Cryptocurrency, Imperfect Information, and Fraud

Li, Yiting and Wang, Chien-Chiang

National Taiwan University, National Taiwan University

May 2019

Cryptocurrency, Imperfect Information, and Fraud

Yiting Li[†]
National Taiwan University

Chien-Chiang Wang[‡][§]
National Taiwan University

Abstract

We study cryptocurrency in a monetary economy with imperfect information. The network imperfection provides traders opportunities to engage in double spending fraud, but the trackability of transaction messages allows us to impose proof-of-work (PoW), proof-of-stake (PoS), and currency exclusion to mitigate fraud incentives. However, PoW consumes energy, and PoS requires extra cryptocurrency to be held as deposits, so deterring fraud may not be optimal. We find that forks can serve as signals to detect double spending fraud and to trigger punishments. If the probability is high that forks appear under double spending, imposing PoW and PoS to deter fraud is optimal; otherwise, it is optimal to save the cost but allow for double spending. Finally, by endogenizing the incentives to double spend and the size of PoW and PoS, we show that cryptocurrency economy can achieve efficient allocation as the imperfectness of the internet is sufficiently low.

Keywords: cryptocurrency, money, search, imperfect information, fraud

JEL classification: E40, D80, G10

[†] Department of Economics, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan. E-mail: yitingli@ntu.edu.tw.

[‡] Corresponding author. Department of Economics, National Taiwan University, No. 1, Sec. 4, Roosevelt Rd., Taipei 10617, Taiwan. E-mail: chienwang@ntu.edu.tw.

[§] We thank David Andolfatto, Jonathan Chiu, Bill Dupor, Christopher Waller, Steve Williamson, participants in the 2018 Summer Workshop on Money, Banking, Payments and Finance at St. Louis Fed and 2019 NTU-GRIPS joint workshop for helpful comments.

1 Introduction

Cryptocurrency is a relatively new means of payment based on electronic systems that maintain a public transaction ledger in a distributed manner. Everyone can have his or her own copy of the public ledger, and there is no central authority placing control or restrictions on the right to manage, store, or distribute the ledger. People can freely create an account and participate in the system, and payers update the public ledger by sending transaction messages to other participants through peer-to-peer networks. These features impart many properties into cryptocurrency that do not exist in traditional payment methods. For example, the value of cryptocurrency is exempted from the risk and control of a central authority. Moreover, traders and record makers are anonymous, which, together with the feature of electronic transfers, positions cryptocurrency as a favorable payment method in the black market and a way to circumnavigate international sanctions.[1] These properties do not come without a cost, however. In Bitcoin, the very first and the most successful cryptocurrency, a record maker (referred to as a miner) is required to solve a hash problem, called proof-of-work (PoW), that is intrinsically meaningless but consumes a substantial amount of time and computing power. In Ethereum, the second most popular cryptocurrency, proof-of-stake (PoS) is proposed in addition to PoW, which requires record makers to deposit a massive amount of cryptocurrency in order to update the public ledger. Why do cryptocurrencies require PoW and PoS? How does the use of PoW and PoS influence the liquidity of a cryptocurrency? Under what circumstances can cryptocurrency serve as an efficient payment system?

This paper aims to answer these questions. We argue that the imperfectness of networks provides traders opportunities for fraud and that PoW and PoS can mitigate traders' incentives to engage in fraud and improve the efficiency of cryptocurrency. Cryptocurrency operates in a network with uncertainty, missing information, and delays. Through this imperfect network, there is no guarantee that all participants receive the transaction messages or that participants receive the messages in the same order, and thus cryptocurrency relies on consensus algorithms to achieve agreement among participants regarding the order of

[1] For example, Bitcoin enthusiasm in Sudan is driven by U.S. sanctions imposed on the country (see "Bitcoin is a hit in countries where locals face currency troubles," Stevis-Gridneff, M. and Kantchev, G., Jan 4, 2018, *The Wall Street Journal.*)

sent messages.[2] This imperfection provides traders with opportunities for “double spending fraud”: an attacker can send an initial message making a payment to a merchant, receive the purchased good or service, and then send another message—the double spending message—that transfers the currency to another account, either one owned by the attacker herself or one owned by another merchant. The double spending message and the original message conflict with each other, and there is a chance that the double spending message, instead of the original one, is confirmed by the consensus algorithm. If this occurs, the original merchant will not receive the payment for its products.[3]

We study cryptocurrency in a monetary search model based on Lagos and Wright (2005) with heterogeneous agents similarly to Rocheteau and Wright (2005). In the model, buyers and sellers meet bilaterally in a decentralized market. Traders are anonymous, and there is no commitment, so unsecured credit is not feasible. There is no fiat money or physical assets that can be used as a means of payment. However, there is a cryptocurrency system that allows traders to make payments by sending transaction messages to all other agents through a consensus algorithm. If a message is confirmed by the consensus algorithm, the message will be observable by all agents, and if only the original message is sent, there is no doubt that the message will be confirmed by the consensus algorithm. However, if both the original and the double spending message are sent, one of the following three results will occur. One, the double spending message rather than the original message is confirmed by the consensus algorithm; we call this a “false agreement.” Two, only the original message is confirmed by the algorithm, and the double spending message is not; we call this a “correct agreement.” Three, both messages are confirmed by the algorithm; we call this a “fork.”[4] We capture the imperfectness of the network by the probabilities that the above agreements occur under double spending attacks. If the network is perfect, the receipt of the messages

[2] For example, in Bitcoin, blockchain and mining competition are applied to achieve consensus among record makers (miners).

[3] The imperfect message sending we consider in cryptocurrency is also related to imperfect memory or monitoring. See Kocherlakota and Wallace (1998) and Kocherlakota (1998).

[4] Forks can be categorized as “malicious forks” and "natural forks." Malicious forks are caused by double spending attacks, and transaction messages in malicious forks must conflict with each other. A natural fork is a natural result in cryptocurrency systems with blockchains such as Bitcoin and Ethereum and occurs if two or more miners simultaneous append the new blocks into the blockchain. In a natural fork, messages do not conflict with each other in general, and a natural fork is not a consequence of double spending fraud. The forks we discuss in this paper refer to malicious forks.

will be immediate and guaranteed, and a double spending message will have no chance of being misidentified as the original one. The consensus algorithm thus will deliver a correct agreement regardless of whether the buyer double spends, and cryptocurrency is equivalent to a perfect message sending system and can support the social optimal allocation.

If the network is not perfect, then double spending, like credit default, may raise sellers' concerns about not receiving the payment and will decrease their willingness to trade. When one defaults on credit, there is a record attached to one's name, allowing for appropriate consequences to be enacted. Traders in cryptocurrency systems, however, preserve anonymity, so agents who double spend cannot be punished by, for example, excluding them from the market. The properties of digital payments prompt the system to impose multiple unconventional methods in order to mitigate the incentives of double spending and to safeguard against fraudulent transactions. First, we can require each message to be attached with a PoW; attaching PoW is costly, and in our model, we capture the cost by assuming that PoW generates disutility to the message sender. Second, even though traders using cryptocurrency are anonymous, transaction messages are trackable; thus, if double spending is observed, we can exclude the cryptocurrency transferred in the message from future circulations, thereby decreasing the attackers' gain from double spending. Third, we can ask message senders to attach a cryptocurrency deposit to the message, in other words, a PoS, and the deposit can be forfeited if double spending is observed. If the expected gain of conducting double spending is smaller than its cost, the buyer will have no incentive to engage in fraud.

Our results show that applying PoW and PoS to deter double spending is not always social optimal. PoW generates a loss to social welfare because the original message is also required to attach PoW. PoS, although not directly generating a loss, requires extra cryptocurrency to be held as deposits, and the held deposits cannot be used for transactions. If, from society's viewpoint, preventing double spending by imposing PoW or PoS is too costly, saving the cost and allowing for double spending can be socially desirable.[5] We take a mechanism design approach to investigate the optimal cryptocurrency system, taking as given the characteristics of the consensus algorithm—the probabilities of a correct agreement,

[5] In reality, we also observe that double spending attacks happen from time to time in some cryptocurrencies (e.g., Bitcoin Gold, Verge, Monacoin, etc. See "Cryptocurrency Attacks are Rising," Kharif, O., May 30, 2018, *Blooomberg.)*

a false agreement, and a fork when double spending fraud is attempted. We construct two forms of mechanisms as candidates for optimal mechanisms. The first is honest mechanisms, in which PoW and PoS are set only high enough to prevent fraud, and thus buyers do not double spend. The second is double spending mechanisms, in which no PoW or PoS is imposed, and traders find it optimal to double spend in equilibrium. We show that any equilibrium is dominated in terms of social welfare by an equilibrium generated by an honest mechanism or by a double spending mechanism, so the following questions remain: How do the characteristics of a consensus algorithm influence welfare generated by both mechanisms? Under what circumstance do honest mechanisms yield higher welfare over double spending mechanisms, and vice versa?

Although both forks and false agreements are caused by network imperfections, they influence the efficiency of cryptocurrency in different ways. In an honest mechanism, a correct agreement is the only agreement that occurs in equilibrium, and a false agreement and a fork would occur only if the buyer had deviated to double spend. However, because other agents cannot tell that a message is an original message or a double spending one, a false agreement is not distinguishable from a correct agreement; therefore, only forks can serve as signals for deviations and be used to trigger off-equilibrium punishments. When a fork occurs, the cryptocurrency transferred in the message is excluded from circulation; attackers' payoffs from forks are thus eliminated, and the sizes of PoW and PoS can be set just high enough to offset their payoffs from false agreements. As the probability of false agreements becomes sufficiently small, the cost of preventing fraud will be substantially reduced, and honest mechanisms can then support the social optimal allocation.

Forks are also applied to trigger the forfeiting of PoS deposits, and therefore the amount of PoS deposits required to prevent fraud could be lower if the probability that forks occur is higher. The cost of PoW, however, materializes at the moment it is attached to a transaction, regardless of whether a fork occurs. Thus, if the probability that a fork occurs is sufficiently high, PoS will be more efficient than PoW in preventing double spending. For the same reason, the social welfare of equilibria generated by honest mechanisms also increases with the probability of forks.

In double spending mechanisms, however, an increase in the probability of forks may result in a decrease in social welfare. The reason is as follows. In this mechanism, buyers double spend in equilibrium, so if the probability that forks occur under double spending attacks increases and crowds out the frequency of correct agreements, this crowding will decrease the seller's payoff and in turn decrease the quantity of transactions in the bilateral meeting. As a consequence, when forks occur sufficiently frequently and crowd out the probability of correct agreements, honest mechanisms can generate greater social welfare than that generated by double spending mechanisms, which means that we should apply PoW and PoS to deter double spending. If forks rarely occur, however, then mechanisms that allow for double spending but save the cost of PoW and PoS would generate greater social welfare than mechanisms that utilize them to prevent double spending fraud.

1.1 Literature Review

Nakamoto (2008) developed Bitcoin, in which PoW and blockchain purport to solve the double spending problem. In the computer science literature, Bitcoin has been studied in an environment where the number of honest and malicious players is taken as given;[6] however, traders' incentives to be honest or malicious are not considered. In the literature on monetary economics, Chiu and Koeppl (2017) studies the incentive problem in Bitcoin under a monetary-search framework, and Bitcoin is an inefficient means of payment in their model due to the resource-intensive competition for updating the blockchain. In our model, the opportunity for double spending originates from the network imperfection, and through endogenizing PoW and PoS to mitigate the incentive to double spend, we can show that efficient allocation is achievable when the imperfection of the internet is sufficiently low.

Different from others who examine cryptocurrency, we do not model blockchain and mining competitions. The reason is that blockchains and mining competitions are not universal features among cryptocurrencies, and the optimal strategies of traders and record makers in different consensus algorithms and environments can be different.[7] Our abstraction on the consensus algorithm minimizes the details in the formation of consensus, which allows us to

[6] See, for example, Garay, Kiayias, and Leonardos (2015) and Pass, Seeman, and Shelat (2016).

[7] For example, in IOTA, there is no blockchain and mining competition. Instead, payers do PoW themselves, and the structure of its public ledger is a directed acyclic graph (DAG) named Tangle.

focus on how the characteristics of a consensus algorithm influence the optimal design and efficiency of cryptocurrency.

The present paper is also closely related to the literature on counterfeiting and asymmetric information including Li, Rocheteau, and Weill (2012) and Cavalcanti and Nosal (2011). Although Li, Rocheteau, and Weill (2012) show that no counterfeiting is an equilibrium result, both our paper and Cavalcanti and Nosal (2011) conclude that eliminating fraud may not always be social optimal.

The rest of the paper is organized as follows. Section 2 sets up the environment. Section 3 discusses the optimal mechanism in the monetary equilibrium. Section 4 concludes.

2 The Environment

The model follows the monetary-search framework of Lagos and Wright (2005) with heterogeneity among economic agents similar to Rocheteau and Wright (2005). Time is indexed by $t = 0, 1, 2, ...$, and in each period, there are two subperiods—the decentralized market (DM) and the subsequent centralized market (CM). There is a large number of agents initially outside the economy. Half of the agents are buyers, and half of the agents are sellers. At the beginning of each CM, mass one of buyers enters the economy and leaves at the end of the next CM; mass one of sellers enters the economy at the beginning of each DM and leaves at the end of the CM of the same period. If an agent leaves the economy, she will never enter again. The assumptions of new entrants and short-lived agent are made to capture the openness feature of cryptocurrency—people can freely create an account and participate in the system with no restrictions—and the anonymity of digital accounts, which will be discussed in detail later. Buyers in the economy consume in the DM and consume and produce in the CM. Sellers in the economy produce in the DM and consume and produce in the CM. In either the DM or the CM, one unit of labor input produces one unit of perishable consumption goods.

An individual buyer who enters the economy at period t CM has preferences given by

$$E_t \left\{ X_t + \beta \left[u(x_{t+1}) + X'_{t+1} \right] \right\},$$

where $X_t, X'_{t+1} \in (-\infty, \infty)$ is the net consumption in the CM, and $x_t > 0$ is consumption in the DM. We assume that $u(\cdot)$ is twice differentiable and $u(0) = 0$, $u'(x) > 0$, $u''(x) < 0$ and $\lim_{x \to 0} u'(x) = \infty$, and $0 < \beta < 1$ is the buyer's discount factor across periods. An individual seller who enters the economy at period t DM has preferences given by

$$E_t \left\{ -l_t + H_t \right\},$$

where $H_t \in (-\infty, \infty)$ is net consumption in the CM, and $l_t > 0$ is labor input in the DM.

There are random matches in the DM: each buyer is matched with a seller. All matches are anonymous, and there is no enforcement or commitment. Thus, a means of payment is essential for the DM trade. There are no physical assets such as fiat money or Lucas trees, but there is a cryptocurrency system. A cryptocurrency system consists of a set of digital addresses and a consensus algorithm, and agents can freely create multiple digital accounts on the digital addresses. Agents in the economy can transfer cryptocurrency by sending transaction messages to all other agents through the consensus algorithm. A transaction message includes the sender's and receiver's digital accounts and the amount of currency transferred. The consensus outcome consists of a subset of all messages sent by agents in the current DM, and if a message is included in the consensus outcome, we say that the message is "confirmed" by the consensus algorithm. The consensus outcome is observable by all agents, whether the agent is inside or outside the economy. In this system of message sending, the history of consensus outcomes—the public ledger—does not require a centralized authority to manage or maintain, but an agent can infer the public ledger and the balance of an account on the ledger by tracking the consensus outcomes she previously observed.

