Cryptocurrency and Double Spending History: Transactions with Zero Confirmation

Kang, Kee-Youn

Yonsei University

6 May 2019

Cryptocurrency and Double Spending History: Transactions with Zero Confirmation

Kee-Youn Kang*

Yonsei University

November 7, 2019

Abstract

We develop a general equilibrium model of cryptocurrency to study a double spending prevention mechanism without payment confirmations. Agents trade cryptocurrency using a digital wallet, and the cryptocurrency system provides a means to verify a wallet's double spending history. Double spending can be prevented without payment confirmations under some conditions if a wallet has a good reputation for transaction history. As the difficulty of mining work increases, incentives for double spending decrease. We provide new insights into the properties of Bitcoin transaction fees, quantitatively assess the current Bitcoin system, and evaluate the welfare gain from fast transactions without payment confirmations.

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. I have benefited from discussion with Yongsung Chang, Jonathan Chiu, Inkee Jang, Young Sik Kim, Seungduck Lee, Emiliano Pagnotta, Harald Uhlig, Christopher Waller, Stephen Williamson, Randall Wright, and Menghan Xu as well as with all seminar participants at 2019 Summer Workshop on Money, Banking, Payments and Finance at the Bank of Canada, Korea University, Seoul National University, Yonsei University, and Xiamen University. This work was supported (in part) by the Yonsei University Research Fund of 2019-22-0117. A previous version of this paper circulated as "Cryptocurrency, Delivery Lag, and Double Spending History".

1 Introduction

Blockchain-based cryptocurrencies (hereafter called cryptocurrencies), especially Bitcoin, have received extensive 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, which is called a 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, which is called mining work, is costly, making 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 after receiving a sufficient number of payment confirmations in the blockchain, as illustrated in Chiu and Koeppl (2017). However, the waiting time caused by precautionary confirmations is a nonpecuniary, but nonetheless, real cost, and the slow speed of cryptocurrency transactions has been criticized as an important factor that prevents cryptocurrencies, such as Bitcoin, from being widely used for 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 the double spending risk without precautionary confirmations and to quantitatively evaluate the welfare gain from eliminating delivery lags in the current Bitcoin trading environment. For this purpose, we develop a general equilibrium model of a cryptocurrency by incorporating key features of cryptocurrencies into the Lagos and Wright (2005) model. In the model, the cryptocurrency serves as a medium of exchange, 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, then this information

[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 this delay may seem rather brief by the standard of settlement in the mainstream financial system, it can be regarded as lengthy by users who have adopted Bitcoin for its promise of instantaneous settlement. In particular, one hour is a long time in the realm of retail transactions. The use of Bitcoin as a medium of exchange currently appears limited: it has been used as a means to transfer funds outside of traditional and regulated channels and presumably as a speculative investment opportunity.

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 yet belong to the seller.

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 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 store information on all unconfirmed transactions slightly different from the current Bitcoin system, and Mempools are publicly observable.[3] This structure implies that, combined with the fact that the blockchain records all past confirmed transactions, agents can verify the double spending history of any digital wallets. Thus, a digital wallet may obtain a good reputation for no double spending attempts based on its transaction history. As a result, two types of wallets exist: 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 with a bad digital wallet, then the seller delivers the goods after payment confirmations in the blockchain to prevent a double spending attack. The delayed consumption, however, leads the utility from consuming goods to be discounted by the discount factor for the confirmation time. On the other hand, the seller may deliver goods immediately without payment confirmations if the payment is made through a good digital wallet as long as the cost of losing a good wallet outweighs the short-run gain from double spending.

In equilibrium, double spending does not occur, but depending on the degree of the double

[3]Under the current Bitcoin system, if a transaction 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 rejected, the funds remain at the bitcoin address from which they were sent. Furthermore, the Bitcoin system removes all transactions that conflict with transactions recorded in the blockchain from the Mempool.

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 such that the cost of losing a good wallet is not adequately high to prevent double spending attempts. Thus, a good reputation of a digital wallet does not expedite the trading process, and sellers deliver goods after payment confirmations. Second, in the threat of double spending equilibrium, the cost of losing a good wallet is sufficiently enough to incentivize agents to refrain from double spending, and sellers therefore provide goods immediately without delivery lags. However, the binding incentive constraint that prevents double spending restricts the trade volume. Finally, in the no threat of double spending equilibrium, agents have no incentives for double spending due to the sufficiently high cost of losing a good wallet, and sellers deliver goods without precautionary payment confirmations.

The key determinant of the equilibrium type and economic activities, such as the trade volume and mining work, is the time for each confirmation, which is determined by the difficulty of the PoW. Specifically, as the confirmation time increases, the utility loss from delayed delivery of goods due to precautionary confirmations increases, and the trade volume and mining work in the delivery lag equilibrium decrease. Because trading with a bad wallet is accompanied by precautionary confirmations, an increase in the confirmation time decreases the value of trading with a bad wallet, which, in turn, reduces incentives to double spend with a good wallet. Thus, as the confirmation time increases, 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. By the same rationale, an increase in the confirmation time in the threat of double spending equilibrium relaxes the binding incentive constraint that prevents double spending, which increases the trade volume and mining work. Finally, in the no threat of double spending equilibrium, economic activities are the same as those in an economy where double spending is not a possibility and the confirmation time has no effect on allocations.

One result of the welfare analysis is that welfare increases with the quantity of goods traded in equilibrium, although a higher trade volume implies a higher welfare cost from mining work.

This implies that as the confirmation time increases, welfare increases (decreases) in the threat of double spending equilibrium (delivery lag equilibrium), and the confirmation time has no effect on welfare in the no threat of double spending equilibrium.

The supply of cryptocurrency controlled by the cryptocurrency system also affects real allocations and welfare. Specifically, 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. Therefore, welfare decreases with the cryptocurrency growth rate in both equilibria. In the threat of double spending equilibrium, however, an increase in the cryptocurrency growth rate may increase the quantity of goods traded by relaxing the binding incentive constraint that prevents double spending, and the effects on welfare are not evident.

We then use the model to provide new insights into Bitcoin transactions and its transaction fees, and to evaluate the current Bitcoin system. The current Bitcoin system does not support building a good reputation for digital wallets; therefore, retail transactions have delivery lags due to precautionary confirmations to prevent double spending, which is equivalent to the outcomes of the delivery lag equilibrium in the model. The model shows the positive relationship between the transaction volume and transaction fees and the negative correlation between transaction volume and the ratio of fees to the transaction volume, consistent with the pattern of Bitcoin data. Our calibrated model shows that the welfare gain from eliminating delivery lags in the Bitcoin system is substantial: the welfare gain from switching from the delivery lag equilibrium to the no threat of double spending equilibrium is 0.21% of consumption.

Literature review The economic literature on cryptocurrencies is relatively limited, despite 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), Choi and Rocheteau (2019), and Pagnotta (2019) study cryptocurrency pricing in a monetary model where cryptocurrency can be held for a speculative motive.

Another body of literature seeks to identify problems with cryptocurrencies and studies whether cryptocurrencies can function as a real currency. Böhme et al. (2015) discuss cryptocurrency's potential to disrupt existing payment systems and perhaps even monetary systems. Yermack (2015) examines whether Bitcoin is a currency 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 compared to current practice. Fernández-Villaverde and Sanches (Forthcoming) study cryptocurrencies as privately issued currencies by adding currency-providing entrepreneurs to the Lagos and Wright (2005) model and analyze whether currency competition can achieve price stability and efficient allocation. 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. We also analyze the pattern of cryptocurrency transactions to provide new insights into the relationship between Bitcoin transaction volume and its transaction fees. Thus, 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 the Lagos and Wright (2005) model to understand how a cryptocurrency system affects 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 the

delivery of goods, but the reward scheme of the current Bitcoin system for mining work has an inefficient design. According to these authors, 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 cryptocurrency transaction fees and the 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 delayed 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 roles 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) and Bethune et al. (2018) show endogenous credit cycles in models of credit with limited commitment. Sanches and Williamson (2010) introduce credit with limited commitment into the Lagos and Wright (2005) model 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 a penalty is imposed on defaulters, such as exclusion from future credit markets for a certain period. By contrast, in our model, a digital wallet rather than a wallet holder obtains a good reputation if it does not have a 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

[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 problems 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 required for those works.

does not have a good reputation after committing double spending attacks. Therefore, no explicit penalty, such as exclusion from markets, is imposed on double spenders in our model. The only disadvantage is that the seller delivers goods only after receiving a sufficient number of payment confirmations. The idea of dissociating agents from their digital wallets that obtain a reputation in the model can be interpreted as a means of circumventing a penalty on dishonest agents, and a similar reputation system can be applied to other related issues. For instance, Cavalcanti and Wallace (1999a) and Cavalcanti and Wallace (1999b) assume that society keeps a public record of the actions of bankers, but a bank can close and re-open under a different name in reality.

The rest of the paper is organized as follows. Section 2 presents the environment of the model, section 3 solves 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 extends the model with a block size limit, and section 7 concludes the paper. The omitted proofs are relegated to the Appendix.

2 The model of blockchain-based cryptocurrency

The basic framework of 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 two sub-periods exist within each period; the centralized market (CM) followed by the decentralized market (DM). A continuum of buyers and sellers exists, each with unit mass. Additionally, η number of miners exists. 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

$$\text{Buyers: } U_t(X_t, H_t, q_t, e_t^s) = X_t - H_t + \widehat{\delta}(\tau)^N u(q_t) - e_t^s$$

$$\text{Sellers: } U_t(X_t, H_t, h_t) = X_t - H_t - h_t$$

$$\text{Miners: } U_t(X_t, H_t, e_t) = X_t - H_t - e_t.$$

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 the effort to update the blockchain in the *DM*, i.e., appending a new block to the blockchain, which is called the mining work. $N \in \{0,1,\ldots\overline{N}\}$ is the number of payment confirmations, τ is the confirmation time that equals the block generation interval, and $\widehat{\delta} : \mathbb{R}_+ \to [\beta, 1)$ is a decreasing function of τ representing the discount factor for the confirmation interval. Specifically, if a buyer receives and consumes *DM* goods after N confirmations, the utility from consuming *DM* goods is discounted by $\widehat{\delta}(\tau)^N$, in the *DM*.

