Working Paper Series

The Cost of Information in the Blockchain: A Discussion of Routledge and Zetlin-Jones (2018)

WP 21-02

Bruno Sultanum
Federal Reserve Bank of Richmond

FEDERAL RESERVE BANK OF RICHMOND®
Richmond ▪ Baltimore ▪ Charlotte

The Cost of Information in the Blockchain[*]

A Discussion of Routledge and Zetlin-Jones (2018)

Bruno Sultanum

The Federal Reserve Bank of Richmond

January 21, 2021

Abstract

The volatility of crypto currencies hinders their ability to be media of exchange or stores of value, leading to the implementation of exchange-rate pegs in an attempt to stabilize these currencies. This strategy has been used by crypto currencies such as US Dollar Tether, Steem Backed Dollar and TrueUSD; and was previously adopted in countries such as Brazil, Mexico and Argentina. However, an exchange-rate peg is vulnerable to speculative attacks if it is not 100% backed by reserves, as discussed in Obstfeld (1996). Using insights from the bank-run literature, Routledge and Zetlin-Jones (2018) build on Green and Lin (2003) and propose a model of speculative attacks. They show that adjustments to the exchange rate can prevent speculative attacks in equilibrium. They also show how to implement such contracts using blockchain technology. In this discussion paper, I provide a cautionary tale. I show also in a version of Green and Lin (2003) that the information content in the blockchain prevents agents from attaining all the gains from risk sharing—highlighting the downsides of too much public information.

[*]Contact: Bruno Sultanum: bruno@sultanum.com. The views expressed are those of the author and not necessarily those of the Federal Reserve Bank of Richmond or the Federal Reserve System.

1 Introduction

Crypto currencies tend to be extremely volatile, which hinders their ability to be media of exchange or stores of value. A common solution to reduce exchange-rate volatility is to peg the exchange rate. This solution has been previously used in countries such as Brazil, Mexico and Argentina, and is currently being used by managers of crypto currencies such as US Dollar Tether, Steem Backed Dollar and TrueUSD. However, as pointed out in Obstfeld (1996), an exchange-rate peg is vulnerable to speculative attacks if it is not 100% backed by reserves. These attacks are similar in spirit to bank runs caused by a fixed redemption rate, and Routledge and Zetlin-Jones (2018) build on Green and Lin (2003) to show how the same approach used to prevent bank runs can also be used to prevent speculative attacks on exchange-rate pegs.

In the Green and Lin (2003) setting, Routledge and Zetlin-Jones (2018) propose a sophisticated contract, which arguably is more adequate in the context of crypto currencies. The reason for this is twofold. First, it is a complex contract that would be hard to implement if not by a script. Second, and more importantly, it requires commitment. Ennis and Keister (2009a) have shown that common solutions to bank runs fail in a setting where the planner cannot commit to a payment scheme. This can happen even with a benevolent planner. One could imagine the same issue would arise here, but with crypto currencies, this is not a problem. Once the contract is coded into the blockchain, there is no going back. The decentralized nature of the ledger serves as a commitment device.

Encoding smart contracts in a decentralized ledger creates a new world of possibilities. As mentioned before, commitment is not a problem since individual parties cannot change the code, and the contracts can be made very complex. This allows governments, firms and individuals to issue and invest in extremely contingent liabilities. And the processes of issuing and investing both become simpler since they do not rely on a legal infrastructure. In principle, anyone can write (or buy) a smart contract in a platform such as Ethereum—making smart contracts accessible to the general public.[1]

[1]For reference, Routledge and Zetlin-Jones (2018) have a great online tutorial and GitHub repository that can help anyone to get started on programming their own smart contracts.

There are difficulties associated with smart contracts, too. Many of them are technical. For example, how to link the outside world with the blockchain? If you are financing a house or investing in US treasuries, how do you post it as collateral? If you have to add an intermediary, such as a bank or other legal entity, the process could undermine some of the advantages of smart contracts.