There are two stages in the DM. The first is a trading stage, in which the buyer in a meeting makes a take-it-or-leave-it offer to the seller: the buyer asks for x_t units of DM goods in exchange for transferring Z_t units of cryptocurrency. The seller can accept or reject the offer. If the seller accepts the offer, then she transfers x_t units of DM goods to the buyer, and the buyer sends a transaction message to the consensus algorithm to transfer Z_t units of cryptocurrency to the seller. If the seller rejects the offer, then nothing further happens, and the pair separates at the end of the trading stage. The property of digital payment allows currency subsidies (or fee charges) to be imposed with the messages in the cryptocurrency system. Let T_t denote the amount of currency subsidized with the transfer by the cryptocurrency system, and T_t can be positive or negative. If a sender sends a transaction message to make Z_t units of transfers, then Z_t units of cryptocurrency will be taken away from the sender's account, and $\hat{Z}_t = Z_t + T_t$ units of cryptocurrency will be added to the receiver's account. Let ϕ_t denote the price of the cryptocurrency in terms of the CM consumption good at time t, and let $1 + \pi_t = \frac{\phi_t}{\phi_{t+1}}$; then π_t denotes the inflation rate of the cryptocurrency. In the discussion hereafter, we use the quantity of assets in real terms. Let z_t and τ_t denote the real quantity of the transfer and subsidy at time t, then

$$\begin{aligned} \tau_t &= \phi_t T_t, \\ z_t &= \phi_t Z_t. \end{aligned}$$

Let $\hat{z}_t$ denote the amount of transfer that the receiver receives; then $\hat{z}_t = z_t + \tau_t$.

The second stage is a settlement stage, and the outcome of the consensus algorithm is realized at the end of this stage. In the settlement stage, before the consensus outcome is realized, a buyer can send a second message that transfers the cryptocurrency to another account owned by herself. Because agents are short-lived and new entrants constantly flow into the economy, the anonymity of accounts can be preserved; that is, people cannot distinguish whether a newly created account is owned by a seller or by a buyer who intends to double spend. Thus, the message that makes transfer to the buyer's another account is not distinguishable from the first message sent; this anonymity provides the buyer with opportunities to conduct double spending fraud.[8]

Note that sending a second message does not necessarily imply that the buyer double spends. Double spending occurs if and only if, first, the two messages make transfers from the same account, and, second, the account balance is not sufficient to fulfill both payments.

[8] Suppose that we consider the standard Lagos and Wright (2005) framework with a fixed set of infinitely lived agents. There can then exist an equilibrium in which agents are honest and each of them uses only one account to trade. Thus, given that there is a fixed pool of digital accounts being used for transactions, if an attacker intends to deviate to double spend and creates a new account, the newly created account will be identified, and double spending can be easily detected; PoW and PoS thus will not be needed to prevent fraud. In actuality, however, double spending cannot be detected so easily because new traders enter the system often and new accounts are constantly created.

To simplify the analysis, we confine our attention to the cases in which the buyer sends the second message with the purpose of engaging in double spending fraud, and we make the following assumptions. First, the first and the second messages sent in the DM must make transfers from the same account. Second, the transfer made by a message sent in the DM must draw the total balance in that account. Under these assumptions, sending a second message in the settlement stage is equivalent to double spending, and the buyer's post-trade decision becomes binary: to engage in double spending fraud or not. Hereafter, we call the message sent in the trading stage the "original message" and the message sent in the settlement stage the "double spending message."[9]

The consensus algorithm works as follows. In a DM meeting, if only the original message is sent (i.e. the buyer is honest), the message will always be confirmed by the consensus algorithm (see Figure 1 for an illustration). If both the original and the double spending messages are sent, one of the following will occur. 1) a correct agreement: only the original message is confirmed by the consensus algorithm; 2) a false agreement: only the double spending message is confirmed by the consensus algorithm; 3) a fork: both messages are confirmed by the consensus algorithm (see Figure 2 for an illustration). Let $R \equiv (r_s, r_b, r_{sb})$ denote the probabilities that the consensus algorithm delivers a correct agreement, a false agreement, and a fork under the double spending attack, respectively, and $r_s + r_b + r_{sb} = 1$. We assume that R is exogenously given by the technology, and we make the following assumptions:

Assumption 1. $r_s > 0, r_b > 0, r_{sb} > 0$

Assumption 2. $r_s > r_b$

Assumption 1 captures the fact that the network is not perfect in the DM, so conducting double spending fraud always has a chance to generate a fork or a false agreement. Assumption 2 captures the property that the double spending message must be sent in the settlement stage, after the original message was sent, a situation which gives the original message the advantage of being confirmed by the consensus algorithm.[10] We say that an agreement is a

[9] Because in the current model the buyer can meet only one merchant in the DM, we do not consider the case where the buyer sends the double spending message to make transfers to other merchants to purchase goods.

[10] In general, an agent may also send a message to transfer cryptocurrencies to herself during or before the trade. However, by doing so, the message may be detected by the seller and decrease the seller's willingness

single agreement if it is a correct or false agreement. Because other agents cannot tell that a message is an original message or a double spending one, if the consensus outcome delivers a single agreement, they cannot tell whether the agreement is a correct agreement or a false agreement; they can only observe that the agreement is a single agreement or a fork.

Note that a buyer can also send a message, either in the trading or the settlement stage, to make a transfer to herself without making a transfer to the seller in advance, and we call this "internal transfers." A buyer may have an incentive to conduct internal transfers in order to, for example, obtain a subsidy from the system. For simplicity, we exclude internal transfers from the benchmark model by assuming that buyers cannot send a message to transfer currencies to herself without transferring to the seller in advance. We incorporate internal transfers into the model in the supplementary appendix and show that the main implications of the present model still hold.[11]

Because consensus outcomes are observable by all agents, agents can recognize or reject the receipt of a transfer conditional on whether the agreement is a single agreement or a fork. If a transfer is recognized, the amount transferred is added to the receiver's account; if a transfer is rejected, that transfer is not added to any account and is equivalent to being deleted. We assume that there are public signaling devices, such as sunspots, allowing agents to coordinate regarding whether the currency in a transaction message is added to the receiver's account.[12] Because the amount transferred in a transaction message is also observable by all agents, the probability that a transfer is recognized can also be conditional on the amount transferred, $\hat{z}$.[13] Let $p_1(\hat{z}_t)$ denote the probability that the transfer is added

to produce. (See Li, Rocheteau, and Weill, 2012 for a model in which people commit fraudulent payment before they trade.) In Bitcoin transfers, sellers can wait for a period of time before they deliver the goods to ensure that the buyer does not cheat, and this strategy is called "delay delivery" (See Chiu and Koeppl, 2017). In this paper, we do not endogenize delay delivery but make assumptions on the timing of sending messages instead.

[11] In the supplementary appendix, we allow buyers to conduct internal transfers. Internal transfers cannot be equilibrium strategies, but will result in a more constrained cryptocurrency mechanism because the mechanism has to deter the buyer's incentive to conduct internal transfer.

[12] The use of lotteries or sunspots to determine the allocation of indivisible liquidity is applied in Berentsen, Molico, and Wright (2002). As described in Shell and Wright (1993), a sunspot has an advantage in serving as a coordination device.

[13] In Bitcoin and Ethereum, the balance of an account and the amount of transfer made in a message are observable by the public; moreover, a transaction that moves a large amount will attract traders' attention. See, for example, "The Bitcoin Whales: 1,000 People Who Own 40 Percent of the Market," Kharif, O., Dec 8, 2017, *Bloomberg.*

to the receiver's account when the transfer is $\hat{z}$ and if the consensus algorithm delivers a single agreement; if the consensus algorithm delivers a fork, we denote it by $p_2(\hat{z}_t)$. In the supplementary appendix, we consider a more restrictive cryptocurrency system in which the receipt of the transfer cannot be conditional on the amount of currency transferred, and we show that the main results still hold.

We assume that the network is perfect in the CM: the transaction messages can be received immediately by all participants. Thus, a consensus algorithm is not required in the CM, and there are no double spending problems. Moreover, we assume that there is no transaction subsidy in the CM.

To prevent double spending, a cryptocurrency system can require PoW be attached to a message. PoW costs the message sender k units of disutility. If k is greater than the gain from double spending, the buyer will have no incentive to commit fraud. We assume that only the buyer can provide PoW and therefore it is the buyer who bears the disutility k.[14] The second way to increase the cost of double spending is to require PoS, in which a message must be attached with δ units of cryptocurrency as a deposit. The PoS deposit cannot be used as payment in the DM trade. The return of the deposit occurs after the consensus outcome is delivered and can also be conditional on the type of agreements and the amount transferred. We denote $q_1(\hat{z}_t)$ and $q_2(\hat{z}_t)$ the probabilities of returning the deposit in a single agreement and a fork, respectively. If a deposit is not returned, it is equivalent to being deleted from the cryptocurrency system.

2.1 The Trading Game and The Buyer's Problem

Agents in the economy take as given the inflation rate π_t, transaction subsidy, τ_t, PoW, k, PoS, δ, and the probabilities $P(\hat{z}_t) = (p_1(\hat{z}_t), p_2(\hat{z}_t))$ and $Q(\hat{z}_t) = (q_1(\hat{z}_t), q_2(\hat{z}_t))$. We analyze the transaction between the buyer and the seller in the DM as an extensive form game. The time line of the game is as follows.

1. CM: the buyer purchases cryptocurrency in the CM.

[14] We can also assume that the seller can provide PoW. In this case, the buyer must pay more currency to compensate for the seller's cost, and this increases the trading cost. Thus, the efficient bargaining outcome will be that the buyer provides PoW, and we make the assumption in order to simplify the analysis.

2. DM: there are two stages:
   - trading stage: the buyer makes an offer to the seller. The seller decides to accept or reject the offer.
   - settlement stage: the buyer decides whether or not to send a double spending message.

The game tree in the DM is demonstrated in Figure 3, and the consensus algorithm serves as Nature to randomly assign an agreement.

A seller (or a buyer) receives the transfer if, first, the message that makes the transfer to the seller (or the buyer) is confirmed by the consensus algorithm, and, second, the receipt of the transfer is recognized by all agents. If the buyer is honest, the consensus algorithm will deliver a correct agreement with probability one. Thus, the probability that the seller receives the transfer is $p_1(\hat{z}_t)$, and the probability that the buyer receives the transfer is zero. If the buyer double spends, the seller receives the payment only if the agreement is a correct agreement (with probability r_s) or a fork (with probability r_{sb}), and the respective probabilities that the seller receives the payment in a correct agreement and a fork are $p_1(\hat{z}_t)$ and $p_2(\hat{z}_t)$; the buyer receives the payment only if the consensus algorithm delivers a false agreement (with probability r_b) or a fork (with probability r_{sb}), and the respective probabilities that the buyer receives the payment in a false agreement and a fork are $p_1(\hat{z}_t)$ and $p_2(\hat{z}_t)$. Let $\alpha_i(\hat{z}_t)$ and $\theta_i(\hat{z}_t)$ denote the probability that the seller and the buyer receive the currency transferred given that the buyer is honest ($i = h$), or engages in double spending ($i = d$). Then according to the above discussion,

$$\begin{aligned}
\alpha_h(\hat{z}_t) &= p_1(\hat{z}_t), \\
\theta_h(\hat{z}_t) &= 0, \\
\alpha_d(\hat{z}_t) &= p_1(\hat{z}_t)r_s + p_2(\hat{z}_t)r_{sb}, \\
\theta_d(\hat{z}_t) &= p_1(\hat{z}_t)r_b + p_2(\hat{z}_t)r_{sb}.
\end{aligned} \tag{1}$$

Now we turn to the probabilities that the buyer receives the deposit that she attached to a message. If the buyer is honest, the consensus system delivers a single agreement with probability one, and the buyer receives the deposit back with probability $q_1(\hat{z}_t)$. If the buyer double spends, the probabilities that the consensus algorithm delivers a single agreement and a fork are $r_s + r_b$ and r_{sb}, respectively, and the corresponding probabilities that the buyer receives the deposit in a single agreement and a fork are $q_1(\hat{z}_t)$ and $q_2(\hat{z}_t)$. Let $\eta_i(\hat{z}_t)$ denote the probability that the buyer receives the deposit; then

$$\begin{aligned} &\eta_h(\hat{z}_t) = q_1(\hat{z}_t), \\ &\eta_d(\hat{z}_t) = q_1(\hat{z}_t)(r_s + r_b) + q_2(\hat{z}_t)r_{sb}. \end{aligned} \tag{2}$$

In the post-trade stage, the buyer decides to be honest or to engage in double spending. Let $\varphi_h(\hat{z}_t)$ and $\varphi_d(\hat{z}_t)$ denote the buyer's post-trade gain for the honest and double spending strategies, respectively. If the buyer is honest, she will take back the deposit δ with probability $\eta_h(\hat{z}_t)$. If the buyer sends the double spending message, she has to incur k units of disutility to solve the hash problem again but will receive the cryptocurrency transferred $\hat{z}$ with probability $\theta_d(\hat{z}_t)$ and will receive the deposit δ with probability $\eta_h(\hat{z}_t)$. Thus,

$$\begin{aligned} &\varphi_h(\hat{z}_t) = \eta_h(\hat{z}_t)\delta \\ &\varphi_d(\hat{z}_t) = \theta_d(\hat{z}_t)\hat{z} + \eta_d(\hat{z}_t)\delta - k. \end{aligned} \tag{3}$$

We also consider the mixed strategy: let σ_t denote the buyer's strategy on the probability of being honest and $1 - \sigma_t$ the probability of double spending; then the buyer's post-trade gain is

$$\varphi(\hat{z}_t, \sigma_t) = \sigma_t \varphi_h(\hat{z}_t) + (1 - \sigma_t)\varphi_d(\hat{z}_t). \tag{4}$$

The buyer chooses her strategy by comparing $\varphi_h(\hat{z}_t)$ and $\varphi_d(\hat{z}_t)$. If $\varphi_h(\hat{z}_t) > \varphi_d(\hat{z}_t)$, the buyer will be honest ($\sigma_t = 1$); if $\varphi_h(\hat{z}_t) < \varphi_d(\hat{z}_t)$, the buyer will double spend; if $\varphi_h(\hat{z}_t) = \varphi_d(\hat{z}_t)$, the buyer will be indifferent about being honest or double spending, so she can use a mixed strategy ($\sigma_t \in [0, 1]$). Let $B(\hat{z}_t)$ denote the best response correspondence of the buyers after trade; then

$$B(\hat{z}_t) = \begin{cases} 1 & \text{if } \theta_d(\hat{z}_t)\hat{z}_t < k + [\eta_h(\hat{z}_t) - \eta_d(\hat{z}_t)]\,\delta \\ [0, 1] & \text{if } \theta_d(\hat{z}_t)\hat{z}_t = k + [\eta_h(\hat{z}_t) - \eta_d(\hat{z}_t)]\,\delta \\ 0 & \text{if } \theta_d(\hat{z}_t)\hat{z}_t > k + [\eta_h(\hat{z}_t) - \eta_d(\hat{z}_t)]\,\delta \end{cases} . \tag{5}$$

Now we turn to the seller's strategy. Given the buyer's transfer, $\hat{z}_t$, and the seller's belief regarding the buyer's post-trade strategy, $\hat{\sigma}_t$, the buyer will set the DM production x_t to make the seller indifferent:

$$x_t = \tilde{x}(\hat{z}_t, \hat{\sigma}_t) \equiv \left[\hat{\sigma}_t \alpha_h(\hat{z}_t) + (1 - \hat{\sigma}_t)\alpha_d(\hat{z}_t)\right] \hat{z}_t. \tag{6}$$

Let $w(z_t, \sigma_t, \hat{\sigma}_t)$ be the buyer's gain in the bilateral meeting, then

$$w(\hat{z}_t, \sigma_t, \hat{\sigma}_t) = -(\hat{z}_t - \tau_t) - \delta - k + u\left[\tilde{x}(\hat{z}_t, \hat{\sigma}_t)\right] + \varphi(\hat{z}_t, \sigma_t),$$

which consists of the cost due to the transfer, $\hat{z}_t - \tau_t$; the PoS deposit, δ; the PoW for the original message, k; the gain from consuming DM goods, $u\left[\tilde{x}(\hat{z}_t, \sigma_t)\right]$; and the post-trade gain, $\varphi(\hat{z}_t, \sigma_t)$. In equilibrium, the buyer's strategy must be rational, so we must have $\sigma_t \in B(\hat{z}_t)$. Moreover, the seller's belief must be consistent with the buyer's strategy; that is, $\sigma_t = \hat{\sigma}_t$, and hence we abuse notations by denoting $w(\hat{z}_t, \sigma_t) \equiv w(\hat{z}_t, \sigma_t, \sigma_t)$ hereafter.