The utility function, $u(q)$, over the *DM* goods is a strictly increasing, strictly concave, and twice continuously differentiable function with $u(0) = u'(\infty) = 0, u'(0) = \infty$, and $-q\frac{u''(q)}{u'(q)} \geq 1$ for all $q > 0$. 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 the effort for mining work in the *DM* does 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 and no device is available to record credit histories, which would allow the possibility of punishing someone who does not honor debt obligations. Consequently, 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. However, we assume that the seller cannot commit to the timing of the delivery of goods, although the seller ultimately provides goods in the *DM* as long as he/she receives the payment.

In this economy, a digital currency called cryptocurrency exists. Although cryptocurrency does not have any intrinsic value, it can potentially be used as a means of payment similar to 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 a 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, and a cryptocurrency transaction takes place between two wallets, each of which is 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. In the next *CM*, the agent must choose one of the wallets and destroy the others.

Blockchain as a decentralized ledger 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 a blockchain. A block is a set of information on transactions conducted between cryptocurrency users in a given period. The ledger consists of a chain of blocks that contains all the information starting from the first block, and the ledger is therefore called the blockchain.

The blockchain is a decentralized ledger where blockchain data are stored in miners' nodes, which are storage devices such as computers or even bigger servers. All nodes on the blockchain system are connected to each other and they constantly exchange the latest blockchain data with each other such that all nodes remain up to date. Finally, the blockchain is publicly observable, and anyone can therefore verify any transactions and the balance amounts of all users.

Record keeping through the mining process We assume that cryptocurrency transactions in the *CM* are automatically recorded in the blockchain. However, transactions in the *DM* must be recorded in the blockchain by miners through the mining process. Specifically, the following steps are taken to settle cryptocurrency transactions in the *DM*.

If a buyer instructs his/her digital wallet to transfer cryptocurrency to the seller's wallet, then this instruction information is distributed to the $Mempools$ of all miners. A Mempool is a device that stores all unconfirmed transactions in the *DM* until they are recorded in the blockchain, and

Mempools are publicly observable. At this stage, the seller receives a message that the buyer sent the cryptocurrency to his/her wallet, but the cryptocurrency does not yet belong to the seller.

The next step is moving transaction information from the Mempool to the blockchain. Specifically, each miner creates a block with transaction data collected from his/her Mempool. To create a block with transaction data, miners must solve a mathematical problem by expending their own effort e in the DM. Specifically, miners must find an arbitrary number y such that the hash function $f(y)$ is less than a tolerance level ε.[5] The hash function $f(\cdot)$ is so complex that the only reliable method of finding y is to try out many different values of y until the condition is satisfied, and the speed with which a solution is found increases with effort e.[6] However, a proposed solution y can be easily verified simply by inputting it into the hash function, $f(y)$. Finding a solution y 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 proposed block. When a miner accepts the block, his/her node saves and stores the block on top of his/her own chain of existing blocks. If more than half of miners accept the block and use it for the next block creation, then the block successfully updates the blockchain. At this stage, the transaction by which the buyer cedes ownership of cryptocurrency to the seller is validated, and the seller receives a message of a single payment confirmation, i.e., $N = 1$. As more blocks are added to the blockchain following the block containing the buyer's payment information, the number of confirmations, N, increases. We assume that $\overline{N}$ number of blocks are added to the blockchain in the DM. Finally, after transaction information is recorded in the blockchain, it is removed from miners' Mempools.

It seems worth to discuss the confirmation time τ, which is the time required for updating the blockchain with a new block. Because miners must solve mathematical problems to create blocks, the confirmation time τ depends on the time required to solve the mathematical problems. Thus, miners' effort level, in principle, may also affect τ. However, the cryptocurrency system can

[5]The hash function $f(\cdot)$ depends on information of the current blockchain and a proposed block, and part of finding the solution y involves verifying that no cryptocurrency transacted in the proposed block has already been spent in the existing blockchain.

[6]For example, a miner can increase the pace of mining work by investing in greater computing power.

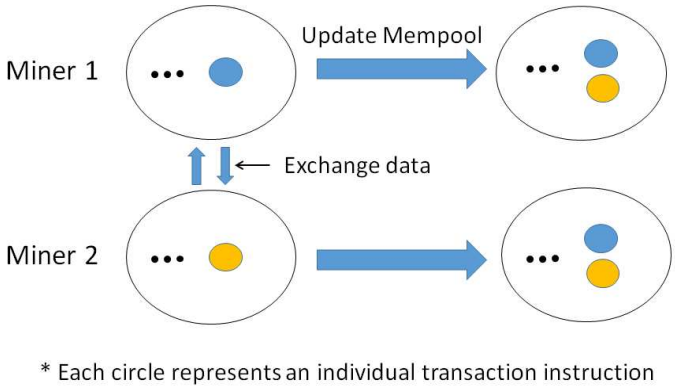

Figure 1: Updating rule of Mempool data

dynamically adjust the tolerance level ε of the mathematical problem to target the confirmation time τ at a certain level.[7] For this reason, we assume that miners' efforts do not influence the confirmation time τ and that the cryptocurrency system determines τ.

However, there are technical restrictions on the confirmation time τ. First, the delivery of goods must occur within the subperiod because consumption goods are perishable. Thus, an upper bound exists on τ as $\tau \leq \widehat{\delta}^{-1}(\beta^{1/N}) \equiv \overline{\tau}$, where $\widehat{\delta}^{-1}(\cdot)$ is an inverse of $\widehat{\delta}(\cdot)$. Second, as explained in Velde (2013), to maintain the stability of a cryptocurrency system based on blockchain technology, the mining process should not be easy and the confirmation time τ should not be too short.[8] Thus, we introduce the lower bound on the confirmation time as $\tau \geq \underline{\tau}$ such that $\widehat{\delta}(\underline{\tau}) \equiv \overline{\delta} < 1$.

Mempool In contrast to the current Bitcoin system, Mempools, in our model, are more than an interim storage device in which transaction instructions stay until they are recorded in the blockchain. Therefore, the technical features of Mempools are described in detail.

Mempool data are stored in miners' nodes, which continuously exchange the latest Mempool data with each other. Specifically, if two (or more) miners have different Mempool data, then the

[7]For example, the current Bitcoin system is programmed to automatically adjust the tolerance level ε 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.

[8]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, then some nodes on the other side of the globe may not be able to catch up with the latest transaction data, which may cause nodes to be no longer correctly aligned, leading to chain splits (forks), which blockchains must avoid as much as possible to remain secure.

miners update their Mempool with the union of data in all Mempools (see Figure 1).[9] More importantly, Mempools store all unconfirmed transactions until they are recorded in the blockchain, which is a bit different from the current Bitcoin system. Under the current Bitcoin system, an unconfirmed transaction can be rejected by the Bitcoin network after approximately seven days, and furthermore, all unconfirmed transactions that conflict with transactions recorded in the blockchain disappear in the Mempool.[10] In contrast to the current Bitcoin system, we assume that all unconfirmed transactions, including conflicting transactions, remain in the Mempool.[11]

Consensus protocol Because miners create their own blocks and try to add their blocks to the blockchain, two (or more) miners may 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 must reach a consensus regarding which state is considered 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 (see Figure 2).[12]

Blocks in the non-consensus chain are called orphaned blocks, and transactions in orphaned blocks are automatically moved to 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 conflicting transaction cannot be recorded in the blockchain and remains in the Mempool forever.

Rewards for mining work Because mining work is costly, a reward scheme is needed for mining to take place. In our model, such rewards are financed by transaction fees and the creation of

[9] By virtue of the updating rule of Mempool data, all Mempools can store all unconfirmed transaction data unless, for example, a hacker attacks all Mempools and deletes some unconfirmed transaction data at the same time, which occurs with a zero probability in the model economy.

[10] If a transaction is rejected in the Bitcoin network, then the funds remain at the Bitcoin address from which they were sent.

[11] 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, which is called the rejected pool. For this study, we need any transaction information that enters the cryptocurrency system to be stored in one of the storage devices, such as the Mempool, blockchain, or rejected pool, of the cryptocurrency system.

[12] 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.

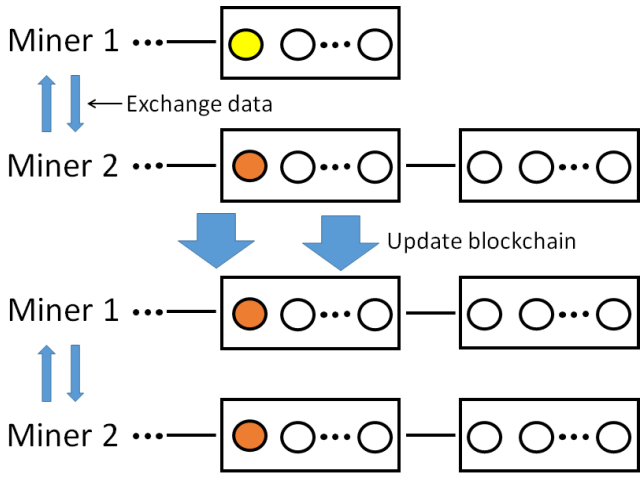

Figure 2: Updating rule of blockchain data

new cryptocurrencies. First, buyers must pay k units of cryptocurrency in terms of CM goods as transaction fees to use the cryptocurrency as a medium of exchange in the DM. Specifically, buyers choose fees k to have their transactions be incorporated into a specific block. Although buyers optimally choose transaction fees k, the cryptocurrency system sets the minimum transaction fee $k_{\min} > 0$ to prevent spam transactions; thus, $k \geq k_{\min}$. We assume that $k_{\min}$ is sufficiently small such that the trade surplus of buyers in the DM, when they pay $k_{\min}$ as transaction fees, is positive. 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, as $S_t = (\gamma - 1)M_t$. 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.

Building a reputation One of the main objectives of this paper is to study how the reputations of digital wallets affect the set of feasible equilibrium allocations. Specifically, the cryptocurrency system in this economy allows agents to verify the history of double spending attempts of any digital wallets, and a digital wallet may have a good or bad reputation based on its double spending attempt history. The means of tracking the double spending history of a digital wallet will be discussed after analyzing the double spending strategy. The issue here is the means of assigning a good reputation to digital wallets.

