *Journal of Economic Perspectives*, 29, 213–238.

CARAPELLA, F. AND S. WILLIAMSON (2015): "Credit Markets, Limited Commitment, and Government Debt," *Review of Economic Studies*, 82, 963–990.

CHIU, J. AND T. KOEPPL (2017): "The Economics of Cryptocurrencies - Bitcoin and Beyond," Working Papers 1389, Queen's University, Department of Economics.

CHOI, M. AND G. ROCHETEAU (2019): "Money Mining and Price Dynamics," Working paper.

CONG, L. W., Y. LI, AND N. WANG (2018): "Tokenomics: Dynamic Adoption and Valuation," Working paper, Ohio State University, Charles A. Dice Center for Research in Financial Economics.

EASLEY, D., M. O'HARA, AND S. BASU (Forthcoming): "From Mining to Markets: The Evolution of Bitcoin Transaction Fees," *Journal of Financial Economics*.

GANDAL, N. AND H. HALABURDA (2014): "Competition in the Cryptocurrency Market," Working Papers 14-17, NET Institute.

GANDAL, N., J. HAMRICK, T. MOORE, AND T. OBERMAN (2018): "Price manipulation in the Bitcoin ecosystem," *Journal of Monetary Economics*, 95, 86–96.

GLASER, F., M. HAFERKORN, M. WEBER, AND K. ZIMMERMANN (2014): "How to price a Digital Currency? Empirical Insights on the Influence of Media Coverage on the Bitcoin Bubble," *Banking and information technology*, 15, 1404–1416.

GU, C., F. MATTESINI, C. MONNET, AND R. WRIGHT (2013): "Endogenous Credit Cycles," *Journal of Political Economy*, 121, 940–965.

HELLWIG, C. AND G. LORENZONI (2009): "Bubbles and Self-Enforcing Debt," *Econometrica*, 77, 1137–1164.

KANG, K.-Y. AND S. LEE (2019): "Money, Cryptocurrency, and Monetary Policy," Working paper.

KEHOE, T. J. AND D. K. LEVINE (1993): "Debt-Constrained Asset Markets," *Review of Economic Studies*, 60, 856–888.

LAGOS, R. AND G. ROCHETEAU (2005): "Inflation, output, and welfare," *International Economic Review*, 46, 495–522.

LAGOS, R., G. ROCHETEAU, AND R. WRIGHT (2017): "Liquidity: A new monetarist perspective," *Journal of Economic Literature*, 55, 371–440.

LAGOS, R. AND R. WRIGHT (2005): "A unified framework for monetary theory and policy analysis," *Journal of Political Economy*, 113, 463–484.

LO, S. AND J. C. WANG (2014): "Bitcoin as Money?" Federal Reserve Bank of Boston Current Policy Perspectives 14-4.

NAKAMOTO, S. (2008): "Bitcoin: A peer-to-peer electronic cash system," .

NARAYANAN, A., J. BONNEAU, E. W. FELTEN, A. MILLER, S. GOLDFEDER, AND J. CLARK (2016): *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*, Princeton University Press.

NOSAL, E. AND G. ROCHETEAU (2011): *Money, payments, and liquidity*, MIT press, Cambridge.

ROCHETEAU, G. AND R. WRIGHT (2005): "Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium," *Econometrica*, 73, 175–202.

SANCHES, D. AND S. WILLIAMSON (2010): "Money and credit with limited commitment and theft," *Journal of Economic Theory*, 145, 1525–1549.

SANCHES, D. R. (2018): "Bitcoin vs. the Buck: Is Currency Competition a Good Thing?" Federal reserve bank of philadelphia economic insights articles, Federal Reserve Bank of Philadelphia.

SCHILLING, L. AND H. UHLIG (2018): "Some simple Bitcoin Economics," NBER Working Papers 24483, National Bureau of Economic Research, Inc.

VELDE, F. R. (2013): "Bitcoin: A primer," Chicago Fed Letter 317.