In this discussion paper, I put aside the technical difficulties related to smart contracts and focus on a problem with more economic content—the incentives of agents associated with the information structure. In particular, I focus on how the information content in smart contracts can limit agents' ability to share risk. Smart contracts are implemented in decentralized ledgers and are public information. However, in order to implement constrained efficient allocations, it might be desirable to reduce the information agents have because their actions have to be incentive compatible for each possible information set available to them. As a result, by giving more information, the contract increases the number of incentive constraints that have to be satisfied, which potentially decreases the set of implementable allocations and welfare.

Building also on the bank model of Green and Lin (2003), I illustrate this point using a variation of their model with only a small change to preferences and the distribution of shocks. These changes can be understood as a generalization of Green and Lin (2003) and follow more closely Andolfatto et al. (2017). I then compare two versions of the model–one in which depositors observe the redemption decisions of other depositors and one in which they do not observe.

The interpretation of these two different information structures is that if the contract is implemented by an intermediary, such as a bank, it has the option to reveal or not what the redemption rates are. However, if the contract is decentralized, using blockchain technology through a smart contract, the redemption rates are always observed since they are written in the decentralized ledger. I show how the constrained efficient allocation in the economy where depositors have information on redemption rates can always be implemented in the economy without information, but not the other way around. As a result, agents have higher expected utility when the contract reveals less information.

It is worth mentioning that Cong and He (2019) also point out that more information embedded in smart contracts can lead to lower welfare. However, the mechanism that they highlight is different. In Cong and He (2019), more information allows firms to punish deviations and make it easier for firms to collude, which can harm consumers. So the extra information improves firms' profits but at the expense of other agents in the economy. Here, as we show, every agent can end up being *ex ante* worse off. That is because the information limits the ability of agents to engage in risk-sharing contracts.

The bank-run literature has studied different information structures. The information structure in Green and Lin (2003) has agents knowing their queue position—but not the previous announcements—while Andolfatto et al. (2007) study a setting where agents know the history of announcements, in addition to knowing their queue positions, and the information structure in Peck and Shell (2003) is one where agents do not have any information besides their own types. Follow-up papers have mostly considered one of these information structures. Ennis and Keister (2009b) share the same information structure as Green and Lin (2003) when studying the role of independent types, while Andolfatto and Nosal (2008) share the information structure as Peck and Shell (2003) when studying the incentives of self-interested banks, and Cavalcanti et al. (2011) compare the welfare associated with these two information structures in large economies. Finally, Nosal and Wallace (2009) and, more recently, Huang (2021) study optimal information disclosure. While these papers focus on the existence of bank runs, my focus here is simply to point out how the information structure embedded in a blockchain can make the optimal risk-sharing arrangement impossible to implement.

Finally, I emphasize that it is understood in the literature that information disclosure can reduce the set of implementable allocations in general, and that this is true in some versions of the Diamond and Dybvig (1983) model—which is implied by some of the numerical examples in Nosal and Wallace (2009). The contribution I make in this discussion paper is not to point this out, but to relate this finding to the information structure embedded in blockchains.

The paper is organized as follows. Section 2 describes the environment; Section 3 discusses the two information structures, defines the incentive compatibility constraints and the optimal allocation problem for each one; Section 4 provides the main results; Section 5 concludes; and Appendix A provides the proofs.

2 Environment

To better understand how information changes agents' incentives, I consider a generalized version of Green and Lin (2003) along the lines of Andolfatto et al. (2017).

There are three dates: 0, 1 and 2. There are $N \geq 1$ agents in the economy, and each one is endowed with Y/N units of date-1 good. A constant returns to scale investment technology transforms y units of date-1 goods into $yR > y$ units of date-2 goods, where $R > 1$. All resources are deposited in a bank, or retained virtually using a smart contract, and agents make withdrawal decisions in sequence.