A wallet's reputation must be an outcome of normal transactions. Thus, a mechanism that assigns a reputation to digital wallets must discourage any incentives for distorting transaction behaviors just to obtain a good reputation considering many factors, such as the number of transactions, the total transaction fees that a wallet paid for past transactions, and transaction patterns, etc.

First, a wallet must have a sufficiently long transaction history without double spending attempts. However, the number of past transaction should not be a single criterion for assigning a good reputation. For example, if no minimum transaction fees are applied as in the Bitcoin system and the reputation only depends on the number of transactions, then an agent can overstate transaction numbers by making a sufficient number of spam transactions without transaction fees between his/her wallets. Thus, transaction fees that a wallet has paid must be also taken as an important factor when assigning a good reputation to the wallet.

In this paper, we are not interested in identifying the optimal mechanism for assigning a good reputation to digital wallets, which may be a direction for future work. Instead, we propose one mechanism that works in a stationary equilibrium, which we will focus on when characterizing equilibrium, based on the above argument. In particular, a wallet obtains a good reputation if it has been used for more than $\frac{\log\left(1+\frac{v}{k_{\min}}\left(1-\frac{\beta}{\gamma}\right)\right)}{\log\gamma-\log\beta}$ transactions consecutively in the past, where v is the value of a good reputation in a stationary equilibrium, and has paid at least the minimum transaction fees, $k_{\min}$, for each transaction. This implies that the present value of total transaction fees that the wallet has paid in a given period is higher than the value of a good reputation, and that fees have been paid over time instead of the total fees being paid in a single transaction.[13] Thus, agents have no incentives to distort trading behaviors to obtain a good reputation of their digital wallets.

We introduce the above mechanism into the model in the following manner using the risk neutral preferences in the *CM*. Specifically, we assume that a new wallet obtains a good reputation

[13] In a stationary equilibrium, inflation is given as $\frac{\phi_t}{\phi_{t+1}}=\gamma$, and sum of the present value of the minimum transaction fee, $k_{\min}$, for T number of past transactions is $\frac{\left(\frac{\gamma}{\beta}\right)^T-1}{1-\frac{\beta}{\gamma}}k_{\min}$, which is higher than v for all $T\geq\frac{\log\left(1+\frac{v}{k_{\min}}\left(1-\frac{\beta}{\gamma}\right)\right)}{\log\gamma-\log\beta}$.

with the probability $\rho < Min\left\{\frac{\log\gamma-\log\beta}{\log\left(1+\frac{\nu}{k_{\min}}\left(1-\frac{\beta}{\gamma}\right)\right)},1\right\}$, so $\frac{1}{\rho}$ number of transactions is required on average without double spending attempts in the *DM* for a new digital wallet to obtain a good reputation. Note that buyers must pay at least $k_{\min}$ units of real cryptocurrency for each transaction; thus, the total transaction fees that a wallet must pay to obtain a good reputation is higher than the value of a good reputation on average. Thus, buyers have no incentives to create or distort transactions to obtain a wallet's good reputation given the risk neutrality in the *CM*.

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.

The analysis can be simplified by making two observations. First, 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 choice of asset portfolio is independent of initial asset holdings.[14] 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*. For instance, a buyer will not bring more than the quantity of cryptocurrency necessary to buy a certain amount of goods in the *DM*.

Second, in this economy, the confirmation time, τ, affects equilibrium outcomes through a decreasing function $\widehat{\delta}(\tau)$, which represents the discount factor for each confirmation time. Additionally, as explained in the previous section, the cryptocurrency system adjusts the difficulty of PoW to target the confirmation time τ. Therefore, in the following analysis, we assume that the cryptocurrency system determines the discount factor $\widehat{\delta}(\tau)$, and we let $\widehat{\delta}(\tau) = \delta$ if no risk of

[14] See Williamson and Wright (2010), Nosal and Rocheteau (2011), and Lagos et al. (2017) for detailed information on the Lagos and Wright (2005) framework.

confusion exists.

For a straightforward analysis, we also assume throughout the main part of the paper that there is no limit on the block size. Therefore, no congestion occurs, and all transactions in the *DM* in a given period can be included in a single block, implying that all buyers will post the minimum transaction fee, $k_{\min}$, for their transactions in the *DM*. In section 6, we extend the model with the block size limit such that buyers strategically post transaction fees to have their transactions be included in a specific block in the blockchain.

3.1 Miners' problem

In the *DM*, miners mine $\overline{N}$ number of blocks updating the blockchain sequentially. Because no limit is imposed on the block size, which will be relaxed in section 6, the first block contains all transactions in the *DM* thereby validating them. All other blocks are empty and verify the update of the first block raising the number of confirmations of each transaction included in the first block.

Because a mathematical problem that must be solved to create a block depends on the information of the latest blockchain, miners cannot update the blockchain with their blocks if the blockchain has already been updated by other miners. Thus, miners compete to update the blockchain in the *DM*, and the probability that miner i will win the mining competition for updating the blockchain 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 to solve the PoW and update the blockchain with the probability $\frac{e_i}{\Lambda}$, as explained in Chiu and Koeppl (2017).[15]

By winning the competition in the *DM*, a miner updates the blockchain with his/her block and receives R units of cryptocurrency as a reward that consists of transaction fees and newly created cryptocurrency. A miner i takes the choice of other miners as given and thus solves the following

[15] Note that the difficulty of the PoW affects the expected time needed to solve the mathematical problem, but it does not affect the probability of winning the mining competition (see Chiu and Koeppl (2017) for detailed information and a micro-foundation for this probability of winning).

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. By 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 more than $1,000,000$ unique individuals are mining Bitcoins in the world.[16] Thus, mining work is quite competitive, and to capture this fact, we let $\eta \to \infty$ for the remainder of the paper, 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 to zero, and the aggregate mining effort converges to the aggregate rewards for the mining work, i.e., $\Lambda \to \beta \phi_{+1} R$.*

[16] 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.

3.2 Buyers' problem

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.[17] To initiate a transaction, the buyer instructs his/her digital wallet to transfer payment to the seller's digital wallet, and we call this transaction an honest transaction. At this point, the digital wallet application distributes the transaction instruction to miners' Mempools, and the seller receives a message indicating the buyer's payment.

However, receiving this message may be sufficient for the seller to deliver *DM* goods immediately because the buyer can always secretly initiate an alternative transaction to undo the payment, committing a double spending attack. Specifically, suppose that the seller delivers goods to the buyer immediately without payment confirmations, i.e., $N = 0$. Then, the buyer can open a new wallet in the *DM* temporarily and sends the same cryptocurrency to his/her new wallet.[18] We call this secret transaction a fraudulent transaction and the instruction for a fraudulent transaction is also distributed to miners' Mempools.

The honest and fraudulent transactions cannot be contained in the same block because the same cryptocurrency is used for both transactions. However, these two transactions can be contained in two separate blocks by two different miners. Then, the final outcome depends on which transaction is recorded in 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, allowing the double spending attempt to succeed.[19] Figure 3 illustrates a case in which a double spending attack succeeds or fails.

[17] Note that the seller cannot commit to the timing of delivery. Thus, the number of payment confirmations in the blockchain, $N \in \{0,\dots\overline{N}\}$, cannot be a part of the terms of trade.

[18] Under the current Bitcoin system, each cryptocurrency has its own unspent transaction output (UTXO) which is the output of a transaction that a user received in the past and is able to spend in the future. Using the same Bitcoin indicates that the same UTXO is used to create multiple transactions, and transaction instructions with the same UTXO cannot be included in the same block.

[19] In some cases, two blocks are added to the blockchain at the same time, generating a fork in the blockchain. Then, the final outcome depends on which block belongs to the consensus chain, and the transaction in the orphaned block will be moved to miners' Mempools.

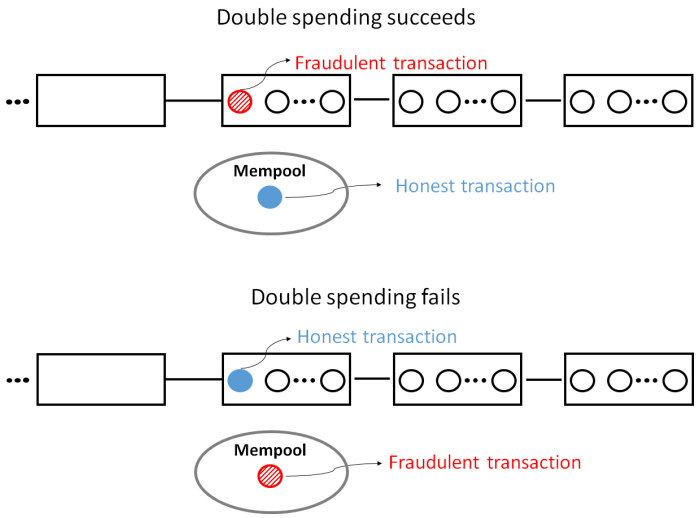

Figure 3: Double spending attacks

Now suppose that the seller delivers DM goods after receiving N number of confirmations. In this case, the buyer must mine N number of blocks first without the honest transaction. After receiving DM goods from the seller, the buyer initiates the fraudulent transaction, includes it in the $N+1^{\text{th}}$ block of his/her blockchain, and then releases the alternative blockchain to the cryptocurrency network to replace the original blockchain that contains the honest transaction. As the number of precautionary confirmations N increases, the total PoW that the buyer must complete to revoke the honest transaction increases, thus increasing the cost of double spending attacks. Therefore, a seller can prevent double spending attacks by holding up the delivery of goods until the payment transaction receives a sufficient number of confirmations, as illustrated in Chiu and Koeppl (2017).

