Cryptocurrency is accounting coordination*

Fernando Barros Jr.† Jefferson Bertolai‡ Matheus Carrijo§

FEARP/USP FEARP/USP FFCLRP/USP
LEMC-FEARP/USP LEMC-FEARP/USP LEMC-FEARP/USP

Abstract

The fundamental monetary innovation embedded into cryptocurrencies is accounting coordination. Decentralized management of digital money's accounting by a network of computers is achieved as a Nash equilibrium of a coordination game among the network's nodes: the so called miners. Equilibrium analysis demands allowing miners to secretly update their accounting, i.e., to privately build multiple blocks of transactions and to deviate from the longest chain rule. We formalize such reasoning by proposing an *accounting* coordination game inspired on the Bitcoin design. In particular, by proposing a model that explicitly tells apart mining costs related to energy consumption from those related to computational capacity, we are able to study how symmetric equilibrium existence depends on well known parameters, like the average time for updating accounting records and the rewards collected from mining (accounting) activities. It is shown that the (off-equilibrium) possibility of double spending makes the attractiveness of the equilibrium strategy a decreasing function of the average time for updating accounting records.

Keywords: cryptocurrency, accounting management, coordination game.

*Jefferson Bertolai and Matheus Carrijo thank institutional support from USP and FEARP/USP to *Laboratório de Economia, Matemática de Computação* (LEMC-FEARP/USP), where this work has been developed. Jefferson Bertolai acknowledges financial support from FAPESP: grant #2018/16888-4, São Paulo Research Foundation (FAPESP).

†E-mail: fabarrosjr@usp.br.

‡Correspondence address: Faculdade de Economia, Administração e Contabilidade de Ribeirão Preto da Universidade de São Paulo, Avenida Bandeirantes, 3900 - Vila Monte Alegre, Ribeirão Preto - SP, 14040-905. E-mail: jbertolai@fearp.usp.br.

§E-mail: matheuslcarrijo@usp.br

1 Introduction

A cornerstone result in monetary theory establishes that *money is memory*, in the sense that money should be seen as a substitute for record-keeping technologies (meaning credit relationships) in solving the problem of double coincidence in economic exchanges.[1] Specifically, money plays the social role of "recording transactions" by evidencing production (of goods and services) done in situations in which no technology for keeping record of individuals' actions is available for playing this role. The possession of money is evidence of past production: it replaces the individual's transaction history demanded by credit relationships (Bertolai and Oliveira, 2020).

From this point of view, according to Bertolai and Oliveira (2020), cryptocurrencies should be evaluated according to their capacity to evidence past production. This allows for recognizing the *Blockchain technology* as the fundamental monetary innovation of the cryptocurrencies, since this is the accounting standard that provides reliance on cryptocurrencies' digital records. It makes feasible decentralized management of digital records by a network of computers connected through the internet.

Decentralized accounting management is what differentiates cryptocurrencies from other forms of digital money, like demand deposits accessible through debit cards. From its very nature, the management of a cryptocurrency's accounting system demands coordination among those responsible for updating it: the network nodes, usually also referred as the *miners*. The update process must be coordinated in order to avoid multiple versions for the state of accounting records, which would imply the network to split into multiple new networks (usually referred as *forks*) and, therefore, multiple new cryptocurrencies.

In addition to organizing ideas around the problem of accounting coordination, we further explore cryptocurrencies' coordination solution by proposing an *accounting* coordination game that incorporates the main features of the Bitcoin design.[2] In particular, two features related to the fact that miners are able to privately update their accounting records emerge as key ingredients: miners are able to both secretly build multiple blocks of transactions and refuse to immediately adopt a new proposed accounting state.[3]

Delayed settlement of payments is another key feature implied by the Bitcoin's design that our model takes into account. Payment settlement is usually not a relevant matter when traditional media of exchange are the payment instrument: transactions are almost instantaneously settled when buyer and seller use money or demand deposit as payment

[1] See Kocherlakota (1998a,b).

[2] On the Bitcoin design, see Nakamoto (2008), Narayanan et al. (2016), Antonopoulos (2017) and Bertolai and Oliveira (2020).

[3] The former feature is usually referred as *selfish mining* (see Eyal and Sirer (2014)), and the latter implies that miners are not bound to follow a key coordination device on the Bitcoin's network, *the longest chain rule*.

instruments. This is not true for exchanges mediated with cryptocurrencies based on Proof-of-Work protocols, like the Bitcoin. Because reliance on Bitcoin digital records increases with time, such transactions are usually associated with delayed delivery of goods and services as an strategy to protect seller from buyer *double spending* its currency.[4]

Among other contributions, Chiu and Koeppl (2019) study the effects of this kind of delayed settlement on exchange terms using an adapted version of the workhorse macroeconomic model proposed by Lagos and Wright (2005). Competition among miners and double spending concerns are explicitly inserted in the macroeconomic environment. On the other hand, presumably as a tractability strategy, *secret mining* and deviations from the *longest chain rule* are ignored when authors compute equilibria in mining competition and derive their no-double-spending condition.[5]

In reality, secret mining and longest chain rule are central features of Bitcoin's network. As discussed in Narayanan et al. (2016) and Antonopoulos (2017), longest chain rule is at the heart of blockchain consensus and double spending attacks require the ability to secretly mine an alternative version of the blockchain until the seller delivers the good or service.[6] In this sense, it would be valuable to know how these two features shape equilibrium existence and double spending incentives by means of simple models of mining competition on Proof-of-Work based cryptocurrencies. Keeping the model's simplicity is attractive in the sense that it allows for embedding the mining competition model in workhorse economic models, as Chiu and Koeppl (2019) successfully did.[7]

Our model for the accounting coordination game provides a contribution towards this objective. In particular, by explicitly telling apart mining costs related to energy consumption from those related to computational capacity, we are able to study how symmetric equilibrium existence depends on well known parameters, like the average time for updating accounting records and the rewards collected from mining (accounting) activities. Also, equilibrium analysis shows that the (off-equilibrium) possibility of double spending makes the attractiveness of the equilibrium strategy a decreasing function of the average time for updating accounting records.

[4]See Halaburda et al. (2015), Narayanan et al. (2016), and Bertolai and Oliveira (2020).

[5]Kang and Lee (2020) also explicitly model miners competition inside the Lagos and Wright (2005)'s environment. Again, secret mining and deviations from the longest chain rule are not considered. Double spending problem is not treated as explicitly as Chiu and Koeppl (2019) has done.

[6]Bertolai and Oliveira (2020) provides an instructive and introductory description of Bitcoin network functioning.

[7]Secret mining and the longest chain rule have actually been studied in fairly general models of mining competition. Biais et al. (2019), for example, have shown that the longest chain rule can be sustained as a Markov perfect equilibrium. Eyal and Sirer (2014) study secret mining as a crucial feature in constructing the kind of attack to Bitcoin network they study, denominated *selfish mining*. Carlsten et al. (2016) shows that secret mining (selfish mining) and the deviations from the longest chain rule are important ingredients in discussing miners' incentives under different schemes of rewards: block rewards or transaction fees.

Our paper can be seen as a contribution to an emerging literature in the economics of cryptocurrency (blockchain). Cong and He (2019), for example, shows how blockchain based smart contracts can mitigate informational asymmetry and improve welfare and consumer surplus by enhancing entry and competition. Biais et al. (2019), in its turn, is closer to our work in the sense equilibrium properties of a mining game are studied for a Proof-of-Work (PoW) based cryptocurrency. They establish that "mining blocks on the longest chain" composes a Markov perfect equilibrium. Also, they argue that the blockchain protocol is a coordination game with multiple equilibria. Specifically, it is shown that equilibria with forks (a coordination failure) can emerge from information delays and software upgrades. Ewerhart (2020) shows that the longest-chain rule constitute a pure-strategy Nash equilibrium in a finite-time mining game. However, he build some exemplos showing that longest-chain rule is not a subgame perfect equilibrium. Departing from costly managed cryptocurrencies, Saleh (2020) studies a mining game intended to model the accounting management of a Proof-of-Stake (PoS) cryptocurrency. Equilibrium conditions are established under which PoS protocol generates consensus in appending blocks to the longest chain.

Our paper differs from Biais et al. (2019), among other things, because we explicit model *multiple* secret mining behavior. While in Biais et al. (2019) miners choose which blockchain follow (adopt), in our environment miners have the option to hide valid blocks in order to create their own longer blockchain. Similarly to Saleh (2020), we show that low rewards can induce an equilibrium where miners coordinate on updating the longest chain. According to Saleh (2020), low rewards for updating blockchains powered by PoS technology induce an equilibrium with no forks (miners append blocks only to the longest chain) because two opposing effects emerge when a miner adds a block to a shorter branch on the blockchain. A low block reward, in terms of coins on that branch, is received at the same time that the value of all coins falls.[8]

In addition to this introduction, this paper is organized in three sections. In section 2, we organize concepts on cryptocurrencies around the problem of accounting coordination and develop our benchmark accounting coordination game. In section 3, the possibility of double spending is introduced in the accounting coordination framework. Also, the benchmark model is extended to incorporate this possibility. Section 4 concludes with some final remarks. Proof and auxiliary results are presented in appendix A and a description of the numerical strategy for computing equilibrium condition is presented in appendix B.

[8]In PoS protocol, miners must have coins in order to participate in the mining game. Then, a fall in the value of coins of a chain branch generates a hard penalty for miners.

2 The *accounting* coordination game

A crucial feature of cryptocurrencies is that their accounting system is decentrally managed by a set of computers interconnected through the internet. As economic exchanges are intermediated by cryptocurrency payments, this set of computers is informed about the corresponding transactions (transfers of cryptocurrency's balances) and must coordinate members to preserve accounting uniformity.

Decentralized management means that there is no central authority to enforce the accounting *standard* and its current *state* (the balance in each account). In principle, each computer is able to organize transactions at its own criterion and to propose other computers its accounting standard and state. A coordination game emerges in which players (computers) must decide which accounting standard to follow and how to update its state. As usual in coordination games, multiple Nash equilibria are expected in the absence of effective coordination devices. In equilibrium, the set of computers can split into multiple subsets according to the accounting standard and state in which its members managed to coordinate.

A set of computers that follow the same accounting standard and agree on the current accounting state is commonly referred as a *network* and its members are called *nodes*. Multiple equilibria prediction on the coordination game discussed above says that a given network is expected to split into multiple networks, usually referred as network's *forks*, in the absence of effective coordination devices.

From the point of view of game theory, therefore, the main challenge for the decentralized management of cryptocurrency accounting systems resides in avoiding forks by coordinating nodes on the same accounting standard and state. In this vein, the so called cryptocurrency's *protocol* can be naturally seen as a key coordination device. It is a commonly shared document that establishes a set of rules to be followed by computers (players) on the *accounting* coordination game discussed above.

In Bitcoin's protocol, the accounting system must be organized as a sequence of groups of transactions: each *transaction* is a digital record in which units of Bitcoin are transferred to users' accounts, each group of transactions is called *block* of transactions and the sequence of blocks is called *blockchain*. Each node is allowed to build and propose to other nodes its own version of the blockchain and must choose among the proposed versions which one to follow. For security purposes, however, the protocol requires an expensive computational task for each new block to be included in a proposed version. This cost can be avoided by building a version composed of blocks for which the computational task has already been executed, but these blocks can be used in the new sequence of blocks *only as predecessors of new blocks*.

This costly mechanism of building new versions to the blockchain is clearly intended to coordinate nodes on previously proposed blocks, especially on those at the beginning of the sequence of blocks. *Ceteris paribus*, the more expensive is the computational task per block, the less attractive is to build new blocks. Also, all new blocks cannot come before already existing ones, i.e., new blocks must come at the end of the sequence of blocks. At extreme situations, nodes would build no new block when this cost is sufficiently high and would propose only new blocks when this cost vanishes. At intermediate situations, nodes would propose versions with some old blocks succeeded by some new blocks.

Assuming nodes are rational players at the accounting coordination game, they must be provided incentives to build new blocks. Otherwise, the accounting system would never be updated by new transactions. For this matter, Bitcoin's protocol allows authors of new blocks to collect both newly minted units of Bitcoin and old units of Bitcoin offered as transaction fees. This collection is implemented by proposing blocks with transactions in which these units of Bitcoin are transferred to an account the block's author indicates. The resulting balance can then be spent in new transactions, i.e., be offered in exchange to either goods and services or another payment instrument.

An important feature emerges here: the rewards for new blocks is effective only on the network formed by those computers that update their blockchain to the version that includes the proposed new block. Because balances in different networks are actually balances in different cryptocurrencies, the value of the reward in terms of goods and services is determined by which computers update their blockchain using the proposed new block. If every node employs the new block in updating its blockchain, rewards are collected according to the Bitcoin's value in terms of goods and services. At the other extreme, if only the block's author updates its blockchain employing the new block, then rewards are collected according to the real value of a newly created cryptocurrency, whose network is composed by only one node (the author's node) and whose value is most likely zero.

As a consequence of the feature just described, Bitcoin's sophisticated reward mechanism for new blocks provides incentives for proposing new blocks that are expected to be adopted by other nodes in updating their versions of blockchain. In game theory language, the reward scheme makes coordination attractive also for new blocks. In particular, it encourages compliance with protocol's requirements in building new blocks, if other nodes are expected to comply with them.

Even though nodes are successful coordinating on the proposition of versions to the blockchain that comply with the protocol's requirements, they must also coordinate on which version to follow. For the protocol requirements are not enough to ensure accounting uniformity among propositions. For example, the very indication of distinct accounts

to collect rewards from new blocks makes them different blocks and, therefore, produces different proposed versions to the blockchain.

In order to avoid the network splitting in forks due to multiple proposed versions, the computational task required for building a block has been chosen in the Bitcoin's protocol so that the amount of time for executing it is random, by construction. That way, nodes finish building their versions at different moments and are communicated about proposed versions sequentially. Thus, the decision each node makes on which version to follow reduces to deciding between two alternatives: either *adopting* the newly proposed version, by discarding previous versions, or *ignoring* the new proposition, by keep following the last version the node has adopted.

Although sequentiality on propositions helps nodes' coordination into fewer options, the current version *vs* the new one, it does not favor one over the other. This is the point in which the so called *longest chain rule* emerges as a key coordination device. Roughly, the rule states that nodes should join the blockchain version whose number of blocks is higher. If every node follows this rule, all computational effort will be allocated into building new blocks at the end of the longest blockchain and such concentration in turn ensures the current longest chain will remain being the longest one. From the accounting system perspective, this result is attractive because it promotes records' *immutability*: a transaction is never erased once it is included in the longest blockchain, in the sense that the network never discards the block's transaction.

Widespread adoption of the longest chain rule also provides incentives for each node *revealing* its state proposition as soon as it finishes building a blockchain longer than the existing ones. Immediately revealing propositions in this situation is expected to ensure reward collection, while delaying such announcement puts rewards at risk: it gives opportunity for other node finishing its computational task, proposing a version expected to be accepted by the network, and collecting the associated rewards.

In summary, protocol's requirements promote nodes' coordination on the accounting *standard*. Also, the longest chain rule and the reward for costly production of new blocks encourage nodes' coordination on the same accounting *state*. Crucially, the relation between rewards and production cost determines the proportion between new and old blocks on a state proposition, since rewards encourage the production of new blocks while costly production discourages it. Ideally, nodes would preserve previous accounting by appending the longest chain with a new block made of only new transactions. As shown in the following benchmark model, this ideal accounting dynamics is sustained in symmetric equilibrium if and only if a balancing between cost and rewards holds.

2.1 The model with multiple secret mining

Time is continuous and the horizon is randomly determined, as shall become clear. There are $n+1 \in \mathbb{N}$ risk-neutral, rational, and strategic players, called *miners*, each of them running a node on the Bitcoin network. The set of miners is called *the network* and is denoted $N = \{0, 1, \cdots, n\}$. Miners compete for two prizes and each prize provides payoff $R > 0$ to the winner and nothing to other miners.

After being informed about transactions at $t = 0$, miners gather them together in a block of transactions and start executing an computational task associated to this block. A block for which the computational task has been finished is called a *valid block* and the execution of the associated tasks is also referred as a search for a valid block. Searches for valid blocks are sequentially ordered in the sense that the search for a second valid block can only be started after a first valid block has been found. Such sequentiality is made explicit by saying that a second valid block can only be found `after` (or `above`) a first valid block.

Finding a valid block requires some computational effort, whose energy consumption costs $\kappa > 0$ per unit computation. If $\phi > 0$ denotes the amount of computation per unit of time, the energy cost in searching for a valid block for Δ units of time using constant computational effort ϕ is $\kappa\phi\Delta$.

The exact amount of time each miner must search until finding a valid block is randomly determined as follows. The *amount of computation* miner $i \in N$ must execute until finding a valid block is denoted by X_i and is assumed to follow an exponential distribution with parameter $\lambda > 0$, whose cumulative distribution function is $F(x) = 1 - \exp(-\lambda x)$. The *amount of time* miner i must search until finding a valid block is denoted by Y_i and depends on the computational effort exerted during the search. In the simplest case, in which computational effort is held constant at a rate $\phi_i > 0$, the amount of time is given by $Y_i = X_i/\phi_i$ and follows an exponential distribution with parameter $\lambda\phi_i > 0$, whose cumulative distribution function is $F(y|\phi_i) = 1 - \exp(-\lambda\phi_i y)$.

Each miner i is assumed to choose a computational capacity $h_i \geq 0$ and a trajectory of computational effort, $\phi_i : \mathbb{R}_+ \mapsto [0, h_i]$ in order to maximize its expected payoff from mining. For tractability, we assume that ϕ_i is held constant until new information arrives to miner i, that is, miners update their computational effort only when they find a new valid block or they are informed that the network has found a new valid block. Computational capacity is rented *ex ante* at a cost $\rho > 0$ for each unit of capacity. For simplicity, miners are assumed to not discount future payoffs.

Reward R for the last (second) valid block is collected by the miner who finds the second block and communicates such accomplishment to the network before any other miner does so. Reward R for the first valid block, on the other hand, *is collected by the*

miner who has found the valid block above which the second valid block was found. In this sense, block rewards are collected only after two valid blocks are found.

After finding a first valid block, miner i must decide between *revealing* its accomplishment to other miners and *hiding* this information. The former action allows other miners to join the search for a second valid block *above miner i's valid block.* This can be attractive, since each additional effort in the search for this second valid block increases the probability miner i will collect rewards for the first block, R. On the other hand, the latter action makes i the only miner able to search this second valid block. This can be attractive, since it increases the probability miner i will find this second block before other miners (it actually makes unfeasible for other miners to do so) and because other miners would still need to find their first block before starting to search for a second one. Upon being successful in finding this second valid block before other miners find their second valid block, miner i collects rewards from two blocks, $2R$.

After being informed miner $j \neq i$ has found a first valid block, miner i must decide between persisting in the search for a first valid block and joining the search for a second valid block above miner j's valid block. By taking the latter action, which we refer to as *adopting*, i gives up collecting rewards from a first valid block. This can be attractive, since i becomes able to start the search for a second valid block before finding a first valid block. On the other hand, the former action keeps the possibility of double reward available. We refer to this action as *ignoring* the network.

The multiple possibilities of strategies implied by the actions just described are available to all miners. The choice each miner makes between *revealing* and *hiding*, as well as, between *adopting* and *ignoring*, shapes the payoff other miners expect to get. Because we are interested on symmetric equilibrium behavior, expected payoffs are computed in next subsection assuming other miners are all following the same strategy.

2.2 The symmetric equilibrium with single secret mining

In order to study the symmetric Nash equilibrium (SNE) in which every miner immediately reveal its valid blocks and immediately join the longest chain, consider the problem miner $i = 0$ faces when each miner $j \in N \setminus \{0\}$ is assumed to be following the equilibrium strategy. Assume also that each miner $j \neq 0$ has rented computational capacity $\bar{h} \geq 0$ and will hold computational effort at the level $\phi_j^{(k)} \geq 0$ when searching for block $k \in \{1, 2\}$.