Agents are *ex ante* identical, and on date 1 turn out to be one of two types: $t \in T = \{1, 2\}$. As usual in the literature, I label a type $t = 1$ agent "impatient" and a type $t = 2$ agent "patient." Agents privately observe their own types. The utility function for an impatient agent is $U(c^1, c^2; 1) = u(c^1)$, and the utility function of a patient agent is $U(c^1, c^2; 2) = \rho u(c^1 + c^2)$, where c^1 is date-1 consumption and c^2 is date-2 consumption. The number of patient agents is drawn from the distribution $\pi = (\pi_0, \ldots, \pi_N)$, where $\pi_n \in (0, 1)$ is the probability that there are $n \in \mathbb{N} \equiv \{0, 1, \ldots, N\}$ patient agents.

Agents take action in sequence according to a queue, which the literature refers to as the sequential service constraint. Following the notation in Andolfatto et al. (2017), a queue is a vector $t^N = (t_1, \ldots, t_N) \in T^N$, where $t_k \in T$ is the type of the agent who occupies the k^{th} queue position. Let $P_n = \{t^N \in T^N | \ p(t^N) = n\}$ and $Q_n(t^N) = \{j \mid t_j = 2 \text{ for } t^N \in P_n\}$, where $p(t^N) = \sum_n t_n - N$ denotes the number of patient agents in the queue t^N. That is, P_n is the set of queues with n patient agents, and $Q_n(t^N)$ is the set of queue positions of the n patient agents in queue $t^N \in P_n$. For simplicity, we omit the argument t^N in the function $Q_n(t^N)$ throughout the paper.

All queues with n patient agents are equally likely, so the probability of a queue $t^N \in P_n$ is $\pi_n / \binom{N}{n}$, where the binomial $\binom{N}{n}$ is the number of queues $t^N \in P_n$. Agents are randomly assigned to queue positions, where the unconditional probability that an agent is assigned to position k is $1/N$. I label an agent assigned to position k as agent k. The queue realization, t^N, is observed by no one; not by the agents nor the planner.

Figure 1: Sequence of Actions (Andolfatto et al. (2017)).

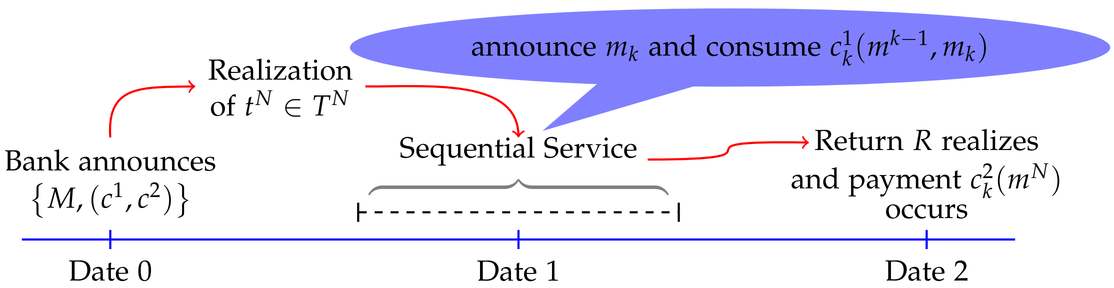

Figure 1 depicts the sequence of actions, which is extracted from Andolfatto et al. (2017). At date 0, the planner constructs a mechanism that determines how date-1 and date-2 consumption are allocated among the N agents. A mechanism consists of a set of announcements, M, and an allocation rule, $c = (c^1, c^2)$, where $c^1 = (c^1_1, \ldots, c^1_N)$ and $c^2 = (c^2_1, \ldots, c^2_N)$. We focus on direct mechanism so the set of announcements is just the agents' types (that is, $M = T$). Agents meet the planner sequentially on date 1, and each agent k makes an announcement $m_k \in M$. Due to the sequential service constraint, the planner allocates date-1 consumption to agent k based on the announcements of agents $j \leq k$, (m^{k-1}, m_k), where $m^{k-1} = (m_1, \ldots, m_{k-1})$, and each agent k consumes $c^1_k(m^{k-1}, m_k)$ from his date-1 meeting with the planner. Date 1 ends after all agents meet the planner, and there is one meeting on date 2 to pay $c^2 = (c^2_1, \ldots, c^2_N)$.