Because the main focus of this paper is to study a mechanism supporting cryptocurrency transactions with zero confirmation, we introduce this feature into the model in a simple way: We assume that a transaction that received N_c number of confirmations cannot be revoked.[20] Therefore, if the seller believes that a positive probability of double spending attacks exists given the terms of trade (q,d), then he/she will deliver the goods after N_c number of payment confirmations

[20]In reality, the number of blocks N_c must depend on other economic factors, such as the transaction volume and aggregate mining efforts. For example, Chiu and Koeppl (2017) show that as the transaction volume increases, the precautionary confirmation lags, N_c, rise. However, for our purposes this is a detail, and we treat N_c as an exogenous variable focusing on how to improve the cryptocurrency system.

to prevent double spending attacks. On the other hand, if the terms of trade incentivize the buyer to not attempt double spending attacks even without payment confirmations, then the seller would transfer goods immediately in the DM, i.e., $N = 0$, and double spending does not occur. In either case, all offers in equilibrium are double spending-proof, i.e., double spending does not occur given the terms of trade (q,d), which is re-emphasized in the next proposition.[21]

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

Double spending history As one can see from the double spending strategy described above, a buyer must create a fraudulent transaction that conflicts with an honest transaction to double spend.[22] The information about these two transactions is either in the blockchain or in the Mempool, and both the blockchain and Mempool are publicly observable (see Figure 3). Therefore, agents can verify the history of double spending attempts from any digital wallets by looking at the blockchain and Mempool.[23]

This implies that a digital wallet can build a reputation regarding double spending attempts based on the reputation building process as discussed in the previous section. We call a wallet with a good reputation a good wallet and a wallet without a good reputation a bad wallet. Because a good reputation may have its own value, we consider buyers' value with both types of wallets. Specifically, let $V^j(m)$ denote the value function for a buyer holding m units of cryptocurrency in

[21] If a seller can commit to the timing of delivery $N \in \{0,\dots\overline{N}\}$ such that N 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 an 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.

[22] One may argue that the buyer can 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 an orphaned block for a moment. However, the honest transaction does not conflict with previous transactions in the blockchain and is therefore a valid transaction. This implies that the honest transaction will be moved to miners' Mempools and be recorded in the consensus blockchain later so double spending fails. Therefore, the buyer must create fraudulent transactions for double spending.

[23] In principle, a double spender can attack miners' Mempools to delete his/her transaction instructions for double spending. However, unless the double spender deletes the related information from all miners' 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 rationale, we assume that manipulating the history of double spending attempts is impossible.

the $j \in \{g,b\}$ type of wallet at the beginning of the *CM*, where $j = g$ represents a good wallet and $j = b$ stands for a bad wallet.

Notably, however, although the cryptocurrency system provides all information about recorded transactions in the blockchain and unconfirmed transactions in the Mempool, it does not provide any information about the identities of wallet holders. Therefore, 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, which does not have a good reputation based on the reputation building process, to trade cryptocurrency whenever the agent wants.

Double spending incentive without payment confirmations We now study a double spending prevention mechanism without payment confirmations in the blockchain, i.e., $N = 0$. 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*. Now suppose that the seller delivers *DM* goods without any confirmations, i.e., $N = 0$. 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 manner.

First, the buyer broadcasts the honest transaction with the minimum transaction fee, $k_{\min}$, and then generates the fraudulent transaction with the transaction fee $k_f = k_{\min} + \varepsilon_f$ where $\varepsilon_f > 0$. Because miners care about fee revenue, they will include the fraudulent transaction in their blocks such that double spending succeeds with certainty. In principle, the buyer can secretly mine a block with a fraudulent transaction for double spending by investing his/her own effort. However, it is optimal for the buyer not to mine a block by himself/herself given the result of lemma 1. Note that double spending succeeds for any $\varepsilon_f > 0$, and thus, we take the limit $\varepsilon_f \to 0$ in the following analysis because the buyer wants to minimize the transaction fees. Then, the expected payoff from the double spending attacks is given as q.

However, if the buyer double spends the cryptocurrency, then he/she must 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

$$\beta[V^j(0) - V^b(0)] \geq q, \tag{2}$$

then the buyer has no incentives for double spending even though the seller delivers goods without payment confirmations in the blockchain.

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 (2) is that $V^j(0) > V^b(0)$. Thus, if a buyer holds a bad wallet, i.e., $j = b$, then the incentive constraint (2) cannot hold. As a result, the buyer always has incentives for double spending if no precautionary confirmations exist. Knowing the buyer's double spending incentive, the seller delivers goods after receiving N^c number of confirmations 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, then a seller always delivers DM goods after receiving N_c number of confirmations to prevent double spending attacks.*

Proposition 2 shows that a delivery lag will occur if a buyer makes a payment from a bad wallet. However, the result of proposition 2 also applies to the cryptocurrency system in which a wallet cannot reveal its history of double spending attempts. Suppose that miners' Mempools do not store any transaction instructions that conflict with the transaction history in the blockchain as in the current Bitcoin system. Then, agents cannot verify the double spending history of a digital wallet. Therefore, a wallet cannot build a good reputation, implying that a sufficient number of confirmations is required to prevent double spending, which is consistent with the current practice in Bitcoin transactions.

Given the result of proposition 2, a buyer holding a bad wallet optimally chooses terms of trade in the *DM* considering the delivery lag. Then, the value of a buyer entering the *CM* with m units

of cryptocurrency in a bad wallet, $V^b(m)$, is given as

$$V^b(m) = \phi m + \underset{q \geq 0}{Max} \left\{ -\frac{\gamma}{\beta} q - k_{\min} + \delta^{N_c} u(q) + \beta \left[\rho V^g(0) + (1-\rho) V^b(0) \right] \right\}, \tag{3}$$

where we discount the buyer's utility in the *DM* by δ^{N^c} because the buyer receives goods after N^c number of confirmations. Note, from (3), that each buyer takes the probability ρ that a new wallet obtains a good reputation as given. However, the probability ρ must satisfy the rule of assigning a good reputation in equilibrium to prevent incentives for distorting trading behavior simply to obtain a good reputation as discussed in the previous section.

Now suppose that 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 (2), which leads the seller to deliver goods immediately without precautionary confirmations.[24] In this case, the value function of buyers with a good wallet, $V^g(m)$, is given as

$$V^g(m) = \phi m + \underset{q \geq 0}{Max} \left\{ -\frac{\gamma}{\beta} q - k_{\min} + u(q) + \beta V^g(0) \right\} \tag{4}$$

subject to

$$\beta [V^g(0) - V^b(0)] \geq q, \tag{5}$$

where (5) is the incentive constraint (2) 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 (5) 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 after N_c number of confirmations. Thus, no economic difference exists between good and bad wallets.

[24] Here, we implicitly assume that sellers deliver *DM* goods immediately if buyers have no incentives for double spending without payment confirmations.

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* $\{\delta,\ \gamma,\ k_{\min},\ \rho\}$*, a stationary cryptocurrency equilibrium is a list* $\{z,\ r,\ q,\ k,\ \{e_i\}_{i=1}^{\eta},\ \Lambda\}$ *where* $z \equiv \phi M$ *and* $r \equiv \phi R$ *such that:*

1. *Given* $\{\delta,\gamma,k_{\min}\}$, $\{q,k\}$ *solves the buyer's problem.*
2. *Given* $\{\gamma,\ r,\ \{e_j\}_{j\neq i}\}$, $e_i = e$ *solves the problem of miner i for all* $i = 1,\dots\eta$
3. *Aggregate mining effort is the sum of mining effort of all miners as* $\Lambda = \eta e$
4. *Reward r is generated by* (γ,k) *and the real cryptocurrency demand*
5. *The cryptocurrency market clears in the CM as*

$$z = \frac{\gamma q}{\beta} + k. \tag{6}$$

The reward R for winning the mining competition is the sum of transaction fees and newly created cryptocurrency. First, when no limit is imposed on the block size, there is no congestion in the mining process, and all buyers therefore pay the minimum transaction fee, $k_{\min}$, for their transaction in the DM. Second, the aggregate quantity of the new cryptocurrency, S, is determined by the growth rate γ as $S = (\gamma-1)M$. Finally, we assume that the $\overline{N}$ block winners share the total reward equally for simplicity. Consequently, the reward per block is given as $R = \frac{1}{\overline{N}}\left\{(\gamma-1)M + \frac{k_{\min}}{\phi}\right\}$. Then, using the market clearing condition (6) and the result of lemma 1, we obtain,

$$\Lambda = \beta\phi_{+1}R = \frac{(\gamma-1)q + \beta k_{\min}}{\overline{N}}, \tag{7}$$

which expresses the aggregate mining effort per block as a function of the trade volume q.

The equilibrium quantity of goods traded, q, in the DM, can be obtained by solving the buyer's problem. In equilibrium, three relevant cases are possible for the buyer's problem depending on whether a delivery lag exists in the DM and whether the incentive constraint (5) that prevents

double spending without precautionary confirmations binds.

1. (*Delivery lag equilibrium*) Sellers deliver goods in the *DM* after the precautionary payment confirmations in the blockchain, i.e., there is a delivery lag for *DM* goods.
2. (*Threat of double spending equilibrium*) No delivery lag occurs for goods in the *DM* and the incentive constraint (5) that prevents double spending binds.
3. (*No threat of double spending equilibrium*) No delivery lag occurs for goods in the *DM* and the incentive constraint (5) that prevents double spending does not bind.

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

- The quantity of goods traded in the *DM*:

$$q_R^* \equiv u'^{-1}\left(\frac{\gamma}{\beta}\right) \tag{8}$$

$$q_R^{**} \equiv u'^{-1}\left(\frac{\gamma+1-\beta(1-\rho)}{\beta}\right). \tag{9}$$

- The functions of q and δ:

$$\Phi(q) \equiv -\frac{\gamma+1-\beta(1-\rho)}{\beta}q + u(q) \tag{10}$$

$$\Omega(\delta) \equiv -\frac{\gamma}{\beta}\widehat{q}_{N_c}(\delta) + \delta^{N_c}u(\widehat{q}_{N_c}(\delta)), \tag{11}$$

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

Given these definitions, the next proposition characterizes the existence of each type of equilibrium.