Given the inflation rate π_t, the buyer chooses m_t and $\hat{z}_t$ in the CM to maximize her expected payoff. Note that the DM trade volume x_t depends on the seller's belief on the buyer's post-trade behavior (to double spend or not), and thus the game can have multiple subgame perfect equilibria because the seller's belief can vary. For example, according to (5), if the buyer proposes $\hat{z}_t$ such that $\theta_d(\hat{z}_t)\hat{z}_t = k + \left[\eta_h(\hat{z}_t) - \eta_d(\hat{z}_t)\right]\delta$, then σ_t can be any value between zero and one, so x_t can be equal to $\left[\sigma_t \alpha_h(\hat{z}_t) + (1 - \sigma_t)\alpha_d(\hat{z}_t)\right] \hat{z}_t$ for all $\sigma_t \in [0, 1]$. We thus focus on the Pareto-dominant SPE, that is, the SPE such that there is no other SPE that makes every player at least as well off and at least one player strictly better off in terms of the CM expected value. Because the buyer makes a take-it-or-leave-it offer to the seller, the seller's expected gain must be zero. Thus, the Pareto-dominant SPE is the SPE that maximizes the buyer's expected payoff in the CM:

$$\begin{array}{c} \max_{m_{t-1} \geq 0, \hat{z}_t, \sigma_t \in B(\hat{z}_t)} X_{t-1} + \beta \left\{ \frac{m_{t-1}}{1+\pi_{t-1}} + w(\hat{z}_t, \sigma_t) \right\} \\ \text{subject to} \left\{ \begin{array}{l} m_{t-1} = -X_{t-1} \\ \hat{z}_t - \tau_t + \delta \leq \frac{m_{t-1}}{1+\pi_{t-1}} \end{array} \right. \end{array} . \tag{7}$$

The first constraint in (7) says that the buyer's end-of-period real cryptocurrency balance m_{t-1} is equal to the net production in the CM, $-X_{t-1}$; the second constraint is the budget constraint, in which the real cryptocurrency balance at the beginning of the DM is equal to the balance in the previous CM discounted by the inflation rate, $\frac{m_{t-1}}{1+\pi_{t-1}}$, and the budget can be used as the deposit, δ, and the transfer, $z_t = \hat{z}_t - \tau_t$.

2.2 Monetary Equilibrium

We first consider the money market clearing condition. Let $\bar{m}_t$ denote the real aggregate holdings of cryptocurrency at the end of the DM in period t. Since the aggregate quantity of cryptocurrency does not change from the end of the DM to the end of the CM, $\bar{m}_t$ also denotes the aggregate cryptocurrency holdings at the end of the CM in period t. Then the aggregate cryptocurrency holdings at the beginning of the DM in period t are equal to $\frac{\bar{m}_{t-1}}{1+\pi_{t-1}}$. Nonetheless, the aggregate quantity of cryptocurrency can change within DM transactions as a result of, for example, the buyer's strategy on double spending, σ_t, and the probabilities of receiving the transfer and deposit, $P(\hat{z}_t)$ and $Q(\hat{z}_t)$, a situation that is characterized as follows:

$$\bar{m}_t = \frac{\bar{m}_{t-1}}{1+\pi_{t-1}} - (\hat{z}_t - \tau_t + \delta) + \left\{ \begin{array}{c} [\sigma_t \alpha_h(\hat{z}_t)\hat{z}_t + (1-\sigma_t)\,\alpha_d(\hat{z}_t)\hat{z}_t] \\ +\,[\sigma_t \eta_h(\hat{z}_t)\delta + (1-\sigma_t)\,(\theta_d(\hat{z}_t)\hat{z}_t + \eta_d(\hat{z}_t)\delta)] \end{array} \right\}. \tag{8}$$

Condition (8) says that the total amount of cryptocurrency at the end of the DM, $\bar{m}_t$, is equal to the amount at the beginning of the DM, $\frac{\bar{m}_{t-1}}{1+\pi_{t-1}}$, minus the transfer and PoS deposit that are taken from the buyers' accounts, $\hat{z}_t - \tau_t + \delta_t$, plus the amount of transfer added to the sellers' accounts, $\sigma_t \alpha_h(\hat{z}_t) + (1-\sigma_t)\,\alpha_d(\hat{z}_t)$, and the amount of transfer and deposit return received by buyers, $\sigma_t \eta_h(\hat{z}_t)\delta + (1-\sigma_t)\,(\theta_d(\hat{z}_t)\hat{z}_t + \eta_d(\hat{z}_t)\delta)$. Note that the old buyers and the sellers will leave the economy at the end of the CM, and thus they sell all their cryptocurrency holdings $\bar{m}_t$ in the CM. The new buyers are the only agents who live across periods, and m_t is their cryptocurrency demand. Thus, the CM money market clears if and only if

$$m_t = \bar{m}_t. \tag{9}$$

A necessary condition for the clearing of the CM money market is

$$\frac{1+\pi_t}{\beta} \geq 1. \tag{10}$$

The interpretation is as follows. If a buyer purchases cryptocurrency in the CM at period t and resells it in the CM at period $t+1$, the rate of return in terms of utility is $\frac{\beta}{1+\pi_t}$. Therefore, if $\frac{1+\pi_t}{\beta} < 1$, a buyer's demand for cryptocurrency will be infinite, and (9) cannot hold. Given that (10) holds, it is not beneficial for a buyer to hold extra currency without using it to purchase goods in the DM. Thus, for simplicity, we assume that a buyer uses all her cryptocurrency holdings to purchase DM goods, so the budget constraint in (7) must bind:

$$\hat{z}_t - \tau_t + \delta = \frac{m_{t-1}}{1+\pi_{t-1}}. \tag{11}$$

Now the problem (7) can be rewritten as

$$\max_{\hat{z}_t, \sigma_t \in B(\hat{z}_t)} \bar{V}_t(\hat{z}_t, \sigma_t), \tag{12}$$

where $\bar{V}_t(\hat{z}_t, \sigma_t)$ is the buyer's expected payoff in the CM:

$$\begin{aligned} \bar{V}_t(\hat{z}_t, \sigma_t) = -(1+\pi_{t-1})\left(\hat{z}_t - \tau_t + \delta\right) \\ +\beta \left\{ \begin{array}{l} u\left[\sigma_t \alpha_h(\hat{z}_t)\hat{z}_t + (1-\sigma_t)\alpha_d(\hat{z}_t)\hat{z}_t\right] - k \\ +\sigma_t \eta_h(\hat{z}_t)\delta + (1-\sigma_t)\left[-k + \theta_d(\hat{z}_t)\hat{z}_t + \eta_d(\hat{z}_t)\delta\right] \end{array} \right\}. \end{aligned} \tag{13}$$

The buyer's strategy $(\hat{z}_t, \sigma_t)$ must satisfy

$$(\hat{z}_t, \sigma_t) \in \arg \max_{\hat{z}'_t, \sigma'_t \in B(\hat{z}')} \bar{V}_t(\hat{z}'_t, \sigma'_t). \tag{14}$$

We name (14) the individual optimality condition.

We focus on the stationary monetary equilibrium. Combining (8), (9), (11), and dropping the time subscripts, we obtain the new CM money market clearing condition:

$$\sigma\left[\alpha_h(\hat{z})\hat{z} + \eta_h(\hat{z})\delta\right] + (1-\sigma)\left[\left(\alpha_d(\hat{z}) + \theta_d(\hat{z})\right)\hat{z} + \eta_d(\hat{z})\delta\right] = (1+\pi)\left(\hat{z} - \tau + \delta\right), \tag{15}$$

where the left side is the CM money supply and also the aggregate quantity of cryptocurrency at the end of the DM; the right side is the CM money demand. Condition (15) illustrates that, given the DM transfer $\hat{z}$, an increase in the quantity of the cryptocurrency during the DM transactions will result in an increase in the inflation rate π, or the transaction subsidy τ has to fall to withdraw the cryptocurrency from the market. From (13), an increase in the inflation rate or a fall in the transaction subsidy will increase the buyer's cost of the DM trade, $(1+\pi)(\hat{z}-\tau+\delta)$. We call this channel the general equilibrium effect, and through this effect, an individual buyer's strategy on double spending not only influences her counterparty's incentive to produce but also generates externality to other buyers by influencing their cost of trade through changing the inflation rate or the transaction subsidy.

Finally, in an equilibrium, a buyer must be individually rational to participate in the cryptocurrency system, as argued by Andolfatto (2007). That is, a buyer's expected value in the CM when she enters the economy must be greater than zero, otherwise the buyer will not purchase cryptocurrency in the CM and will not trade in the DM. By (13), in a stationary equilibrium, the participation constraint holds if and only if

$$\bar{V}(\hat{z},\sigma) = -(1+\pi)(\hat{z}-\tau+\delta) + \beta \left\{ \begin{array}{l} u\left[\sigma\alpha_h(\hat{z})\hat{z} + (1-\sigma)\alpha_d(\hat{z})\hat{z}\right] - k \\ +\sigma\eta_h(\hat{z})\delta + (1-\sigma)\left[-k + \theta_d(\hat{z})\hat{z} + \eta_d(\hat{z})\delta\right] \end{array} \right\} \geq 0 \tag{16}$$

We define a stationary monetary equilibrium to be a mechanism $M = (k, \delta, \tau, \pi, P, Q)$ and a strategy $S = (\hat{z}, \sigma)$ such that 1) agents optimize (agents' strategies form a Pareto-dominant SPE of the trading game); 2) the CM money market clears; 3) buyers are willing to participate in the system. First of all, $\frac{1+\pi}{\beta} \geq 1$ is a necessary condition for the existence of monetary equilibrium. Given that $\frac{1+\pi}{\beta} \geq 1$, then, first, $(\hat{z}, \sigma)$ is a Pareto-dominant SPE if and only if the individual optimality condition (14) is satisfied; second, the CM money market clears if and only if (15) holds; third, buyers are incentivized to participate in the system if and only if the participation constraint (16) holds. We define a stationary monetary equilibrium as follows:

Definition 1 *A stationary monetary equilibrium is a tuple* $\mathbf{E}=(\mathbf{M},\mathbf{S})$ *such that* $\frac{1+\pi}{\beta} \geq 1$, *and (14), (15), (16) hold.*

We say that $\mathbf{M}$ generates an equilibrium $\mathbf{E}$ if $\mathbf{E} = (\mathbf{M}, \mathbf{S})$ for some $\mathbf{S}$.

2.3 Social Planner's Problem

We now study the social planner's problem in a stationary equilibrium, in which the planner assigns the buyer's production in the CM, X, and the seller's production in the DM, x, to maximize the aggregate utility of buyers and sellers. We assume that the social planner can allocate resources between buyers and sellers freely, but he cannot enforce agents to participate, so buyers and sellers must be individually rational in order to participate the planner's arrangement at any point in time. Let γ denote the discount factor of the social planner and reflect how she weights the utilities of different generations, and we assume that $\gamma = \beta$. Then the social planner's problem can be written as

$$\begin{aligned} \max_{x \geq 0} \qquad & u\left(x\right) - x \\ \text{subject to} \qquad & -x + \beta u(x) \geq 0, \end{aligned} \tag{17}$$

where $-x + \beta u(x) \geq 0$ is the buyer's participation constraint in the CM. (See Appendix A for the derivation of the social planner's problem.) We first assume that the participation constraint is not binding; then, the unconstrained optimal DM production, say $\bar{x}$, solves $u'\left(\bar{x}\right) - 1 = 0$. If $\bar{x}$ does not satisfy the participation constraint, then the optimal DM production is equal to $\hat{x}$, wherein $\hat{x}$ solves the binding participation constraint $-\hat{x} + \beta u(\hat{x}) = 0$. Thus, the solution of the social planner's problem is $x^e = \min\{\hat{x}, \bar{x}\}$, and this is the social optimal allocation; the welfare level generated by the optimal allocation is $W^e = u\left(x^e\right) - x^e$, and this is the social optimal welfare.

3 Optimal Mechanisms in Monetary Equilibrium

We take a mechanism design approach to find the mechanism that generates a monetary equilibrium with the highest social welfare. Compared with the social planner's problem

(17), in a monetary equilibrium, social welfare includes an extra term, $\sigma k + (1-\sigma)2k$, which is the social loss due to PoW, so the social welfare function is

$$u\ (x) - x - [\sigma k + (1-\sigma)2k]\,. \tag{18}$$

By the definition of monetary equilibrium (Definition 1), the optimal mechanism problem can be written as

$$\max_{(k,\delta,\pi,\tau,P(\hat{z}),Q(\hat{z}),\hat{z},\sigma)} u\ [\tilde{x}(\hat{z},\sigma)] - \tilde{x}(\hat{z},\sigma) - [\sigma k + (1-\sigma)2k] \tag{19}$$

$$\text{subject to } \frac{1+\pi}{\beta} \geq 1, \text{ and } (14), (15) \text{ and } (16)$$

Because the set of optimal mechanisms can be profound, we construct two forms of candidates for the optimal mechanisms: "simple honest mechanisms" and "simple double spending mechanisms," and we prove that any equilibrium is weakly dominated by an equilibrium generated by either a simple honest mechanism or a simple double spending mechanism. Thus, when we look for an optimal equilibrium of cryptocurrency systems, it is sufficient to look for it within the set of equilibria generated by the simple honest mechanisms or double spending mechanisms. In the following discussion, we first establish simple honest mechanisms and then simple double spending mechanisms.