Finally, the expected utility of an agent (before she learns his type) associated with allocation rule $c = (c^1, c^2)$ when agents announce truthfully $m = (t_1, \ldots, t_N)$ is

$$\mathbb{E}\{U[c^1_k(t^{k-1}, t_k)\}, c^2_k(t^N); t_k], \tag{1}$$

where the expectation is taking over the queue realizations $t^N \in T^N$, and for any vector $x^N = (x_1, \ldots, x_N)$, x^j_i denotes $(x_i, \ldots, x_j)$. The allocation rule $c = (c_1, c_2)$ is feasible, or resource feasible, if

$$\sum_{k=1}^{N} [Rc^1_k(t^{k-1}, t_k) + c^2_k(t^N)] \leq RY \tag{2}$$

for all possible queue realizations $t^N \in T^N$.

3 Comparing information structures

One disadvantage of implementing a risk-sharing arrangement in a blockchain is that the information on payments is public as part of the decentralized ledger. In the context of the current model, this means that when agent k makes an announcement $m_k \in M$, she knows his queue position k as well as the previous announcements m^{k-1}. In contrast, if the arrangement is implemented by a centralized institution, such as a bank, it has the option to conceal such information from agents.

In this section, I compare the optimal mechanisms under these two information structures. I start with the case where agents do not observe their queue position and previous announcements, which I label the bank information structure. Then I study the case where agents observe their queue position and previous announcements, which I label the blockchain information structure.

3.1 The bank information structure

The problem described here is the same as in Section 3 of Andolfatto et al. (2017). Under the bank information structure, each agent k makes an announcement $m_k(t_k) \in M$ as a function of his type t_k. An allocation rule c must be incentive-compatible—that is, no agent k has reason to announce $m_k(t_k) \neq t_k$. Since an impatient agent k only values date-1 consumption, she always announces $m_k(1) = 1$. A patient agent k has no incentive to defect from the strategy $m_k(2) = 2$, assuming that other agents announce truthfully, if

$$\mathbb{E}_k\Big\{\mathbb{E}_{t^N|t^k=2}\Big\{u[c_k^1(t^{k-1},2) + c_k^2(t^N)] - u[c_k^1(t^{k-1},1) + c_k^2(t^{k-1},1,t_{k+1}^N)]\Big\}\Big\} \geq 0, \tag{3}$$

where the expectation is taking over the queue position of the agent k, and the possible queue realizations $t^N \in T^N$ conditional on agent k type $t^k = 2$.

Definition 1. *The best allocation rule under the bank information structure, $c^{bk} = (c_1^{bk}, c_2^{bk})$, achieves the maximum of equation* (1), *with $m_k = t_k$ for all $k \in \mathbb{N}$, subject to the resource* *constraint* (2) *and the bank incentive compatibility constraint* (3).

3.2 The blockchain information structure

Under the blockchain information structure, each agent k makes an announcement $m_k(t_k; m^{k-1}) \in M$ as a function of his type t_k and the previous announcement from other agents, m^{k-1}. As in the previous section, since an impatient agent k only values date-1 consumption, she announces $m_k(1; m^{k-1}) = 1$ for any possible $m^{k-1} \in T^{k-1}$. A patient agent k has no incentive to defect from the strategy $m_k(2; m^{k-1}) = 2$, assuming that other agents announce truthfully, if

$$\mathbb{E}_{t^N|(t^{k-1},2)}\left\{u[c_k^1(t^{k-1},2) + c_k^2(t^N)] - u[c_k^1(t^{k-1},1) + c_k^2(t^{k-1},1,t_{k+1}^N)]\right\} \geq 0, \tag{4}$$

where the expectation is taking over the possible queue realizations $t^N \in T^N$ conditional on agent k type $t^k = 2$, and the type of previous agents t^{k-1}.