WEBER, B. (2016): "Bitcoin and the legitimacy crisis of money," *Cambridge Journal of Economics*, 40, 17–41.

WILLIAMSON, S. AND R. WRIGHT (2010): "New monetarist economics: Models," in *Handbook of Monetary Economics*, Elsevier, vol. 3, 25–96.

YERMACK, D. (2015): "Is Bitcoin a Real Currency? An economic appraisal," *The Handbook of Digital Currency*, 31–43.

Appendix A: Omitted proofs

Proof of lemma 2. The expected payoff from double spending (2) increases with the number of fraudulent transactions τ. Thus, the optimal choice for τ is given as $\tau = \overline{\tau}$.

Next, to derive the optimal choice for $\overrightarrow{e_s}$, we first show that it is optimal for the buyer to focus on mining a single secret block for double spending. Note that given $e_s = \sum_{n=1}^{n=\tau} e_{s,n}$, the expected payoff (2) increases with $\widehat{\theta}(\overrightarrow{e_s})$. Thus, the buyer chooses $\overrightarrow{e_s} = [e_{s,1}, \ldots, e_{s,\tau}]$ to maximize $\widehat{\theta}(\overrightarrow{e_s})$. Now suppose that $\widehat{\theta}(\overrightarrow{e_s})$ is maximized by mining $l \in \{2, \ldots, \tau\}$ number of secret blocks with l number of fraudulent transactions. Without loss of generality, assume that $e_{s,n} > 0$ for all $n \in \{1, \ldots, l\}$ and $e_{s,n} = 0$ for all $n \in \{l+1, \ldots, \tau\}$. Then, the probability $\widehat{\theta}(\overrightarrow{e_s})$ that the buyer updates the blockchain with one of his/her secret blocks is given as

$$\widehat{\theta}(\overrightarrow{e_s}) = 1 - \left(1 - \frac{e_{s,1}}{\Lambda + e_s}\right) \cdots \left(1 - \frac{e_{s,l-1}}{\Lambda + e_s}\right) \left(1 - \frac{e_{s,l}}{\Lambda + e_s}\right).$$

Now, consider $\overrightarrow{e_s}'$ such that $e'_{s,l-1} = e_{s,l-1} + e_{s,l}$, $e'_{s,l} = 0$, and $e'_{s,n} = e_{s,n}$ for all $n \in \{1, \ldots, l-2, l+1, \ldots, \tau\}$, so the total effort level for secret mining does not change as $\sum_{n=1}^{n=\tau} e'_{s,n} = \sum_{n=1}^{n=\tau} e_{s,n} = e_s$.

However, the probability $\widehat{\theta}(\overrightarrow{e_s}')$ is given as

$$\begin{aligned}\widehat{\theta}(\overrightarrow{e_s}') &= 1-\left(1-\frac{e_{s,1}}{\Lambda+e_s}\right)\cdots\left(1-\frac{e_{s,l-2}}{\Lambda+e_s}\right)\left(1-\frac{e_{s,l-1}+e_{s,l}}{\Lambda+e_s}\right)\\ &> 1-\left(1-\frac{e_{s,1}}{\Lambda+e_s}\right)\cdots\left(1-\frac{e_{s,l-2}}{\Lambda+e_s}\right)\left(1-\frac{e_{s,l-1}}{\Lambda+e_s}\right)\left(1-\frac{e_{s,l}}{\Lambda+e_s}\right)\\ &= \widehat{\theta}(\overrightarrow{e_s}),\end{aligned}$$

which is a contradiction. Thus, the buyer must focus on mining a single secret block, i.e., $l=1$, if he/she is willing to update the blockchain with fraudulent transactions for double spending.