Figure 1 represents the implied miner $i = 0$'s problem using a decision tree that is not so usual and, therefore, deserves careful description. Competition among miners starts at node 22, after $i = 0$ has rented computational capacity $h \geq 0$ and each miner $j \neq 0$ has rented $\bar{h}$ units of computational power. Label 22 is intended to remember that $i = 0$ is

searching for 2 blocks from this node on, the first entry in 22, and that remaining miners are searching for 2 blocks from this node on, the second entry in 22.

Under probability W_{22}, miner 0 wins the competition for the first block, in the sense that miner 0 finds a first valid block before everyone else. Formally, the realization $y \geq 0$ of the time until miner $i = 0$ finds a first valid block, the random variable Y_0^1, is less than realization $m \geq 0$ of the time until other miners finds a first valid block, the random variable $M^1 \equiv \min\{Y_i^1 : i \in N \setminus \{0\}\}$. Under probability $L_{22} \equiv 1 - W_{22}$, miner 0 loses first competition in the sense that $y > m$. Because we are assuming other miners are following equilibrium strategies, the successful miner communicates such accomplishment in this case.

Remark 1 *Let $\bar{\phi}^1 = (1/n)\sum_{i=1}^n \phi_i^1$. Lemma 5 in appendix A implies that M^1 follows an exponential distribution with parameter $\lambda n\bar{\phi}^1$. Also, if miner 0 exert constant effort ϕ_0 in the first competition, then $W_{22} = \phi_0/(\phi_0 + n\bar{\phi}^1)$ and the expected amount of time until someone finds a first valid block is given by $\mathbb{E}[\min\{Y_0^1, M^1\}] = 1/\lambda(\phi_0^1 + n\bar{\phi}^1)$.*

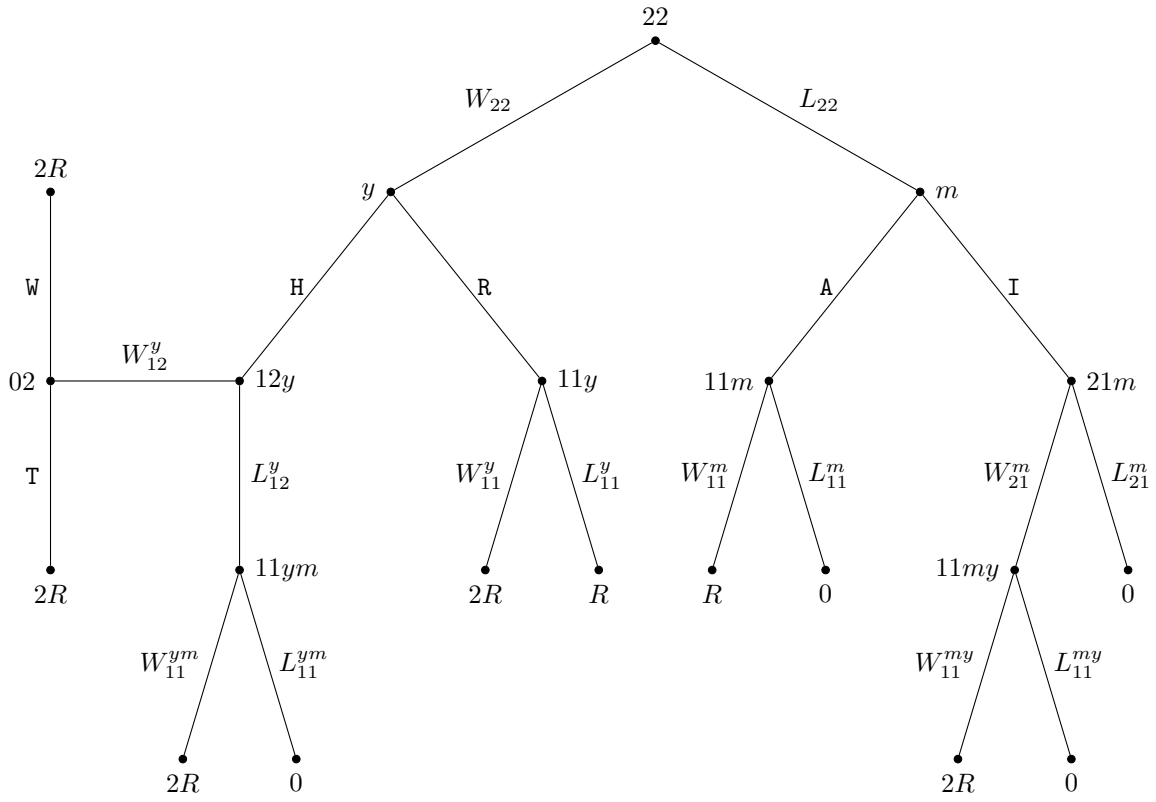


Figure 1: Tree representation of miner 0's problem

When $y < m$, miner 0 must decide between hiding its block and revealing it to the network. The corresponding decision node is indicated in figure 1 to the left of node 22 and is indexed by y. Because time is continuous, there is actually a continuum of such

decision nodes. Actions `H` and `R`, and only them, are available in this node: `H` stands for hiding and `R` stands for revealing. Because other miners are assumed to be following equilibrium strategies, action `R` implies that other miners will immediately start to search for a second block above miner 0's first valid block. This is indicated by labeling next node to the right as $11y$. Action `H` makes $i = 0$ the only miner able to search for a valid block above the valid block just found. This is indicated by labeling next node to the left as $12y$, since remaining miners keep searching for a first valid block in this case.

When $j \neq 0$ wins first competition (i.e., j finds a first valid block before everyone else) and communicates the network such accomplishment, miner 0 must decide about giving up the search for a first valid block. This decision node is indicated in figure 1 to the right of node 22 and is indexed by m. Again, because time is continuous, there is actually a continuum of such decision nodes for each $j \neq 0$. Actions `A` and `I`, and only them, are available in this node: `A` stands for adopting and `I` stands for ignoring. Action `A` means that miner 0 gave up searching for a first valid block and started to search for a second valid block above the block just found by $j \neq 0$. This is indicated by labeling next node to the left as $11m$. Action `I` means that miner 0 is still searching for a first valid block and this implies that next node to the right should be labeled as $21m$.

From node $21m$ on, two possibilities can emerge. In the first one, which happens under probability L_{21}^{m}, miner 0 gets no reward since other miner finds a second valid block before $i = 0$ completes the task of finding any valid block. This is indicated in figure 1 by labeling the next node to the right as 0. In the second possibility, which happens under probability W_{21}^{m}, $i = 0$ finds a first valid block and starts to search for a second valid block above it. This is indicated in figure 1 by labeling the next node to the left as $11my$.

From node $12y$, two possibilities can emerge. In the first one, which happens under probability W_{12}^{y}, miner 0 finds a second valid block before other miners complete the task of finding a first valid block. This is indicated in figure 1 by labeling the next node to the left as 02. In the second possibility after node $12y$, which happens under probability L_{12}^{y}, the network completes its first task and starts to search for a second valid block. This is indicated in figure 1 by labeling the next node as $11ym$.

Actions `W` and `T`, and only them, are available at node 02: `T` stands for immediately revealing valid blocks to the network, terminating competition, and `W` stands for waiting someone else find and communicate a first valid block before revealing the two blocks. Because network is assumed to be adopting the longest version of the blockchain, actions `W` and `T` provide miner 0 the same payoff, $2R$.

From node $11ym$ on, all miners compete for the second block: miner 0 is searching a block above its *hidden* first block and the network is searching for a block above the

commonly known first valid block. Again, two possibilities can emerge. In the first one, which happens under probability W_{11}^{ym}, miner 0 wins competition and gets reward $2R$. This is indicated in figure 1 by labeling the next node to the left as $2R$. In the second possibility, which happens under probability L_{11}^{ym}, miner 0 loses competition and gets no reward. This is indicated in figure 1 by labeling the next node as 0. The situation from node $11my$ is almost identical. The only difference is that winning probability equals W_{11}^{my} and losing probability equals L_{11}^{my}.

From node $11y$ on, all miners compete for the second block: everyone is searching for a block above the *commonly known* first valid block miner 0 has found and revealed. Again, two possibilities can emerge. In the first one, which happens under probability W_{11}^{y}, miner 0 wins competition and gets reward $2R$. This is indicated in figure 1 by labeling the next node to the left as $2R$. In the second possibility, which happens under probability L_{11}^{y}, miner 0 loses competition and gets reward for only the first block. This is indicated in figure 1 by labeling the next node to the right as R. The situation from node $11m$ is very similar, but now everyone is searching for a block above the *commonly known* first valid block miner $j \neq 0$ has found and revealed. Miner 0 wins under probability W_{11}^{m}, in case 0's rewards equal R, and loses under probability L_{11}^{m}, in case miner 0 gets no reward.

In summary, given that other miners are assumed to be following equilibrium strategies, miner 0 maximizes expected payoff by choosing a computational effort $\phi_i \in [0, h]$ for each decision node $x \in \{22, 12y, 11y, 11m, 21m, 11ym, 11my\}$ and a vector of actions $(a_y, a_m, a_{02}) \in \{\mathtt{H}, \mathtt{R}\} \times \{\mathtt{A}, \mathtt{I}\} \times \{\mathtt{W}, \mathtt{T}\}$. In lemma 1, backward induction and tree representation in figure 1 are employed to solve miner 0's optimization problem for each computational capacity $h \geq 0$.

Lemma 1 *Suppose $r \equiv R - \kappa/\lambda > 0$ and define $z_h = h/n\bar{h}$. Maximum payoff miner 0 expects to get from mining, given its computational capacity $h \geq 0$, is*

$$\Pi(z_h) \equiv \begin{cases} 2r\pi_{RA}(z_h) & \text{if } 0 \leq z_h < R/r \\ 2r\pi_{HI}(z_h) & \text{if } R/r \leq z_h \end{cases}, \tag{1}$$

where $\pi_{RA}(z) \equiv z/(1+z)$ and $\pi_{HI}(z) \equiv (z^3 + 3z^2 + (1 - R/r)z)/(1+z)^3$. Optimal policy entails miner $i = 0$ choosing maximum computation effort $\phi_0 = h$ in all effort decision node $x \in \{22, 12y, 11y, 11m, 21m, 11ym, 11my\}$,

$$(a_y, a_m) = \begin{cases} (\mathtt{R}, \mathtt{A}) & \text{if } 0 \leq z_h \leq R/r \\ (\mathtt{H}, \mathtt{I}) & \text{if } R/r < z_h \end{cases}, \qquad \text{and} \qquad a_{02} \in \{\mathtt{W}, \mathtt{T}\}.$$

Proof. See appendix A. ■

If miner 0's computational power is h, then the maximum expected payoff miner 0 gets from following equilibrium strategy $\phi_0 = h$ at all effort decision nodes and $(a_y, a_m, a_{02}) = (\mathtt{R}, \mathtt{A}, \mathtt{T})$ is given by $2r\pi_{\mathtt{RA}}(z_h)$. On the other hand, if miner 0 chooses the best deviation from equilibrium strategies, by following $\phi_0 = h$ at all effort decision nodes and $(a_y, a_m, a_{02}) = (\mathtt{H}, \mathtt{I}, a_{02})$ for some $a_{02} \in \{\mathtt{W}, \mathtt{T}\}$, then the expected payoff $i = 0$ gets from the mining competition is given by $2r\pi_{\mathtt{HI}}(z_h)$. Under computational capacity is h such that $z_h = R/r$, miner 0 is indifferent between these two alternatives, as a consequence of lemma 7 in appendix A. Most important, lemma 1 shows that only relative computational power z_h is relevant for miner 0 maximum payoff.

The case expected energy cost per block is higher than the rewards per block ($r = R - \kappa/\lambda < 0$) is not considered in lemma 1. In this case, mining activity is not profitable and, therefore, equilibrium existence demands $r > 0$.

In any symmetric Nash equilibrium (SNE), every miner chooses the same computational capacity $\bar{h}$. From lemma 1, a SNE in which every miner immediately reveal its valid blocks and immediately join the longest chain exist if and only if every miner $i \in I$ chooses computational effort $\phi_i = \bar{h}$ in every effort decision node, $h = \bar{h}$ maximizes $\Pi(z_h) - \rho h$ and $z_{\bar{h}} \leq R/r$. Proposition 1 establishes these equilibrium conditions can be summarized by a function $E(1/n, r/R)$. It also shows that symmetric equilibrium exists for sufficiently low $1/n$ and r/R and does not exists for $(1/n, r/R) \approx (1, 1)$.

Proposition 1 *Suppose $r > 0$ and let $h_{HI} \in \arg\max_{h \geq n\bar{h}R/r}\{2r\pi_{HI}(z_h) - \rho h\}$. There is a SNE in which every miner follows $(a_y, a_m) = (\mathtt{R}, \mathtt{A})$ if, and only if, $\bar{h} = 2rn/\rho(1+n)^2$ and*

$$E\left(1/n, r/R\right) \equiv 1 - \frac{\pi_{HI}\left(z_{h_{HI}}\right) - (\rho/2r)h_{HI}}{\pi_{RA}\left(1/n\right) - (\rho/2r)\bar{h}} \geq 0. \tag{2}$$

Also, for each $x \in \mathbb{R}^2_+$ such that $\|x\| = 1$, there is a unique $\varepsilon \in (0, 1/\max_i\{x_i\})$ such that $E\left[(1,1) - \varepsilon x\right] = 0$ and $E\left[(1,1) - tx\right](t - \varepsilon) > 0$ for all $t \in (0, 1/\max_i\{x_i\})$ such that $t \neq \varepsilon$.

Proof. Existence and uniqueness of the cutoff ε are established by Lemma 4 in appendix A. Because $z_h = 1/n$ under $h = \bar{h}$, equilibrium condition $z_{\bar{h}} \leq R/r$ is equivalent to $r \leq nR$, which is always satisfied since $r < R$ and $n \geq 1$. Thus, it must be clear that the inequality in (2) is necessary and sufficient for equilibrium existence. In what follows, we establish that function $E(1/n, r/R)$ is well defined.

Optimality of $h = \bar{h}$ requires $\Pi(z_h) - \rho h$ reaching a local maximum at $h = \bar{h}$. Using $z_{\bar{h}} \leq R/r$ and that $\pi_{\mathtt{RA}}(z_h)$ is strictly concave in h, as implied by lemma 7 in appendix A, local optimality of $\bar{h}$ is equivalent to $\rho = \Pi'(z_{\bar{h}})z'_{\bar{h}}$. Then, $\rho = 2r\pi'_{\mathtt{RA}}(z_{\bar{h}})z'_{\bar{h}} = [2r/(1 + 1/n)^2](1/n\bar{h})$ and, therefore, $\bar{h} = 2rn/\rho(1+n)^2$. As a consequence, $\pi_{\mathtt{RA}}(z_{\bar{h}}) - (\rho/2r)\bar{h} = (1/n)/(1 + 1/n) - n/(1+n)^2 = (1+n)^{-2}$ is determined by, and only by, $(1/n, r/R)$.

The ratio $z_{h_{\mathtt{HI}}} = h_{\mathtt{HI}}/n\bar{h}$ is invariant to both ρ and changes in (R, r) that keeps r/R unchanged. In effect, usual optimality conditions for maximizing a strict concave objective function ensures that $h_{\mathtt{HI}}$ can be characterized by $h_{\mathtt{HI}} \geq n\bar{h}R/r$, $2r\pi'_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) z'_{h_{\mathtt{HI}}} \leq \rho$, and $[2r\pi'_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) z'_{h_{\mathtt{HI}}} - \rho][h_{\mathtt{HI}} - n\bar{h}R/r] \geq 0$. If $h_{\mathtt{HI}} = n\bar{h}R/r$, then $z_{h_{\mathtt{HI}}} = R/r$ and the result is trivial. Suppose $h_{\mathtt{HI}} > n\bar{h}R/r$ so that $\rho/2r = \pi'_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) z'_{h_{\mathtt{HI}}} = \pi'_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right)/n\bar{h}$ must hold. Imposing $\bar{h} = 2rn/\rho(1+n)^2$, it follows that $\pi'_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) = \rho n\bar{h}/2r = (n/(1+n))^2$. Because $\pi'_{\mathtt{HI}}(z_h)$ is invariant to ρ, depends on (R, r) only through r/R, and depends on h only through z_h, we have established that $z_{h_{\mathtt{HI}}}$ is determined by, and only by, $(1/n, r/R)$. Similarly, because $\pi_{\mathtt{HI}}(z_h)$ is invariant to ρ, depends on (R, r) only through r/R, and depends on h only through z_h, this last result allows us to conclude that

$$\pi_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) - \frac{\rho}{2r}h_{\mathtt{HI}} = \pi_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) - \frac{\rho}{2r}n\bar{h}z_{h_{\mathtt{HI}}} = \pi_{\mathtt{HI}}\left(z_{h_{\mathtt{HI}}}\right) - \left(\frac{n}{1+n}\right)^2 z_{h_{\mathtt{HI}}}$$

is determined by, and only by, $(1/n, r/R)$. ■

Proposition 1 has established the existence of a cutoff function ε_x that characterizes the set of parameters under which a SNE with $(\mathtt{R}, \mathtt{A})$ exists. The contour plot for $E(1/n, r/R)$ is presented in figure 2 and its level curve $E(1/n, r/R) = 0$ suggests that ε_x is actually a continuous function.[9]

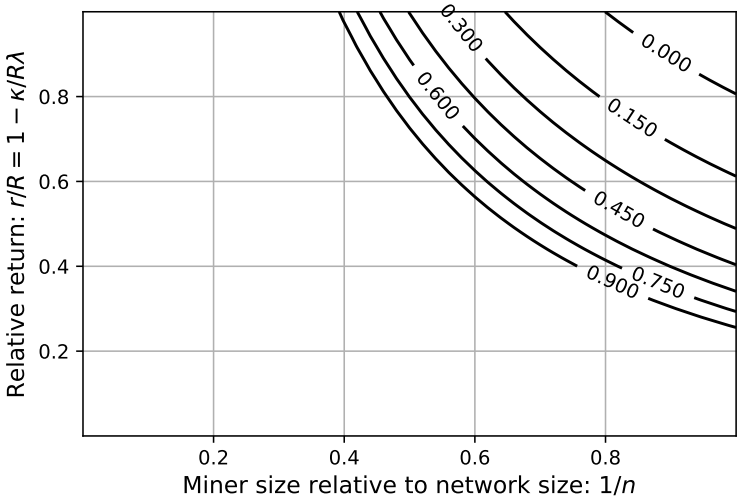


Figure 2: Contour plot for $E(1/n, r/R)$.

From figure 2, the SNE with $(\mathtt{R}, \mathtt{A})$ does not exist when a sufficiently low $\kappa/R\lambda$ is combined with a sufficiently low n. In words, the longest chain rule and immediate proposition of valid blocks do not compose a SNE when few miners are operative and

[9]Appendix B briefly describes a standard numerical strategy for computing $E(1/n, r/R)$.

the expected mining cost κ/λ is low when compared to the mining reward R. In this case, miners find it more profitable hiding its valid blocks and ignoring the network's proposition. This result makes precise the importance of a balancing between costs and rewards implied by the production of blocks of transactions. As relative cost $\kappa/R\lambda$ increases or as the network size $(n+1)$ increases, the SNE with immediate proposition of valid blocks and adoption of the longest chain emerges. In words, equilibrium existence requires a sufficiently high relative energy cost.