Proposition 3 *Define the cutoff levels of the discount factor δ and set the probability ρ as*

$$\widetilde{\delta}_1 = \begin{cases} \Omega^{-1}\left(\Phi(q_R^*)\right) & \text{if } \Phi(q_R^*) \geq 0 \\ -\varepsilon_\delta & \text{if } \Phi(q_R^*) < 0 \end{cases} \tag{12}$$

$$\widetilde{\delta}_2 = \Omega^{-1}\left(\Phi(q_R^{**})\right), \tag{13}$$

$$\rho < Min\left\{ \frac{\log\gamma - \log\beta}{\log\left(1 + \frac{\bar{v}}{k_{\min}}\left(1 - \frac{\beta}{\gamma}\right)\right)}, 1 \right\} \tag{14}$$

where $\varepsilon_\delta > 0$ and $\bar{v} = \frac{1}{1-\beta}\left\{-\frac{1}{\beta}u'^{-1}\left(\frac{1}{\beta}\right) - k_{\min} + u\left(u'^{-1}\left(\frac{1}{\beta}\right)\right)\right\}$. Then, given a set of parameters $\{\delta, \gamma, k_{\min}, \rho\}$, a unique stationary equilibrium exists as follows:

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

Proof. See Appendix ■

Proposition 3 describes how buyer's double spending incentives and the equilibrium type depend on the discount factor δ. As explained in proposition 2, a seller always delivers goods in the *DM* after receiving N_c number of payment confirmations if a buyer makes the payment from a bad wallet. In this case, the confirmation time τ affects the total time τN_c that the buyer must wait before receiving goods, which affects the buyer's utility through the discount factor, $\widehat{\delta}(\tau)$, in the *DM*.[25] Specifically, as τ increases, δ falls, which reduces the trade surplus, $-\frac{\gamma}{\beta}q - k_{\min} + \delta^{N_c}u(q)$, and the value of trading with a bad wallet given by (3). Because the buyer loses the good wallet

[25]The confirmation lags, N^c, that prevent double spending attacks can potentially be a function of the confirmation time τ as $N^c(\tau)$. For example, two confirmations may be sufficient to discourage double spending attacks when the confirmation time is one hour while we may need six confirmations when the confirmation time is 10 minutes. However, the main results do not change as long as the total time for creating $N^c(\tau)$ number of blocks, given as $N^c(\tau)\tau$, increases with the time for creating each block, τ.

and will have to start trading with a bad wallet from the next period if he/she commits a double spending attack, the buyer has less incentives for double spending as δ decreases. Thus, as δ decreases due to an increase in the time for each confirmation τ, 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.

As explained in the previous section, a new wallet obtains a good reputation with the probability ρ following the reputation building rule. Note, from (4), that the value of a good reputation, $V^g(0)$, is maximized when $\gamma = 1$ and the incentive constraint (5) does not bind. Therefore, $\frac{1}{1-\beta}\left\{-\frac{1}{\beta}u'^{-1}\left(\frac{1}{\beta}\right) - k_{\min} + u\left(u'^{-1}\left(\frac{1}{\beta}\right)\right)\right\}$, is the upper bound for the value of a good reputation that can be attainable in any equilibrium. Then, as long as (14) holds, buyers have no incentives to create spam transactions just to obtain a good reputation as discussed in the previous section.

We now study the determinants of the trade volume, q, and the aggregate mining effort, Λ, in each type of equilibrium. Note, from (7), that the aggregate mining effort, Λ, can be obtained by substituting the equilibrium q into (7); therefore, we focus on analyzing the equilibrium quantity of goods traded, q, in the *DM*.

Proposition 4 *In each type of equilibrium, the quantity of goods, q, traded in the DM is as follows:*

1. *In the delivery lag equilibrium,* $q = \widehat{q}_{N_c}(\delta) \equiv u'^{-1}\left(\frac{\gamma}{\delta^{N_c}\beta}\right)$.
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 after receiving N_c number of payment confirmations in the blockchain to prevent double spending attacks. Thus, a buyer optimally chooses $q = \widehat{q}_{N_c}(\delta)$ to maximize the trade surplus, $-\frac{\gamma}{\beta}q - k_{\min} + \delta^{N_c}u(q)$, considering delivery lags.

Next, in the threat of double spending equilibrium, a seller transfers goods to a buyer immediately without confirmations in the *DM* and the buyer does not commit double spending in

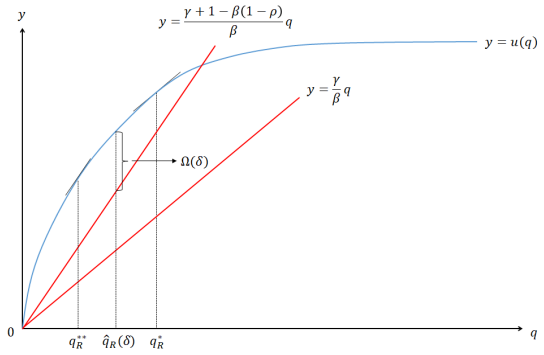

Figure 4: Trade volume q in the threat of double spending equilibrium

equilibrium. However, the incentive constraint (5) that prevents double spending without confirmations binds, and the binding incentive constraint (5) restricts the quantity of goods, q, traded in the *DM*. More precisely, substituting (3) with $q = \widehat{q}_{N_c}(\delta)$ in the delivery lag equilibrium, (4), and (7) into the binding incentive constraint (5) and using the definitions of $\Phi(q)$ and $\Omega(\delta)$ provided in (10) and (11), respectively, we obtain

$$\Phi(q) = \Omega(\delta), \tag{15}$$

which determines q given δ. Note, from (9) and (10), that $\Phi(q)$ is maximized when $q = q_R^{**}$. Thus, if $\Phi(q_R^{**}) < \Omega(\delta)$, then there is no q that satisfies (15). When $\Phi(q_R^{**}) \geq \Omega(\delta)$, there are two values of q that satisfy (15), but only q that is higher than q_R^{**} is the equilibrium quantity of goods traded because otherwise, the objective function (4) is not maximized. At the same time, q cannot be higher than q_R^* to have the binding incentive constraint (5). Figure 4 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 have no incentives for double spending, and sellers deliver goods instantly without payment confirmations. The quantity of *DM* goods traded, q, 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 (4).

Comparative statics Having characterized the existence of each equilibrium, we now discuss some comparative statics of the set of parameters $\{\delta, \gamma, \rho\}$ on the quantity of goods, q, traded in the *DM* and the aggregate mining efforts, Λ, per block. Here, we conduct comparative statics of δ instead of τ. However, the comparative statics of τ can be obtained by taking the opposite effects of changing δ on equilibrium allocations because $\delta = \widehat{\delta}(\tau)$ decreases with τ.

In the delivery lag equilibrium, the marginal utility of the buyer in the *DM* with delayed consumption increases. Thus, the trade volume $q = \widehat{q}_{N_c}(\delta)$ and the aggregate mining effort, Λ, given by (7), increase with respect to δ. 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. Next, substituting $\widehat{q}_{N_c}(\delta) \equiv u'^{-1}\left(\frac{\gamma}{\delta^{N_c}\beta}\right)$ into (7), we obtain $\Lambda = \frac{[\delta^{N_c}\beta u'(\widehat{q}_{N_c}(\delta))-1]\widehat{q}_{N_c}(\delta)+\beta k_{\min}}{\overline{N}}$, which decreases with respect to $\widehat{q}_N(\delta)$. Thus, the aggregate mining effort, Λ, increases with γ. This is because an increase in γ implies an increase in the reward for mining works, and miners therefore invest more effort in the mining competition even though an increase in γ reduces the real value of the cryptocurrency by decreasing the trade volume q.

In the threat of double spending equilibrium, the quantity of goods traded in the *DM*, given by $q = \widehat{q}_R(\delta) \in [q_R^{**}, q_R^*)$, decreases with respect to δ as one can see from Figure 4, 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, reducing the cost of losing a good wallet through double spending. This tightens the incentive constraint (5), and q decreases as a consequence. By the same rationale, 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 and hence double spending incentives.[26] The aggregate mining effort, Λ, given in (7), increases with q, and thus 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, an increase in γ raises the cryptocurrency holding cost, which pushes down q. On the other hand, an increase in γ implies a decrease in the value of trading with a bad wallet

[26]More precisely, $\frac{\partial \Phi(q)}{\partial \rho} < 0$ in (10). 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.

	Delivery lag			Threat of double spending			No threat of double spending		
	δ	γ	ρ	δ	γ	ρ	δ	γ	ρ
q	$+$	$-$	0	$-$	?	$-$	0	$-$	0
Λ	$+$	$+$	0	$-$	?	$-$	0	$+$	0

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

given by (3), which relaxes the incentive constraint (5), pushing up q. Which effect dominates over the other and thus 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 $\widehat{q}_{N_c}(\delta)$.[27] Similarly, whether the aggregate mining effort, Λ, given in (7), increases with γ is unclear.

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. Specifically, an increase in γ reduces the trade volume q_R^* because of the increased holding cost of cryptocurrency. Next, using the definition of q_R^* in (8), the aggregate mining effort is given as $\Lambda = \frac{[\beta u'(q_R^*)-1]q_R^*+\beta k_{\min}}{\overline{N}}$, which decreases with q_R^*. Therefore, Λ increases with γ, for the same reason as in the case of delivery lag equilibrium. Table 1 summarizes the above analysis.

We close this section with the further analysis of δ. The 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 δ, suppose that $\beta < \widetilde{\delta}_1 < \widetilde{\delta}_2 < \overline{\delta}$, which 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 3). Then, by the definition of $\widetilde{\delta}_1 = \Omega^{-1}(\Phi(q_R^*))$ in (12) and $\widehat{q}_R(\delta)$ in proposition 4, we obtain $\lim_{\delta \to \widetilde{\delta}_1} \widehat{q}_R(\delta) = q_R^*$. Next, from (9)

[27] From (10), (11), and (15), we obtain

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

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 $\widehat{q}_{N_c}(\delta) \gtreqless \widehat{q}_R(\delta)$.

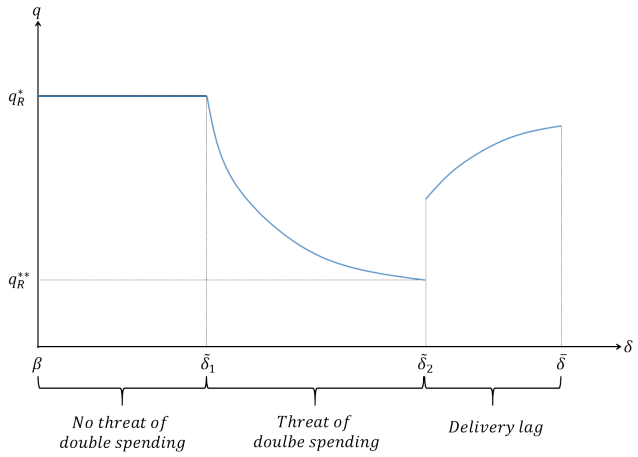

Figure 5: Quantity of goods q traded in the *DM* and the discount factor δ

- (11), $\widetilde{\delta}_2 = \Omega^{-1}(\Phi(q_R^{**}))$ and $\widehat{q}_{N_c}(\delta) \equiv u'^{-1}\left(\frac{\gamma}{\delta^{N_c}\beta}\right)$, we obtain

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

which implies $\widehat{q}_{N_c}(\widetilde{\delta}_2) > q_R^{**}$. 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 5 describes the above analysis, and the effects of δ on the aggregate mining effort Λ given by (7) show a similar pattern.