Now take any $\kappa \in \{1,\ldots,\overline{\tau}\}$ given that the buyer create $\overline{\tau}$ number of fraudulent transactions, and let $e_{s,n}=0$ for $n\neq\kappa$. Then, from (2), the buyer's maximization problem for double spending is written as

$$\underset{e_{s,\kappa}}{Max}\left\{\widehat{\theta}(e_{s,\kappa})\left[\beta\phi_{+1}R+\left(1-\frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}}q\right]+\left[1-\left(1-\frac{1}{\overline{\tau}+1}\right)^{\overline{\tau}}\right]q-e_{s,\kappa}\right\}, \tag{21}$$

where $\widehat{\theta}(e_{s,\kappa})=\frac{e_{s,\kappa}}{\beta\phi_{+1}R+e_{s,\kappa}}$ by using the fact that $\Lambda\to\beta\phi_{+1}R$ as $\eta\to\infty$. Then, the first order condition for $e_{s,\kappa}$ is given by (3). Finally, substituting (3) into (21), the expected payoff from secret mining is given by equation (4). ■

Proof of propositions 3 and 4. Here, we prove propositions 3 and 4 at the same time by solving the buyer's problem.

Because we need $V^n(0)$ to derive the incentive constraint (9), we first look at the case where there is a delivery lag of goods in the DM. The first-order condition of the buyer's problem (7) is

$$\delta u'(q)=\frac{\gamma(1+f)}{\beta}.$$

Thus, $q=\widehat{q}_N(\delta)\equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$ in the delivery lag equilibrium. Substituting $q=\widehat{q}_N(\delta)$ into (7),

we obtain

$$V^b(m) = \phi m + \frac{1}{1-\beta(1-\rho)} \left\{ -\frac{\gamma(1+f)}{\beta} \widehat{q}_N(\delta) + \delta u\left(\widehat{q}_N(\delta)\right) + \beta\rho V^g(0) \right\}. \tag{22}$$

We now study the buyer's problem (8) in which sellers deliver goods immediately without a delivery lag. The first-order condition is

$$u'(q) - \frac{\gamma(1+f)}{\beta} - \lambda \frac{\partial \left\{ \left[\sqrt{\beta\phi_{+1}R + \frac{q}{\exp(1)}} - \sqrt{\beta\phi_{+1}R} \right]^2 + \left[1 - \frac{1}{\exp(1)}\right] q \right\}}{\partial q} = 0, \tag{23}$$

where $\lambda \geq 0$ is the Lagrange multiplier associated with the incentive constraint (9) that prevents double spending.

Case 1 In the no threat of double spending equilibrium, the incentive constraint (9) does not bind, and hence $\lambda = 0$ in (23). Then, the quantity of goods traded in the DM is given as $q = q_R^* \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\beta}\right)$. Substituting $q = q_R^*$ into (8), we obtain

$$V^g(0) = \frac{1}{1-\beta} \left\{ -\frac{\gamma(1+f)}{\beta} q_R^* + u(q_R^*) \right\}. \tag{24}$$

For this to be an equilibrium, the incentive constraint (9) should not bind. Substituting the equilibrium condition (11), (22) and (24) into (9), we obtain

$$\begin{aligned} \Phi(q_R^*) &\equiv -\frac{\gamma(1+f) + \omega\left[1-\beta(1-\rho)\right]}{\beta} q_R^* + u(q_R^*) \\ &\geq -\frac{\gamma(1+f)}{\beta} \widehat{q}_N(\delta) + \delta u\left(\widehat{q}_N(\delta)\right) \equiv \Omega(\delta), \end{aligned} \tag{25}$$

where $\omega = \left\{ \sqrt{\gamma(1+f) - 1 + \frac{1}{\exp(1)}} - \sqrt{\gamma(1+f)-1} \right\}^2 + 1 - \frac{1}{\exp(1)}$, as the non-binding incentive constraint (9). Note that $\Omega(\delta)$ in (25) increases with δ. Because $\Omega(\delta) \geq 0$, if $\Phi(q_R^*) < 0$, (25) cannot be satisfied. On the other hand, if $\Phi(q_R^*) \geq 0$, then for all $\delta \leq \Omega^{-1}(\Phi(q_R^*))$, (25) holds. Define $\widetilde{\delta}_1$ as described in (17). Then, if $\beta \leq \widetilde{\delta}_1$, the incentive constraint (9) does not bind for all

$\delta \in [\beta, \widetilde{\delta}_1]$ and the no threat of double spending equilibrium exists. If $\beta > \widetilde{\delta}_1$, the no threat of double spending equilibrium does not exist for all $\delta \in [\beta, \overline{\delta}]$.