2.3 Bitcoin's average time target

Result in figure 2 show how equilibrium existence depends on κ/λ and $1/n$. In particular, low $1/\lambda$ helps making equilibrium strategy `RA` attractive. This is instructive since $1/\lambda$ is periodically adjusted in Bitcoin network in order to keep

$$\mathbb{E}\left(\min_{i\in N}\{Y_i\}\right) = \frac{1}{\lambda(n+1)\bar{h}} = \frac{\rho(1/n+1)}{2\lambda r} = \frac{\rho(1/n+1)}{2(R\lambda-\kappa)}, \tag{3}$$

the equilibrium average time the network spends to find a valid block, around 10 minutes. For example, improvements in computational technology, like ASIC's development, make computational capacity cheaper to rent (it lowers ρ) and, therefore, induce higher equilibrium computational capacity $\bar{h}$.[10] Higher equilibrium $\bar{h}$ is also motivated by higher mining reward R and lower energy cost κ. Network's equilibrium computational capacity $(n+1)\bar{h}$ can also increase as a result of a larger network, i.e., larger n. All such changes are compensated by adjustments in λ in order to make $\mathbb{E}\left(\min_i\{Y_i\}\right) = 10$ minutes. This is accomplished by every miner imposing itself a new and common difficult in finding new valid blocks, represented in our model by the parameter $1/\lambda$.

We now incorporate such feature on the equilibrium existence analysis by setting the average time $a = \mathbb{E}\left(\min_i\{Y_i\}\right)$ as a parameter and adjusting λ accordingly: $\lambda = (\kappa + \rho(1/n+1)/2a)/R$. As a consequence $\kappa/\lambda = \frac{R}{1+\rho(1/n+1)/2\kappa a}$ and

$$\frac{r}{R} = \left(1 + \frac{2a\kappa}{\rho(1+1/n)}\right)^{-1}. \tag{4}$$

From figure 2, we know that equilibrium strategy `RA` becomes more attractive as either r/R or $1/n$ decreases. Now, (4) shows that r/R is low when $\frac{2a\kappa}{\rho(1+1/n)}$ is high. Then, equilibrium strategy attractiveness is definitely decreasing in $1/n$: it obviously increases itself and, as implied by (4), also increases r/R. For fixed $1/n$, equilibrium strategy is made more attractive by increasing $a\kappa/\rho$. For $1/n > 80\%$, equilibrium existence is

[10] ASIC stands for Application Specific Integrated Circuit.

roughly given by $1.8 \geq r/R + 1/n = 1/n + \left(1 + \frac{a\kappa/\rho}{1+1/n}\right)^{-1}$, so that it resumes to high enough $a\kappa/\rho$ when $1/n$ is kept fixed: the equilibrium expected mining cost $a\kappa$ should be sufficiently high relative to the computational capacity cost ρ.

3 The double spending problem

The *accounting* coordination game discussed in section 2 has presented mining competition as a coordination device to preserve accounting uniformity. The model for mining competition presented in subsection 2.1 has established that a SNE featuring accounting uniformity and accounting immutability emerges if and only if network size $(n+1)$ is not small or $\kappa/R\lambda = 1 - r/R$ is sufficiently far from zero, but still lower than one. If the network is small, then there must be some expected mining cost κ/λ, although it cannot be higher than rewards R. If relative cost $\kappa/R\lambda$ is small, then the network size must be sufficiently large.

The attractiveness of multiple secret mining, hereafter MSM, is the main strategic point in the mining competition discussed in section 2. Because in equilibrium every node is following the longest chain rule and immediately revealing valid blocks, there cannot be incentives for double secret mining as a strategy to manipulate coordination to an accounting state that provide double rewards to deviators. Equilibrium existence conditions, intermediate $\kappa/R\lambda$ or large enough n, operate to make unprofitable deviations of this nature.

The discussion on accounting coordination presented so far omits an important source of attractiveness for MSM. In section 2, nodes has no interest on transactions' processing beyond collecting the transaction fees offered in exchange for this task. The very reward mechanism, however, makes clear that nodes must get involved in economic exchanges intermediated by cryptocurrency payments in order to collect their rewards. Nodes actually generate transactions and, therefore, have interest in the processing of some transactions that goes beyond the collection of transaction fees.

A critical interest payers might have in the processing of their digital transactions resides in erasing digital records after receiving the purchased item. By erasing their payments from the accounting state, payers get the associated balances back to their accounts and become able to spend them once more. The possibility of this *double spending* operation, of course, makes payees less willing to accept digital payments in economic exchanges.

Double spending incentives clearly harm accounting immutability. They can be tamed in centralized accounting system by making the system manager accountable for erased transactions. In decentralized accounting systems, however, double spending emerges

as a critical problem. Because in this case the accounting state is updated through coordination among nodes, miners can successful double spend their balances if they are able to induce network coordination in modifying previous transactions. This would be accomplished by secretly mining multiple blocks that do not include the spending transactions while the network coordinate on a state that both records such transactions and convinces the payee to transfer the purchased item. After receiving the item, the target transactions would be erased by coordinating the network on the accounting state that does not include them and that has been secretly built on the meantime.

As in the standard MSM studied in section 2, the attractiveness of MSM for double spending purposes depends on the behavior other nodes are expected to be following. Also, it crucially depends on the delivery behavior payees are following, i.e., on the accounting state that convinces payees to deliver the purchased item. The following discussion extends the model of section 2.1 in order to study double spending attractiveness and, in particular, its dependency on the payees' delivery policy.

3.1 The model with double spending and double reward

We now extend the mining model proposed in section 2.1 in order to accommodate miners involvement in exchanges intermediated with Bitcoin and, therefore, to make room for double spending. Consider an economic exchange in which one individual (the *payee*, the *seller*) wants to buy units of Bitcoin and the other individual (the *payer*, the *buyer*) wants to buy units of consumption good. The buyer *pays* $d \geq 0$ units of Bitcoin in exchange for one unit of good, whose consumption provides utility $u \geq d$, and the payee delivers the unit of good after $w \in \{0, 1, 2\}$ *confirmations* of transaction d on blockchain records.

Buyer pays d when he or she inform all miners about transferring d to the seller. Payment d must be recorded on blockchain before seller is able to use d to buy goods. While transaction d is not included in any valid block, it has not been confirmed yet ($w = 0$). One confirmation ($w = 1$) means that transaction d is included in the last valid block added to the blockchain and two confirmations ($w = 2$) means that transaction d is included in the valid block whose successor is the last valid block added to the blockchain.

Double spending is made feasible by assuming the buyer is able to rent computation capacity h at rate ρ in order to participate in the mining competition. Exchange terms (w, d) are assumed fixed, for simplicity. Extending the model to allow for endogenous exchange terms should not be a challenging task, but it is beyond the scope of this work.

Upon deciding to participate in the mining competition using computational capacity $h \geq 0$, the payer must decide about processing transaction d by including it in his or her accounting. Including transaction d is referred as choice `In`, excluding it is denoted as choice `Ex`, and the maximum expected payoff implied by choice $c \in \{\texttt{In}, \texttt{Ex}\}$ is denoted

by $\Pi_c^w(z_h)$ when seller's waiting policy is w and buyer's relative computational capacity is $z_h = h/n\bar{h}$.

Observe that, by choosing `In`, buyer gets involved on a mining competition very similar to the one presented in figure 1, if all other miners are expected to include d in their blocks. In effect, because in this case transaction d will be recorded on the next valid block for sure, buyer always receive the good and never recovers d, no matter the value of w. The mining competition miner 0 face can therefore be described by figure 3, which results from adding payoff u to every terminal node of figure 1.

Extending notation from section 2.1, let $a^{w\texttt{In}} = (a_y^{w\texttt{In}}, a_m^{w\texttt{In}}, a_{02}^{w\texttt{In}})$ denote the vector of actions chosen for decision nodes of figure 3 when seller's policy is w. Because figures 1 and 3 differs only by a constant, the proof of lemma 1 can be easily extended to establish claim 1.

Claim 1 *Suppose $r = R - \kappa/\lambda > 0$ and $h \geq 0$. Then,*

$$\Pi_{\texttt{In}}^w(z_h) = u + \Pi(z_h) = \begin{cases} u + 2r\pi_{RA}(z_h) & \text{if } 0 \leq z_h \leq R/r \\ u + 2r\pi_{HI}(z_h) & \text{if } R/r < z_h \end{cases}, \quad \forall w \in \{0,1,2\}. \tag{5}$$

Optimal policy entails miner $i = 0$ choosing maximum computation effort $\phi_0 = h$ in all contingencies, and for $x \in \{W, T\}$

$$\left(a_y^{w\texttt{In}}, a_m^{w\texttt{In}}, a_{02}^{w\texttt{In}}\right) = \begin{cases} (R, A, x) & \text{if } 0 \leq z_h \leq R/r \\ (H, I, x) & \text{if } R/r < z_h \end{cases}, \quad \forall w \in \{0,1,2\}. \tag{6}$$

The game buyer faces by choosing to mine a block *without* transaction d, when all other miners are expected to include d in their block, is a nontrivial modification of game tree in figure 1. Figures 4, 5 and 6 represent this new situation assuming that seller's waiting choice is $w = 0$ in figure 4, $w = 1$ in figure 5 and $w = 2$ in figure 6.

First, compare figure 4 to figure 1. Because buyer receives the good for sure when $w = 0$, payoff u is added to all terminal nodes. Since winning mining competition on nodes $12y$, $11ym$ and $11my$ implies miner 0 first block to be accepted by all network, and given this block does not include transaction d, payoff d must be added to terminals nodes that follows miner 0's victories at nodes $12y$, $11ym$ and $11my$. Payoff d must also be added to all nodes that follow node $11y$, because miner 0's first block is assumed to be accepted by all network after miner 0 reveals it.

Now, consider the case $w = 1$ represented in figure 5. Contingencies in which buyer recovers d are the same ones discussed for $w = 0$. So, payoff d is added to the same terminal nodes in figure 4 and in figure 5. On the other hand, buyer receives the good only in some contingencies when $w = 1$. Because $w = 1$ in figure 5, buyer receives the

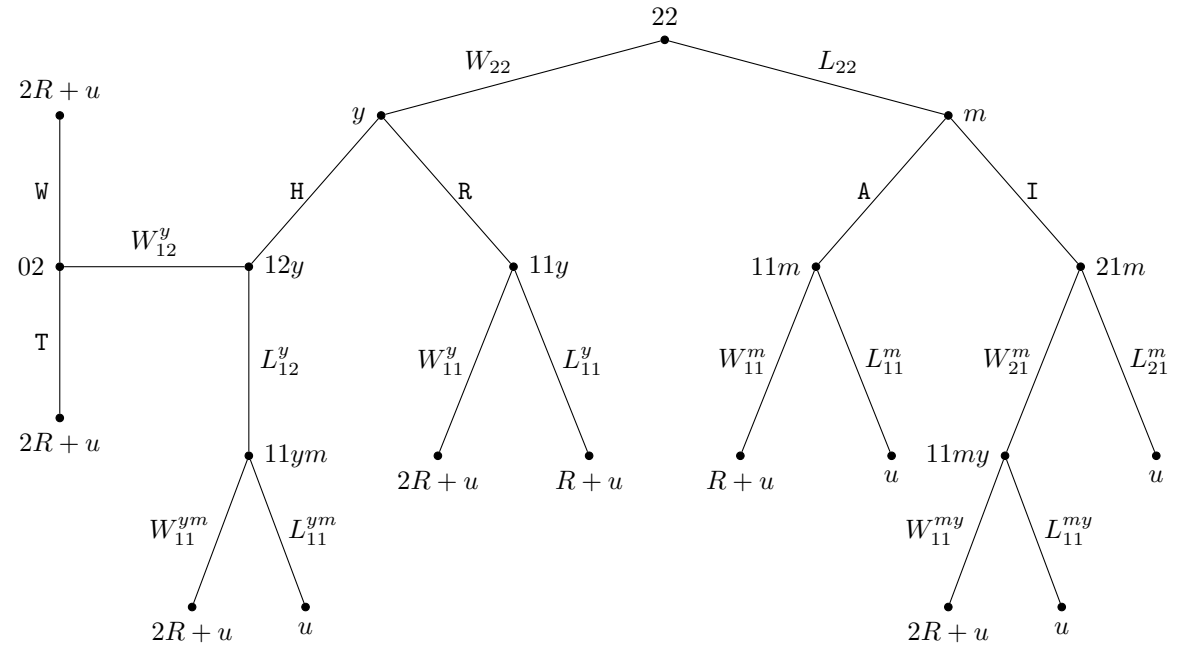


Figure 3: Tree representation of buyer's problem with d included

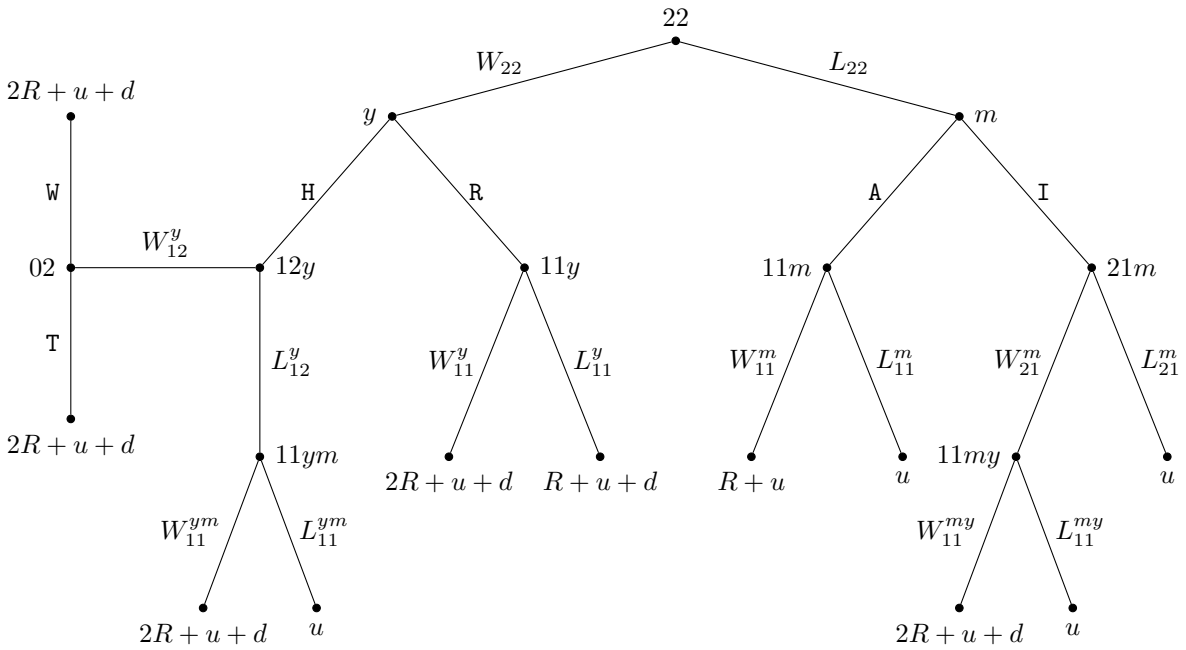


Figure 4: Tree representation of buyer's problem under $w = 0$

good if, and only if, first announced valid block includes d. As a result, payoff u must not be added to, and only to, terminal nodes that follow miner 0 revealing his or her first valid block before the remaining network announces its own. This is why payoff u has not been added to terminal nodes that follow actions (H,T) and R in figure 5.

Finally, consider the case $w = 2$ represented in figure 6. Contingencies in which buyer

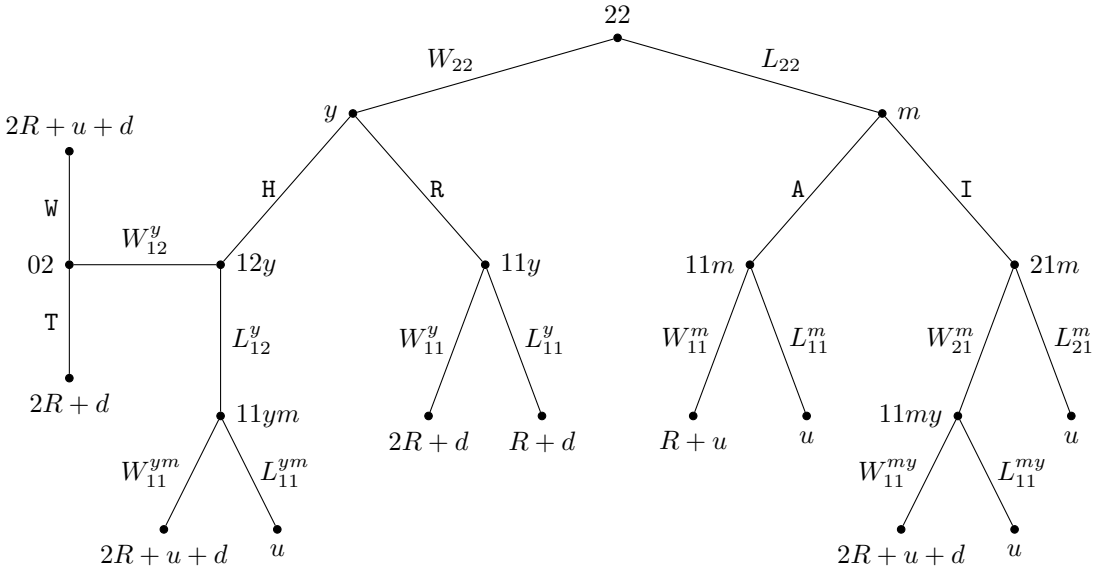


Figure 5: Tree representation of buyer's problem under $w = 1$

recovers d are the same ones discussed for $w = 0$ and $w = 1$. So, payoff d is added to the same terminal nodes in figures 4, 5 and 6. On the other hand, seller delivers the good if, and only if, d is included in the first block of the final version of the blockchain. This is why payoff u has not been added in figure 6 to, and only to, terminal nodes in which d has been added.

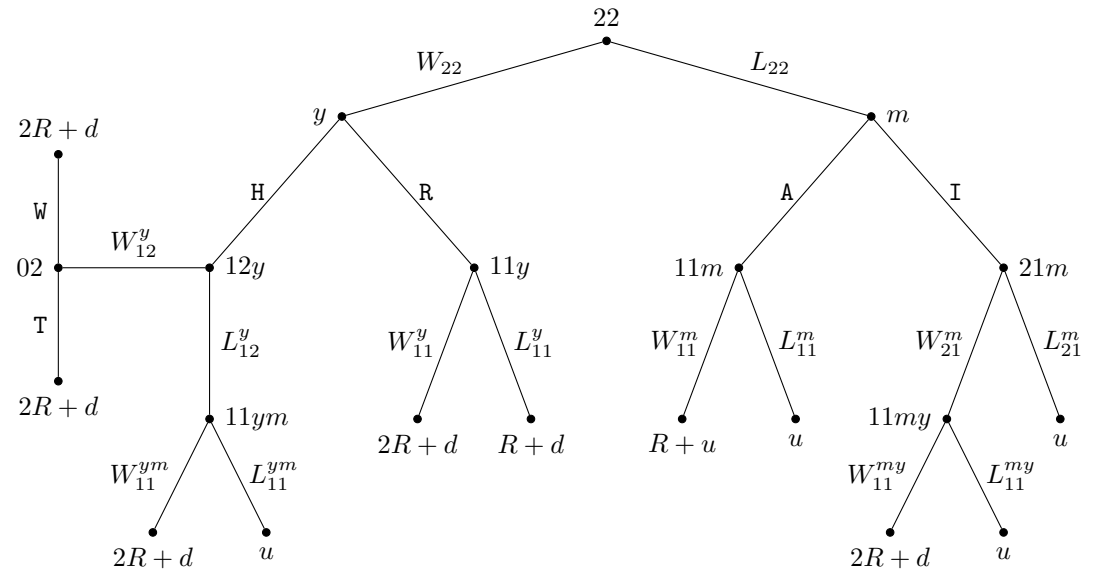


Figure 6: Tree representation of buyer's problem under $w = 2$

Remark 2 *Since u and d are never collected together in figure 6, double spending is actually not possible when $w = 2$. As a consequence of this and $d \leq u$, buyer's optimal policy when $w = 2$ must entail $c =$ `In`.*

For the case double spending is feasible ($w \neq 2$), buyer's mining problem is solved using backwards induction, similarly to the way it has been solved in lemma 1. Optimal solution is presented in lemma 2.