Definition 2. *The best allocation rule under the blockchain information structure, $c^{bc} = (c_1^{bc}, c_2^{bc})$, achieves the maximum of equation* (1)*, with $m_k = t_k$ for all $k \in \mathbb{N}$, subject to the resource constraint* (2) *and the blockchain incentive compatibility constraint* (4).

4 Main result

A risk-sharing arrangement is *ex ante* beneficial to all agents; however, they may not have incentives to truthfully reveal the realization of preference shocks *ex post*. In order to guarantee agents truthfully reveal the preference shocks, the contract has to satisfy an incentive compatibility constraint.

The information structure determines what this constraint looks like. Under the blockchain information structure, agents know their queue position k and the previous announcement m^{k-1}. As a result, for each possible realization of k and m^{k-1}, they only take expectation over the shock of agents $k' = k+1, \ldots, N$ later in the queue. Under the bank information structure, agents are not aware of their queue position k or the previous announcements m^{k-1}. As a result, they take expectation over both, as well as expectation on the shock of agents $k' = k+1, \dots, N$ later in the queue, when deciding whether it is worth it to misreport their preference shock. Since the bank incentive compatibility constraint takes expectation over each realization of k and m^{k-1}, it only has to satisfy it on average, while the blockchain incentive compatibility constraint has to be satisfied one by one—which implies the following result.

Proposition 1. *The expected utility given by equation* (1) *associated with the best allocation rule under the bank information structure, $c^{bk} = (c_1^{bk}, c_2^{bk})$, is at least as high as the one associated with the best allocation rule under the blockchain information structure, $c^{bc} = (c_1^{bc}, c_2^{bc})$.*

Proposition 1 is simple yet powerful. A planner would not want to give more information to its agents because that only adds more constraints to the mechanism-design problem. This could, in principle, reduce the welfare by limiting risk-sharing possibilities. But when does it actually reduce welfare? In the next proposition, I provide conditions under which the welfare in the blockchain information structure is strictly lower than in the bank information structure.

Proposition 2. *Assume that*

- *there are $N = 3$ agents;*
- *the distribution of patient agents in the economy is given by*

$$\pi = (\pi_0, \pi_1, \pi_2, \pi_3) = (\epsilon^2, \epsilon, \epsilon^2, 1 - \epsilon - 2\epsilon^2),$$

  where the parameter ϵ is in the interval $(0, 1/2)$;
- *the utility function $u(\cdot)$ is a CRRA with parameter $\gamma > 0$—that is, $u(x) = \frac{x^{1-\gamma}-1}{1-\gamma}$; and*
- *the parameters R and ρ satisfy the inequalities $0 < \left(\frac{3-R}{2}\right)^{\gamma} < R\rho < 1$.*

Then, there exists constant $\bar{\epsilon} > 0$ such that for all $\epsilon \in (0, \bar{\epsilon})$, the expected utility given by equation (1) *associated with the best allocation rule under the bank information structure, $c^{bk} = (c_1^{bk}, c_2^{bk})$, is strictly higher than the one associated with the best allocation rule under the blockchain information structure, $c^{bc} = (c_1^{bc}, c_2^{bc})$.*

5 Concluding remarks

In this discussion paper, I provide a cautionary tale on the unintended consequences of blockchain technology. When agents use decentralized ledgers to write and implement contracts, the information on agents' actions are necessarily public—distributed in the blockchain. This transparency can definitely be beneficial. However, in certain instances, too much information can hamper agents' abilities to implement risk-sharing arrangements. I exemplify this possibility in a bank model built on the Diamond and Dybvig (1983) literature. Specifically, I use the model in Andolfatto et al. (2017).