3.1 Simple Honest Mechanism

In a simple honest mechanism, we set $p_2(\hat{z}) = q_2(\hat{z}) = 0$ to punish buyers who deviate to double spending; that is, whenever a fork occurs, the receivers of transaction messages will not receive the transfers. Moreover, we set $p_1(\hat{z})$ and $q_1(\hat{z})$ to be indicator functions; that is,

$$p_1(\hat{z}) = q_1(\hat{z}) = \mathbb{1}_y(\hat{z}) \equiv \begin{cases} 1 \text{ if } \hat{z} = y \\ 0 \text{ otherwise} \end{cases}, \text{ for some } y > 0,$$

and we name y the target value of the simple honest mechanism. By setting the equation thusly, we impose a strict requirement on the amount transferred that will be recognized: the receiver receives the transfer and the sender receives the deposit return only if $\hat{z} = y$; if a transfer $\hat{z}$ is different from y, the transfer and the PoS deposit will be deleted as a punishment for deviation. Moreover, we set k and δ just high enough to deter double spending. Let

$$\begin{aligned} &\alpha_h^s = 1; \quad \theta_h^s = 0; \quad \eta_h^s = 1; \\ &\alpha_d^s = r_s; \quad \theta_d^s = r_b; \quad \eta_d^s = (r_s + r_b), \end{aligned}$$

then by (1) and (2), $p_1(\hat{z}) = \mathbb{1}_y(\hat{z})$ and $p_2(\hat{z}) = 0$ imply $\alpha_i(y) = \alpha_i^s, \theta_i(y) = \theta_i^s$; and $q_1(\hat{z}) = \mathbb{1}_y(\hat{z})$ and $q_2(\hat{z}) = 0$ imply $\eta_i(y) = \eta_i^s$. Then k and δ are set to satisfy $k + (\eta_h^s - \eta_d^s)\,\delta = \theta_d^s y$. If k and δ are too small such that $k + (\eta_h^s - \eta_d^s)\,\delta < \theta_d^s y$, the buyer will double spend; if k and δ are too large such that $k + (\eta_h^s - \eta_d^s)\,\delta > \theta_d^s y$, the excessive PoW and PoS will generate waste. Finally, because any transfer deviated from y will not be received by the receiver, the inflation rate π does not influence the buyer's marginal decision on the amount of transfer as long as $\frac{1+\pi}{\beta} \geq 1$. For the purpose of exposition, we set π equal to zero, and let τ be chosen passively to satisfy the money market clearing condition (15). Then, given that $\alpha_h(y) = \eta_h(y) = 1$, and $\sigma = 1$, (15) implies $\tau = 0$. To summarize, we define a simple honest mechanism as follows:

Definition 2 *(**Simple honest mechanisms**) A mechanism* $\mathbf{M}^h$=$(k, \delta, \pi, \tau, P(\hat{z}), Q(\hat{z}))$ *is a simple honest mechanism if*

(i) There is a $y > 0$ *such that* $p_1(\hat{z}) = q_1(\hat{z}) = \mathbb{1}_y(\hat{z})$ *and* $p_2(\hat{z}) = q_2(\hat{z}) = 0$*;*

(ii) (k, δ) *satisfies* $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\,\delta$*;*

(iii) (π, τ) *satisfies* $\pi = 0, \tau = 0$*.*

The remaining questions concern whether the buyer will make transfer $\hat{z} = y$ and be honest ($\sigma = 1$) under the simple honest mechanism, and whether the simple honest mechanism can generate an equilibrium. We show that it suffices to check that the participation constraint (16) holds. Given a simple honest mechanism $\mathbf{M}^h$ with target value y, we denote its corresponding honest strategy by $\mathbf{S}^h = (\hat{z}, \sigma)$ such that $\hat{z} = y, \sigma = 1$. We first argue that $\mathbf{S}^h$ is an optimal strategy under $\mathbf{M}^h$ if the participation constraint (16) is satisfied, as shown in the following lemma.

Lemma 1 *Let $\mathbf{M}^h$ be a simple honest mechanism with target value y, and let $\mathbf{S}^h = (\hat{z}, \sigma)$ be a strategy such that $\hat{z} = y$, $\sigma = 1$. Then $(\mathbf{M}^h, \mathbf{S}^h)$ satisfies the individual optimality condition (14) if $(\mathbf{M}^h, \mathbf{S}^h)$ satisfies the participation constraint (16).*

Proof. *See Appendix B.1.* ■

The proof is sketched as follows. We show that under $\mathbf{M}^h$, $\mathbf{S}^h$ generates the highest CM value to the buyer among all strategies. First, suppose that the buyer makes a transfer $\hat{z} = y$. From Definition 2 (ii), because $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\,\delta$, any $\sigma \in [0, 1]$ can be a best response. However, because $p_2(y) = 0$, the seller's expected payoff will be lower when the buyer double spends than when the buyer is honest, which in turn generates a smaller DM consumption to the buyer, so any strategy in which $\sigma < 1$ will be dominated by the honest strategy ($\sigma = 1$). Second, suppose that the buyer makes a transfer $\hat{z} \neq y$, then neither the buyer nor the seller will receive the transfer, and thus the buyer's CM value will be non-positive. Because $(\mathbf{M}^h, \mathbf{S}^h)$ satisfies the participation constraint, it generates non-negative CM value to the buyer, and thus $\mathbf{S}^h$ also weakly dominates all strategies such that $\hat{z} \neq y$ and therefore satisfies the individual optimality constraint (14).

To show that $(\mathbf{M}^h, \mathbf{S}^h)$ forms an equilibrium, we must check that $\frac{1+\pi}{\beta} \geq 1$ and the money market clearing condition (15) holds, and both of which hold by the construction of the simple honest mechanism (Definition 2 (iii)). Thus, we have the following proposition:

Proposition 1 *Let $\mathbf{M}^h$ be a simple honest mechanism with target value y, and let $\mathbf{S}^h = (\hat{z}, \sigma)$ be a strategy such that $\hat{z} = y$, $\sigma = 1$. Then $(\mathbf{M}^h, \mathbf{S}^h)$ is an equilibrium if and only if it satisfies the participation constraint (16).*

We name an equilibrium generated by a simple honest mechanism a "simple honest equilibrium."

3.2 Simple Double Spending Mechanism

In a simple double spending mechanism, we set $k = \delta = 0$, and buyers double spend in this mechanism. As in a simple honest mechanism, we also set $p_1(\hat{z}) = \mathbb{1}_y(\hat{z})$ to punish transfers deviating from y, and we set $p_2(\hat{z}) = 0$ to delete transfers in forks; however, because double spending is an equilibrium strategy, the reason that the transfers in forks are deleted is not to punish deviations but is as follows. Because $r_s > r_b$, if the agreement is single, the seller has a higher probability than the buyer to receive the transfer; if the agreement is a fork, the probabilities for a buyer and a seller to receive the transfer are identical. However, only the transfer received by the seller can facilitate the DM trade, but both the transfers received by the buyer and the seller incur a trade cost to other participants through the general equilibrium effect. By setting $p_2(\hat{z}) = 0$, we recognize transfers in single agreements but not in forks and therefore minimize the cost of the DM trade. We also set $\pi = 0$ in a simple double spending mechanism and let τ be chosen passively to satisfy the money market clearing condition (15); then given that $\alpha_d(y) = \alpha_d^s$, $\theta_d(y) = \theta_d^s$, and $\sigma = 0$, (15) implies $\tau = (1 - \alpha_d^s - \theta_d^s)\, y$. Finally, because δ is set to be zero, $q_1(\hat{z})$ and $q_2(\hat{z})$ will have no impact on the buyer's post-trade gain thus can take any value in $[0, 1]$. We name y the target value of the simple double spending mechanism, and summarize the definition of a simple double spending mechanism as follows:

Definition 3 ***(Simple double spending mechanisms)*** *A mechanism* $\mathbf{M}^d$=$(k, \delta, \pi, \tau, P(\hat{z}), Q(\hat{z}))$ *is a simple double spending mechanism if*

(i) There is a $y > 0$ *such that* $p_1(\hat{z}) = \mathbb{1}_y(\hat{z})$, $p_2(\hat{z}) = 0$*;*

(ii) (k, δ) *satisfies* $k = 0$, $\delta = 0$*;*

(iii) (π, τ) *satisfies* $\pi = 0, \tau = (1 - \alpha_d^s - \theta_d^s)\, y$.

Given a simple double spending mechanism $\mathbf{M}^d$ with target value y, we denote its corresponding double spending strategy by $\mathbf{S}^d = (\hat{z}, \sigma)$ such that $\hat{z} = y$ and $\sigma = 0$. We argue that $(\mathbf{M}^d, \mathbf{S}^d)$ is an equilibrium if it satisfies the buyer's participation constraint (16). We first show that $\mathbf{S}^d$ is an optimal strategy under $\mathbf{M}^d$ if the buyer's participation constraint (16) is satisfied:

Lemma 2 *Let* $\mathbf{M}^d$ *be a simple double spending mechanism with target value* y*, and let* $\mathbf{S}^d = (\hat{z}, \sigma)$ *be a strategy such that* $\hat{z} = y$*,* $\sigma = 0$*. Then* $\left(\mathbf{M}^d, \mathbf{S}^d\right)$ *satisfies the individual optimality condition (14) if* $(\mathbf{M}^d, \mathbf{S}^d)$ *satisfies the participation constraint (16).*

Proof. *See Appendix B.2.* ■

We sketch the proof as follows. Suppose that the buyer makes a transfer $\hat{z} = y$, then because $k = 0$ and $\delta = 0$, conducting double spending ($\sigma = 0$) is the buyer's only best response. Alternatively, suppose the buyer makes a transfer $\hat{z} \neq y$; then the buyer's CM value will be non-positive. Because $(\mathbf{M}^d, \mathbf{S}^d)$ satisfies the participation constraint (16), it generates a non-negative CM value to the buyer, so $\mathbf{S}^d$ weakly dominates all strategies such that $\hat{z} \neq y$ and thus satisfies the individual optimality condition (14).

By the construction of the simple double spending mechanism (Definition 3 (iii)), $(\mathbf{M}^d, \mathbf{S}^d)$ also satisfies $\frac{1+\pi}{\beta} \geq 1$ and the money market clearing condition (15), and thus $(\mathbf{M}^d, \mathbf{S}^d)$ forms an equilibrium:

Proposition 2 *Let $\mathbf{M}^d$ be a simple double spending mechanism with target value y, and let $\mathbf{S}^d = (\hat{z}, \sigma)$ be a strategy such that $\hat{z} = y$, $\sigma = 0$. Then $(\mathbf{M}^d, \mathbf{S}^d)$ is an equilibrium if and only if it satisfies the participation constraint (16).*

We name an equilibrium generated by a simple double spending mechanism a "simple double spending equilibrium."

3.3 Optimal Equilibrium

We prove that any equilibrium is either weakly dominated by a simple honest equilibrium or a simple double spending equilibrium. Let $\mathbf{E}^* = (k^*, \delta^*, \pi^*, \tau^*, P^*, Q^*, z^*, \sigma^*)$ be an equilibrium; then we denote $\hat{p}_j^* = p_j^*(\hat{z}^*), \hat{q}_j^* = q_j^*(\hat{z}^*), \hat{\alpha}_i^* = \alpha_i^*(\hat{z}^*)$, $\hat{\theta}_i^* = \theta_i^*(\hat{z}^*)$, $\hat{\eta}_i^* = \eta_i^*(\hat{z}^*)$. The strategy of the proof is as follows. First, we show that an equilibrium with zero DM production is dominated by a simple double spending equilibrium and therefore cannot be optimal. Second, we show that an equilibrium with nonzero DM production is weakly dominated by a simple honest equilibrium if PoW and PoS are sufficiently high $(k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* \geq \hat{\theta}_d^* \hat{z}^*)$ and is weakly dominated by a simple double spending equilibrium if PoW and PoS are low $(k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* < \hat{\theta}_d^* \hat{z}^*)$.

Let $\mathcal{E}$ denote the collection of $\mathbf{E}$ that are equilibria, and let $\mathcal{Z} = \{\mathbf{E} \in \mathcal{E}\colon\ \tilde{x}(\hat{z}, \sigma) = 0\}$ be the set of equilibria with zero DM productions. Then the following proposition holds:

Proposition 3 *Let $\mathbf{E}^* \in \mathcal{Z}$, then $\mathbf{E}^*$ is dominated by a simple double spending equilibrium.*

The proof is straightforward. Because the DM production is zero in $\mathcal{Z}$, welfare of $\mathbf{E}^*$ must be non-positive. Moreover, because $\lim_{x\to 0} u'(x) = \infty$, we can construct a simple double spending equilibrium with positive welfare if the target value y is set to be sufficiently small. By proposition 3, in the following discussion, we exclude those equilibria in $\mathcal{Z}$ and denote $\mathcal{N} = \mathcal{E}\backslash\mathcal{Z}$.

Proposition 4 *Let* $\mathbf{E}^* = (k^*, \delta^*, \pi^*, \tau^*, P^*(\hat{z}), Q^*(\hat{z}), \hat{z}^*, \sigma^*) \in \mathcal{N}$

(i) If $k^* + [\hat{\eta}_h^* - \hat{\eta}_d^*]\,\delta^* \geq \hat{\theta}_d^* \hat{z}^*$*, there is a simple honest equilibrium which (weakly) dominates* $\mathbf{E}^*$;

(ii) If $k^* + [\hat{\eta}_h^* - \hat{\eta}_d^*]\,\delta^* < \hat{\theta}_d^* \hat{z}^*$*, there is a simple double spending equilibrium which (weakly) dominates* $\mathbf{E}^*$.

Proof. *See Appendix B.3.* ■

The proof is sketched as follows. We divide $\mathcal{N}$ into three cases: 1) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* = \hat{\theta}_d^* \hat{z}^*$; 2) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* > \hat{\theta}_d^* \hat{z}^*$; and 3) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* < \hat{\theta}_d^* \hat{z}^*$. First, in the case of $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* = \hat{\theta}_d^* \hat{z}^*$, PoW and PoS are large enough such that the buyer is willing to be honest given the DM transfer $\hat{z}^*$. In a simple honest equilibrium, because $p_2(\hat{z}) = q_2(\hat{z}) = 0$, we minimize the buyer's gain from double spending and PoW and PoS relative to the volume of DM trade. Thus, given $\mathbf{E}^*$, we can construct a simple honest equilibrium that generates the same DM production x^* but with a smaller cost of trade and therefore generates higher social welfare compared with $\mathbf{E}^*$.

In the case of $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* > \hat{\theta}_d^* \hat{z}^*$, the extra PoW and PoS are waste. Thus, we can construct an $\mathbf{E}'$ that makes the same transfer $\hat{z}^*$ but with smaller k and δ that are just enough to prevent double spending, so $\mathbf{E}'$ generates higher social welfare than $\mathbf{E}^*$ does. Then, we use the same argument as in case 1) to find a simple honest equilibrium that dominates $\mathbf{E}'$ and therefore also dominates $\mathbf{E}^*$.

Finally, in the case of $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\,\delta^* < \hat{\theta}_d^* \hat{z}^*$, PoW and PoS are not large enough to prevent double spending, and thus PoW and PoS only generates waste. As a consequence, we can decrease k and δ to zero to save the cost of PoW and PoS without influencing the amount of DM trade. Moreover, by setting $p_2(\hat{z}) = 0$, we minimize the cost of trade, as discussed in Section 3.2. Thus, we can find a simple double spending equilibrium that generates the same DM production x^* but with weakly higher welfare, and thus it weakly dominates the equilibrium.

By Proposition 3 and Proposition 4, when we are looking for an optimal equilibrium, it suffices to discuss the simple honest and simple double spending equilibria. Thus, we confine our attention to the optimal welfare generated by these two forms of equilibria. When comparing both mechanisms, notice that the cost of PoW and PoS is saved in a simple double spending mechanism, but given the DM transfer y, the amount of DM trade is smaller in a simple double spending mechanism than in a simple honest mechanism. In the following discussion, we study under what circumstance the simple honest equilibria can generate higher social welfare than simple double spending equilibria and vice versa.