Lemma 2 *Suppose* $r = R - \kappa/\lambda > 0$ *and define* $f(x) = \sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}} - \left(1 + \frac{r}{2x}\right)$ *if* $x > 0$ *and* $f(0) = (d+R)/r$. *For* $h \geq 0$,

$$\Pi^0_{\texttt{Ex}}(z_h) = u + \begin{cases} (2r+d)\,\pi_{\texttt{RA}}(z_h) & \text{if } 0 \leq z_h \leq \frac{R}{d+r} \\ 2r\pi^0_{\texttt{RI}}(z_h) & \text{if } \frac{R}{d+r} < z_h \leq \frac{d+R}{r} \\ 2r\pi^0_{\texttt{HI}}(z_h) & \text{if } \frac{d+R}{r} < z_h \end{cases}, \tag{7}$$

$$\Pi^1_{\texttt{Ex}}(z_h) = u + \begin{cases} \left[r + (d+r-u)^+\right]\pi_{\texttt{RA}}(z_h) & \text{if } 0 \leq z_h \leq f(\min\{u, d+r\}) \\ 2r\pi^1_{\texttt{HA}}(z_h) & \text{if } f(\min\{u, d+r\}) < z_h \leq \frac{R}{d+r} \\ 2r\pi^1_{\texttt{HI}}(z_h) & \text{if } \frac{R}{d+r} < z_h \end{cases}, \tag{8}$$

and

$$a^{0\texttt{Ex}} = \left(a_y^{0\texttt{Ex}}, a_m^{0\texttt{Ex}}, a_{02}^{0\texttt{Ex}}\right) = \begin{cases} (\texttt{R}, \texttt{A}, x) & \text{if } 0 \leq z_h \leq \frac{R}{d+r} \\ (\texttt{R}, \texttt{I}, x) & \text{if } \frac{R}{d+r} < z_h \leq \frac{d+R}{r} \\ (\texttt{H}, \texttt{I}, x) & \text{if } \frac{d+R}{r} < z_h \end{cases} \quad \text{for } x \in \{\texttt{W}, \texttt{T}\}, \tag{9}$$

$$a^{1\texttt{Ex}} = \left(a_y^{1\texttt{Ex}}, a_m^{1\texttt{Ex}}, a_{02}^{1\texttt{Ex}}\right) = \begin{cases} (\texttt{R}, \texttt{A}, \texttt{W}) & \text{if } 0 \leq z_h \leq f(\min\{u, d+r\}) \\ (\texttt{H}, \texttt{A}, \texttt{W}) & \text{if } f(\min\{u, d+r\}) < z_h \leq \frac{R}{d+r} \\ (\texttt{H}, \texttt{I}, \texttt{W}) & \text{if } \frac{R}{d+r} < z_h \end{cases}, \tag{10}$$

where $\pi^0_{\texttt{RI}}(z) \equiv \pi_{\texttt{HI}}(z) + \frac{(d/r)z^3 + (3d/r-1)z^2 + (d/r+R/r)z}{2(1+z)^3}$, $\pi^1_{\texttt{HA}}(z) \equiv \pi_{\texttt{HI}}(z) + \frac{(d/r)z^3 + (2d/r-1)z^2 + (R/r)z_h}{2(1+z_h)^3}$, *and* $\pi^0_{\texttt{HI}}(z) = \pi^1_{\texttt{HI}}(z) \equiv \pi_{\texttt{HI}}(z) + \frac{3+z_h}{2(1+z_h)^3}(d/r)z^2$. *Optimal effort policy when*

- $w = 0$ *entails miner* $i = 0$ *choosing maximum computational effort* $\phi_0 = h$ *in all contingencies.*
- $w = 1$ *entails miner* $i = 0$ *choosing maximum computational effort* $\phi_0 = h$ *in all contingencies when* $r \geq u - d$ *and does not competing for the first block (by turning computers off) if, and only if,* $z_h < f(d+r)$ *and* $r < u - d$.

Proof. See appendix A. ■

Observe from (9) and (10) that the cases in which (H,A,W) and (R,I,x) are optimal vanish when $(u, d) \to (0, 0)$ so that $\Pi^w_{\texttt{Ex}}(z_h)$ converges to $\Pi(z_h)$.[11] That $\Pi^w_{\texttt{In}}(z_h)$ converges

[11] In effect, $\lim_{u \to d^+} f(\min\{u, d+r\}) = f(d)$ and $\lim_{d \to 0^+} f(d) = R/r$, since it equals

$$\lim_{d \to 0^+} \frac{\sqrt{r^2 + 4d(d+r+R)} - (2d+r)}{2d} = \lim_{d \to 0^+} \frac{1}{2}\left(\frac{2(2d+r+R)}{\sqrt{r^2 + 4d(d+r+R)}} - 2\right).$$

to $\Pi(z_h)$ as $(u,d) \to (0,0)$ can be trivially inferred from (5) in claim 1.

From Claim 1 and Lemma 2, buyer gets expected payoff $\Pi^w_{\texttt{In}}(z_h)$ by including transaction d in his or her accounting and gets expected payoff $\Pi^w_{\texttt{Ex}}(z_h)$ by searching for a first block without transaction d. Then, including transaction d is optimal if, and only if, $\Pi^w_{\texttt{In}}(z_h) \geq \Pi^w_{\texttt{Ex}}(z_h)$.

Lemma 3 *Optimal policy entails miner $i = 0$ choosing maximum computation effort $\phi_0 = h$ in all contingencies and*

$$(c_0, a^{0c_0}) = \begin{cases} (\textit{Ex}, [\texttt{R}, \texttt{A}, x]) & \text{if } 0 \leq z_h \leq R/(d+r) \\ (\textit{Ex}, [\texttt{R}, \texttt{I}, x]) & \text{if } R/(d+r) < z_h \leq (d+R)/r \\ (\textit{Ex}, [\texttt{H}, \texttt{I}, x]) & \text{if } (d+R)/r < z_h \end{cases}, \tag{11}$$

$$(c_1, a^{1c_1}) = \begin{cases} (\textit{In}, [\texttt{R}, \texttt{A}, \texttt{W}]) & \text{if } 0 \leq z_h \leq f(d) \\ (\textit{Ex}, [\texttt{H}, \texttt{A}, \texttt{W}]) & \text{if } f(d) < z_h \leq R/(d+r) \\ (\textit{Ex}, [\texttt{H}, \texttt{I}, \texttt{W}]) & \text{if } R/(d+r) < z_h \end{cases}, \tag{12}$$

$$(c_2, a^{2c_2}) = \begin{cases} (\textit{In}, [\texttt{R}, \texttt{A}, x]) & \text{if } 0 \leq z_h \leq R/r \\ (\textit{In}, [\texttt{H}, \texttt{I}, x]) & \text{if } R/r < z_h \end{cases}, \tag{13}$$

where $x \in \{\texttt{W}, \texttt{T}\}$. As a consequence, for $\pi^w(z) \equiv \max\{\Pi^w_{\textit{In}}(z), \Pi^w_{\textit{Ex}}(z)\}$, it holds $\pi^0(z_h) = \Pi^0_{\textit{Ex}}(z_h)$, $\pi^2(z_h) = \Pi^2_{\textit{In}}(z_h)$, and

$$\pi^1(z_h) = \begin{cases} \Pi^1_{\textit{In}}(z_h) & \text{if } 0 \leq z_h \leq f(d) \\ \Pi^1_{\textit{Ex}}(z_h) & \text{if } f(d) < z_h \end{cases}. \tag{14}$$

Proof. Conditions $\pi^2(h) = \Pi^2_{\texttt{In}}(z_h)$ and (13) follow from remark 2. Conditions $\pi^0(h) = \Pi^0_{\texttt{Ex}}(z_h)$ and (11) must hold because all payoffs in figure 4 are greater than the corresponding payoffs in figure 3 and, therefore, including transaction d cannot be optimal when $w = 0$. Consider now the case $w = 1$. Observe that $f[d(d+r)/(d+r+R)] = R/(d+r) < R/r$. Then, $\Pi^1_{\texttt{In}}(z) - \Pi^1_{\texttt{Ex}}(z)$ equals

$$\begin{cases} \pi_{\texttt{RA}}(z)\,[r - (d+r-u)^+] & \text{if } 0 \leq z \leq f(\min\{u, d+r\}) \\ 2r[\pi_{\texttt{RA}}(z) - \pi_{\texttt{HI}}(z)] - \frac{dz^3 + (2d-r)z^2 + Rz}{(1+z)^3} & \text{if } f(\min\{u, d+r\}) < z \leq f\left(\frac{d(d+r)}{d+r+R}\right) \\ 2r[\pi_{\texttt{RA}}(z) - \pi_{\texttt{HI}}(z)] - \frac{3+z}{(1+z)^3} dz^2 & \text{if } f\left(d\frac{d+r}{d+r+R}\right) < z \leq R/r \\ -\frac{3+z}{(1+z)^3} dz^2 & \text{if } R/r < z \end{cases}.$$

Thus, it is clear that $\Pi^1_{\texttt{In}}(z) < \Pi^1_{\texttt{Ex}}(z)$ when $z > R/r$. Since $u \geq d$, we have $r \geq (d+r-u)^+$. Thus, $\Pi^1_{\texttt{In}}(z) \geq \Pi^1_{\texttt{Ex}}(z)$ if $0 \leq z \leq f(\min\{u, r+d\})$. For the remaining cases, suppose

$f(\min\{u, r+d\}) < z < R/r$. Then, $[\Pi^1_{\mathtt{In}}(z) - \Pi^1_{\mathtt{Ex}}(z)](1+z)^3/z$ equals

$$\begin{cases} R - (r+2d)\,z - dz^2 & \text{if } f(\min\{u, r+d\}) < z \leq R/(d+r) \\ 2R - (2r+3d)\,z - dz^2 & \text{if } R/(d+r) < z \leq R/r \end{cases}.$$

For $P(z) \equiv 2R - (2r+3d)\,z - dz^2$, we have $P'(z) < 0$ for all $z \geq 0$ and $P[R/(d+r)] = -dR(d+r+R)/(d+r)^2 < 0$. It follows that $P(z) < 0$ for all $z \geq R/(d+r)$ and, therefore, $\Pi^1_{\mathtt{In}}(z) < \Pi^1_{\mathtt{Ex}}(z)$ for all $z \geq R/(d+r)$. For $Q(z) \equiv R - (r+2d)\,z - dz^2$, it holds $Q'(z) < 0$ for all $z \geq 0$ and $Q[f(d)] = 0$, since $f(d)^2 = \left[\sqrt{\left(\frac{r}{2d}\right)^2 + \frac{d+r+R}{d}} - \left(1 + \frac{r}{2d}\right)\right]^2 = \left[\frac{\sqrt{r^2+4d(d+r+R)} - (2d+r)}{2d}\right]^2$ and, therefore,

$$\begin{aligned} f(d)^2 d &= \frac{r^2 + 4d(d+r+R) - 2\sqrt{r^2+4d(d+r+R)}(2d+r) + (2d+r)^2}{4d} \\ &= \frac{r^2 + 2d(2d+2r+R) - [2df(d) + (2d+r)](2d+r)}{2d} \\ &= \frac{2d[2d+r+R - [f(d)+1](2d+r)]}{2d} = R - f(d)(2d+r). \end{aligned}$$

This allows us to conclude that (i) $\Pi^1_{\mathtt{In}}(z) < \Pi^1_{\mathtt{Ex}}(z)$ for all z such that $f(d) < z \leq R/(d+r) = f[d(d+r)/(d+r+R)]$; and (ii) $\Pi^1_{\mathtt{In}}(z) \geq \Pi^1_{\mathtt{Ex}}(z)$ for all z such that $f(\min\{u, d+r\}) < z \leq f(d)$. Then, we have established (14) and (12). ■

We are again interested in symmetric Nash equilibria in which every miner chooses $(a^w_y, a^w_m) = (\mathtt{R}, \mathtt{A})$ and $h = \bar{h}$. From (11), (12) and (13), $(\mathtt{R}, \mathtt{A})$'s optimality and $z_h = 1/n$ require $1 \leq nR/(d+r)$ if $w = 0$, $1 \leq nf(d)$ if $w = 1$, and $1 \leq nR/r$ if $w = 2$. Also, optimality of $h = \bar{h}$ requires $\bar{h} \in \arg\max_{h \geq 0} \{\pi^w(h) - \rho h\}$ for each w. Using notation $A_i(j) \equiv 1 + (j/2)(1 - i/2)(1 - i)$, $h = \bar{h}$'s optimality under $(\mathtt{R}, \mathtt{A})$ can be written as

$$2r\pi^w_{\mathtt{RA}}(z_{\bar{h}})A_w(d/r) - \rho\bar{h} \geq 2r\pi^w_k(z_{h^w_k}) - \rho h^w_k, \quad \forall (w, \mathtt{k}) \in OE, \tag{15}$$

where $OE = \{(0, \mathtt{RI}), (0, \mathtt{HI}), (1, \mathtt{HA}), (1, \mathtt{HI}), (2, \mathtt{HI})\}$ and $h^w_{\mathtt{k}} \in \arg\max_{h \geq 0}\{2r\pi^w_{\mathtt{k}}(z_h) - \rho h\}$, with $\pi^2_{\mathtt{HI}}(z) = \pi_{\mathtt{HI}}(z)$. Condition (15) requires $h = \bar{h}$ being a choice better than all capacity choices that can be chosen under optimal deviation $\mathtt{k}$. The set OE contains the relevant out-of-equilibrium deviations $\mathtt{k}$ for each $w \in \{0, 1, 2\}$.

Proposition 2 *For $w \in \{0, 1, 2\}$, there is a SNE whose outcome entails (**R**,**A**) if, and only if, $\bar{h} = A_w(d/r)[2rn/\rho(n+1)^2]$ and for each $\mathtt{k}$ such that $(w, \mathtt{k}) \in OE$*

$$E^w_k(1/n, r/R, d/r) \equiv 1 - \frac{\pi^w_k(z_{h^w_k}) - (\rho/2r)h^w_k}{A_w(d/r)\pi^w_{RA}(z_{\bar{h}}) - (\rho/2r)\bar{h}} \geq 0. \tag{16}$$

Proof. The result for $w = 2$ is a direct consequence of proposition 1. Suppose $w \in \{0, 1\}$. It should be clear that (R,A) is optimal under $h = \bar{h}$ only if $d \leq nR - r$ when $w = 0$ and $1 \leq nf(d)$ when $w = 1$. Then, $E^0_{\mathtt{RI}}(1/n, r/R, d/r) \geq 0$ implies $d \leq nR - r$ and $E^1_{\mathtt{HA}}(1/n, r/R, d/r) \geq 0$ implies $1 \leq nf(d)$.

Condition $\bar{h} \in \arg\max_{h \geq 0} \{\pi^w(z_h) - \rho h\}$ requires $\rho / ((1-w)d + 2r) = \pi'_{\mathtt{RA}}(z_{\bar{h}})\, z'_{\bar{h}} = 1/n\bar{h}(1 + z_{\bar{h}})^2$ and, therefore, $\bar{h} = n((1-w)d + 2r)/\rho(n+1)^2$. Clearly, inequality in (16) for each $\mathtt{k} \in OE$ is necessary and sufficient for $(\bar{h}, \mathtt{R}, \mathtt{A})$'s global optimality. In what follows, we establish that function $E^w_{\mathtt{k}}(1/n, r/R, d/r)$ is well defined. The reasoning for that is very similar to the one employed in proposition 1's proof. We present it here for completeness.

Choice $h = \bar{h}$ provides payoff $u + [2r + (1-w)d]\, \pi_{\mathtt{RA}}(z_{\bar{h}}) - \rho\bar{h}$, which equals

$$u + [(1-w)d + 2r] \left(\frac{z_{\bar{h}}}{1 + z_{\bar{h}}} - \frac{n}{(n+1)^2} \right) = u + \frac{(1-w)d + 2r}{(n+1)^2}.$$

As a consequence, $[1 + (1-w)d/2r]\pi_{\mathtt{RA}}(z_{\bar{h}}) - (\rho/2r)\bar{h} = [1 + (1-w)d/2r]/(1+n)^2$ is determined by, and only by, $(1/n, r/R, d/r)$.

The ratio $z_{h^w_{\mathtt{k}}} = h^w_{\mathtt{k}}/n\bar{h}$ is invariant to both ρ and changes in (n, R, r, d) that keeps r/R and d/r unchanged. In effect, the result for $(w, \mathtt{k}) \in \{(0, \mathtt{HI}), (1, \mathtt{HI})\}$ is proved in a way similar to that used in proposition's 1 proof. Suppose $(w, \mathtt{k}) \in \{(0, \mathtt{RI}), (1, \mathtt{HA})\}$. If $h^w_{\mathtt{k}} = 0$, then the result trivially holds. Suppose $h^w_{\mathtt{k}} > 0$ so that interior optimality condition ensures that $h^w_{\mathtt{k}}$ can be characterized by $\rho/[2r + d(1-w)] = \pi'_{\mathtt{k}}(z_{h_{\mathtt{k}}})\, z'_{h_{\mathtt{k}}} = \pi'_{\mathtt{k}}(z_{h_{\mathtt{k}}})/n\bar{h}$ must hold. Imposing $\bar{h} = [1 + (d/2r)(1-w)]2rn/\rho(1+n)^2$, it follows that $\pi'_{\mathtt{k}}(z_{h_{\mathtt{k}}}) = \rho n\bar{h}/[2r + d(1-w)] = (n/(1+n))^2$. Because $\pi'_{\mathtt{k}}(z_h)$ is invariant to ρ, depends on (n, R, r, d) only through r/R and d/r, and depends on h only through z_h, we have established that $z_{h_{\mathtt{k}}}$ is determined by, and only by, $(1/n, r/R, d/r)$. Similarly, because $\pi_{\mathtt{k}}(z_h)$ is invariant to ρ, depends on (R, r, d) only through r/R and d/r, and depends on h only through z_h, this last result allows us to conclude that

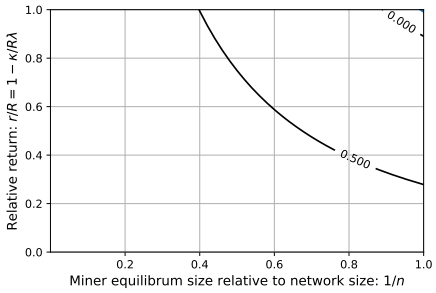
$$\pi_{\mathtt{k}}(z_{h_{\mathtt{k}}}) - \frac{\rho}{2r} h_{\mathtt{k}} = \pi_{\mathtt{k}}(z_{h_{\mathtt{k}}}) - \frac{\rho}{2r} n\bar{h} z_{h_{\mathtt{k}}} = \pi_{\mathtt{k}}(z_{h_{\mathtt{k}}}) - \left[1 + \frac{d}{2r}(1-w)\right] \left(\frac{n}{1+n}\right)^2 z_{h_{\mathtt{k}}}$$

is determined by, and only by, $(1/n, r/R, d/r)$. ■

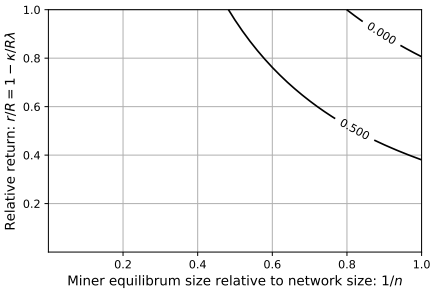
Contour plots $E^w_{\mathtt{k}}(1/n, r/R, d/r)$ are presented in figures 2, 7 and 8.[12] The contour plot for $E^2_{\mathtt{HI}}(1/n, r/R, d/r)$ coincides with that presented in figure 2 since $E^2_{\mathtt{HI}}(1/n, r/R, d/r) = E(1/n, r/R)$ for each d/r. As a consequence, equilibrium analysis presented in section 2.1 applies to the economy with double spending possibility and the maximum delayed

[12] Appendix B presents a standard numerical strategy for computing $E^w_{\mathtt{k}}(1/n, r/R, d/r)$.