5 Welfare analysis

We now examine the model's normative properties in terms of social welfare and to find the optimal cryptocurrency system. We restrict our attention to stationary allocations and define the sum of expected utilities in a steady state equilibrium across agents as our welfare measure, which is given as

$$W = \widehat{\delta}(\tau)^N u(q) - q - \overline{N}\Lambda, \tag{16}$$

where N is the number of precautionary confirmations of the payment. 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 (7) into (16), we obtain

$$W = \widehat{\delta}(\tau)^N u(q) - \gamma q - \beta k_{\min} \tag{17}$$

as our welfare measure in equilibrium.

Thus far, we have taken parameters, such as τ (hence δ), γ, $k_{\min}$, and ρ, as exogenously given. Here, what items are under the control of the cryptocurrency system? First, the probability that a bad wallet obtains a good reputation ρ is not under the control of the cryptocurrency system but is determined by a reputation building mechanism as discussed in the previous section. Second, the cryptocurrency system can control the confirmation time τ by adjusting the level of difficulty with which a mathematical problem is solved to create a new block, and τ affects equilibrium allocations through its effects on the discount factor δ. Third, the system determines the growth rate of cryptocurrency γ, which also affects equilibrium allocations, by changing the supply of new cryptocurrency provided to miners. Finally, the system sets the minimum transaction fee, $k_{\min}$, but $k_{\min}$ does not affect equilibrium allocations, and setting $k_{\min} = 0$ is therefore optimal. However, the minimum transaction fee, $k_{\min}$, helps the system prevent spam transactions in reality and is related to the reputation building mechanism. Determining the optimal reputation building mechanism and $k_{\min}$ may also be interesting, but we leave further analysis on this topic to future work. In the following section, we focus on analyzing the effects of τ and γ on welfare.

5.1 Confirmation time τ and welfare

In this subsection, we analyze how the confirmation time τ affects welfare and study its optimal level, denoted as τ^*, given other parameters $(\gamma, \rho, k_{\min})$. Note that $\widehat{\delta}(\tau)$ is a decreasing function of τ, and τ affects equilibrium allocations through the discount factor $\widehat{\delta}(\tau)$. Thus, finding the optimal confirmation time, τ, is the same as finding the optimal discount factor, δ, and we analyze the effects of δ on welfare in the following analysis.

To study the effects of δ on welfare, we first analyze the effects of trade volume q on welfare.

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, a higher trade volume corresponds to a higher real value of cryptocurrency, which increases the social cost from mining work due to increased competition. Combined together, the effects of q on welfare are not clear as one can see from (17). 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 2 *Given a set of parameters* $\{\delta, \gamma, \rho, k_{\min}\}$*, welfare increases with the quantity of goods, q, traded in the DM in equilibrium.*

Proof. See Appendix ■

Given the result of lemma 2, we can analyze the effects of an increase in δ, caused by a decrease in τ, on welfare in each type of equilibrium. First, in the delivery lag equilibrium, as δ increases, the trade volume, $q = \widehat{q}_{N_c}(\delta)$, rises, and welfare loss from the delayed consumption due to delivery lags in the *DM* falls. 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 2. Finally, in the no threat of double spending equilibrium, changing δ has no effects on the trade volume q and hence welfare. However, in this equilibrium, the economy achieves $q = q_R^*$, which is the highest trade volume attainable in the *DM* given a set of parameters $(\gamma, \rho, k_{\min})$, and there is no welfare loss from delivery lags. Thus, welfare is maximized in the no threat of double spending equilibrium.

Based on the above analysis, the next proposition describes the optimal level of the discount factor, denoted by δ^*, and the optimal confirmation time, τ^*, as a function of δ^* given other parameters.

Proposition 5 *Given* $(\gamma, \rho, k_{\min})$*, the optimal confirmation time is given as* $\tau^* = \widehat{\delta}^{-1}(\delta^*)$*, where* δ^* *is given as follows:*

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

3. *When* $\widetilde{\delta}_1 < \beta^{1/\overline{N}} \leq \widetilde{\delta}_2 \leq \overline{\delta}$,

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

4. *When* $\widetilde{\delta}_2 < \beta^{1/\overline{N}}$, $\delta^* = \overline{\delta}$.

Proof. See Appendix ■

The main implication of proposition 5 is as follows. Because welfare is maximized in the no threat of double spending equilibrium, making the incentive constraint (5) slack by setting $\delta \in [\beta^{1/\overline{N}}, \widetilde{\delta}_1]$ whenever feasible is optimal, which requires $\beta \leq \widetilde{\delta}_1$. Next, when the threat of double spending equilibrium is the only feasible equilibrium, it is optimal to minimize δ, i.e., $\delta^* = \beta^{1/\overline{N}}$, to maximize the trade volume and welfare. One the other hand, if the only feasible equilibrium is the delivery lag equilibrium, then maximizing δ, i.e., $\delta^* = \overline{\delta}$, is optimal to minimize the welfare loss from delivery lags. Finally, if the threat of double spending equilibrium and the delivery lag equilibrium are both feasible, the optimal level of discount factor, δ^*, is either $\beta^{1/\overline{N}}$ or $\overline{\delta}$ depending on the value of maximized welfare in both types of equilibrium.

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, denoted by γ^*, given other parameter values $(\delta, \rho, k_{\min})$. Note, from (17), 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, whether welfare increases or decreases in response to an increase in

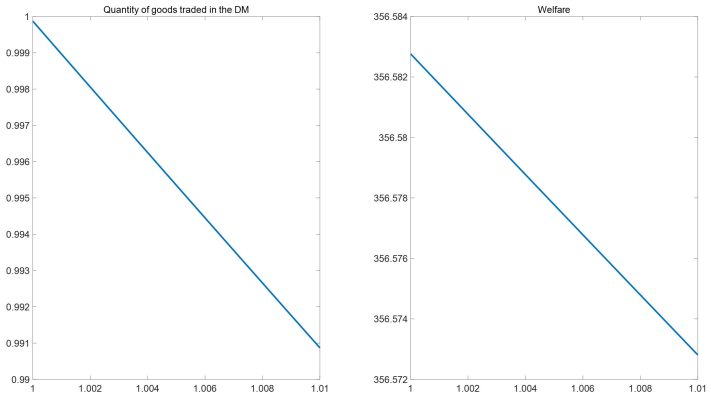

Figure 6: Effects of cryptocurrency growth

γ is not clear.

To better understand the effects of γ on welfare, we conduct numerical exercises with the buyer's utility function in the *DM* as $u(q) = \frac{(q+\xi)^{1-\alpha}-\xi^{1-\alpha}}{1-\alpha}$ where $\alpha > 1$ and $\xi \approx 0$. The length of the time period is one day, and we set $\beta = 0.95^{1/365}$ with an annual discount factor of 0.95, so the annual real interest rate on an illiquid bond is 5.2%. The estimates for the curvature of $u(q)$ vary widely, and we use $\alpha = 1.1$, which is within the range of previous studies. We choose $k_{\min} = 0.00071$ to target the average ratio of transaction fees to the Bitcoin transaction volume for the period 2016 to 2017, which is 0.0007, when $\gamma = 0.057$ which is the average annual growth rate for the same period.[28] We set $\rho = 0.0002$, so it takes $50,000$ number of honest transactions on average for a bad wallet to obtain a good reputation.[29] Finally, we use $\delta = \beta^{1/144}$, $N_c = 6$, and $\overline{N} = 144$, which implies that it takes 10 minutes on average for a transaction to be recorded in the blockchain, and the average waiting time before receiving goods in the *DM* in the delivery lag equilibrium is one hour.[30]

Figure 6 shows how welfare responds to a change in the growth rate of cryptocurrency γ when γ changes from 1 to 1.01. Based on our calibration, the probability ρ is sufficiently low to make the

[28] Source for Bitcoin data: blockchain.info

[29] The probability ρ quantitatively affects real allocations only in the threat of double spending equilibrium. Thus, the main results, such as the welfare gain by eliminating delivery lags in the current Bitcoin trading environment, do not hinge on the value of ρ.

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

incentive constraint (5) slack for all $\gamma \geq 1$.[31] Thus, the no threat of double spending equilibrium exist for all $\gamma \geq 1$. Because the quantity of goods traded, q, in the *DM* and welfare decrease with γ in the no threat of double spending equilibrium, the optimal growth rate is given as $\gamma^* = 1$.

5.3 Evaluation of the current Bitcoin system

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.[32] Thus, in retail transactions, goods are recommended to be delivered after receiving a sufficient number of precautionary confirmations, 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 equilibrium with $\gamma = 1.057^{1/365}$ to welfare when (δ, γ) is set optimally. Specifically, we measure the welfare gain as the fraction of additional consumption that the economy needs such 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 $\gamma = 1$, and suggests that the welfare gain from adopting the optimal design of Bitcoin system is 0.21% of consumption in terms of the consumption equivalent measure. In particular, most of the welfare gain (more than 99.99%) comes from eliminating the delivery lag, and a minute amount welfare gain comes from setting the growth rate optimally, i.e., $\gamma = 1$.

[31] If we set $\rho = 0.00155$, all types of equilibrium can exist depending on the value of γ, and the equilibrium type changes from the delivery lag to the threat of double spending and then to the no threat of double spending equilibrium as γ increases from 1 to 1.01. However, setting $\rho = 0.00155$ is not consistent with the reputation building process in the model economy.

[32] 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. Furthermore, the current Bitcoin system deletes all transaction instructions that conflict with the transaction record in the blockchain from the Mempool. Thus, agents may not be able to track the full transaction instruction history of a particular digital wallet and thus cannot check the double spending history.