3.4 Optimal Simple Double Spending Equilibrium

We first discuss the optimal simple double spending equilibrium. By Proposition 2, a simple double spending equilibrium is a simple double spending mechanism and a corresponding double spending strategy $(\mathbf{M}^d, \mathbf{S}^d)$ that satisfy the participation constraint (16). Let y be the target value of $(\mathbf{M}^d, \mathbf{S}^d)$, and given the social welfare function (18) and the participation constraint (16) under $(\mathbf{M}^d, \mathbf{S}^d)$, the optimal simple double spending equilibrium solves

$$\begin{aligned} \max_{y} \quad & u\left(\alpha_d^s y\right) - \alpha_d^s y \\ \text{subject to} \quad & -(\alpha_d^s + \theta_d^s) y + \beta \left\{ u\left(\alpha_d^s y\right) + \theta_d^s y \right\} \geq 0. \end{aligned} \tag{20}$$

Let $x = \alpha_d^s y$ denote the DM production, and because $\alpha_d^s = r_s$, $\theta_d^s = r_b$, we rewrite the mechanism design problem as

$$\begin{aligned} \max_{x} \quad & u\left(x\right) - x \\ \text{subject to} \quad & -\left(\frac{1}{\beta} + \frac{1-\beta}{\beta}\frac{r_b}{r_s}\right) x + u(x) \geq 0. \end{aligned} \tag{21}$$

Let $W_d(R)$ denote the welfare level of optimization problem (21), then the key value that determines $W_d(R)$ is $\frac{r_b}{r_s}$ in the participation constraint. The interpretation is as follows. In a simple double spending equilibrium, when the buyer transfers y units of cryptocurrency, the seller only receives $r_s y$ units of cryptocurrency in the DM, and the buyer receives $r_b y$ units. Unlike the transfer received by the seller, the transfer received by the buyer does not facilitate the DM transaction. However, both transfers received by the buyer and the seller generate costs of trade through the general equilibrium effect. Thus, the ratio $\frac{r_b}{r_s}$ is a measure of the inefficiency of cryptocurrency, and a smaller $\frac{r_b}{r_s}$ will result in higher social welfare.

To understand how the network imperfection affects efficiency, we study the impact of changes in $R = (r_s, r_b, r_{sb})$ on $W_d(R)$. Note that $r_s + r_b + r_{sb} = 1$, so a change in one probability must result in corresponding changes in other probabilities. In the following discussion, we study the bilateral trade-off between the probabilities of one agreement and another. Let Φ denote the feasible set of R:

$$\Phi = \left\{(r_s, r_b, r_{sb}) \in \mathbb{R}^3_{>0} : r_s + r_b + r_{sb} = 1, r_s > r_b\right\}.$$

The following lemma shows how an increase in r_s influences the optimal welfare of simple double spending equilibria:

Lemma 3 *An increase in r_s and a corresponding decrease in either r_b or r_{sb} result in an increase in $W_d(R)$. That is, given $\triangle > 0$, for $R = (r_s, r_b, r_{sb}) \in \Phi$,*

(i) If $R' = (r_s + \triangle, r_b, r_{sb} - \triangle) \in \Phi$, then $W_d(R') \geq W_d(R)$;

(ii) If $R' = (r_s + \triangle, r_b - \triangle, r_{sb}) \in \Phi$, then $W_d(R') \geq W_d(R)$.

The holding of Lemma 3 can be directly observed from Problem (20) and (21). First, an increase in r_s will increase the seller's expected payoff given the amount transferred y. If the increase in r_s crowds out r_{sb}, but r_b is not affected, then the buyer's expected payoff relative to the seller's will decrease ($\frac{r_b}{r_s}$ decreases). As a consequence, the inefficiency of cryptocurrency decreases, and welfare increases. If the increase in r_s results in a corresponding decrease in r_b, then $\frac{r_b}{r_s}$ decreases even more than in the first case, so welfare will also increase more than in the first case.

By using symmetric arguments, we have the following properties for the impact of an increase r_b on the optimal welfare of simple double spending equilibria:

Lemma 4 *An increase in r_b and a corresponding decrease in either r_{sb} or r_s result in a decrease in $W_d(R)$. That is, given $\triangle > 0$, for $R = (r_s, r_b, r_{sb}) \in \Phi$,*

(i) If $R' = (r_s, r_b + \triangle, r_{sb} - \triangle) \in \Phi$, then $W_d(R') \leq W_d(R)$;

(ii) If $R' = (r_s - \triangle, r_b + \triangle, r_{sb}) \in \Phi$, then $W_d(R') \leq W_d(R)$.

Combining Lemma 3 and Lemma 4, we see that the impact of changes in r_{sb} on $W_d(R)$ depends on it crowds out r_b or r_s. Lemma 3 (i) implies that an increase in r_{sb} and a corresponding decrease in r_s result in a decrease in $W_d(R)$; however, Lemma 4 (i) implies that an increase in r_{sb} and a corresponding decrease in r_b result in an increase in $W_d(R)$. We summarize the properties of $W_d(R)$ in the following proposition:

Proposition 5 *When considering the bilateral trade-off between the probabilities of agreements, the welfare of the optimal simple double spending equilibrium $W_d(R)$ is positively related to r_s and negatively related to r_b. Moreover, the impact of increasing r_{sb} is positive if it crowds out r_b and negative if it crowds out r_s.*

We take the buyer's DM utility function as constant relative risk aversion (CRRA) for example and demonstrate the iso-welfare curves of $W_d(R)$ in Figure 4. If the participation constraint is binding in the social planner's problem, then $W_d(R)$ approaches the social optimal welfare if and only if $\frac{r_b}{r_s}$ approaches zero (see Figure 4, left). If the participation constraint is non-binding in the social planner's problem, the buyer is willing to tolerate a small cost to trade with efficient allocation, and there is $\lambda > 0$ such that $W_d(R)$ achieves the social optimal welfare if and only if $\frac{r_b}{r_s} \leq \lambda$ (see Figure 4, right).

Proposition 6 *If the participation constraint of the social planner's problem is binding, then $W_d(R) \to W^e$ as $\frac{r_b}{r_s} \to 0$. If the participation constraint of the social planner's problem is not binding, then $W_d(R) = W^e$ for $\frac{r_b}{r_s} \leq \lambda$, where λ solves $-\left(\frac{1}{\beta} + \frac{1-\beta}{\beta}\lambda\right) x^e + u(x^e) = 0$.*

3.5 Optimal Simple Honest Equilibrium

We then discuss the optimal simple honest equilibrium. By Proposition 1, a simple honest equilibrium is a simple honest mechanism and a corresponding honest strategy $(\mathbf{M}^h, \mathbf{S}^h)$ that satisfy the participation constraint. Let y be the target value of $(\mathbf{M}^h, \mathbf{S}^h)$; then the participation constraint (16) under $(\mathbf{M}^h, \mathbf{S}^h)$ is $-(y+\delta)+\beta\{u(y)+\delta-k\} \geq 0$, and the social welfare function (18) is $u(y)-y-k$. Moreover, in a simple honest equilibrium, k and δ can be chosen to meet the constraint that $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\delta$. Thus, an optimal simple honest equilibrium solves

$$\begin{array}{ll} \max_{y,k,\delta} & u(y)-y-k \\ \text{subject to} & \begin{cases} -(y+\delta)+\beta\{u(y)+\delta-k\} \geq 0 \\ \theta_d^s y = k + (\eta_h^s - \eta_d^s)\delta \end{cases} . \end{array} \tag{22}$$

Let $x = y$ denote the DM production. By the constraint $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\delta$ in problem (22), we divide the DM production x into the part supported by PoW, $x^k = \frac{1}{\theta_d^s}k$ and the part supported by PoS, $x^\delta = \frac{\eta_h^s - \eta_d^s}{\theta_d^s}\delta$; then $x = x^k + x^\delta$. Moreover, given that $\theta_d^s = r_b$ and $\eta_h^s - \eta_d^s = r_{sb}$, we rewrite (22) as

$$\begin{array}{ll} \max\limits_{x^k, x^\delta} & u\left(x^k + x^\delta\right) - (1+r_b)x^k - x^\delta \\ \text{subject to} & -(\frac{1}{\beta}+r_b)x^k - \left(\frac{1}{\beta} + \frac{1-\beta}{\beta}\frac{r_b}{r_{sb}}\right)x^\delta + u(x^k + x^\delta) \geq 0. \end{array} \tag{23}$$

Let $W_h(R)$ denote the welfare level of optimization problem (23). In the following discussion, we study PoW and PoS separately to investigate the channel through which changes in R influence $W_h(R)$. We first shut down PoS in simple honest mechanisms by setting $\delta = 0$ ($x^\delta = 0$), and we call the mechanisms "pure PoW mechanisms"; then we shut down PoW by setting $k = 0$ ($x^k = 0$), and we call the mechanisms "pure PoS mechanisms". Finally, we consider both PoW and PoS in the simple honest mechanism as in optimization problem (23).

Optimal Pure PoW Equilibrium. An optimal pure PoW equilibrium solves the following problem

$$\begin{array}{ll} \max\limits_{x^k} & u\left(x^k\right) - (1+r_b)x^k \\ \text{subject to} & -\left(\frac{1}{\beta}+r_b\right)x^k + u(x^k) \geq 0, \end{array} \tag{24}$$

which is equivalent to setting $x^\delta = 0$ in the optimization problem (23). Let $W_h^k(R)$ denote the welfare level of the optimization problem (24), we observe that $W_h^k(R)$ is only determined by the probability of a false agreement, r_b. This is because we punish forks by setting $p_2(\hat{z}) = 0$, and thus the buyer gains from double spending only when a false agreement occurs. Thus, r_b determines the required size of PoW to prevent double spending fraud: an increase in r_b directly decreases social welfare, and also tightens the participation constraint. In Figure 5, we demonstrate the iso-welfare curves of the optimal PoW equilibrium. Because PoW generates a loss to social welfare, given that r_b is greater than zero, $W_h^k(R)$ must be smaller than the social optimal welfare, W^e, regardless of whether the participation constraint binds or not, and $W_h^k(R) \to W^e$ as $r_b \to 0$.

Proposition 7 *$W_h^k(R)$ approaches the social optimal welfare as $r_b \to 0$.*

Optimal Pure PoS Equilibrium. An optimal pure PoS equilibrium solves the following problem

$$\begin{aligned} \max_{x^\delta} \quad & u\left(x^\delta\right) - x^\delta \\ \text{subject to} \quad & -\left(\frac{1}{\beta} + \frac{1-\beta}{\beta}\frac{r_b}{r_{sb}}\right) x^\delta + u(x^\delta) \geq 0, \end{aligned} \tag{25}$$

which is equivalent to setting $x^k = 0$ in the optimization problem (23). Let $W_h^\delta(R)$ denote the welfare level of the optimization problem (25), then similar to pure PoW equilibria, the buyer's gain from double spending is also determined by r_b. However, because PoS utilizes forks as signals to detect double spending and to trigger the punishment for double spending, a higher r_{sb} will result in a smaller required size of PoS to prevent fraud. Thus, the welfare of the optimal pure PoS equilibrium is determined by the ratio $\frac{r_b}{r_{sb}}$, and a smaller $\frac{r_b}{r_{sb}}$ will result in higher social welfare. In Figure 6, we depict the iso-welfare curves of the optimal PoW equilibrium on Φ. Similar to the optimization problem of the double spending equilibrium, when the participation constraint in the social planner's problem is binding, $W_h^\delta(R)$ approaches social optimum if $\frac{r_b}{r_{sb}} \to 0$ (Figure 6, left). When the participation constraint in the social planner's problem is nonbinding, the social optimum can be achieved given the small cost of PoS. (Figure 6, right).

Proposition 8 *If the participation constraint of the social planner's problem is binding, then $W_h^{\delta}(R) \to W^e$ as $\frac{r_b}{r_{sb}} \to 0$. If the participation constraint of the social planner's problem is not binding, then $W_h^{\delta}(R) = W^e$ for $\frac{r_b}{r_{sb}} \leq \lambda$, where λ solves $-\left(\frac{1}{\beta} + \frac{1-\beta}{\beta}\lambda\right) x^e + u(x^e) = 0$.*

Proof-of-Work and Proof-of-Stake In this section, we utilize both PoW and PoS to obtain the optimal simple honest equilibrium as in problem (23). According to the above discussion, the differences between pure PoW and pure PoS mechanisms are twofold: 1) PoW generates disutility to the buyer and causes a direct loss to social welfare, but PoS does not; 2) PoS relies on forks to trigger punishments, but PoW does not; thus, given r_b, if r_{sb} decreases, the cost of applying PoS to prevent fraud will increase, but the cost of applying PoW remains the same.

We solve problem (23) in an example with a CRRA utility function and demonstrate the results in Figure 7. We first consider the case that the participation constraint in the social planner's problem is binding (Figure 7 left). We observe from the figure that given r_b, when r_{sb} is low, the optimal simple honest equilibrium is generated by a pure PoW mechanism (e.g., the pink region in the Figure); when r_{sb} is high, the optimal equilibrium is generated by a pure PoS mechanism (e.g., the blue region in the Figure). Moreover, because PoW and PoS work differently in affecting efficiency, a combination of PoW and PoS may improve social welfare; thus, there is a region between the pure PoW and pure PoS equilibrium in which both PoW and PoS are utilized in the optimal equilibrium (e.g., the gray region in the Figure). If the participation constraint is non-binding in the social planner's problem (Figure 7, right), then given r_b, if r_{sb} is high, the optimal equilibrium is a pure PoS mechanism. If r_{sb} is low, PoW is required in the optimal equilibrium; however, PoS is also essential, and that is, the optimal equilibrium applies both PoS and PoW to deter double spending.

In the following lemma, we discuss how an increase in r_{sb} influences the optimal welfare of simple honest equilibria:

Lemma 5 *An increase in r_{sb} and a corresponding decrease in either r_s or r_b result in an increase in $W_h(R)$. That is, given $\triangle > 0$, for $R = (r_s, r_b, r_{sb}) \in \Phi$,*

(i) If $R' = (r_s - \triangle, r_b, r_{sb} + \triangle) \in \Phi$, then $W_h(R') \geq W_h(R)$;

(ii) If $R' = (r_s, r_b - \triangle, r_{sb} + \triangle) \in \Phi$, then $W_h(R') \geq W_h(R)$.

The holding of Lemma 5 can be directly observed from Problem (23). First, an increase in r_{sb} increases the probability that double spending is detected. Moreover, if the increase in r_{sb} results in a decreases in r_s but r_b remains the same, then the gain from double spending does not change. In this case, the efficiency of PoW is unchanged, but the efficiency of PoS increases, and thus $W_h(R)$ increases because of the increase in the efficiency of PoS. Furthermore, if the increase in r_{sb} results in a decrease in r_b, then the gain from double spending decreases. Thus both the efficiency of PoS and PoW increase, and the welfare increases even more than in the first case. With symmetric arguments, we see the following properties of the impact of changes in r_b on the optimal welfare of simple honest equilibria:

Lemma 6 *An increase in r_b and a corresponding decrease in either r_s or r_{sb} result in a decrease in $W_h(R)$. That is, given $\triangle > 0$, for $R = (r_s, r_b, r_{sb}) \in \Phi$,*

(i) If $R' = (r_s - \triangle, r_b + \triangle, r_{sb}) \in \Phi$, then $W_h(R') \leq W_h(R)$;

(ii) If $R' = (r_s, r_b + \triangle, r_{sb} - \triangle) \in \Phi$, then $W_h(R') \leq W_h(R)$.

Note that Lemma 5 (i) implies that an increase in r_s and a corresponding decrease in r_{sb} result in a decrease in $W_h(R)$; moreover, Lemma 6 (i) implies that an increase in r_s and a corresponding decrease in r_b result in an increase in $W_h(R)$. Thus, the impact of an increase in r_s on $W_h(R)$ depends on if it crowds out r_b or r_{sb} correspondingly. We summarize the properties of $W_h(R)$ in the following proposition:

Proposition 9 *When considering the bilateral trade-off between the probabilities of agreements, the welfare of the optimal simple honest equilibrium $W_h(R)$ is positively related to r_{sb} and negatively related to r_b. Moreover, the impact of increasing r_s is positive if it crowds out r_b and negative if it crowds out r_{sb}.*

3.6 Simple Honest Equilibrium and Simple Double Spending Equilibrium

Proposition 5 and Proposition 9 show that changes in r_{sb} and r_s have different impacts on the optimal welfare under different mechanisms. Specifically, if we fix r_b, an increase in r_{sb} and a decrease in r_s will result in an increase in $W_h(R)$ but a decrease in $W_d(R)$. This occurs because forks and correct agreements play different roles in these two forms of equilibria. In a simple honest equilibrium, forks serve as signals to trigger off-equilibrium punishment on double spending, but a correct agreement cannot be so used. In a simple double spending equilibrium, however, forks are equilibrium outcomes, and an increase in r_{sb} and a decrease in r_s will decrease the relative probability that the seller receives the transfer and thus decrease the efficiency of cryptocurrency.