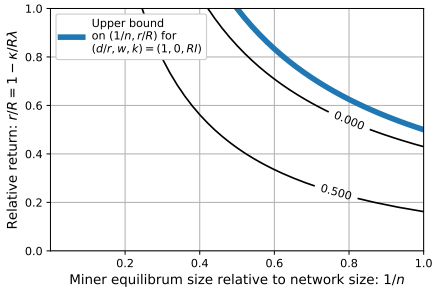
delivery ($w = 2$).



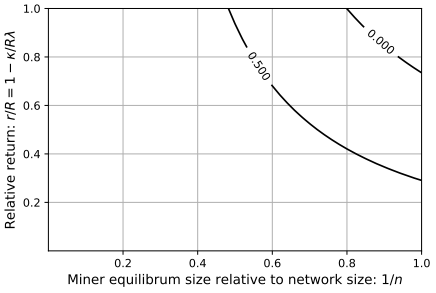
(a) $(\mathtt{k}, d/r) = (\mathtt{RI}, 0)$.



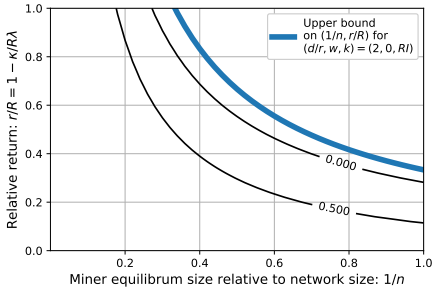
(b) $(\mathtt{k}, d/r) = (\mathtt{HI}, 0)$.



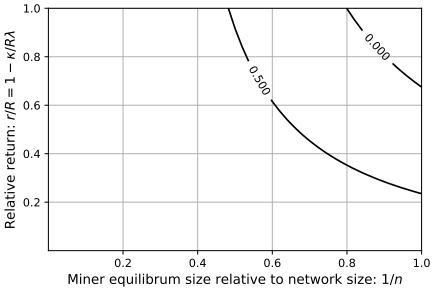
(c) $(\mathtt{k}, d/r) = (\mathtt{RI}, 1)$.



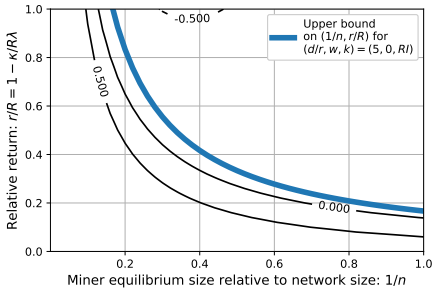
(d) $(\mathtt{k}, d/r) = (\mathtt{HI}, 1)$.



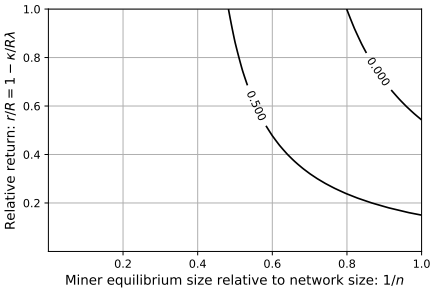
(e) $(\mathtt{k}, d/r) = (\mathtt{RI}, 2)$.



(f) $(\mathtt{k}, d/r) = (\mathtt{HI}, 2)$.



(g) $(\mathtt{k}, d/r) = (\mathtt{RI}, 5)$.



(h) $(\mathtt{k}, d/r) = (\mathtt{HI}, 5)$.

Figure 7: Contour plots for existence condition when $w = 0$.

Results in figure 7 show that, for $w = 0$, the possibility of double spending makes MSM more attractive, in the sense that *ignoring* others' valid blocks and *hiding* their

own becomes more attractive as d/r increases. Hiding valid blocks, however, becomes bad idea for large values of d/r. This is so because double rewards become relative low when compared to double spending: since delivered has already occurred ($w = 0$), revealing valid blocks (ensuring double spending) becomes better than hiding them (seeking for double rewards and risking losing double spending) as d/r increases.

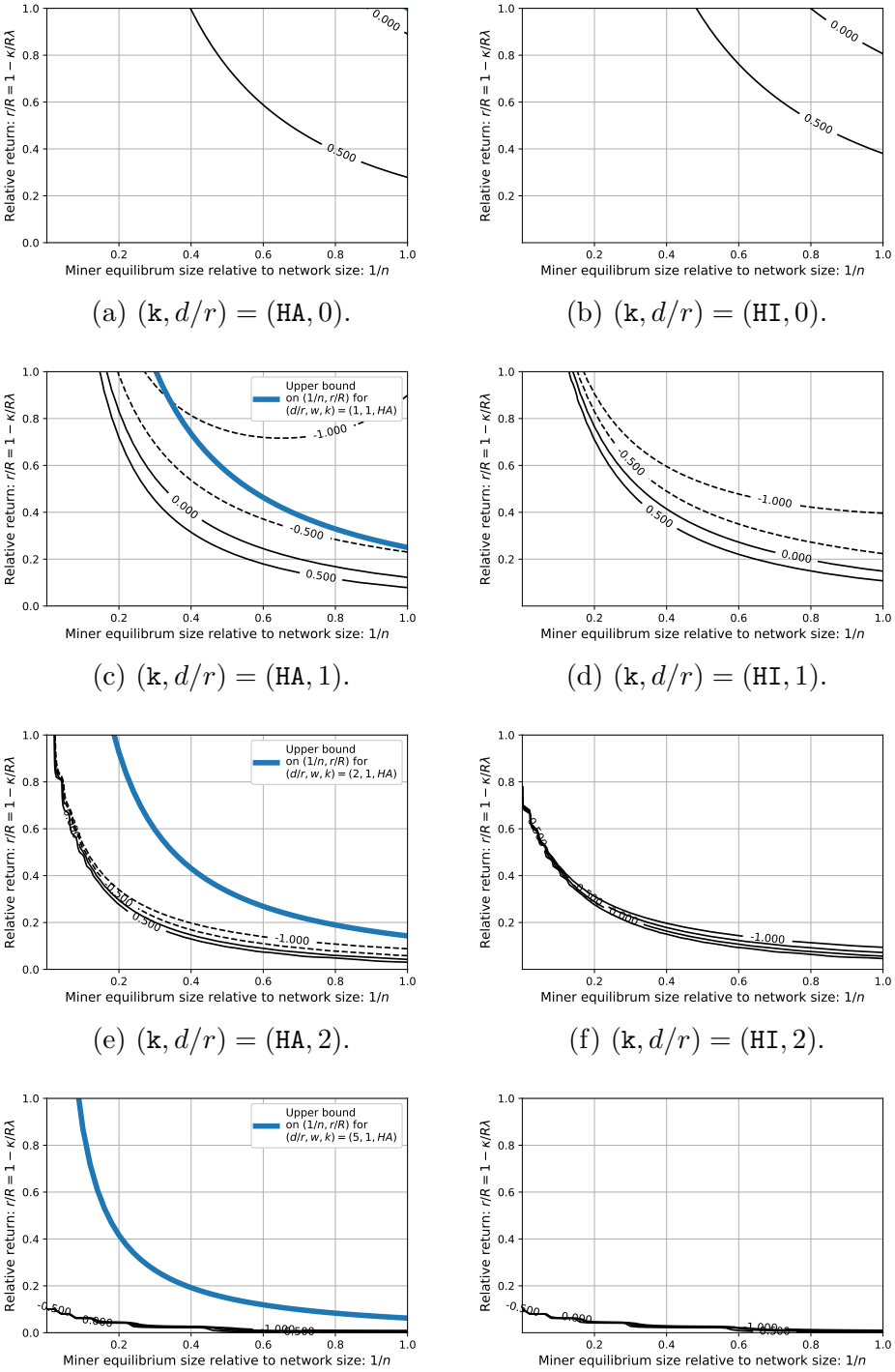
Contour map for $E^0_{\mathtt{k}}(1/n, r/R, d/r)$ is presented in figure 7 for each $\mathtt{k} \in \{\mathtt{RI}, \mathtt{HI}\}$ and for selected values to d/r. The thicker curve presented in cases with $\mathtt{k} = \mathtt{RI}$ is defined by the equation $d/r = nR/r - 1$ and shows that, as discussed in proposition 1's proof, $E^0_{\mathtt{RI}}(1/n, r/R, d/r) \geq 0$ only when $d/r \leq nR/r - 1$. Contour plots for $E^0_{\mathtt{HI}}(1/n, r/R, d/r)$ and $E^0_{\mathtt{RI}}(1/n, r/R, d/r)$ are qualitatively similar to that presented in figure 2: changes in $(1/n, r/R)$ affect incentives for deviating from $\mathtt{RA}$ to $\mathtt{k} \in \{\mathtt{RI}, \mathtt{HI}\}$ so that the strategy of *hiding* and *ignoring* new valid blocks becomes more attractive as $r/R = 1 - \kappa/R\lambda$ or $1/n$ increases. Also, both $\mathtt{RI}$ and $\mathtt{HI}$ becomes strictly more attractive than $\mathtt{RA}$ when $(1/n, r/R) \to (1, 1)$.

As d/r increases, condition $E^0_{\mathtt{k}}(1/n, r/R, d/r) \geq 0$ requires lower and lower values for $1/n$ and r/R. Also, for sufficiently low values of d/r, the relevant equilibrium condition is $E^0_{\mathtt{HI}}(1/n, r/R, d/r) \geq 0$ so that $\mathtt{HI}$ is the only relevant deviation from $\mathtt{RA}$. This is expected, since maximum expected payoffs from mining converges to $\Pi(z_h)$ as $d \to 0$. Because $E^0_{\mathtt{HI}}(1/n, r/R, d/r)$'s sensitiveness to d/r is much lower than that for $E^0_{\mathtt{RI}}(1/n, r/R, d/r)$, however, $\mathtt{RI}$ becomes the only relevant deviation when d/r is sufficiently large.

Figure 8 presents contour plots for $E^1_{\mathtt{k}}(1/n, r/R, d/r)$ for each $\mathtt{k} \in \{\mathtt{HA}, \mathtt{HI}\}$ and for selected values to d/r. The thicker curve presented in cases with $\mathtt{k} = \mathtt{HA}$ is defined by the equation $1 = nf(d)$, which can be simplified to $d/r = (nR/r - 1)n/(1 + 2n)$.[13] Qualitatively, the behavior of $E^1_{\mathtt{k}}(1/n, r/R, d/r)$ is similar to the behavior of $E^0_{\mathtt{k}}(1/n, r/R, d/r)$: the optimal deviations from the equilibrium strategy becomes more attractive with increases in $1/n$, r/R, and d/r. However, when $w = 1$, both incentives for optimal deviations are much more sensitive to changes in d/R and optimal deviations always entail *hiding* valid blocks.

As expected from the convergence to $\Pi(z_h)$ of maximum expected payoff from mining as $d \to 0$, *ignoring* composes the only relevant deviaton when d/r is sufficiently close to zero. As d/r increases, $\mathtt{HI}$ remains the relevant deviation for high r/R combined with low $1/n$, but $\mathtt{HA}$ becomes slightly more attractive than $\mathtt{HI}$ for low values of r/R combined with high $1/n$. Most important, there is no equilibrium for large values of d/r when r/R is sufficiently high, no matter the value of $1/n$.

[13] In effect, $1 = nf(d)$ is equivalent to $r + 2d(n+1)/n = \sqrt{r^2 + 4d(d + r + R)}$. This can be rewritten as $r^2 + 4d(d + r + R) = (r + 2d(n+1)/n)^2 = r^2 + 4rd(n+1)/n + 4d^2[(n+1)/n]^2$, which is equivalent to $d/r = (nR/r - 1)n/(2n + 1)$ when $d > 0$.



(a) $(\mathtt{k}, d/r) = (\mathtt{HA}, 0)$. (b) $(\mathtt{k}, d/r) = (\mathtt{HI}, 0)$.

(c) $(\mathtt{k}, d/r) = (\mathtt{HA}, 1)$. (d) $(\mathtt{k}, d/r) = (\mathtt{HI}, 1)$.

(e) $(\mathtt{k}, d/r) = (\mathtt{HA}, 2)$. (f) $(\mathtt{k}, d/r) = (\mathtt{HI}, 2)$.

(g) $(\mathtt{k}, d/r) = (\mathtt{HA}, 5)$. (h) $(\mathtt{k}, d/r) = (\mathtt{HI}, 5)$.

Figure 8: Contour plots for existence condition when $w = 1$.

Remark 3 *There is no equilibrium for large values of d/r when r/R is sufficiently high, no matter the value of $1/n$.*

Analogously to the case $w = 0$, results in figure 8 show that, for $w = 1$, the possibility

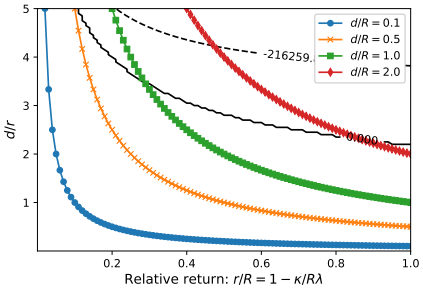
of double spending makes MSM more attractive, in the sense that *ignoring* others' valid blocks and *hiding* their own becomes more attractive as d/r increases. On the other hand, hiding valid blocks always compose the relevant optimal deviation when $w = 1$. This is so because recovering d without losing u requires convincing the payee to deliver the good, which is accomplished only after the network publishes a valid block ($w = 1$).

Ignoring others' valid blocks does not compose the relevant optimal deviaton when $1/n$ is high and r/R is low, although strategies `HA` and `HI` provide similar deviation expected payoffs. For high r/R and low $1/n$, on the other hand, ignoring is decisively more attractive than *adopting*. The attractiveness of `HI` as the optimal deviation for high r/R is so extreme that symmetric equilibrium actually vanishes for large d/r, no matter the value of $n \in \mathbb{N}$. This is a striking result considering that the equilibrium number of network's nodes is usually deemed as a measure of the network's robustness.

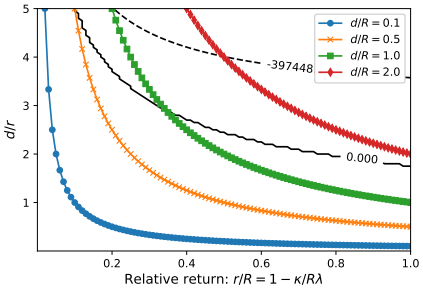
The result on nonexistence takes place for high levels of $r/R = 1 - \kappa/R\lambda$ and $d/r = d/(R - \kappa/\lambda)$. For fixed (R, d), this shows that κ/λ plays a crucial and non-trivial role on equilibrium existence. When $\kappa/\lambda \to R$, we have $(r/R, d/r) \to (0, \infty)$, while $(r/R, d/r) \to (1, d/R)$ as $\kappa/\lambda \to 0$. Lower r/R makes equilibrium strategy `RA` more attractive, but higher d/r operates to make `HI` an attractive deviation. Which force dominates is illustrated in figure 9 for selected values for $1/n$.

Figure 9 presents the contour map for $E^1_{\mathtt{k}}(1/n, r/R, d/r)$ for each $\mathtt{k} \in \{\mathtt{HA}, \mathtt{HI}\}$ and each $1/n \in \{10^{-3}, 1/3, 2/3, 1\}$. It also presents curves $d = R/10$, $d = R/2$, $d = R$, and $d = 2R$, so that it is possible to figure out how changes in r that keeps d/R fixed modify $(r/R, d/r)$. As established in figure 2, subfigures 9g and 9h show that there is not symmetric equilibrium for $r/R > 0.8$ when $d/r = 0$ and $1/n > 0.8$. As expected from figure 8, there is not symmetric equilibrium when both d/r and r/R are large, no matter $1/n$. Subfigures 9a and 9b show that equilibrium existence for low $1/n$ demands low d/R and high $r = R - \kappa/\lambda$ for a fixed (d, R), i.e., low κ/λ. This is also the case in subfigures 9c and 9d, but it can be seen that higher $1/n$ reduces the sensitiveness of equilibrium condition to changes on κ/λ that keep d/R fixed. Such sensitiveness becomes even less relevant when $1/n$ is further increased, as can be inferred from the remaining subfigures. For these cases, low d/R is the relevant factor for equilibrium existence.

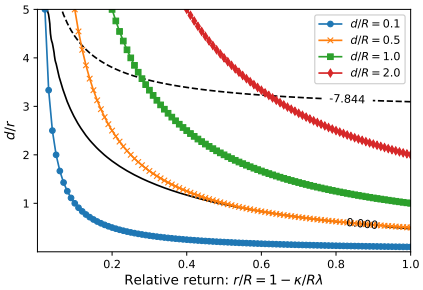
Comparing results in figures 2 and 9, the possibility of double spending ($d > 0$) changes the effect r has on equilibrium existence. If d/r could be made fixed in figure 9 as r/R changes, then higher r/R makes equilibrium strategy `RA` less attractive, as was the case in figure 2. Because $d/r > 0$ is decreased by increases in r, however, it is possible that `RA` becomes more attractive as r/R increases. This is actually the case for subfigures 9a and 9b when, for example, $d/R = 1$ and for subfigures 9c and 9d when $0.1 < d/R < 0.5$. For high $1/n$, increases in r/R that keeps d/R fixed increases



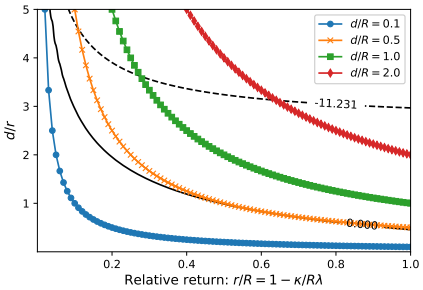
(a) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 10^{-3})$.



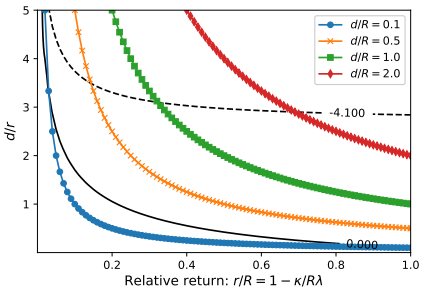
(b) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 10^{-3})$.



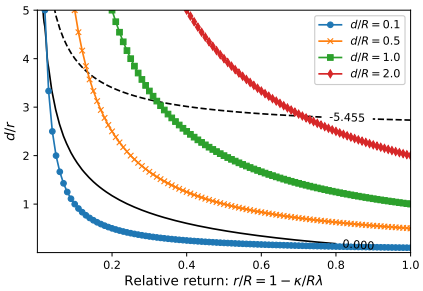
(c) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 1/3)$.



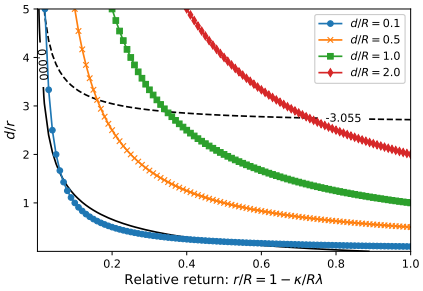
(d) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 1/3)$.



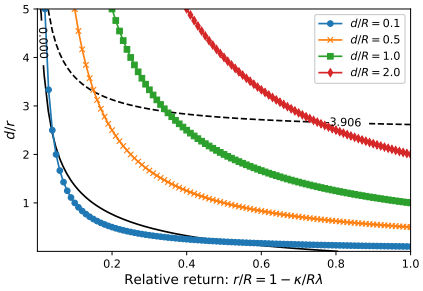
(e) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 2/3)$.



(f) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 2/3)$.