Case 2 In the threat of double spending equilibrium, the incentive constraint (9) binds with $\lambda > 0$ in (23). Thus, it must be $q < q_R^*$ by (23). Substituting (8), (11), and (22) into the binding incentive constraint (9), we obtain

$$\begin{aligned} \Phi(q) &\equiv -\frac{\gamma(1+f)+\theta\left[1-\beta(1-\rho)\right]}{\beta} q + u(q) \\ &= -\frac{\gamma(1+f)\widehat{q}_N(\delta)}{\beta} + \delta u\left(\widehat{q}_N(\delta)\right) \equiv \Omega(\delta), \end{aligned} \tag{26}$$

which determines the quantity of goods, q, traded given δ. Note that the left-hand side of (26) is maximized with $q = q_R^{**}$ where q_R^{**} is defined in (13). Thus, if $\Phi(q_R^{**}) < \Omega(\delta)$, then there is no solution to (26). Define $\widetilde{\delta}_2$ as described in (18). Then, the necessary condition for the threat of double spending equilibrium to exist is $\delta \leq \widetilde{\delta}_2$, because $\Omega(\delta)$ increases with δ. Given $\delta \leq \widetilde{\delta}_2$, i.e., $\Omega(\delta) \leq \Phi(q_R^{**})$, there are two solutions to equation (26) in general: one that is higher than q_R^{**} and the other that is lower than q_R^{**}. However, the solution to (26) that is lower than q_R^{**} does not maximize the objective function (8) in the buyer's problem. Thus, the solution to (26) that is higher than q_R^{**} must be the quantity of goods traded in the DM in the threat of double spending equilibrium.

Let $\widehat{q}_R(\delta)$ be the solution to (26) that is higher than q_R^{**}. Next, the binding incentive constraint (9) requires $\widehat{q}_R(\delta) < q_R^*$ to satisfy (23) with $\lambda > 0$. Note that $\widehat{q}_R(\delta)$ decreases with respect to δ for $\widehat{q}_R(\delta) \geq q_R^{**}$, and $\widehat{q}_R(\delta)$ goes to q_R^* as $\delta \to \Omega^{-1}\left(\Phi(q_R^*)\right)$. Thus, it must be $\delta > \Omega^{-1}\left(\Phi(q_R^*)\right)$ to obtain the binding incentive constraint (9). Thus, the necessary condition for the threat of double spending equilibrium to exist is $\delta \in (\widetilde{\delta}_1, \widetilde{\delta}_2]$ where $\widetilde{\delta}_1$ and $\widetilde{\delta}_2$ are defined in (17) and (18), respectively. However, δ cannot be lower than β. Thus, if $\widetilde{\delta}_1 \geq \beta$, then the threat of double spending equilibrium exists for all $\delta \in (\widetilde{\delta}_1, \widetilde{\delta}_2]$. Next, if $\widetilde{\delta}_1 < \beta \leq \widetilde{\delta}_2$, then the threat of double equilibrium exists for $\delta \in [\beta, \widetilde{\delta}_2]$. Finally, if $\widetilde{\delta}_2 < \beta$, then the threat of double spending equilibrium does not exist.