We depict the optimal equilibrium in an example with the CRRA utility function in Figure 8. We first discuss the case that the participation constraint is binding in the social planner's problem (Figure 8, left). Given r_b, if r_{sb} is high, the optimal simple honest equilibrium dominates the optimal simple double spending equilibrium, so the optimal equilibrium is a simple honest equilibrium. If r_{sb} is low, the optimal simple double spending equilibrium dominates the optimal simple honest equilibrium, so the optimal equilibrium is a simple double spending equilibrium. If the participation constraint is non-binding in the social planner's problem (Figure 8, right), the result is similar to the case in which the participation constraint is binding, but there is a region in which both the optimal simple double spending and honest equilibrium achieve the social optimum.

Note that PoS and the double spending mechanism both result in extra cryptocurrency circulations for the DM trade, and we can observe from the participation constraints in problems (21) and (23) that the cost of holding extra cryptocurrency increases as the time preference β decreases. However, the cost of PoW is generated at the moment that transaction happens and is not influenced by the time preference. Therefore, when the time preference β is smaller, PoW will be more advantageous than PoS, and the simple honest equilibrium will be more advantageous than the simple double spending equilibrium. There may be other factors that also influence the cost of holding extra cryptocurrency that we do not consider in the model. For example, a decrease in the matching rate in the DM may exaggerate the cost of holding extra cryptocurrency as the PoS deposit, and the PoW mechanisms will have more advantages over PoS under this environment because PoW occurs only if traders are successfully matched at the DM.

4 Conclusion

We have revealed the relationships between network imperfection, incentives to engage in fraud, and trade-offs underlying different cryptocurrency mechanisms. By endogenizing the roles of PoW and PoS, we discover a key implication that the cost of running cryptocurrency comes from the imperfectness of the internet. As the technology of the internet improves, the probability that a false agreement occurs under double spending may decrease, and the probability that a correct agreement or a fork occurs may increase. The efficiency of cryptocurrencies is thus expected to increase with the development of the internet, and cryptocurrencies can serve as favorable means of payment and may even achieve efficient allocation.

While this framework has been abstracted from some technical details of consensus formation, it captures the main features of the consensus system and can be applied to more complicated scenarios in order to determine additional theoretical implications. For example, double spending may result in a fork with a long branch and a short branch in the blockchain, in which the long branch can be taken as the original one, and the short branch can be taken as the double spending one. This agreement can help one more easily identify the original message and subsequently impose punishment on the defrauder. The existence of such identification can further increase the efficiency of cryptocurrency systems. Furthermore, this paper focuses the role of different consensus agreements on the efficiency of cryptocurrency while taking their probabilities as given. In Bitcoin, however, a greater size of PoW may prolong the time required to generate a new block and therefore influence the probability that correct agreements, false agreements and forks occur under double spending attacks. A study that endogenizes the characteristics of consensus algorithms would complement our research and be crucial for further investigation of the optimal design of cryptocurrency.

The framework presented here not only provides guidance for the design of a cryptocurrency system for private-sector use but also has implications for policymakers who wish to adopt cryptocurrency, for example, in large-value payments or for interbank payment and settlement. Our model is explicit about the frictions facing cryptocurrencies, that is, the imperfectness of the internet and the threat of double spending, both of which are distinct from the frictions in traditional payment systems such as counterfeiting and theft problems in fiat money, and limited commitment problems in bank deposit. One can extend our framework to discuss issues regarding the coexistence of fiat money and cryptocurrency, currency competitions, and the conduct of monetary policy in an environment in which cryptocurrency is widely used as a means of payment.

References

Andolfatto, D. (2007). Incentives and the limits to deflationary policy. *manuscript*.

Berentsen, A., M. Molico, and R. Wright (2002). Indivisibilities, lotteries, and monetary exchange. *Journal of Economic Theory 107*(1), 70–94.

Cavalcanti, R. and E. Nosal (2011). Counterfeiting as private money in mechanism design. *Journal of Money, Credit and Banking, 43*(Supplement 2), 625–636.

Chiu, J. and T. Koeppl (2017). The economics of cryptocurrencies: Bitcoin and beyond. *Working Paper*.

Garay, J., A. Kiayias, and N. Leonardos (2015). The bitcoin backbone protocol: Analysis and applications. *In Advances in Cryptology-EUROCRYPT 2015*, 281–310.

Kocherlakota, R. N. (1998). Money is memory. *Journal of Economic Theory 81*(2), 232–251.

Kocherlakota, R. N. and N. Wallace (1998). Incomplete record-keeping and optimal payment arrangements. *Journal of Economic Theory 81*, 272–289.

Lagos, R. and R. Wright (2005). A unified framework for monetary theory and policy analysis. *Journal of Political Economy 113*(3), 463–484.

Li, Y., G. Rocheteau, and P.-O. Weill (2012). Liquidity and the threat of fraudulent assets. *Journal of Political Economy 120*(5), 815–846.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf*.

Pass, R., L. Seeman, and A. Shelat (2016). Analysis of the blockchain protocolin asynchronous networks. *IACR Cryptology ePrint Archive*, 281–310.

Rocheteau, G. and R. Wright (2005). Money in search equilibrium, in competitive equilibrium, and in competitive search equilibrium. *Econometrica 73*(1), 175–202.

Shell, K. and R. Wright (1993). Indivisibilities, lotteries, and sunspot equilibria. *Economic Theory 3*, 1–17.

A Social Planner's Problem

We study the social planner's problem in this section. We assume that the social planner can allocate resources between buyers and sellers freely but cannot enforce agents to participate, so buyers and sellers must be individual rational to accept the allocation at any point of time. We denote γ the discount factor of the social planner, which reflects how she weights the utilities of different generations. That is, the weight of a generation entering the market at period t is γ^t. We denote the initial generation by -1, and we set $\gamma = \beta$. The initial cryptocurrency is held by the initial generation buyers at the beginning of the DM. In a stationary equilibrium, the discounted aggregation of the buyers' utility is

$$\begin{aligned} & \beta^{-1}\left\{\beta\left[u(x)+X'\right]\right\}+\beta^{0}\left\{X+\beta\left[u(x)+X'\right]\right\}+\beta^{1}\left\{X+\beta\left[u(x)+X'\right]\right\}+\cdots \\ = & \sum_{t=0}^{\infty}\beta^{t}\left[u(x)+X'+X\right]. \end{aligned}$$

The discounted aggregation of the sellers' utility is

$$\begin{aligned} & \beta^{0}\left\{-l+H\right\}+\beta^{1}\left\{-l+H\right\}+\cdots \\ = & \sum_{t=0}^{\infty}\beta^{t}\left[-l+H\right]. \end{aligned}$$

Thus, the social welfare is

$$\sum_{t=0}^{\infty}\beta^{t}\left\{\left[u(x)+X'+X\right]+\left[-l+H\right]\right\}.$$

The social planner maximizes the social welfare subject to agents' participation constraints and the resource constraints. First, the buyer's participation constraint at the CM where they enter and leave are

$$\begin{aligned} X+\beta\left[u(x)+X'\right] &\geq 0; \\ X' &\geq 0, \end{aligned}$$

and the seller's participation constraint at the DM is

$$-l + H \geq 0.$$

Second, the resource constraints at the CM and DM must bind, so $X' + X + H = 0$ and $x = l$. Substitute the resource constraint into the social welfare function and the participation constraints, the social planner's problem can be written as

$$\max_{x,X',X} \quad u(x) - x \tag{26}$$

$$\text{subject to} \quad \begin{cases} X + \beta\left[u(x) + X'\right] \geq 0 \\ X' \geq 0 \\ -x - X' - X \geq 0 \end{cases} . \tag{27}$$

Where the first and the second constraints are the buyer's participation constraints, and the third constraint is the seller's participation constraint. Suppose that the seller's participation constraint does not bind, then we can increase X until the seller's participation constraint binds, which does not influence the value of the objective function, and the buyer's constraints still hold. Thus, we can assume that the seller's participation constraint binds when we solve the optimization problem. In the constraint $X + \beta\left[u(x) + X'\right] \geq 0$, we see that X' is discounted by the time preference, but X is not, so it is optimal to set $X' = 0$. Thus, we can rewrite the social planner's problem as problem (17).

B Proofs of Propositions and Lemmas

B.1 Proof of Lemma 1

Suppose that $(\mathbf{M}^h, \mathbf{S}^h)$ satisfies the participation constraint (16). 1) $\hat{z} = y$: because $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\,\delta$ implies $B(y) = [0, 1]$, so σ can take any value between zero and one. Moreover,

$$\begin{aligned}
\bar{V}(y, \sigma = 1) &= -(y + \delta) + \beta \left\{u(\alpha_h^s y) + \eta_h^s \delta - k\right\} \\
&\geq -(y + \delta) + \beta \left\{u(\sigma \alpha_h^s y + (1 - \sigma)\alpha_d^s y) + \sigma\,(\eta_h^s \delta - k) + (1 - \sigma)\,(\theta_d^s y + \eta_d^s \delta - 2k)\right\} \\
&= \bar{V}(y, \sigma) \text{ for all } \sigma \in [0, 1].
\end{aligned}$$

The inequality holds because $\alpha_d^s < 1$ and $\theta_d^s y = k + (\eta_h^s - \eta_d^s)\,\delta$ implies that $\eta_h^s \delta - k = \theta_d^s y + \eta_d^s \delta - 2k$. 2) $\hat{z} \neq y$: the buyer and the seller will not receive any transfer and deposit return in the DM. Thus, the buyer's spending on the purchases of cryptocurrency in the CM will have no payoff, and its CM value will be non-positive. Because $(\mathbf{M}^h, \mathbf{S}^h)$ satisfies the participation constraint (16), we have $-(y + \delta) + \beta \left\{u(\alpha_h^s y) - k + \eta_h^s \delta\right\} \geq 0$, so making a transfer $\hat{z} \neq y$ is weakly dominated by $\hat{z} = y$, $\sigma = 1$. Thus, $\mathbf{S}^h$ weakly dominates all other strategies, so $\mathbf{S}^h$ satisfies the optimality condition (14).

B.2 Proof of Lemma 2

Suppose that $(\mathbf{M}^d, \mathbf{S}^d)$ satisfies the participation constraint (16). 1) $\hat{z} = y$: Note that $k = 0$, $\delta = 0$, and $\hat{z} = y > 0$ imply $B(y) = \{0\}$, so the buyer must double spend. 2) $\hat{z} \neq y$: the buyer's CM value will be non-positive for the same reason as in the proof of Lemma 1. Because $(\mathbf{M}^d, \mathbf{S}^d)$ satisfies the participation constraint (16), the buyer's value in the CM must be non-negative. Thus, $\mathbf{S}^d$ weakly dominates all other strategies and therefore solves the optimality condition (14).

B.3 Proof of Proposition 4

Let $\mathbf{E}^* = (k^*, \delta^*, \pi^*, \tau^*, P^*, Q^*, \hat{z}^*, \sigma^*) \in \mathcal{N}$, and let $\hat{p}_j^* = p_j^*(\hat{z}^*), \hat{q}_j^* = q_j^*(\hat{z}^*), \hat{\alpha}_i^* = \alpha_i^*(\hat{z}^*)$, $\hat{\theta}_i^* = \theta_i^*(\hat{z}^*)$, $\hat{\eta}_i^* = \eta_i^*(\hat{z}^*)$, then $x^* = \tilde{x}(\hat{z}^*, \sigma^*) = \left[\sigma_h^* \hat{\alpha}_h^* + (1 - \sigma^*)\hat{\alpha}_d^*\right] \hat{z}^* > 0$. Thus, we must have $\hat{z}^* > 0$ and $[\sigma^* \hat{\alpha}_h^* + (1-\sigma^*)\hat{\alpha}_d^*] > 0$, and which implies, $\hat{p}_1^* > 0$ or $\hat{p}_2^* > 0$. Therefore, we must have $\hat{\theta}_d^* > 0$. We divide $\mathcal{N}$ into the following three cases: 1) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* = \hat{\theta}_d^* \hat{z}^*$;2) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* > \hat{\theta}_d^* \hat{z}^*$;3) $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* < \hat{\theta}_d^* \hat{z}^*$;

Case 1: $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* = \hat{\theta}_d^* \hat{z}^*$:

We further divide case 1 into two subcases. In step 1, we study that $\hat{\eta}_h^* - \hat{\eta}_d^* \geq 0$; in step 2, we study that $\hat{\eta}_h^* - \hat{\eta}_d^* < 0$.

Step 1: $\hat{\eta}_h^* - \hat{\eta}_d^* \geq 0$: Because $x^* = [\sigma^* \hat{\alpha}_h^* + (1-\sigma^*)\hat{\alpha}_d^*]\, \hat{z}^*$, $\hat{\theta}_d^* \hat{z}^* = k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^*$, and $\hat{\theta}_d^* > 0$, we have

$$x^* = \left[\sigma^* \frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*} + (1-\sigma^*)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right] [k^* + (\eta_h^* - \eta_d^*)\, \delta^*] \, .$$

Then, we divide x^* into two parts: the part supported by PoW, x^{k*}, and the part supported by PoS, $x^{\delta *}$. That is, we denote

$$x^{k*} = \left[\sigma^* \frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*} + (1-\sigma^*)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right] k^* \geq 0, \tag{28}$$

$$x^{\delta *} = \left[\sigma^* \frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*} + (1-\sigma^*)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right] (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* \geq 0, \tag{29}$$

then

$$x^* = x^{k*} + x^{\delta *}. \tag{30}$$

Note that x^{k*} and $x^{\delta *}$ are well-defined because $\hat{\theta}_d^* > 0$. We construct a simple honest mechanism $\mathbf{M}^\dagger$ with target value x^*, and $k^\dagger$ and $\delta^\dagger$ are constructed to satisfy

$$x^{k*} = \frac{\alpha_h^s}{\theta_d^s} k^\dagger, \tag{31}$$

$$x^{\delta *} = \frac{\alpha_h^s}{\theta_d^s} [\eta_h^s - \eta_d^s]\, \delta^\dagger. \tag{32}$$

By (30), (31), (32), and $\alpha_h^s = 1$, we have $k^\dagger + (\eta_h^s - \eta_d^s)\, \delta^\dagger = \theta_d^s x^*$. Let $\mathbf{S}^\dagger = (\hat{z}^\dagger, \sigma^\dagger)$ such that $\hat{z}^\dagger = x^*$, $\sigma^\dagger = 1$, then $\tilde{x}(\hat{z}^\dagger, \sigma^\dagger) = x^*$, and that is, the DM production in $\mathbf{E}^\dagger$ is equal to the DM production in $\mathbf{E}^*$. We first show that $\mathbf{E}^\dagger = (\mathbf{M}^\dagger, \mathbf{S}^\dagger)$ is an equilibrium, then we show that $\mathbf{E}^\dagger$ generates weakly higher welfare than $\mathbf{E}^*$ does.