(g) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 1)$.



(h) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 1)$.

Figure 9: Existence condition under $w = 1$.

equilibrium strategy attractiveness when r/R is low and reduces it when r/R is high.

3.2 Bitcoin's average time target

Results in figure 9 show how equilibrium existence depends on $\kappa/R\lambda$, d/R and $1/n$ when $w = 1$. As noted in subsection 2.3, $1/\lambda$ represents the difficult established among nodes for finding a valid block. Because $\bar{h} = 2rn/\rho(1+n)^2$ holds in equilibrium when $w = 1$, the equilibrium average time the network spends to find a valid block, $a = \mathbb{E}\left(\min_{i\in N}\{Y_i\}\right)$, is again given by (3) so that r/R is again given by (4). As a consequence,

$$\frac{d}{r} = \frac{d}{R}\left(1 + \frac{2a\kappa}{\rho(1+1/n)}\right).$$

This suggests studying equilibrium existence under $w = 1$ as a function of $(d/R, a\kappa/\rho, 1/n)$. Results for this study is presented in figure 10.

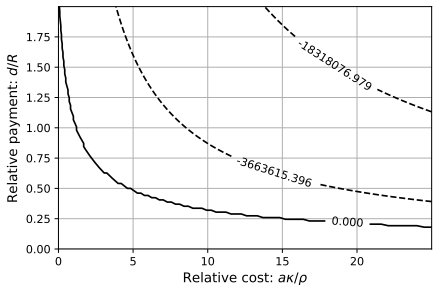
Figure 10 presents the contour map for $E^1_{\mathtt{k}}(1/n, r/R, d/r)$ for each $\mathtt{k} \in \{\mathtt{HA}, \mathtt{HI}\}$ and each $1/n \in \{10^{-3}, 1/3, 2/3, 1\}$ after imposing (4). As already established in figure 2 for the case $d/r = 0$, there is equilibrium in all cases with $1/n < 80\%$ and equilibrium existence vanishes when $1/n \approx 1$ and $a\kappa/\rho \approx 0$ (so that $r/R \approx 1$), as implied by subfigures 10g and 10h. Also, as already suggested by figure 9, figure 10 shows that the effect of $a\kappa/\rho$ on the attractiveness of equilibrium strategy dramatically changes when $d/R > 0$. For sufficiently low d/R and $1/n$ not close to 1, there is equilibrium for all reported values of $a\kappa/\rho$. However, for levels as reasonable as $d/R = 1$,[14] there is equilibrium only if both $1/n$ and $a\kappa/\rho$ are sufficiently low.

The necessity of sufficiently low $a\kappa/\rho$ for equilibrium existence shows that MSM motivated by double spending is quite different from MSM motivated by double rewards. While the latter can be made less attractive by increasing the target a for the average time valid blocks are found in equilibrium, the former is actually promoted by higher a. Of course, the same reasoning applies for the relative cost κ/ρ, but (κ, ρ) is exogenously given.

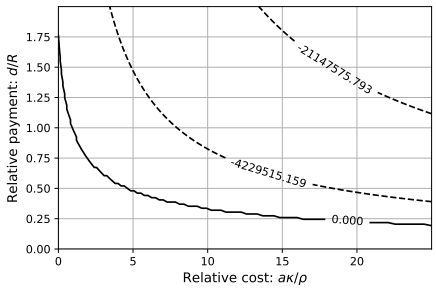
Further exploring results from figure 10 for the case average updating time is set to a, observe that equilibrium expected payoff is given by

$$2r\pi_{\mathtt{RA}}(1/n) - \rho\bar{h} = 2r\left(\frac{1/n}{1+1/n} - \frac{n}{(n+1)^2}\right) = \frac{2r}{(n+1)^2},$$

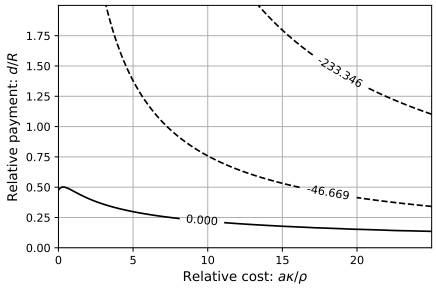
[14] For example, a miner collects all his or her mining reward by selling $d = R$ units of bitcoins.



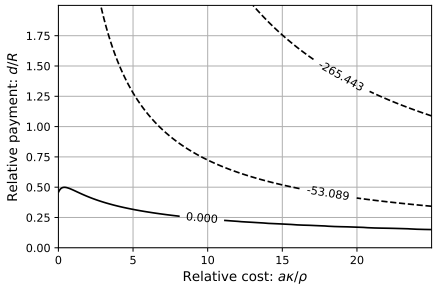
(a) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 10^{-3})$.



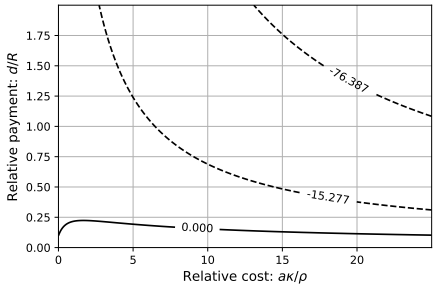
(b) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 10^{-3})$.



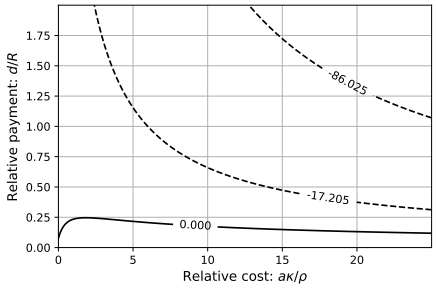
(c) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 1/3)$.



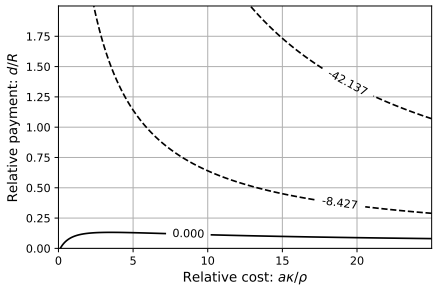
(d) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 1/3)$.



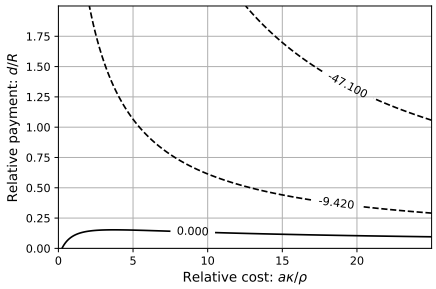
(e) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 2/3)$.



(f) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 2/3)$.



(g) $(\mathtt{k}, 1/n) = (\mathtt{HA}, 1)$.



(h) $(\mathtt{k}, 1/n) = (\mathtt{HI}, 1)$.

Figure 10: Existence condition when $w = 1$ with average time target a.

while off-equilibrium strategy HI provides expected payoff

$$\begin{aligned} 2r\pi^1_{\mathtt{HI}}(z) - \rho z n \bar{h} &= 2r\left[\pi_{\mathtt{HI}}(z) - z\frac{n^2}{(n+1)^2} + \frac{3z^2+z^3}{(1+z)^3}\frac{d}{2r}\right] \\ &= 2r\left[\pi_{\mathtt{HI}}(z) - z\frac{n^2}{(n+1)^2} + \frac{3z^2+z^3}{2(1+z)^3}\left(1+\frac{2a\kappa}{\rho(1+1/n)}\right)\frac{d}{R}\right], \end{aligned}$$

where $\pi_{\texttt{HI}}(z) = (z^3+3z^2+(1-R/r)z)/(1+z)^3 = (z^3+3z^2-2a\kappa z/\rho(1+1/n))/(1+z)^3$. Therefore,

$$\frac{2r\pi^1_{\texttt{HI}}(z)-\rho z n\bar{h}}{2r\pi_{\texttt{RA}}(1/n)-\rho\bar{h}} = (n+1)^2\left[\pi_{\texttt{HI}}(z) - z\frac{n^2}{(n+1)^2} + \frac{3z^2+z^3}{2(1+z)^3}\left(1+\frac{2a\kappa}{\rho(1+1/n)}\right)\frac{d}{R}\right], \quad (17)$$

which is clearly increasing in d/R, as already illustrated in figure 10. In words, optimal deviation attractiveness increases with d/R. The derivative of (17) with respect to $a\kappa/\rho$ is given by

$$z\frac{n(n+1)}{(1+z)^3}\left[(3z+z^2)\frac{d}{R}-2\right], \quad (18)$$

for each $z \geq 0$. It is clearly negative when $d/R = 0$ and z is optimally chosen as $z_{h_{\texttt{HI}}}$, as found in figure 2. If the optimal deviation on the relative computational capacity $z_{h_{\texttt{HI}}}$ does not converge to 0 as d/R increases, then derivative (18) becomes positive. In words, optimal deviation attractiveness increases with $a\kappa/\rho$ for large enough d/R. This is the case found in figure 10.

Claim 2 *The effect of $a = \mathbb{E}\left(\min_{i\in N}\{Y_i\}\right)$, the target for the average time network finds valid blocks in equilibrium, on the condition for equilibrium existence depends on d/R. Target $a \geq 0$ promotes the attractiveness of the equilibrium strategy if $d/R \approx 0$ but makes it less attractive otherwise.*

4 Final remarks

We have provided a game theory standard framework for understanding cryptocurrencies. It brings consistency to so many features of the Bitcoin design that we fell pretty comfortable in stating that *cryptocurrency is accounting coordination*. We have formalized the framework by proposing an accounting coordination game intended to model the management of a cryptocurrency's accounting system. It has shown useful for studying how equilibrium existence depends on well known parameters, like mining rewards, mining energy costs, computational power cost and the average time blocks are found in equilibrium.

An interesting result emerges from equilibrium analysis. Off-equilibrium multiple secret mining is made less attractive as the target for average time blocks are found increases, if there is no room for double spending. When double spending possibility is introduced in the accounting coordination game, however, the relationship is opposite: a higher target promotes off-equilibrium multiple secret mining.

For clarity and conciseness, the proposed model consciously abstracts from some features that could be shown useful by future research. In particular, restricting mining

competition to a finite number of blocks (actually only two) has shown useful for modeling accounting coordination, but equilibrium existence condition presumably changes with longer horizon. Also, we have studied existence only for symmetric equilibria, while equilibrium distribution of computational power among Bitcoin miners is actually concentrated on few players. It is our understanding, however, that our simple model does a good job formalizing the accounting coordination framework proposed to understand the essence of cryptocurrencies.

References

A. M. Antonopoulos. Mastering Bitcoin: Programming the Open Blockchain. " O'Reilly Media, Inc.", 2017.

J. D. P. Bertolai and V. A. d. A. Oliveira. Criptomoedas e Teoria Monetária: uma introdução. Análise Econômica, 38(76), 2020.

B. Biais, C. Bisiere, M. Bouvard, and C. Casamatta. The blockchain folk theorem. The Review of Financial Studies, 32(5):1662–1715, 2019.

M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan. On the instability of bitcoin without the block reward. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, pages 154–167, 2016.

J. Chiu and T. V. Koeppl. The Economics of cryptocurrencies—Bitcoin and beyond. 2019.

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

C. Ewerhart. Finite blockchain games. Economics Letters, 197:109614, 2020.

I. Eyal and E. G. Sirer. Majority is not enough: Bitcoin mining is vulnerable. In International conference on financial cryptography and data security, pages 436–454. Springer, 2014.

H. Halaburda, M. Sarvary, et al. Beyond bitcoin. The Economics of Digital Currencies, 2015.

K.-Y. Kang and S. Lee. Money, bitcoin, and monetary policy. 2020.

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

N. R. Kocherlakota. The technological role of fiat money. Federal Reserve Bank of Minneapolis. Quarterly Review-Federal Reserve Bank of Minneapolis, 22(3):2, 1998b.

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

S. Nakamoto. Bitcoin: A peer-to-peer electronic cash system. Whitepaper, 2008.

A. Narayanan, J. Bonneau, E. Felten, A. Miller, and S. Goldfeder. Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction. Princeton University Press, 2016.

F. Saleh. Blockchain without Waste: Proof-of-Stake. The Review of Financial Studies, 07 2020. ISSN 0893-9454. doi: 10.1093/rfs/hhaa075. URL https://doi.org/10.1093/rfs/hhaa075. hhaa075.

A Proofs and auxiliary results

Lemma 1 *Suppose $r \equiv R - \kappa/\lambda > 0$ and define $z_h = h/n\bar{h}$. Maximum payoff miner 0 expects to get from mining, given its computational capacity $h \geq 0$, is*

$$\Pi(z_h) \equiv \begin{cases} 2r\pi_{RA}(z_h) & \text{if } 0 \leq z_h < R/r \\ 2r\pi_{HI}(z_h) & \text{if } R/r \leq z_h \end{cases}, \tag{1}$$

where $\pi_{RA}(z) \equiv z/(1+z)$ and $\pi_{HI}(z) \equiv (z^3 + 3z^2 + (1 - R/r)z)/(1+z)^3$. Optimal policy entails miner $i = 0$ choosing maximum computation effort $\phi_0 = h$ in all effort decision node $x \in \{22, 12y, 11y, 11m, 21m, 11ym, 11my\}$,

$$(a_y, a_m) = \begin{cases} (R, A) & \text{if } 0 \leq z_h \leq R/r \\ (H, I) & \text{if } R/r < z_h \end{cases}, \qquad \text{and} \qquad a_{02} \in \{W, T\}.$$

Proof. Random variables Y_0^1 and M^1 are exponential random variables, as implied by lemma 5. Then, $W_{22} = \Pr(Y_0^1 \leq M^1) = \phi_0/(\phi_0 + n\bar{\phi})$ if miner 0 employs constant effort ϕ_0. Now, consider the situations at decision nodes $11y$ and $11m$. Because $i = 0$ and the remaining miners are starting to search for a second valid block at the same time, the probability miner 0 will find the next valid block before the network using constant effort ϕ_0 is $W_{11}^y = \Pr(Y_0^2 \leq M^2) = \phi_0/(\phi_0 + n\bar{\phi})$ at node $11y$ and $W_{11}^m = \Pr(Y_0^2 \leq M^2) = \phi_0/(\phi_0 + n\bar{\phi})$ at node $11m$, as implied by Lemma 5.

Probabilities at the remaining nodes deserve detailed examination. Consider the situation at node $12y$, in which remaining miners have been looking for a first valid block for y

units of time. Miner 0 finds a second valid block before a first valid block is found by other miners under conditional probability $W_{12}^{y} = \Pr\left(Y_0^2 \leq M^1 - y | M^1 > y\right)$. From Lemma 6, memoryless property of exponential random variables implies $W_{12}^{y} = \phi_0/(\phi_0 + n\bar{\phi})$ if miner 0 employs effort ϕ_0. The situation at node $21m$ is similar. Miner 0 has been looking for a valid first block for m units of time and, therefore, $i = 0$ completes this task before other miners find a second valid block under probability $W_{21}^{m} = \Pr\left(Y_0^1 - m \leq M^2 | Y_0^1 > m\right)$. Again, using memoryless property and Lemma 6, this probability equals $\phi_0/(\phi_0 + n\bar{\phi})$ if miner 0 employs effort ϕ_0.

At node $11ym$, $i = 0$ has been looking for a second valid block for m units of time and other miners are just starting to do so. Thus, miner 0 finds a second valid block before other miners under conditional probability $W_{11}^{ym} = \Pr(Y_0^2 - m \leq M^2 | Y_0^2 > M) = \phi_0/(\phi_0 + n\bar{\phi})$, where the memoryless property explain the last equality. Similarly, at node $11my$, other miners has been looking for a second valid block for y units of time and $i = 0$ are just starting to do so. Thus, miner 0 finds a second valid block before other miners under conditional probability $W_{11}^{my} = \Pr(Y_0^2 \leq M^2 - y | M^2 > y) = \phi_0/(\phi_0 + n\bar{\phi})$, where the memoryless property again explain the last equality.

Miner 0 faces the equivalent optimization problems at nodes $11ym$ and $11my$. Then, for $t \in \{ym, my\}$,

$$\begin{aligned} V_{11}^{t} &\equiv \max_{0 \leq \phi_0 \leq h} \left\{ 2RW_{11}^{t} + 0L_{11}^{t} - \kappa\phi_0 \mathbb{E}\left(\min\{Y_0^2 - m, M^2\} | Y_0^2 > m\right)\right\} \\ &= \max_{0 \leq \phi_0 \leq h} \left\{ \frac{\phi_0}{\phi_0 + n\bar{h}} \left(2R - \frac{\kappa}{\lambda}\right)\right\} = \frac{h}{h + n\bar{h}}(R + r) = \frac{z_h}{1 + z_h}(R + r), \end{aligned} \tag{19}$$

where the second equality is implied by Lemma 6 and the third equality follows from $R + r > 0$. At nodes $11y$ and $11m$, winning mining competition increases payoff in R units. Then, for $t \in \{m, y\}$ and $(s_y, s_m) = (R, 0)$ we have

$$\begin{aligned} V_{11}^{t} &\equiv \max_{0 \leq \phi_0 \leq h} \left[W_{11}^{t}\left(R + s_t\right) + L_{11}^{t} s_t - \kappa\mathbb{E}\left(\min\{Y_0^2, M^2\}\right)\phi_0\right] \\ &= s_t + \max_{0 \leq \phi_0 \leq h} \left(R - \frac{\kappa}{\lambda}\right) \frac{\phi_0}{\phi_0 + n\bar{\phi}} = s_t + \frac{h}{h + n\bar{\phi}} r = s_t + \frac{z_h}{1 + z_h} r, \end{aligned} \tag{20}$$

Aware of V_{11}^{ym}, the problem miner 0 faces at node $12y$ is

$$\begin{aligned} V_{12}^{y} &\equiv \max_{0 \leq \phi_0 \leq h} \left\{ 2RW_{12}^{y} + L_{12}^{y} V_{11}^{ym} - \kappa\phi_0 \mathbb{E}\left(\min\{Y_0^2, M^1 - y\} | M^1 > y\right)\right\} \\ &= \max_{0 \leq \phi_0 \leq h} \left\{ \frac{\phi_0}{\phi_0 + n\bar{\phi}} \left(2R - \frac{\kappa}{\lambda} - V_{11}^{ym}\right)\right\} + V_{11}^{ym} = V_{11}^{ym} + \frac{h}{h + n\bar{\phi}} \left(R + r - V_{11}^{ym}\right)^{+} \\ &= \frac{z_h}{1 + z_h}\left(R + r\right) + \frac{z_h}{1 + z_h}\left(\frac{R + r}{1 + z_h}\right)^{+} = \frac{(2 + z_h) z_h}{(1 + z_h)^2}\left(R + r\right), \end{aligned} \tag{21}$$

where the second equality again follows from Lemma 6. Fourth equality follows from (19) under $t = ym$. Similarly, aware of V_{11}^{my}, the problem miner 0 faces at node $21m$ is

$$\begin{aligned} V_{21}^{m} &\equiv \max_{0\leq\phi_0\leq h}\left\{W_{21}^{m}V_{11}^{my} + L_{21}^{m}0 - \kappa\phi_0\mathbb{E}\left(\min\{Y_0^1 - m, M^2\}|Y_0^1 > m\right)\right\} \\ &= \max_{0\leq\phi_0\leq h}\left\{\frac{\phi_0}{\phi_0+n\bar{\phi}}\left(V_{11}^{my}-\frac{\kappa}{\lambda}\right)\right\} = \frac{h}{h+n\bar{\phi}}\left(V_{11}^{my}-\frac{\kappa}{\lambda}\right)^{+} \\ &= \frac{z_h}{1+z_h}\left(\frac{z_h\,(R+r)}{1+z_h}+r-R\right)^{+} = \frac{z_h\left[2rz_h-(R-r)\right]^{+}}{(1+z_h)^2}, \end{aligned} \tag{22}$$

where the second equality again follows from Lemma 6. Fourth equality follows from (19) for $t = my$.