6 Transaction fees with the block size limit

We have assumed that there is no restriction on the block size, so all transactions in the *DM* of period t are included in a single block. However, in reality, cryptocurrency users compete for the speed of their transaction confirmation by posting transaction fees. Thus, in this section, we extend the baseline model with the block size limit such that a transaction may be recorded in the later block, causing a verification lag. In particular, we show that this change provides new insights into the relationship between Bitcoin transaction volume and transaction fees but it does not affect the main results of the baseline model.

In this section, we assume that transactions in the *DM* are recorded in the first $\overline{N} - N_c + 1$ number of blocks, and the remaining $N_c - 1$ number of blocks are empty updating the confirmation of transactions in the previous blocks. Buyers now strategically post transaction fees, k, to have their transactions be included in a specific block. Because miners care about fee revenue, they will include transactions with higher fees in earlier blocks. Thus, there will be a decreasing sequence of fees $k_1 \geq k_2 \geq \cdots \geq k_{\overline{N}-N_c+1}$, and in the *DM*, transactions with fees k_1 are recorded in the first block, transactions with fees k_2 are recorded in the second block and so on.

We first study allocations in equilibrium where a good reputation of digital wallets does not have its own value, and sellers therefore deliver goods after receiving N_c number of confirmations, i.e., delivery lag equilibrium. Let q_n and k_n denote the quantity of goods traded and transaction fees, respectively, of a transaction that is recorded in the n^{th} block in the *DM* of a given period, where $n \in \{1, \ldots \overline{N} - N_c + 1\}$. Given the order n, buyers optimally choose q_n and k_n to maximize their trade surplus, S_n, which is given as

$$S_n = \underset{q_n \geq 0, k_n \geq k_{\min}}{Max} \left\{ -\frac{\gamma}{\beta} q_n - k_n + \delta^{n+N_c-1} u(q_n) \right\},$$

which gives

$$q_n = u'^{-1}\left(\frac{\gamma}{\delta^{n+N_c-1}\beta} \right) \equiv \widehat{q}_{n+N_c-1}(\delta) \tag{18}$$

as the quantity of goods traded, q_n, in the delivery lag equilibrium for $n \in \{1, \ldots \overline{N} - N_c + 1\}$.

Regarding transaction fees, notice that buyers will pay the minimum fee, $k_{\min}$, as transaction fees for transactions that are recorded in the $(\overline{N} - N_c + 1)^{\text{th}}$ block, i.e., $k_{\overline{N}-N_c+1} = k_{\min}$. Next, because buyers are homogeneous, they must be indifferent about the order of a block $n \in \{1, \ldots \overline{N} - N_c + 1\}$ in the blockchain. Thus, it must be $S_n = S_{\overline{N}-N_c+1}$ for all $n \in \{1, \ldots \overline{N} - N_c + 1\}$, which gives

$$k_n = k_{\min} - \frac{\gamma}{\beta}\widehat{q}_{n+N_c-1}(\delta) + \delta^{n+N_c-1}u(\widehat{q}_{n+N_c-1}(\delta)) + \frac{\gamma}{\beta}\widehat{q}_{\overline{N}}(\delta) - \delta^{\overline{N}}u\left(\widehat{q}_{\overline{N}}(\delta)\right) \tag{19}$$

as the optimal transaction fees for a transaction that is recorded in the n^{th} block.

How does introducing the block size limit affect allocations in equilibrium without delivery lags and the existence of each type of equilibrium? Buyers will pay the minimum fee, $k_{\min}$, as transaction fees in equilibrium without delivery lags similar to the baseline model because transaction fees do not affect the timing of consumption in the *DM*. Thus, $k_{n=}k_{\min}$ for all $n \in \{1, \ldots \overline{N} - N_c + 1\}$ in equilibrium without delivery lags. However, the quantity of goods, q, traded in the *DM* requires more detailed analysis because it depends on the double spending incentives of buyers.

When a seller delivers goods without payment confirmations, a buyer can successfully double spend the cryptocurrency by creating a fraudulent transaction with fees $k_{\min} + \varepsilon_f$. After committing the double spending attack, the buyer loses the current wallet and starts trading with a bad wallet from the next period onward. Taking the limit $\varepsilon_f \to 0$ as in the baseline model, we obtain (2) as the incentive constraint that prevents double spending without confirmations in the extended model with the block size limit. Thus, sellers provide goods after receiving N_c number of confirmations if a buyer makes the payment from a bad wallet similar to the baseline model as described in proposition 2.

Then, what is the value of trading with a bad wallet in the off-equilibrium path when a limit is imposed on the block size? As explained above, all other buyers pay the minimum fee, $k_{\min}$, as transaction fees in equilibrium without delivery lags. Thus, a buyer with a bad wallet can have

his/her transaction be included in the first block by paying $k_{\min} + \varepsilon_b$ units of real cryptocurrency as transaction fees. Taking the limit $\varepsilon_b \to 0$, the buyer's value function with a bad wallet on the off-equilibrium path is exactly the same as (3), implying that the buyer's problem described by equations (3) - (5) does not change in the extended model. Consequently, the quantity of goods traded, q, in the threat of double spending and no threat of double spending equilibria is given as $\widehat{q}_R(\delta)$ and q_R^*, respectively, which are the same as in the baseline model. Furthermore, proposition 3 characterizes the existence of each type of equilibrium in the extended model. The only difference from the baseline model is the trade volume, q, and transaction fees, k, in the delivery lag equilibrium.

Testable implications for Bitcoin transaction fees As explained in the previous section, the current Bitcoin system does not support reputation building of digital wallets and Bitcoin transactions are accompanied by delivery lags due to precautionary confirmations. Therefore, the behaviors of Bitcoin transactions can be interpreted as outcomes of the delivery lag equilibrium in our model and we can use our model to improve our understanding of Bitcoin transactions. Specifically, from, (18) and (19), we obtain the relationship between transaction volume, q_n, and transaction fees, k_n, in the delivery lag equilibrium as described in the next proposition.

Proposition 6 *In the delivery lag equilibrium with the block size limit, q_n and k_n decrease with n. Furthermore, if $u(q) = \frac{(q+\xi)^{1-\alpha} - \xi^{1-\alpha}}{1-\alpha}$, where $\alpha > 1$ and $\xi \approx 0$, then $\frac{k_n}{q_n}$ increases with n.*

Proof. See Appendix ■

Proposition 6 provides two testable implications for Bitcoin transaction behaviors. First, transaction fees increase with transaction volumes, i.e., $cov(q_n, k_n) > 0$. This result is intuitive because as transaction fees increase, the speed of payment confirmation increases. Then, the utility loss from delayed consumption falls, the marginal utility from the consumption of *DM* goods increases, and the optimal trading volume increases as a consequence. In particular, when the buyer's utility function in the *DM* has a form of $u(q) = \frac{(q+\xi)^{1-\alpha} - \xi^{1-\alpha}}{1-\alpha}$ where $\alpha > 1$ and $\xi \approx 0$, the trade volume, q_n, responds more elastically than transaction fees, k_n, to the speed of payment confirmations,

	k	k/q
corr(q,variable)	0.177	-0.192

Table 2: Properties of Bitcoin transaction fees

which is captured by the order of a block n in the model. Thus, the model shows the negative relationship between the ratio of transaction fees to the trade volume, $\frac{k_n}{q_n}$, and the transaction volume, q_n.

Table 6 shows the relationship between Bitcoin transaction volume and transaction fees using individual Bitcoin transaction data.[33] As one can see from Table 6, the sign of the correlation is consistent with the theoretical predictions in proposition 6. We are obviously being a little loose in this conclusion because a more rigorous empirical analysis should consider other factors, such as the Mempool size that captures the degree of mining congestions and the time required for each transaction to be recorded in the blockchain. However, we leave further empirical analysis to future work.

7 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 the double spending risk due to its digital nature. Current cryptocurrency systems, such as the Bitcoin system, overcome the 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 pre-

[33] Specifically, we randomly collect 250 blocks from the Bitcoin blockchain (from the height 100,001 to the height 600,000), and obtain 247,952 individual transactions after removing transactions with zero trading volume. We then calculate the ratio of transaction fees to transaction volume, $\frac{k}{q}$, using transaction volume, q, and transaction fees, k, for each transactions. Because these variables are highly right-skewed, we drop all data points above the 95th percentile, thus removing 35,362 outliers. Then, we calculate the correlations in Table 6 using 212,590 Bitcoin transaction data.

vented 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 confirmation time that is determined by the level of difficulty of the mining work. 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.

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.

BETHUNE, Z., T.-W. HU, AND G. ROCHETEAU (2018): "Indeterminacy in credit economies," *Journal of Economic Theory*, 175, 556–584.

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.

CAVALCANTI, R. D. O. AND N. WALLACE (1999a): "Inside and Outside Money as Alternative Media of Exchange," *Journal of Money, Credit and Banking*, 31, 443–457.

——— (1999b): "A Model of Private Bank-Note Issue," *Review of Economic Dynamics*, 2, 104–136.

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.

FERNÁNDEZ-VILLAVERDE, J. AND D. SANCHES (Forthcoming): "Can Currency Competition Work?" *Journal of Monetary 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.

PAGNOTTA, E. S. (2019): "Bitcoin as Decentralized Money: Prices, Mining, and Network Security," Working paper.

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 propositions 3 and 4. Here, we prove propositions 3 and 4 together by solving the buyer's problem.

Because we need $V^b(0)$ to derive the incentive constraint (5), we first look at the case where a delivery lag of goods exists in the *DM*. The first-order condition of the buyer's problem (3) is

$$\delta^{N_c} u'(q) = \frac{\gamma}{\beta}.$$

Thus, $q = \widehat{q}_{N_c}(\delta) \equiv u'^{-1}\left(\frac{\gamma}{\delta^{N_c}\beta}\right)$ in the delivery lag equilibrium. Substituting $q = \widehat{q}_{N_c}(\delta)$ into (3), we obtain

$$V^b(m) = \phi m + \frac{1}{1-\beta(1-\rho)}\left\{-\frac{\gamma}{\beta}\widehat{q}_{N_c}(\delta) - k_{\min} + \delta^{N_c} u\left(\widehat{q}_{N_c}(\delta)\right) + \beta\rho V^g(0)\right\}. \tag{20}$$

We now study the buyer's problem (4) in which sellers deliver goods immediately without a delivery lag. The first-order condition is

$$u'(q) - \frac{\gamma}{\beta} - \lambda = 0, \tag{21}$$

where $\lambda \geq 0$ is the Lagrange multiplier associated with the incentive constraint (5).