(a) To show that $\mathbf{E}^\dagger$ is an equilibrium, we first show that $\mathbf{E}^\dagger$ satisfies the participation constraint (16), and that is, we need to show that

$$-x^* - (1-\beta)\delta^\dagger - \beta k^\dagger + \beta u(x^*) \geq 0 \tag{33}$$

First, because $\mathbf{E}^*$ is an equilibrium, $\mathbf{E}^*$ must satisfy (15) and (16). Combining (15) and (16), we have

$$\begin{aligned}&-\left\{\sigma\left[\alpha_h(\hat{z})\hat{z} + \eta_h(\hat{z})\delta\right] + (1-\sigma)\left[\left(\alpha_d(\hat{z}) + \theta_d(\hat{z})\right)\hat{z} + \eta_d(\hat{z})\delta\right]\right\} \\ &+\beta\left\{\begin{array}{l} u\left[\sigma\alpha_h(\hat{z})\hat{z} + (1-\sigma)\alpha_d(\hat{z})\hat{z}\right] - k \\ +\sigma\left[\eta_h(\hat{z})\delta\right] + (1-\sigma)\left[-k + \theta_d(\hat{z})\hat{z} + \eta_d(\hat{z})\delta\right]\end{array}\right\} \geq 0.\end{aligned} \tag{34}$$

Then $\mathbf{E}^*$ satisfies the new participation constraint (34). Because $\sigma^*\hat{\alpha}_h^*\hat{z}^* + (1-\sigma^*)\hat{\alpha}_d^*\hat{z}^* = x^*$ and $\hat{\theta}_d^*\hat{z}^* = k^* + \left(\hat{\eta}_h^* - \hat{\eta}_d^*\right)\delta^*$, by the new participation constraint (34), $\mathbf{E}^*$ must satisfy the following inequalities:

$$\begin{aligned}&-x^* + \beta u\left(x^*\right) - (1-\beta)\left\{\sigma^*\hat{\eta}_h^*\delta^* + (1-\sigma^*)(\hat{\theta}_d^*\hat{z} + \hat{\eta}_d^*\delta^*)\right\} - \beta\left[k^* + (1-\sigma^*)k^*\right] \geq 0 \\ &\Leftrightarrow -x^* + \beta u\left(x^*\right) - (1-\beta)\left\{\sigma^*\hat{\eta}_h^*\delta^* + (1-\sigma^*)\left[k^* + \left(\hat{\eta}_h^* - \hat{\eta}_d^*\right)\delta^* + \hat{\eta}_d^*\delta^*\right]\right\} - \beta\left[k^* + (1-\sigma^*)k^*\right] \geq 0 \\ &\Leftrightarrow -x^* + \beta u\left(x^*\right) - (1-\beta)\left\{\sigma^*\hat{\eta}_h^*\delta^* + (1-\sigma^*)\left[k^* + \hat{\eta}_h^*\delta^*\right]\right\} - \beta\left[k^* + (1-\sigma^*)k^*\right] \geq 0 \\ &\Leftrightarrow -x^* + \beta u\left(x^*\right) - (1-\beta)\hat{\eta}_h^*\delta^* - (1-\sigma^* + \beta)k^* \geq 0\end{aligned} \tag{35}$$

By (35), to show that (33) holds, it is sufficient to show that $\delta^\dagger \leq \hat{\eta}_h^*\delta^*$ and $k^\dagger \leq k^*$. First, we show that $k^\dagger \leq k^*$: by (28) and (31),

$$k^\dagger = \frac{\left[\sigma^*\frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*} + (1-\sigma^*)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right]}{\frac{\alpha_h^s}{\theta_d^s}}k^*. \tag{36}$$

Moreover, we have

$$\begin{aligned}\frac{\alpha_h^s}{\theta_d^s} &= \frac{1}{r_b} \geq \frac{\hat{p}_1^*}{\hat{p}_1^* r_b + \hat{p}_2^* r_{sb}} = \frac{\alpha_h^*}{\theta_d^*} \\ \frac{\alpha_h^s}{\theta_d^s} &= \frac{1}{r_b} \geq \frac{r_s}{r_b} \geq \frac{\hat{p}_1^* r_s + \hat{p}_2^* r_{sb}}{\hat{p}_1^* r_b + \hat{p}_2^* r_{sb}} = \frac{\alpha_d^*}{\theta_d^*}\end{aligned}$$

Therefore,

$$\frac{\left[\sigma^*\frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*}+(1-\sigma^*)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right]}{\frac{\alpha_h^s}{\theta_d^s}}\leq 1, \tag{37}$$

and thus by (36),

$$k^\dagger \leq k^*. \tag{38}$$

Second, we show that $\delta^\dagger = \eta_h^s\delta^\dagger \leq \hat{\eta}_h^*\delta^*$: 1) For $\hat{\eta}_h^* > 0$: then $\hat{q}_1^* > 0$. By (29) and (32),

$$\eta_h^s\delta^\dagger = \frac{\left[\sigma\frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*}+(1-\sigma)\frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right]}{\frac{\alpha_h^s}{\theta_d^s}}\frac{\frac{\hat{\eta}_h^*-\hat{\eta}_d^*}{\hat{\eta}_h^*}}{\frac{\eta_h^s-\eta_d^s}{\eta_h^s}}\eta_h^*\delta^*.$$

Note that $\hat{\eta}_h^* - \hat{\eta}_d^* \geq 0$ if and only if $\hat{q}_1^* \geq \hat{q}_2^* \geq 0$, so

$$\frac{\hat{\eta}_h^*-\hat{\eta}_d^*}{\hat{\eta}_h^*} = \frac{\hat{q}_1^*-\hat{q}_2^*}{\hat{q}_1^*}r_{sb} \leq r_{sb} = \frac{\eta_h^s-\eta_d^s}{\eta_h^s}, \tag{39}$$

and therefore, by (37) and (39), we have $\delta^\dagger = \eta_h^s\delta^\dagger \leq \hat{\eta}_h^*\delta^*$. 2) For $\hat{\eta}_h^* = 0$: Because $\hat{\eta}_h^* - \hat{\eta}_d^* \geq 0$, we have $\hat{\eta}_h^* - \hat{\eta}_d^* = 0$, so $x^{\delta *} = 0$ and thus $\delta^\dagger = 0$. As a consequence, $\delta^\dagger = 0 \leq \hat{\eta}_h^*\delta^*$.

Thus, $\mathbf{E}^\dagger$ satisfies the participation constraint (33), so by Proposition 1, $\mathbf{E}^\dagger$ is a simple honest equilibrium.

(b) Given the social welfare function in the monetary equilibrium, (18), because $x^\dagger = x^*$, $\sigma^\dagger = 1$, and by (38), the simple honest equilibrium $\mathbf{E}^\dagger$ generates weakly higher welfare than $\mathbf{E}^*$ does.

To summarize, by (a) and (b), we construct a simple honest equilibrium $\mathbf{E}^\dagger$ weakly dominating $\mathbf{E}^*$.

Step 2. $\hat{\eta}_h^* - \hat{\eta}_d^* < 0$:

We denote x^{k*} and $x^{\delta *}$ as in (28) and (29). Because $\hat{\eta}_h^* - \hat{\eta}_d^* < 0$, we have $x^{\delta *} \leq 0$ and $x^{k*} \geq x^*$. We construct a simple honest mechanism $\mathbf{M}^\dagger$ with target value x^*, and let $k^\dagger$

satisfies $x^* = \frac{\alpha_h^s}{\theta_d^s} k^\dagger$, and $\delta^\dagger = 0$. Because $\alpha_h^s = 1$, we have $k^\dagger + (\eta_h^s - \eta_d^s)\, \delta^\dagger = \theta_d^s x^*$. Thus,

$$k^\dagger = \frac{x^*}{\frac{\alpha_h^s}{\theta_d^s}} \leq \frac{x^{k*}}{\frac{\alpha_h^s}{\theta_d^s}} = \frac{\left[\sigma^* \frac{\hat{\alpha}_h^*}{\hat{\theta}_d^*} + (1-\sigma^*) \frac{\hat{\alpha}_d^*}{\hat{\theta}_d^*}\right]}{\frac{\alpha_h^s}{\theta_d^s}} k^*$$

Thus, we have $k^\dagger \leq k^*$ and $\hat{\eta}_h^* \delta^\dagger \leq \hat{\eta}_h^* \delta^*$. Then we use the same argument as in **Step 1** to show that $\mathbf{E}^\dagger = (\mathbf{M}^\dagger, \mathbf{S}^\dagger)$ is a simple honest equilibrium which has weakly higher welfare than $\mathbf{E}^*$ does.

Case 2: $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* > \theta_d^* \hat{z}^*$: Note that $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* > \hat{\theta}_d^* \hat{z}^*$ implies $\sigma^* = 1$. In this case, PoW and a PoS are higher than the required size to prevent fraud, so we can decrease k and δ until the buyers are indifferent about double spending or not and preserve the same DM production. Let $\bar{z} = \frac{k^*}{\hat{\theta}_d^*} + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \frac{\delta^*}{\theta_d^*} > \hat{z}^*$. We construct a mechanism $\mathbf{M}'$ such that $k' = \frac{\hat{z}^*}{\bar{z}} k^* \leq k^*$, $\delta' = \frac{\hat{z}^*}{\bar{z}} \delta^* \leq \delta^*$, $P'(\hat{z}) = P^*(\hat{z}), Q'(\hat{z}) = Q^*(\hat{z})$, and a strategy $\mathbf{S}' = (\hat{z}', \sigma')$ such that $\hat{z}' = \hat{z}^*$ and $\sigma' = 1$. Then the DM production in $\mathbf{E}' = (\mathbf{M}', \mathbf{S}')$ is the same as in $\mathbf{E}^* = (\mathbf{M}^*, \mathbf{S}^*)$, but the cost of PoW and PoS are smaller in $\mathbf{E}'$ than in $\mathbf{E}^*$. Thus, the welfare in $\mathbf{E}'$ is weakly higher than in $\mathbf{E}^*$, and $\mathbf{E}'$ also satisfies the participation constraint (34). Moreover, by our construction, $k' + (\eta_d'(\hat{z}') - \eta_d'(\hat{z}'))\, \delta' = \theta_d'(\hat{z}')\hat{z}'$, so we can apply the same argument as in **Case 1** to construct a simple honest equilibrium $\mathbf{E}^\dagger$ which generates weakly higher welfare than $\mathbf{E}'$ does. Therefore, the welfare of the simple honest equilibrium $\mathbf{E}^\dagger$ is also weakly higher than the welfare of $\mathbf{E}^*$. Note that $\mathbf{E}'$ may not be an equilibrium because it may not satisfy the optimality condition (14), but we only apply $\mathbf{E}'$ as a medium to compare the simple honest equilibrium $\mathbf{E}^\dagger$ with the equilibrium $\mathbf{E}^*$.

Case 3: $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* < \hat{\theta}_d^* \hat{z}^*$:

Because k and δ are not high enough to prevent double spending, we can just set k and δ to be zero and to save for the cost of PoW and PoS and achieve the same DM production. Because $k^* + (\hat{\eta}_h^* - \hat{\eta}_d^*)\, \delta^* < \hat{\theta}_d^* \hat{z}^*$, we must have $\sigma^* = 0$, so the DM production is $x^* = \hat{\alpha}_d^* \hat{z}^*$. In the following discussion, we construct a simple double spending equilibrium weakly dominates $\mathbf{E}^*$. Let $\mathbf{M}^\dagger$ be a simple double spending mechanism with target value $\frac{x^*}{\alpha_d^s}$, and $\mathbf{S}^\dagger = (\hat{z}, \sigma)$ such that $\hat{z} = \frac{x^*}{\alpha_d^s}, \sigma = 0$, and let $\mathbf{E}^\dagger = \left(\mathbf{M}^\dagger, \mathbf{S}^\dagger\right)$.

(a) We first show that $\mathbf{E}^\dagger$ satisfies the participation constraint (16). That is, we need to show that

$$-\left[1+(1-\beta)\frac{\theta_d^s}{\alpha_d^s}\right]x^*+\beta u\left(x^*\right)\geq 0$$

Because $\mathbf{E}^*$ is an equilibrium, it must satisfy the constraint (34), and that is,

$$-\left[1+(1-\beta)\frac{\hat{\theta}_d^*}{\hat{\alpha}_d^*}\right]x^*-(1-\beta)\,\hat{\eta}_d^*\delta-2\beta k^*+\beta u\left(x^*\right)\geq 0.$$

Because $\frac{\theta_d^s}{\alpha_d^s}=\frac{r_b}{r_s}\leq\frac{\hat{p}_1^* r_b+\hat{p}_2^* r_{sb}}{\hat{p}_1^* r_s+\hat{p}_2^* r_{sb}}=\frac{\hat{\theta}_d^*}{\hat{\alpha}_d^*}$, $\left(\mathbf{M}^\dagger,\mathbf{S}^\dagger\right)$ satisfies the participation constraint (16). Thus, by Proposition 2, $\mathbf{E}^\dagger$ is a simple double spending equilibrium.

(b) Because the DM production in $\mathbf{E}^\dagger$ is equal to x^* and $k^\dagger=0$, the welfare in $\mathbf{E}^\dagger$ is weakly higher than in $\mathbf{E}^*$. Thus, $\mathbf{E}^\dagger$ is a simple double spending equilibrium that weakly dominates $\mathbf{E}^*$.