This result applies directly to Routledge and Zetlin-Jones (2018) since their basic model carries all the ingredients present in the bank-run literature. However, it is not intend to invalidate the use of blockchain to implement smart contracts in order to stabilize crypto currencies—or any other application of smart contracts. Whether the information available in the blockchain is a problem for agents or not will ultimately depend on details of the model, such as preferences and distributions, and the user of this technology should be aware of this risk when designing smart contracts.

References

Andolfatto, D. and E. Nosal (2008). Bank incentives, contract design and bank runs. *Journal of Economic Theory 142*(1), 28–47.

Andolfatto, D., E. Nosal, and B. Sultanum (2017). Preventing bank runs. *Theoretical Economics 12*(3), 1003–1028.

Andolfatto, D., E. Nosal, and N. Wallace (2007). The role of independence in the green–lin diamond–dybvig model. *Journal of Economic Theory 137*(1), 709–715.

Cavalcanti, R. d. O., J. D. P. Bertolai, and P. Monteiro (2011). A note on convergence of peck-shell and green-lin mechanisms in the diamond-dybvig model.

Cong, L. W. and Z. He (2019). Blockchain disruption and smart contracts. *The Review of Financial Studies 32*(5), 1754–1797.

Diamond, D. and P. Dybvig (1983). Bank runs, deposit insurance, and liquidity. *Journal of Political Economy 91*(3), 401–419.

Ennis, H. M. and T. Keister (2009a). Bank runs and institutions: The perils of intervention. *American Economic Review 99*(4), 1588–1607.

Ennis, H. M. and T. Keister (2009b). Run equilibria in the green–lin model of financial intermediation. *Journal of Economic Theory 144*(5), 1996–2020.

Green, E. J. and P. Lin (2003). Implementing efficient allocations in a model of financial intermediation. *Journal of Economic Theory 109*(1), 1–23.

Huang, X. (2021). Information disclosure and financial fragility. *Unpublished manuscript*.

Nosal, E. and N. Wallace (2009). Information revelation in the diamond-dybvig banking model. *Federal Reserve Bank of Chicago Policy Discussion Paper Series (December)*.

Obstfeld, M. (1996). Models of currency crises with self-fulfilling features. *European Economic Review 40*(3-5), 1037–1047.

Peck, J. and K. Shell (2003). Equilibrium bank runs. *Journal of Political Economy 111*(1), 103–123.

Routledge, B. and A. Zetlin-Jones (2018). Currency stability using blockchain technology. In *2018 Meeting Papers*, Volume 1160. Society for Economic Dynamics.

A Appendix: Proofs

Proof of Proposition 1: The bank incentive compatibility constraint (3) is a weighted average of all the blockchain incentive compatibility constraints of different realizations of k and m^{k-1}, given by equation (4). As a result, any allocation rule, $c = (c_1, c_2)$, that satisfies the constraint (4), must satisfy constraint (3)—including $c^{bc} = (c_1^{bc}, c_2^{bc})$. Since $c^{bc} = (c_1^{bc}, c_2^{bc})$ satisfies the constraints faced by the planner under the bank information structure, the choice of $c^{bk} = (c_1^{bk}, c_2^{bk})$ cannot yield a lower welfare. □

Proof of Proposition 2: First let us consider the first best. That is, the planner's problem without either incentive compatibility constraint—only the resource constraint. When patient agents announce they are patient, they receive zero in date-1 consumption. When either agent in queue position 1 or 2 is the first to announce he is an impatient type, the planner updates its beliefs using Bayes rule. The planner then assigns the value $\frac{1}{1+2\epsilon}$ to the probability of having 2 impatient agents. Note that we do not have to look into payments when the investor is the second to announce he is an impatient type because the probability of that happening is close to zero for ϵ small. That is, for ϵ small the probability of having 2 impatient agents is approximately 0, ex ante, and then it is approximately 1 conditional on having at least 1 impatient agent.