Case 1 In the no threat of double spending equilibrium, the incentive constraint (5) does not bind, and hence $\lambda = 0$ in (21). Then, the quantity of goods traded in the DM is given as $q = q_R^* \equiv u'^{-1}\left(\frac{\gamma}{\beta}\right)$. Substituting $q = q_R^*$ into (4), we obtain

$$V^g(0) = \frac{1}{1-\beta}\left\{-\frac{\gamma}{\beta}q_R^* - k_{\min} + u(q_R^*)\right\}. \tag{22}$$

For this to be an equilibrium, the incentive constraint (5) should not bind. Substituting (20) and (22) into (5), we obtain

$$\begin{aligned}\Phi(q_R^*) &\equiv -\frac{\gamma + 1 - \beta(1-\rho)}{\beta}q_R^* + u(q_R^*) \\ &\geq -\frac{\gamma}{\beta}\widehat{q}_{N_c}(\delta) + \delta^{N_c} u\left(\widehat{q}_{N_c}(\delta)\right) \equiv \Omega(\delta),\end{aligned} \tag{23}$$

as the non-binding incentive constraint (5). Note that $\Omega(\delta)$ in (23) increases with δ. Because $\Omega(\delta) \geq 0$, if $\Phi(q_R^*) < 0$, (23) cannot be satisfied. On the other hand, if $\Phi(q_R^*) \geq 0$, then for all $\delta \leq \Omega^{-1}(\Phi(q_R^*))$, (23) holds. Define $\widetilde{\delta}_1$ as described in (12). Then, if $\beta^{1/\overline{N}} \leq \widetilde{\delta}_1$, the incentive constraint (5) does not bind for all $\delta \in [\beta^{1/\overline{N}}, \widetilde{\delta}_1]$ and the no threat of double spending equilibrium exists. If $\beta^{1/\overline{N}} > \widetilde{\delta}_1$, then the no threat of double spending equilibrium cannot exist.

Case 2 In the threat of double spending equilibrium, the incentive constraint (5) binds with $\lambda > 0$ in (21). Thus, it must be $q < q_R^*$ by (21). Substituting (4) and (20) into the binding incentive constraint (5), we obtain

$$\begin{aligned} \Phi(q) &\equiv -\frac{\gamma + 1 - \beta(1-\rho)}{\beta} q + u(q) \\ &= -\frac{\gamma}{\beta} \widehat{q}_{N_c}(\delta) + \delta^{N_c} u\left(\widehat{q}_{N_c}(\delta)\right) \equiv \Omega(\delta), \end{aligned} \tag{24}$$

which determines the quantity of goods, q, traded given δ. Note that the left-hand side of (24) is maximized with $q = q_R^{**}$ where q_R^{**} is defined in (9). Thus, if $\Phi(q_R^{**}) < \Omega(\delta)$, no solution to (24) exists. Define $\widetilde{\delta}_2$ as described in (13). Because $\Omega(\delta)$ increases with δ, the necessary condition for the threat of double spending equilibrium to exist is $\delta \leq \widetilde{\delta}_2$. Given $\delta \leq \widetilde{\delta}_2$, i.e., $\Omega(\delta) \leq \Phi(q_R^{**})$, two solutions to equation (24) generally exist: one that is higher than q_R^{**} and another that is lower than q_R^{**}. However, the solution to (24) that is lower than q_R^{**} does not maximize the objective function (4) in the buyer's problem. Thus, the solution to (24) 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 (24) that is higher than q_R^{**}. Next, the binding incentive constraint (5) requires $\widehat{q}_R(\delta) < q_R^*$ to satisfy (21) 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 $\delta \to \Omega^{-1}(\Phi(q_R^*))$. Thus, it must be $\delta > \Omega^{-1}(\Phi(q_R^*))$ to obtain the binding incentive constraint (5). 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 (12) and (13), respectively. However, δ cannot be lower than $\beta^{1/\overline{N}}$. Thus, if $\widetilde{\delta}_1 \geq \beta^{1/\overline{N}}$, then the threat of double spending equilibrium exists for all $\delta \in (\widetilde{\delta}_1, \widetilde{\delta}_2]$. Next, if $\widetilde{\delta}_1 < \beta^{1/\overline{N}} \leq \widetilde{\delta}_2$, then the threat of double

equilibrium exists for $\delta \in [\beta^{1/N}, \widetilde{\delta}_2]$. Finally, if $\widetilde{\delta}_2 < \beta^{1/N}$, then the threat of double spending equilibrium cannot exist.

Case 3 In the delivery lag equilibrium, sellers deliver goods after receiving N_c number of confirmations in the blockchain, and hence $q = \widehat{q}_{N_c}(\delta) \equiv u'^{-1}\left(\frac{\gamma}{\delta^{N_c}\beta}\right)$. 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 (5) can be satisfied otherwise. Thus, the delivery lag equilibrium exists for all $\delta \in (\widetilde{\delta}_2, \overline{\delta}]$ if $\widetilde{\delta}_2 \geq \beta^{1/N}$, and for all $\delta \in [\beta^{1/N}, \overline{\delta}]$ if $\widetilde{\delta}_2 < \beta^{1/N}$. Note that a wallet's good reputation does not have its own value in the delivery lag equilibrium, and hence $V^g(m) = V^n(m)$, and the incentive constraint (5) does not hold.

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

Proof of lemma 2. Suppose that $N = 0$. Then, welfare is maximized when $q = u'^{-1}(\gamma) > q_R^*$. 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 a delivery lag occurs in the *DM*, i.e., $N = N^c$, welfare is maximized at $q = u'^{-1}\left(\frac{\gamma}{\delta^{N_c}}\right) > \widehat{q}_N(\delta)$. Thus, in the delivery lag equilibrium, welfare increases in the trade volume q. Combined together, welfare given by (17) 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 $(\gamma, \rho, k_{\min})$ 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 $(\gamma, \rho, k_{\min})$. Thus, if $\beta^{1/N} \leq \widetilde{\delta}_1$, then the optimal level of δ is given as $\delta^* \in [\beta^{1/N}, \widetilde{\delta}_1]$, because the economy is in the no threat of double spending equilibrium for $\delta \in [\beta^{1/N}, \widetilde{\delta}_1]$.

Next, suppose that $\widetilde{\delta}_1 < \beta^{1/\overline{N}}$, the no threat of double spending equilibrium is therefore not feasible. First, if $\widetilde{\delta}_1 < \beta^{1/\overline{N}} \leq \overline{\delta} < \widetilde{\delta}_2$, the threat of double spending equilibrium exists for any level of δ. In this case, welfare decreases with δ, and minimizing δ as $\delta^* = \beta^{1/\overline{N}}$ is therefore optimal. Second, when $\widetilde{\delta}_1 < \beta^{1/\overline{N}} \leq \widetilde{\delta}_2 \leq \overline{\delta}$, the threat of double spending equilibrium exists for $\delta \in [\beta^{1/\overline{N}}, \widetilde{\delta}_2]$ 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 $\delta = \beta^{1/\overline{N}}$, which gives $W|_{\delta=\beta^{1/\overline{N}}} = u(\widehat{q}_R(\beta^{1/\overline{N}})) - \gamma\widehat{q}_R(\beta^{1/\overline{N}}) - \beta k_{\min}$ 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 $W|_{\delta=\overline{\delta}} = \overline{\delta}^{\overline{N}} u(\widehat{q}_{N_c}(\overline{\delta})) - \gamma\widehat{q}_{N_c}(\overline{\delta}) - \beta k_{\min}$. Thus, if $W|_{\delta=\beta} \geq W|_{\delta=\overline{\delta}}$, then $\delta^* = \beta^{1/\overline{N}}$, and $\delta^* = \overline{\delta}$ otherwise.

Finally, if $\widetilde{\delta}_2 < \beta^{1/\overline{N}}$, the only feasible equilibrium is the delivery lag equilibrium, and setting $\delta = \overline{\delta}$ is optimal to minimize welfare loss from delivery lags. ■

Proof of proposition 6. The result that q_n and k_n decrease with n is straightforward from (18) and (19). Thus, we focus on the proof of the second part. Substituting the functional form $u(q) = \frac{(q+\xi)^{1-\alpha} - \xi^{1-\alpha}}{1-\alpha}$ into (18) and (19), we obtain

$$\begin{aligned}
\frac{k_n}{q_n} &= \frac{k_{\min}}{\left(\frac{\delta^{n+N_c-1}\beta}{\gamma}\right)^{\frac{1}{\alpha}} - \xi} - \frac{\gamma}{\beta} + \frac{\delta^{n+N_c-1}}{1-\alpha} \frac{\left(\frac{\delta^{n+N_c-1}\beta}{\gamma}\right)^{\frac{1-\alpha}{\alpha}} - \xi^{1-\alpha}}{\left(\frac{\delta^{n+N_c-1}\beta}{\gamma}\right)^{\frac{1}{\alpha}} - \xi} \\
&\quad + \frac{\gamma}{\beta} \frac{\left(\frac{\delta^{\overline{N}}\beta}{\gamma}\right)^{\frac{1}{\alpha}} - \xi}{\left(\frac{\delta^{n+N_c-1}\beta}{\gamma}\right)^{\frac{1}{\alpha}} - \xi} - \frac{\delta^{\overline{N}}}{1-\alpha} \frac{\left(\frac{\delta^{\overline{N}}\beta}{\gamma}\right)^{\frac{1-\alpha}{\alpha}} - \xi^{1-\alpha}}{\left(\frac{\delta^{n+N_c-1}\beta}{\gamma}\right)^{\frac{1}{\alpha}} - \xi}. \\
&\approx \left\{ k_{\min} \left(\frac{\gamma}{\beta}\right)^{\frac{1}{\alpha}} + \frac{\alpha\gamma}{(\alpha-1)\beta} \delta^{\frac{\overline{N}}{\alpha}} \right\} \left(\frac{1}{\delta}\right)^{\frac{n+N_c-1}{\alpha}} - \frac{\alpha\gamma}{(\alpha-1)\beta}
\end{aligned}$$

where we use $\xi \approx 0$ to obtain the second equation. Then, because $\delta < 1$, $\frac{k_n}{q_n}$ increases with n. ■