Case 3 In the delivery lag equilibrium, sellers deliver goods only after payment information is incorporated in the blockchain, and hence $q = \widehat{q}_N(\delta) \equiv u'^{-1}\left(\frac{\gamma(1+f)}{\delta\beta}\right)$. Because a buyer holding a good wallet always wants to take advantage of its good reputation if possible, the delivery lag equilibrium exists only if a buyer cannot utilize a good reputation. This is the case when $\delta > \widetilde{\delta}_2$, because the incentive constraint (9) can be satisfied otherwise. Thus, the delivery lag equilibrium exists for all $\delta \in (\widetilde{\delta}_2, \overline{\delta}]$ if $\widetilde{\delta}_2 \geq \beta$, and for all $\delta \in [\beta, \overline{\delta}]$ if $\widetilde{\delta}_2 < \beta$. Note that a wallet's good reputation does not have its own value, and hence $V^g(m) = V^n(m)$, and the incentive constraint (9) does not hold.

Finally, by reorganizing the necessary condition for the existence of each case above, we obtain the results of proposition 4. Proof of proposition 3 is already undertaken in the analysis of each case. ■

Proof of lemma 4. Suppose $N = 0$. Then, welfare is maximized when $q = u'^{-1}(\gamma(1+f)) > q_R^*$. Because $q \leq q_R^*$ in any equilibrium, welfare increases in the quantity of goods, q, traded in the DM in equilibrium without delivery lags. Next, when there is a delivery lag in the DM, i.e., $N = 1$, welfare is maximized at $q = u'^{-1}\left(\frac{\gamma(1+f)}{\delta}\right) > \widehat{q}_N(\delta)$. Thus, in the delivery lag equilibrium, welfare increases in the trade volume q. Combined together, welfare given by (20) increases with the quantity of goods, q, traded in the DM in any equilibrium. ■

Proof of proposition 5. First, note that q_R^* is the highest trade volume attainable in the DM given a set of parameters (γ, f, ρ) in this economy. The economy achieves $q = q_R^*$ in the no threat of double spending equilibrium, and there is no welfare loss from delivery lags in this case. Thus, welfare is maximized in the no threat of double spending equilibrium given (γ, f, ρ). Thus, if $\beta \leq \widetilde{\delta}_1$, the optimal delivery lag discount factor is given as $\delta^* \in [\beta, \widetilde{\delta}_1]$, because the economy is in the no threat of double spending equilibrium for $\delta \in [\beta, \widetilde{\delta}_1]$.

Next, suppose that $\widetilde{\delta}_1 < \beta$, so the no threat of double spending equilibrium is not feasible. First, if $\widetilde{\delta}_1 < \beta \leq \overline{\delta} < \widetilde{\delta}_2$, the threat of double spending equilibrium exists for any level of δ. In this case, welfare decreases with δ, so it is optimal to minimize δ as $\delta^* = \beta$. Second, when

$\widetilde{\delta}_1 < \beta \leq \widetilde{\delta}_2 \leq \overline{\delta}$, the threat of double spending equilibrium exists for $\delta \in [\beta, \widetilde{\delta}_2]$ and the delivery lag equilibrium exists for $\delta \in (\widetilde{\delta}_2, \overline{\delta}]$. In the threat of double spending equilibrium, welfare is maximized with $\delta = \beta$, which gives $W|_{\delta=\beta} = u(\widehat{q}_R(\beta)) - \gamma(1+f)\widehat{q}_R(\beta)$ as welfare. On the other hand, welfare increases with δ in the delivery lag equilibrium, so welfare is maximized with $\delta = \overline{\delta}$. Welfare in this case is given as $W|_{\delta=\overline{\delta}} = \overline{\delta}u(\widehat{q}_N(\overline{\delta})) - \gamma(1+f)\widehat{q}_N(\overline{\delta})$. Thus, if $W|_{\delta=\beta} \geq W|_{\delta=\overline{\delta}}$, then $\delta^* = \beta$, and $\delta^* = \overline{\delta}$ otherwise.

Finally, if $\widetilde{\delta}_2 < \beta$, the only feasible equilibrium is the delivery lag equilibrium, and it is optimal to set $\delta = \overline{\delta}$ to minimize welfare loss from delivery lags. ■