The optimal payment to the agent 1 and 2 who first announce he is an impatient type, $c_1^1(1) = c_2^1(2,1) = \bar{c}$, is approximately the solution of the equation

$$2u'(\bar{c}) = 2R\rho u'(R[3-2\bar{c}]) \quad \Longrightarrow \quad c_1^1(1) = c_2^1(2,1) = \bar{c} = \frac{3}{2+\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}}. \tag{5}$$

The optimal payment to the agent 3 who first announce he is an impatient type, $c_3^1(2,2,1)$, is approximately the solution of the equation

$$u'(c_3^1(2,2,1)) = R\rho u'(R[3-\bar{c}]/2) \quad \Longrightarrow \quad c_3^1(2,2,1) = \frac{3}{1+2\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}}. \tag{6}$$

Now let us show that this solution satisfies the bank incentive compatibility constraint. Because ϵ is small, the payoff to a patient agent who announces truthfully is approximately $\rho u(R)$. That is because she believes no other agent is an impatient type. If she deviates and announces she is an impatient type, she believes she will be the only impatient type announcement. As a result, for ϵ close to zero, the allocation is incentive compatible under the bank information structure if

$$u(R) > \frac{1}{3}u(c_1^1(1)) + \frac{1}{3}u(c_2^1(2,1)) + \frac{1}{3}u(c_3^1(2,2,1)) \iff$$
$$2[u(R) - u(\bar{c})] + [u(R) - u(c_3^1(2,2,1))] > 0.$$

To see that $u(R) - u(c_3^1(2,2,1)) > 0$ note that

$$u(R) - u(c_3^1(2,2,1)) > 0 \quad \Leftrightarrow \quad R > \frac{3}{1 + 2\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}} \quad \Leftrightarrow$$
$$2\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}} R > 3 - R \quad \Leftrightarrow \quad R\rho > \left(\frac{3-R}{2}\right)^{\frac{1}{\gamma}},$$

which is satisfied by the condition in the proposition. Similarly, to see that the second term $u(R) - u(\bar{c}) > 0$, note that

$$u(R) - u(\bar{c}) > 0 \quad \Leftrightarrow \quad R > \frac{3}{2 + \rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}} \quad \Leftrightarrow$$
$$\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}} R > 3 - 2R \quad \Leftrightarrow \quad R\rho > (3 - 2R)^{\frac{1}{\gamma}},$$

which is also satisfied because $\left(\frac{3-R}{2}\right)^{\frac{1}{\gamma}} > (3-2R)^{\frac{1}{\gamma}}$ for $R > 1$.

From the above, we can conclude that the efficient allocation satisfies the bank incentive compatibility constraint. Now let us show that it does not satisfy the blockchain incentive compatibility constraint. Consider an agent 2 who is a patient type but has to report after an agent 1 has reported she is an impatient type. If she announces truthfully, she expects to get on date 2 approximately $R[3 - 2\bar{c}]$ for ϵ small. That is because conditional on agent 1 being impatient, she believes that there is another impatient agent almost with probability one. If she deviates and announces she is type impatient, she expects to get on date 1 approximately $\bar{c}$ for ϵ small, because the planner will believe she is the second impatient-type agent.

But note that

$$u(\bar{c}) - u(R[3 - 2\bar{c}]) > 0 \quad \Leftrightarrow \quad \frac{3}{2 + \rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}} > R\left[3 - 2\frac{3}{2 + \rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}}\right] \quad \Leftrightarrow$$

$$\frac{3}{2 + \rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}} > R\frac{3\rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}}{2 + \rho^{\frac{1}{\gamma}} R^{\frac{1-\gamma}{\gamma}}} \quad \Leftrightarrow \quad R\rho < 1,$$

which is satisfied by the condition in the proposition. We can now conclude that the efficient allocation satisfies the bank incentive compatibility constraint, but it does not satisfy the blockchain incentive compatibility constraint. □