Now consider the problem $i = 0$ faces at node y. Miner 0 will choose between V_{12}^{y} and V_{11}^{y} and, therefore, optimal payoff at this node is

$$\begin{aligned} V^{y} &\equiv \max\{V_{12}^{y}, V_{11}^{y}\} = V_{11}^{y} + \max\{V_{12}^{y} - V_{11}^{y}, 0\} \\ &= V_{11}^{y} + \left[\frac{z_h(2+z_h)}{(1+z_h)^2}\,(R+r) - R - \frac{z_h}{1+z_h}r\right]^{+} \\ &= V_{11}^{y} + \left[\frac{(2z_h+z_h^2)(R+r) - R(1+z_h)^2 - r(z_h+z_h^2)}{(1+z_h)^2}\right]^{+} = V_{11}^{y} + \frac{[rz_h - R]^{+}}{(1+z_h)^2} \\ &= \begin{cases} V_{11}^{y} & \text{if } z_h \leq R/r \\ V_{12}^{y} & \text{if } z_h > R/r \end{cases}. \end{aligned}$$

Similarly, miner 0 will choose between V_{21}^{m} and V_{11}^{m} at node m. Observe that $z_h \leq (R-r)/2r$ and (22) imply $V_{21}^{m} = 0 < V_{11}^{m}$. Suppose $z_h > (R-r)/2r$ so that

$$V_{21}^{m} - V_{11}^{m} = \frac{2rz_h^2 - (R-r)z_h}{(1+z_h)^2} - \frac{rz_h}{1+z_h} = \frac{rz_h^2 - Rz_h}{(1+z_h)^2},$$

and, therefore, $V_{21}^{m} \leq V_{11}^{m}$ in this case if and only if $(R-r)/2r < z_h \leq R/r$. In summary, optimal payoff at this node is

$$V^{m} \equiv \max\{V_{11}^{m}, V_{21}^{m}\} = \begin{cases} V_{11}^{m} & \text{if } z_h \leq R/r \\ V_{21}^{m} & \text{if } z_h > R/r \end{cases}.$$

As expected, $V^{y} > V^{m}$ for all $h > 0$. In effect, (20) clearly implies that $V_{11}^{y} - V_{11}^{m} = s_y = R > 0$ and, therefore, $V^{y} = V_{11}^{y} > V_{11}^{m} = V^{m}$ when $z_h \leq R/r$. In case $z_h > R/r$, (21), (22) and $z_h > (R-r)/2r$ imply that $V_{12}^{y} > V_{21}^{m}$ since in this case

$$V_{12}^{y} - V_{21}^{m} = \frac{z_h(2+z_h)(R+r)}{(1+z_h)^2} - \frac{z_h\left[2rz_h-(R-r)\right]}{(1+z_h)^2} = z_h\frac{(3R+r)+(R-r)z_h}{(1+z_h)^2}.$$

As a consequence, $V^y > V^m$ also when $z_h > R/r$. Now, the problem miner 0 faces at node 22 is

$$\begin{aligned} V_{22} &\equiv \max_{0\le\phi_0\le h} \left\{ W_{22}V^y + L_{22}V^m - \kappa\phi_0 \mathbb{E}\left(\min\{Y_0^1, M^1\}\right)\right\} \\ &= V^m + \max_{0\le\phi_0\le h} \left\{ \frac{\phi_0}{\phi_0 + n\bar{\phi}} \left(V^y - V^m - \frac{\kappa}{\lambda}\right)\right\} = V^m + \frac{z_h}{1+z_h}\left(V^y - V^m - \frac{\kappa}{\lambda}\right)^+. \end{aligned}$$

If $z_h \le R/r$, then $V^y - V^m - \kappa/\lambda = V_{11}^y - V_{11}^m - \kappa/\lambda = R - \kappa/\lambda = r$. In this case, $V_{22} = V^m + \frac{z_h}{1+z_h} r = \frac{z_h}{1+z_h} 2r$. Similarly, if $z_h > R/r$, then $V^y = V_{12}^y$ and $V^m = V_{21}^m$. Using again (21) and (22), it follows that $z_h > R/r$ implies

$$\begin{aligned} V_{22} &= V_{21}^m + \frac{z_h}{1+z_h}\left(V_{12}^y - V_{21}^m - \frac{\kappa}{\lambda}\right)^+ \\ &= V_{21}^m + \frac{z_h}{1+z_h}\left(z_h \frac{(3R+r) + (R-r)z_h}{(1+z_h)^2} + r - R\right)^+ \\ &= V_{21}^m + \frac{z_h}{1+z_h} \frac{\left[(3R+r)z_h + (R-r)z_h^2 + (r-R)(1+2z_h+z_h^2)\right]^+}{(1+z_h)^2} \\ &= z_h \frac{2rz_h - (R-r)}{(1+z_h)^2} + z_h \frac{\left[(R+3r)z_h + (r-R)\right]^+}{(1+z_h)^3}. \end{aligned}$$

Since $z_h > R/r$, we have $(R+3r)z_h + (r-R) > R^2/r + 3R + r - R > 0$. Therefore,

$$V_{22} = \frac{(1+z_h)[2rz_h^2 - (R-r)z_h] + z_h\left[(R+3r)z_h + r - R\right]}{(1+z_h)^3} = z_h \frac{2rz_h^2 + 6rz_h - 2(R-r)}{(1+z_h)^3},$$

and the result follows. ■

Lemma 2 *Suppose $r = R - \kappa/\lambda > 0$ and define $f(x) = \sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}} - \left(1 + \frac{r}{2x}\right)$ if $x > 0$ and $f(0) = (d+R)/r$. For $h \ge 0$,*

$$\Pi_{Ex}^0(z_h) = u + \begin{cases} (2r+d)\,\pi_{RA}(z_h) & \text{if } 0 \le z_h \le \frac{R}{d+r} \\ 2r\pi_{RI}^0(z_h) & \text{if } \frac{R}{d+r} < z_h \le \frac{d+R}{r} \\ 2r\pi_{HI}^0(z_h) & \text{if } \frac{d+R}{r} < z_h \end{cases}, \tag{7}$$

$$\Pi_{Ex}^1(z_h) = u + \begin{cases} \left[r + (d+r-u)^+\right]\pi_{RA}(z_h) & \text{if } 0 \le z_h \le f(\min\{u, d+r\}) \\ 2r\pi_{HA}^1(z_h) & \text{if } f(\min\{u,d+r\}) < z_h \le \frac{R}{d+r} \\ 2r\pi_{HI}^1(z_h) & \text{if } \frac{R}{d+r} < z_h \end{cases}, \tag{8}$$

and

$$a^{0Ex} = \left(a_y^{0Ex}, a_m^{0Ex}, a_{02}^{0Ex}\right) = \begin{cases} (R, A, x) & \text{if } 0 \leq z_h \leq \frac{R}{d+r} \\ (R, I, x) & \text{if } \frac{R}{d+r} < z_h \leq \frac{d+R}{r} \\ (H, I, x) & \text{if } \frac{d+R}{r} < z_h \end{cases} \quad \text{for } x \in \{W, T\}, \quad (9)$$

$$a^{1Ex} = \left(a_y^{1Ex}, a_m^{1Ex}, a_{02}^{1Ex}\right) = \begin{cases} (R, A, W) & \text{if } 0 \leq z_h \leq f(\min\{u, d+r\}) \\ (H, A, W) & \text{if } f(\min\{u, d+r\}) < z_h \leq \frac{R}{d+r} \\ (H, I, W) & \text{if } \frac{R}{d+r} < z_h \end{cases}, \quad (10)$$

where $\pi_{RI}^0(z) \equiv \pi_{HI}(z) + \frac{(d/r)z^3+(3d/r-1)z^2+(d/r+R/r)z}{2(1+z)^3}$, $\pi_{HA}^1(z) \equiv \pi_{HI}(z) + \frac{(d/r)z^3+(2d/r-1)z^2+(R/r)z_h}{2(1+z_h)^3}$, *and* $\pi_{HI}^0(z) = \pi_{HI}^1(z) \equiv \pi_{HI}(z) + \frac{3+z_h}{2(1+z_h)^3}(d/r)z^2$. *Optimal effort policy when*

- $w = 0$ *entails miner* $i = 0$ *choosing maximum computational effort* $\phi_0 = h$ *in all contingencies.*
- $w = 1$ *entails miner* $i = 0$ *choosing maximum computational effort* $\phi_0 = h$ *in all contingencies when* $r \geq u - d$ *and does not competing for the first block (by turning computers off) if, and only if,* $z_h < f(d + r)$ *and* $r < u - d$.

Proof. The proof here is a natural extension of the demonstration employed to prove lemma 1. Consider the case $w = 1$ represented in figure 5. Buyer's decision at node 02 is trivial, since $u > 0$: waiting is always optimal at this node since it provides payoff $V_{02} = 2R + u + d > 2R + d$. At nodes $11ym$ and $11my$ buyer face the same problem. Then, for $t \in \{my, ym\}$ we have

$$\begin{aligned} V_{11}^t &\equiv \max_{0 \leq \phi_0 \leq h} \left[W_{11}^t (2R + d + u) + L_{11}^t u - \kappa \mathbb{E}\left(\min\{Y_0, Y_n\}\right) \phi_0\right] \\ &= u + \max_{0 \leq \phi_0 \leq h} \left[W_{11}^t (2R + d) - \frac{\kappa}{\lambda} \frac{\phi_0}{\phi_0 + n\bar{h}}\right] = u + \max_{0 \leq \phi_0 \leq h} \left[\frac{\phi_0}{\phi_0 + n\bar{h}} \left(2R + d - \frac{\kappa}{\lambda}\right)\right] \\ &= u + \frac{h}{h + n\bar{h}} (d + r + R) = u + \frac{z_h}{1 + z_h} (d + r + R). \end{aligned}$$

At nodes $11y$ and $11m$, winning mining competition increases payoff in R units. Then, for $t \in \{m, y\}$ and $(s_y, s_m) = (R + d, u)$ we have

$$\begin{aligned} V_{11}^t &\equiv \max_{0 \leq \phi_0 \leq h} \left[W_{11}^t (R + s_t) + L_{11}^t s_t - \kappa \phi_0 \mathbb{E}\left(\min\{Y_0, Y_n\}\right)\right] \\ &= s_t + \max_{0 \leq \phi_0 \leq h} \left(R - \frac{\kappa}{\lambda}\right) \frac{\phi_0}{\phi_0 + n\bar{h}} = s_t + \frac{h}{h + n\bar{h}} r = s_t + \frac{z_h}{1 + z_h} r. \end{aligned}$$

The problem at node $21m$ is

$$\begin{aligned}
V_{21}^{m} &\equiv \max_{0\leq\phi_0\leq h}\left[W_{21}^{m}V_{11}^{my}+L_{21}^{m}u-\kappa\mathbb{E}\left(\min\{Y_0,Y_n\}\right)\phi_0\right]\\
&= u+\max_{0\leq\phi_0\leq h}\left[W_{21}^{m}\left(\frac{z_h}{1+z_h}\left(d+r+R\right)\right)-\frac{\kappa}{\lambda}\frac{\phi_0}{\phi_0+n\bar{h}}\right]\\
&= u+\max_{0\leq\phi_0\leq h}\frac{\phi_0}{\phi_0+n\bar{h}}\left(\frac{z_h}{1+z_h}\left(d+r+R\right)-\frac{\kappa}{\lambda}\right)\\
&= u+\frac{z_h}{1+z_h}\left(\frac{z_h}{1+z_h}\left(d+r+R\right)+r-R\right)^{+}\\
&= u+\left(\frac{\left(d+r+R\right)z_h^2+(r-R)z_h(1+z_h)}{(1+z_h)^2}\right)^{+}=u+\frac{\left[\left(d+2r\right)z_h^2+(r-R)z_h\right]^{+}}{(1+z_h)^2}.
\end{aligned}$$

The problem at node $12y$ is

$$\begin{aligned}
V_{12}^{y} &\equiv \max_{0\leq\phi_0\leq h}\left[W_{12}^{y}V_{02}+L_{12}^{y}V_{11}^{ym}-\kappa\mathbb{E}\left(\min\{Y_0,Y_n\}\right)\phi_0\right]\\
&= V_{11}^{ym}+\max_{0\leq\phi_0\leq h}W_{12}^{y}\left(2R+d-\frac{z_h}{1+z_h}\left(d+r+R\right)-\frac{\kappa}{\lambda}\right)\\
&= V_{11}^{ym}+\max_{0\leq\phi_0\leq h}\frac{\phi_0}{\phi_0+n\bar{h}}\left(1-\frac{z_h}{1+z_h}\right)\left(d+r+R\right)\\
&= u+\frac{z_h}{1+z_h}\left(d+r+R\right)+\frac{z_h}{(1+z_h)^2}\left(d+r+R\right)=u+\frac{z_h^2+2z_h}{(1+z_h)^2}\left(d+r+R\right).
\end{aligned}$$

Then, the decision between `A` and `I` at node m solves the problem

$$\begin{aligned}
V^{m} &\equiv \max\left\{V_{11}^{m},V_{21}^{m}\right\}=\max\left\{u+\frac{z_h}{1+z_h}r,u+\frac{\left[\left(d+2r\right)z_h^2+(r-R)z_h\right]^{+}}{(1+z_h)^2}\right\}\\
&= u+\frac{z_h}{(1+z_h)^2}\max\left\{r(1+z_h),\left[\left(d+2r\right)z_h+(r-R)\right]^{+}\right\}\\
&= u+\frac{z_h}{(1+z_h)^2}\max\left\{r(1+z_h),\left(d+2r\right)z_h+(r-R)\right\}\\
&= u+\frac{z_h}{(1+z_h)^2}\left[r(1+z_h)+\max\left\{0,\left(d+2r\right)z_h+(r-R)-r(1+z_h)\right\}\right]\\
&= u+\frac{z_h}{(1+z_h)^2}\left[r(1+z_h)+\left(\left(d+r\right)z_h-R\right)^{+}\right].
\end{aligned}$$

and, therefore, `A` is optimal if and only if $0\leq z_h\leq R/(d+r)=f\left[d(d+r)/(d+r+R)\right]$.

Similarly, the decision between H and R at node y solves the problem

$$\begin{aligned} V^y &\equiv \max\{V_{11}^y, V_{12}^y\} = \max\left\{R+d+\frac{z_h}{1+z_h}r, u+\frac{z_h^2+2z_h}{(1+z_h)^2}(d+r+R)\right\} \\ &= R+d+\frac{z_h}{1+z_h}r+\max\left\{0, u-R-d+\frac{z_h^2+2z_h}{(1+z_h)^2}(d+r+R)-\frac{z_h}{1+z_h}r\right\} \\ &= R+d+\frac{z_h}{1+z_h}r+\left[\frac{(u-R-d)(1+z_h)^2+(z_h^2+2z_h)(d+r+R)-rz_h(1+z_h)}{(1+z_h)^2}\right]^+ \\ &= R+d+\frac{z_h}{1+z_h}r+\frac{\left[(u-R-d)+z_h(2u+r)+z_h^2u\right]^+}{(1+z_h)^2}, \end{aligned}$$

and, therefore, R at node y is optimal if and only if $(u-R-d)+z_h(2u+r)+z_h^2u \leq 0$ and $z_h \geq 0$. Equivalently, $z_h \geq 0$ and

$$\frac{-\sqrt{(2u+r)^2-4u(u-R-d)}-(2u+r)}{2u} \leq z_h \leq \frac{\sqrt{(2u+r)^2-4u(u-R-d)}-(2u+r)}{2u}.$$

This can be rewritten as

$$0 \leq z_h \leq \sqrt{\left(1+\frac{r}{2u}\right)^2-\left(1-\frac{R+d}{u}\right)}-\left(1+\frac{r}{2u}\right) = \sqrt{\left(\frac{r}{2u}\right)^2+\frac{d+r+R}{u}}-\left(1+\frac{r}{2u}\right).$$

As a conclusion, R is optimal at node y is optimal only if $0 \leq z_h \leq f(u)$. Because $f(u) \geq 0$ iff $u \leq d+R$, revealing at node y is never optimal if $u > d+R$.

Finally, the problem miner faces at node 22 is

$$\begin{aligned} V_{22} &\equiv \max_{0\leq\phi_0\leq h}\left[W_{22}V^y+L_{22}V^m-\kappa\mathbb{E}\left(\min\{Y_0,Y_n\}\right)\phi_0\right] \\ &= V^m+\max_{0\leq\phi_0\leq h}W_{22}\left[V^y-V^m-\frac{\kappa}{\lambda}\right]. \end{aligned}$$

Observe that the objective function equals

$$\begin{aligned} W_{22}\Bigg[R+d+\frac{z_h}{1+z_h}r+\frac{\left[(u-R-d)+z_h(2u+r)+z_h^2u\right]^+}{(1+z_h)^2}-u-\frac{\kappa}{\lambda} \\ -\frac{z_h}{(1+z_h)^2}\left[r(1+z_h)+\left((d+r)z_h-R\right)^+\right]\Bigg] \\ = W_{22}\frac{\left[(u-R-d)+z_h(2u+r)+z_h^2u\right]^+-z_h\left[(d+r)z_h-R\right]^+-(r+d-u)(1+z_h)^2}{(1+z_h)^2}. \end{aligned}$$

We already know that $\left[(u-R-d)+z_h(2u+r)+z_h^2u\right]^+ = 0$ iff $0 \leq z_h \leq f(u)$. In this case, R is the optimal policy at node y. Otherwise, H is the optimal policy at this node. Also, $\left[(d+r)z_h-R\right]^+ = 0$ iff $0 \leq z_h \leq R/(d+r) = f\left[d(d+r)/(d+r+R)\right]$. In this case,

A is the optimal policy at node m. Otherwise, I is optimal at this node. Because $u \geq d > d(d+r)/(d+r+R)$ and $f(x)$ is strictly decreasing, we have $f(u) < f[d(d+r)/(d+r+R)]$. Then, objective function can be rewritten as

$$\begin{cases} W_{22}(r+d-u) & \text{if } 0 \leq z_h \leq f(u) \\ W_{22}\frac{(r+d)z_h^2+(3r+2d)z_h-(R-r)}{(1+z_h)^2} & \text{if } f(u) < z_h \leq f[d(d+r)/(d+r+R)] \\ W_{22}\frac{(3r+2d+R)z_h-(R-r)}{(1+z_h)^2} & \text{if } f[d(d+r)/(d+r+R)] < z_h \end{cases}, \tag{23}$$

where the subsequent optimal policy is (R, A) in the first case, equals (H,A) in the second case, and is given by (H,I) in the third case.

The objective function in the third case of (23) is nonnegative only if $z_h \geq (R-r)/(3r+2d+R)$. Because $z_h > R/(d+r) = f(d(d+r)/(d+r+R))$ implies $z_h > (R-r)/(3r+2d+R)$, objective function in third case is always positive. The objective function in the second case of (23) is nonnegative only if $z_h \geq f(d+r)$. Also, since $(d+r) > (d+r)d/(d+r+R)$ and $f(x)$ is decreasing, it holds $f(d+r) < f[(d+r)d/(d+r+R)]$.