C Figures

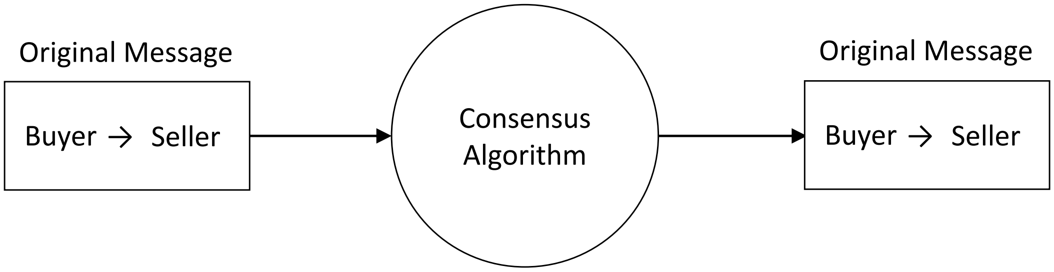

Figure 1: Consensus algorithm: honest

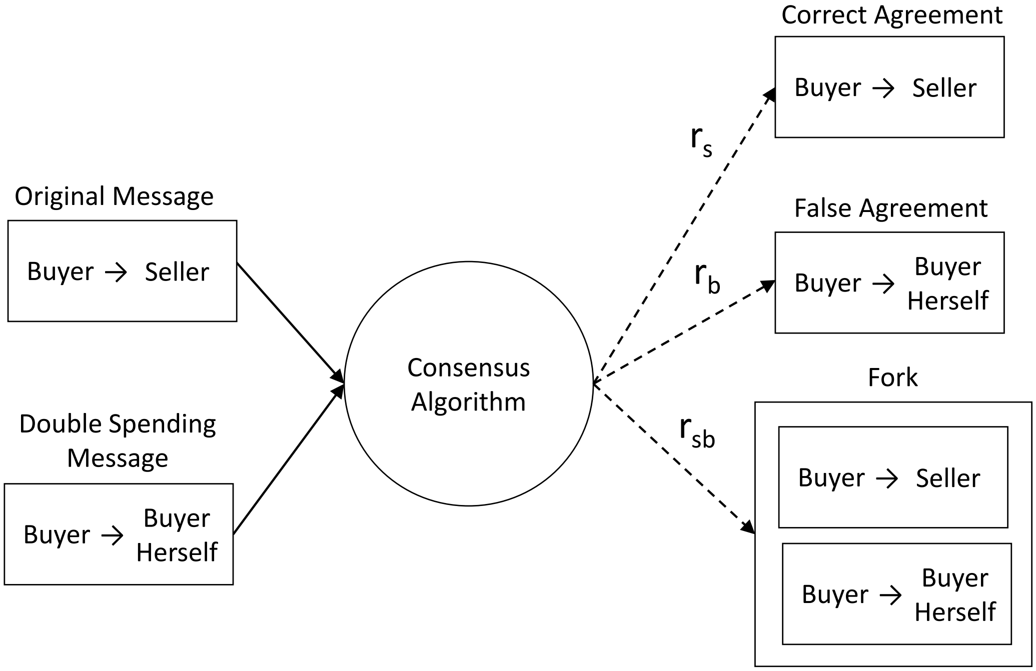

Figure 2: Consensus algorithm: double spending

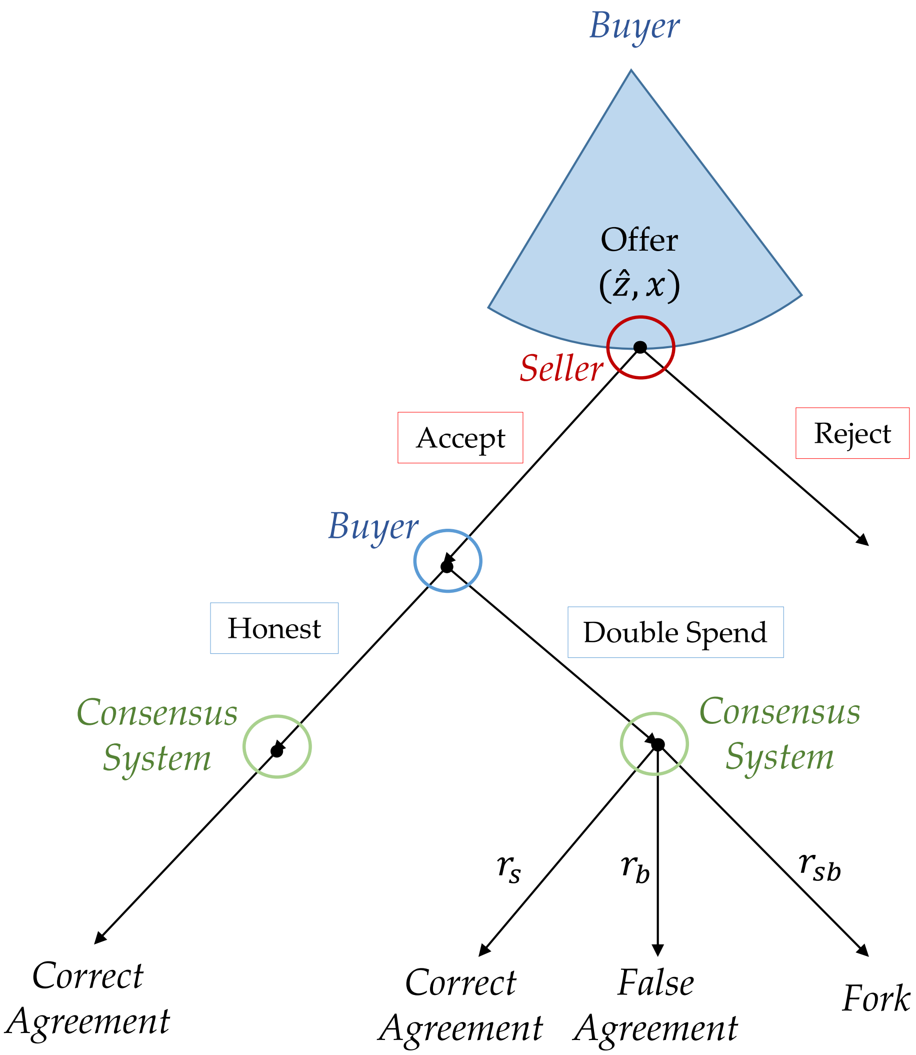

Figure 3: The Game Tree

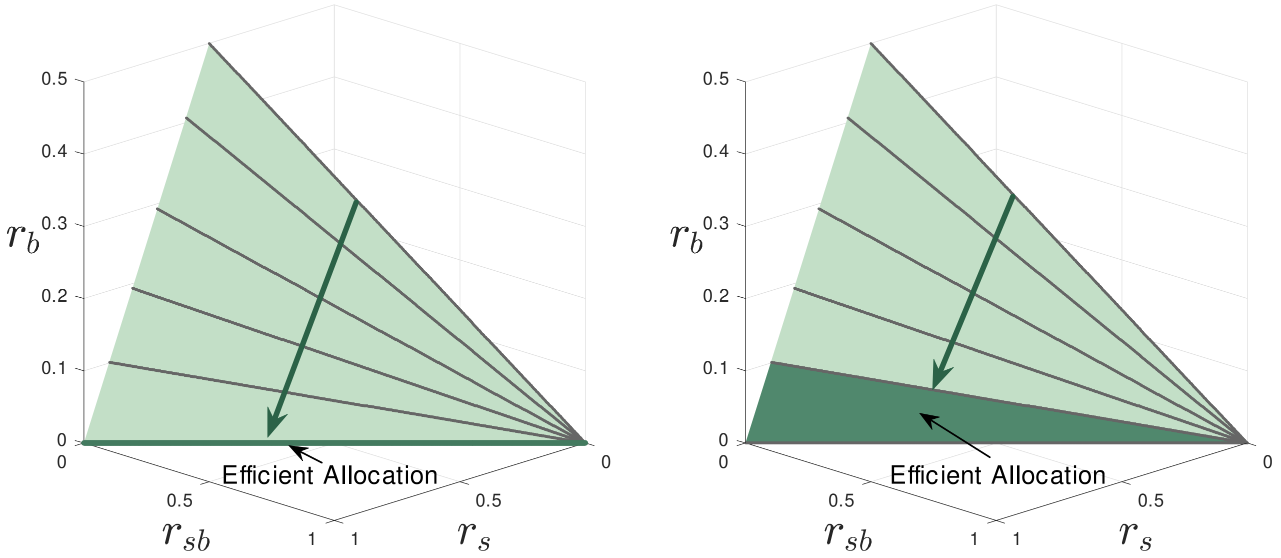

Figure 4: Iso-welfare of optimal simple double spending equilibrium. Which of the arrows represents the direction through which welfare increases. Left graph: the participation constraint is binding in the social planner's problem ($\zeta = 0.11$, $\beta = 0.9$). Right graph: the participation constraint is nonbinding in the social planner's problem ($\zeta = 0.05$, $\beta = 0.9$).

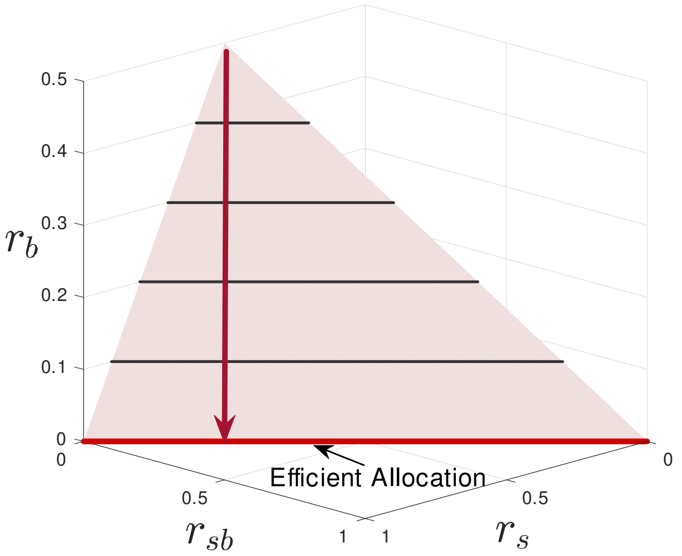

Figure 5: Iso-welfare of optimal pure proof-of-work mechanism. Which of the arrows represents the direction through which welfare increases. The iso-welfare curves in proof-of-work equilibrium exhibit the same pattern given the IR in the social planner's problem is binding or not.

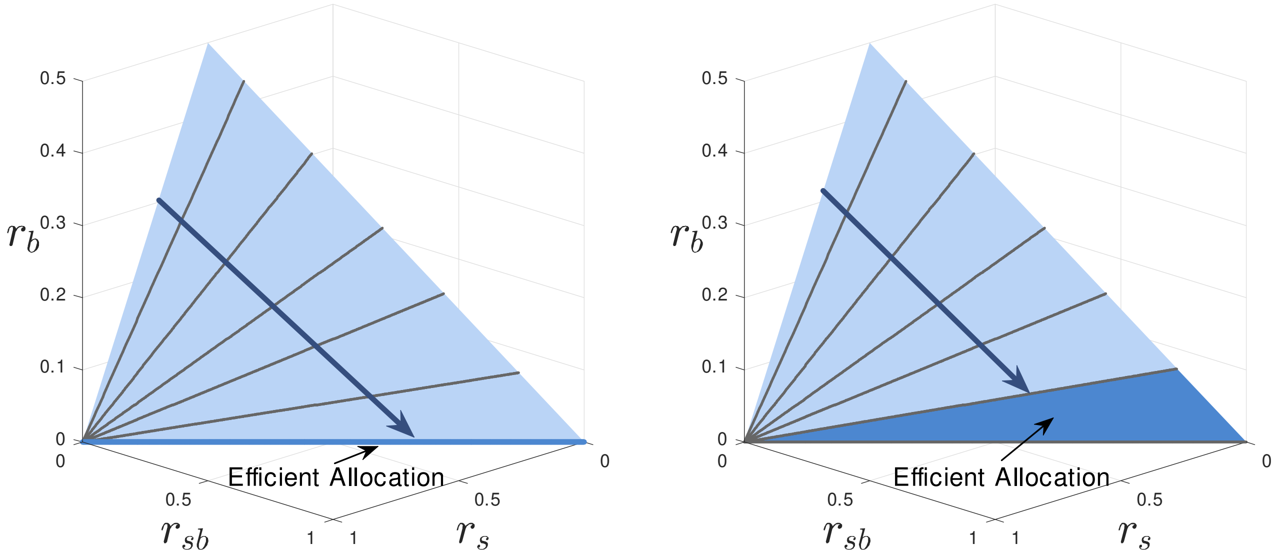

Figure 6: Iso-welfare of optimal pure proof-of-stake mechanism. Which of the arrows represents the direction through which welfare increases. Left graph: the participation constraint is binding in the social planner's problem ($\zeta = 0.11$, $\beta = 0.9$). Right graph: the participation constraint is nonbinding in the social planner's problem ($\zeta = 0.05$, $\beta = 0.9$).

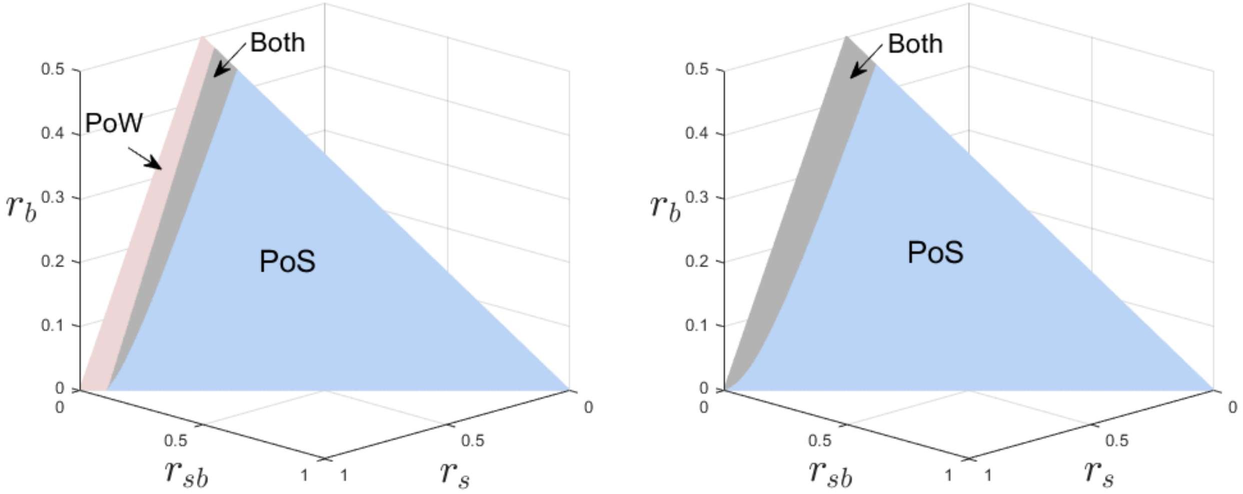

Figure 7: Optimal Simple Honest Mechanism: pink area: proof-of-work only; blue area: proof-of-stake only; gray area: both proof-of-work and proof-of-stake are applied. Left graph: the participation constraint is binding in the social planner's problem ($\zeta = 0.11$, $\beta = 0.9$). Right graph: the participation constraint is nonbinding in the social planner's problem ($\zeta = 0.05$, $\beta = 0.9$).

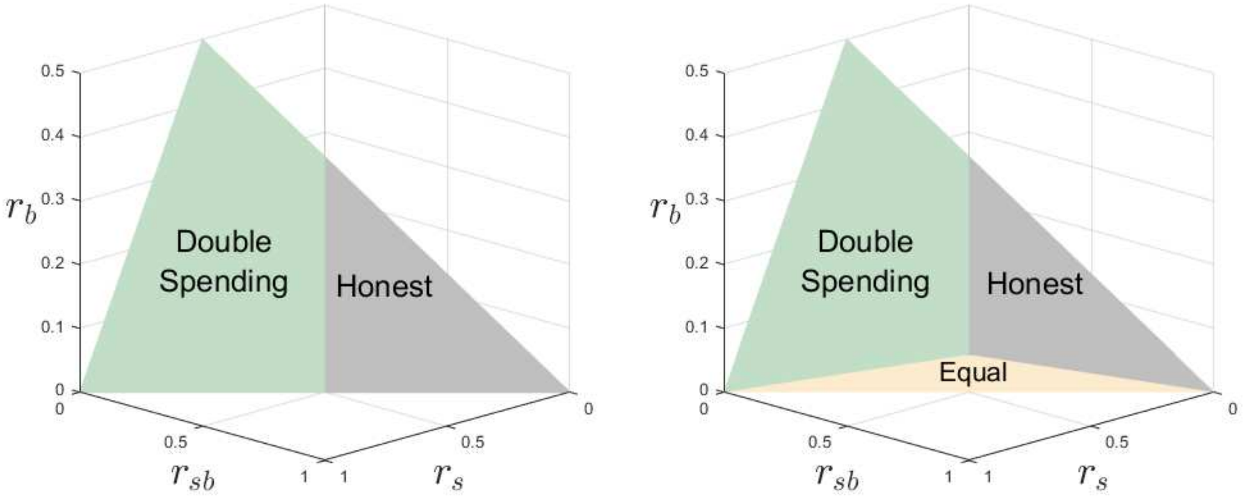

Figure 8: Optimal Mechanism: gray area: optimal honest equilibrium dominates optimal double spending equilibrium; green area: optimal double spending equilibrium dominates optimal honest equilibrium proof-of-stake only; yellow area: optimal honest and optimal double spending equilibrium are equal and both achieve efficient allocation. Left graph: the participation constraint is binding in the social planner's problem ($\zeta = 0.11$, $\beta = 0.9$). Right graph: the participation constraint is nonbinding in the social planner's problem ($\zeta = 0.05$, $\beta = 0.9$).