It follows from these observations that there are two relevant cases in maximizing (23): (i) $d \leq u \leq d+r$ and (ii) $d+r < u$. Suppose (i) so that $W_{22}(r+d-u) \geq 0$ and $f(u) \geq f(d+r)$. Then, objective function is also nonnegative in first and second cases of (23) under (i). Because objective function is nonnegative in all cases under (i), choosing $W_{22} = z_h/(1+z_h)$ maximizes (23) under (i). Now, suppose (ii) so that $W_{22}(r+d-u) < 0$ and $f(u) < f(r+d)$. Then, it is optimal to choose $W_{22} = 0$, by making $\phi_0 = 0$, when z_h satisfy $0 \leq z_h \leq f(r+d)$ and $W_{22} = z_h/(1+z_h)$ otherwise. It follows from this reasoning that V_{22} can be rewritten as

$$V_{22} = \begin{cases} V^m + \frac{z_h}{1+z_h}(r+d-u)^+ & \text{if } 0 \leq z_h \leq f(\min\{u, r+d\}) \\ V^m + \frac{z_h}{1+z_h}\frac{(r+d)z_h^2+(3r+2d)z_h-(R-r)}{(1+z_h)^2} & \text{if } f(\min\{u, r+d\}) < z_h \leq f\left(\frac{d(d+r)}{d+r+R}\right) \\ V^m + \frac{z_h}{1+z_h}\frac{[(3r+2d+R)z_h-(R-r)]}{(1+z_h)^2} & \text{if } f\left(d\frac{d+r}{d+r+R}\right) < z_h \end{cases}.$$

Then, using $V^m = u + \frac{z_h}{(1+z_h)^2}\left[r(1+z_h) + ((d+r)z_h - R)^+\right]$, it follows that V_{22} equals

$$\begin{aligned} u + &\begin{cases} \frac{z_h}{(1+z_h)}\left[r + (r+d-u)^+\right] & \text{if } 0 \leq z_h \leq f(\min\{u, r+d\}) \\ \frac{rz_h}{(1+z_h)} + \frac{(r+d)z_h^3+(3r+2d)z_h^2-(R-r)z_h}{(1+z_h)^3} & \text{if } f(\min\{u, r+d\}) < z_h \leq f\left(\frac{d(d+r)}{d+r+R}\right) \\ \frac{(d+2r)z_h^2-(R-r)z_h}{(1+z_h)^2} + \frac{(3r+2d+R)z_h^2-(R-r)z_h}{(1+z_h)^3} & \text{if } f\left(d\frac{d+r}{d+r+R}\right) < z_h \end{cases} \\ &= u + \begin{cases} \frac{z_h}{(1+z_h)}\left[r + (r+d-u)^+\right] & \text{if } 0 \leq z_h \leq f(\min\{u, r+d\}) \\ \frac{(d+2r)z_h^3+(5r+2d)z_h^2-(R-2r)z_h}{(1+z_h)^3} & \text{if } f(\min\{u, r+d\}) < z_h \leq f\left(\frac{d(d+r)}{d+r+R}\right) \\ \frac{(d+2r)z_h^3+(6r+3d)z_h^2-2(R-r)z_h}{(1+z_h)^3} & \text{if } f\left(d\frac{d+r}{d+r+R}\right) < z_h \end{cases}. \end{aligned}$$

and the result follows.

Now, consider the case $w = 0$. Because this case is easier to solve than the case $w = 1$ and the reasoning for establishing results in both cases are very similar, for $w = 0$ we just report main ideas and results. Clearly, optimal policy at node 02 is $a_{02}^{\texttt{0EX}} \in \{\texttt{W}, \texttt{T}\}$ and $V_{02} = 2R + u + d$. For $t \in \{my, ym\}$, $V_{11}^t = u + \frac{z_h}{1+z_h}(d + r + R)$. For $t \in \{m, y\}$ and $(s_m, s_y) = (u, R + d + u)$, $V_{11}^t = s_t + \frac{z_h}{1+z_h} r$. For nodes $12y$ and $21m$ we have

$$V_{12}^y = u + \frac{2z_h + z_h^2}{(1 + z_h)^2}(d + r + R) \quad \text{and} \quad V_{21}^m = u + \frac{[(d + 2r)z_h^2 - (R - r)z_h]^+}{(1 + z_h)^2}.$$

It follows from these results that $V_{11}^m \leq V_{21}^m$ and $a_m^{\texttt{0Ex}} = \texttt{I}$ if, and only if, $z_h \geq R/(d + r)$. Also, $V_{11}^y \leq V_{12}^y$ and $a_m^{\texttt{0Ex}} = \texttt{H}$ if, and only if, $z_h \geq (d + R)/r$. Thus,

$$\begin{aligned} V^y &= u + \frac{rz_h(1 + z_h) + [rz_h - R - d]^+ + (d + R)(1 + z_h)^2}{(1 + z_h)^2}, \\ V^m &= u + \frac{rz_h(1 + z_h) + z_h\,[(d + r)z_h - R]^+}{(1 + z_h)^2}. \end{aligned}$$

Comparing V^y to V^m in each of three cases, $z_h \in [0, R/(d+r)]$, $z_h \in [R/(d+r), (d+R)/r]$, and $z_h \geq (d + R)/r$, we get (9) and

$$V_{22} = \begin{cases} u + \frac{(d+2r)z_h}{1+z_h} & \text{if } 0 \leq z_h \leq R/(d + r) \\ u + \frac{(d+2r)z_h^3 + (3d+5r)z_h^2 + (d+2r-R)z_h}{(1+z_h)^3} & \text{if } R/(d + r) \leq z_h \leq (d + R)/r \\ u + \frac{(d+2r)z_h^3 + (3d+6r)z_h^2 - 2(R-r)z_h}{(1+z_h)^3} & \text{if } z_h \geq (d + R)/r \end{cases},$$

from which (7) follows from making $\Pi_{\texttt{Ex}}^0(z_h) = V_{22}$. ■

Lemma 4 *Let $x \in \mathbb{R}_+^2$ such that $\|x\| = 1$. Then, there is a unique $\varepsilon > 0$ such that $E\,[(1, 1) - \varepsilon x] = 0$ and $E\,[(1, 1) - tx]\,(t - \varepsilon) > 0$ for all $t \geq 0$ such that $t \neq \varepsilon$.*

Proof. Observe that $E(1/n, r/R) = 1 - [2r\pi_{\texttt{HI}}\,(z_{h_{\texttt{HI}}}) - \rho h_{\texttt{HI}}]/[2r\pi_{\texttt{RA}}\,(z_{\bar{h}}) - \rho\bar{h}]$. We know that $2r\pi_{\texttt{RA}}(z_{\bar{h}}) - \rho\bar{h} > 2r\pi_{\texttt{HI}}\,(z_h) - \rho h$ for all $h \geq 0$ such that $z_h \leq R/r$ and $h \neq \bar{h}$. Therefore, $E(1/n, r/R) > 0$ when $h_{\texttt{HI}} = n\bar{h}R/r > \bar{h}$, where the last inequality follows from $n \geq 1$ and $R > r$.

Because $\pi_{\texttt{HI}}\,(z_h)$ is strictly concave in h for $h \geq n\bar{h}R/r$, as implied by lemma 7, corner solution $h_{\texttt{HI}} = n\bar{h}R/r$ holds iff $\pi'_{\texttt{HI}}\,(R/r)\,z'_{n\bar{h}R/r} \leq \rho/2r$. This is equivalent to $\pi'_{\texttt{HI}}\,(R/r) \leq \rho n\bar{h}/2r = (n/(1 + n))^2$. For $t \geq 0$ such that $(1/n, r/R) = (1, 1) - t(x_1, x_2)$, this is equivalent to

$$C(t) \equiv \left(\frac{n}{1 + n}\right)^2 - \pi'_{\texttt{HI}}\left(\frac{R}{r}\right) = \left(\frac{n}{1 + n}\right)^2 - \frac{1 + 2R/r}{(1 + R/r)^3} \geq 0,$$

where $n = 1/(1-tx_1)$ and $R/r = 1/(1-tx_2)$ must be understood as a function of t. Observe that $0 < r < R$ implies $x_2 > 0$ and, therefore, it follows from $x \in \mathbb{R}^2_+$ that

$$\begin{aligned} C'(t) &= \frac{2n}{(1+n)^3}\frac{\partial n}{\partial t} - \frac{2(1+R/r)^3 - 3(1+R/r)^2(1+2R/r)}{(1+R/r)^6}\frac{\partial (R/r)}{\partial t} \\ &= \frac{2n}{(1+n)^3}\frac{x_1}{(1-tx_1)^2} + \frac{1+4R/r}{(1+R/r)^4}\frac{x_2}{(1-tx_2)^2} > 0. \end{aligned}$$

Also, $C(0) = -1/8 < 0$, $C(t) \to 1/(2-x_1/x_2)^2 > 0$ as $t \to 1/x_2$ when $x_2 \geq x_1$, and $C(t) \to 1 - \frac{1+2/(1-x_2/x_1)}{(1+1/(1-x_2/x_1))^3} > 0$ as $t \to 1/x_1$ when $x_2 < x_1$. Because $C(t)$ is continuous, there exists $\delta > 0$ with $1/\delta > \max\{x_1, x_2\}$ such that $C(\delta) = 0$, $C(t) < 0$ for $t < \delta$ and $C(t) > 0$ for $t > \delta$. It follows from this reasoning that corner solution $h_{\texttt{HI}} = n\bar{h}R/r$ arises if, and only if, $t \geq \delta$ and $(1/n, r/R) = (1,1) - t(x_1, x_2)$, in which case $E(1/n, r/R) > 0$.

In order to study the case $h_{\texttt{HI}} > n\bar{h}R/r$, suppose $(1/n, r/R) = (1,1) - t(x_1, x_2)$ for some $t \geq 0$ such that $C(t) < 0$. Then, $t < \delta$ and $1/\delta > \max\{x_1, x_2\}$. We know that $E(1/n, r/R) > 0$ for $t \approx \delta$ follows from $h_{\texttt{HI}} \approx n\bar{h}R/r$ and $E(1/n, r/R)$'s continuity. In order to study the case $t \approx 0$, observe that $2r\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) - \rho h_{\texttt{HI}} > 2r\pi_{\texttt{HI}}(R/r) - \rho n\bar{h}R/r$, since $h_{\texttt{HI}} > n\bar{h}R/r$ and $2r\pi_{\texttt{HI}}(z_h) - \rho h$ is strictly concave in h for $h \geq n\bar{h}R/r$. For $t = 0$, we have $n = R/r = 1$, which implies $\bar{h} = n\bar{h}R/r = 2r/\rho$ and $\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) - (\rho/2r)h_{\texttt{HI}} > \pi_{\texttt{HI}}(1) - 1$. Then,

$$E(1/n, r/R) = E(1,1) = 1 - \frac{\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) - (\rho/2r)h_{\texttt{HI}}}{\pi_{\texttt{RA}}(1/n) - (\rho/2r)\bar{h}} < 1 - \frac{\pi_{\texttt{HI}}(1) - 1}{\pi_{\texttt{RA}}(1) - 1} = 0,$$

where last equality follows from $\pi_{\texttt{RA}}(R/r) = \pi_{\texttt{HI}}(R/r)$. We now show that $E(1-tx_1, 1-tx_2)$ is strictly increasing in t. Observe that $E(1/n, r/R)$ equals

$$1 - \frac{\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) - (\rho/2r)n\bar{h}z_{h_{\texttt{HI}}}}{\pi_{\texttt{RA}}(z_{\bar{h}}) - (\rho/2r)\bar{h}} = 1 - \frac{\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) - \frac{n^2}{(1+n)^2}z_{h_{\texttt{HI}}}}{1/(1+n)^2} = 1 + n^2 z_{h_d} - (1+n)^2\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}).$$

and

$$\frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial t} = \frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (1/n)}\frac{\partial (\frac{1}{n})}{\partial t} + \frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (r/R)}\frac{\partial (\frac{r}{R})}{\partial t} = (-1)\left[\frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (1/n)}x_1 + \frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (r/R)}x_2\right].$$

Interior $h_{\texttt{HI}}$'s optimality condition is $2r\pi'_{\texttt{HI}}(z_{h_{\texttt{HI}}})z'_{h_{\texttt{HI}}} = \rho$, which implies $\pi'_{\texttt{HI}}(z_{h_{\texttt{HI}}}) = [n/(1+n)]^2$. Using this condition, we get $\frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (r/R)} > 0$ since

$$\begin{aligned} \frac{\partial E(\frac{1}{n}, \frac{r}{R})}{\partial (r/R)} &= \left[n^2 - (1+n)^2\pi'_{\texttt{HI}}(z_{h_{\texttt{HI}}})\right]\frac{\partial z_{h_{\texttt{HI}}}}{\partial (r/R)} - (1+n)^2\frac{\partial \pi_{\texttt{HI}}(z_{h_{\texttt{HI}}})}{\partial (r/R)} = \frac{(1+n)^2 z_{h_{\texttt{HI}}}}{(1+z_{h_{\texttt{HI}}})^3}\frac{\partial (R/r)}{\partial (r/R)} \\ &= \frac{(1+n)^2 z_{h_{\texttt{HI}}}}{(1+z_{h_{\texttt{HI}}})^3}\frac{(-1)}{(r/R)^2} < 0. \end{aligned}$$

Using again $\pi'_{\texttt{HI}}(z_{h_{\texttt{HI}}}) = [n/(1+n)]^2$, we get

$$\frac{\partial E(1/n, r/R)}{\partial(1/n)} = 2[nz_{h_{\texttt{HI}}} - (1+n)\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}})]\frac{\partial(n)}{\partial(1/n)} + \left[n^2 - (1+n)^2\pi'_{\texttt{HI}}(z_{h_{\texttt{HI}}})\right]\frac{\partial z_{h_{\texttt{HI}}}}{\partial(1/n)}$$
$$= 2[nz_{h_{\texttt{HI}}} - (1+n)\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}})]\frac{(-1)}{(1/n)^2} < 0,$$

where the inequality is established in what follows. Strict concavity of $\pi_{\texttt{HI}}(z)$ at each $z \geq R/r$ implies $\pi_{\texttt{HI}}(z) < \pi_{\texttt{HI}}(R/r) + \pi'_{\texttt{HI}}(R/r)[z - R/r]$ for all $z > R/r$. In particular, $\pi_{\texttt{HI}}(z_{h_{\texttt{HI}}}) < \pi_{\texttt{HI}}(R/r) + \pi'_{\texttt{HI}}(R/r)[z_{h_{\texttt{HI}}} - R/r]$. Then,

$$\begin{aligned}
\frac{1}{2n^2}\frac{\partial E(1/n, r/R)}{\partial(1/n)} &< (1+n)\left[\pi_{\texttt{HI}}(R/r) + \pi'_{\texttt{HI}}(R/r)(z_{h_{\texttt{HI}}} - R/r)\right] - nz_{h_{\texttt{HI}}} \\
&= (1+n)\left[\pi_{\texttt{RA}}(R/r) + \pi'_{\texttt{HI}}(R/r)(z_{h_{\texttt{HI}}} - R/r)\right] - nz_{h_{\texttt{HI}}} \\
&= (1+n)\left[\frac{R/r}{1+R/r} + \frac{1+2R/r}{(1+R/r)^3}(z_{h_d} - R/r)\right] - nz_{h_{\texttt{HI}}} \\
&= (1+n)\left[1 - \frac{1+2\frac{R}{r}}{(1+\frac{R}{r})^2}\right]\frac{R/r}{1+\frac{R}{r}} - z_{h_{\texttt{HI}}}\left(n - \frac{(1+n)(1+2\frac{R}{r})}{(1+R/r)^3}\right) \\
&= \frac{(1+n)(R/r)^3 - z_{h_{\texttt{HI}}}[n(1+R/r)^3 - (1+n)(1+2R/r)]}{(1+R/r)^3} \\
&\leq R/r\frac{(1+n)(1+2R/r+(R/r)^2) - n(1+R/r)^3}{(1+R/r)^3} \\
&= (R/r)\frac{1-nR/r}{1+R/r} \leq 0,
\end{aligned}$$

where second inequality follows from $z_{h_{\texttt{HI}}} > R/r$ and $n(1+R/r)^3 - (1+n)(1+2R/r) > 0$, which in turn is implied by

$$\begin{aligned}
n(1+R/r)^3 - (1+n)(1+2R/r) &= n[(1+R/r)^3 - (1+2R/r)] - 1 - 2R/r \\
&= n\left[1 + 3\frac{R}{r} + 3\frac{R^2}{r^2} + \frac{R^3}{r^3} - 1 - 2\frac{R}{r}\right] - 1 - 2\frac{R}{r} \\
&= nR/r[1 + 3R/r + (R/r)^2] - 1 - 2R/r \\
&\geq R/r[3R/r + (R/r)^2 - 1] - 1 \geq [3 + 1 - 1] - 1 = 2.
\end{aligned}$$

where inequalities follow from $n \geq 1$ and $R/r \geq 1$.

For $t \geq 0$ such that $t < \delta$, we have established that $E(1 - tx_1, 1 - tx_2)$ is strictly increasing in t, that $E(1,1) < 0$ and that $E(1 - tx_1, 1 - tx_2) > 0$ for $t \approx \delta$. Because $E(1 - tx_1, 1 - tx_2)$ is continuous in t, there is a unique $\varepsilon \in (0, \delta)$ such that $E(1 - \varepsilon x_1, 1 - \varepsilon x_2) = 0$ and $E(1 - tx_1, 1 - tx_2)(t - \varepsilon) > 0$ for all $t \neq \varepsilon$. ■

Lemma 5 *For each $i \in I$, let $\phi_i \geq 0$ and $Y_i = X_i/\phi_i$, where X_i has cumulative $F(x) =$*

$1-\exp(-\lambda x)$. *Define* $M_0 = \min\{Y_i : i \in I \setminus \{0\}\}$ *and* $\Phi_0 = \sum_{i=1}^n \phi_i$. *Then,* Y_i *is an exponential random variable with the cumulative distribution function* $F_{\phi_i}(y) = 1-e^{-\lambda\phi_i x}$, M_0 *is an exponential random variable with cumulative distribution function given by* $F_{\Phi_0}(y) = 1 - e^{-\lambda\Phi_0 x}$ *and, therefore,*

$$\Pr(Y_0 \leq M_0) = \frac{\phi_0}{\phi_0 + \Phi_0} \qquad \textit{and} \qquad \mathbb{E}\left[\min\{Y_0, M_0\}\right] = \frac{1}{\lambda(\phi_0 + \Phi_0)}.$$

Proof. Let $i \in I$. It follows from $Y_i = X_i/\phi_i$ that $\Pr(Y_i \leq x) = \Pr(X_i \leq x\phi_i) = F_i(x\phi_i) = 1 - \exp(-\lambda\phi_i x)/$ and, therefore, $Y_i \sim \exp(\lambda\phi_i)$. Also,

$$\begin{aligned} F_n(x) &\equiv \Pr(M_0 \leq x) = \Pr\left(\min_{i\in I\setminus\{0\}}\{Y_i\} \leq x\right) = 1 - \Pr\left(\min_{i\in I\setminus\{0\}}\{Y_i\} > x\right) \\ &= 1 - \prod_{i=1}^n \Pr(Y_i > x) = 1 - \prod_{i=1}^n (1 - F(x\phi_i)) = 1 - \prod_{i=1}^n e^{-\lambda\phi_i x} = 1 - \exp(-\lambda\Phi_0 x). \end{aligned}$$

Accordingly, probability density function for M_0 at $y \geq 0$ is given by $f_n(y) = \frac{d}{dx}F_n(x)\big|_{x=y} = \lambda\Phi_0\exp(-\lambda\Phi_0 x)$. It follows that, $\Pr(Y_0 \leq M_0) = \phi_0/(\Phi_0 + \phi_0)$ since

$$\begin{aligned} \Pr(Y_0 \leq M_0) &= \int_0^\infty \Pr(Y_0 \leq M_0 | M_0 = x)\, f_n(x)dx = \int_0^\infty \Pr(Y_0 \leq x)\, \lambda\Phi_0 e^{-\lambda\Phi_0 x}dx \\ &= \lambda\Phi_0 \int_0^\infty \left(1 - e^{-\lambda\phi_0 x}\right) e^{-\lambda\Phi_0 x}dx = \lambda\Phi_0 \int_0^\infty \left(e^{-\lambda\Phi_0 x} - e^{-\lambda(\Phi_0+\phi_0)x}\right) dx \\ &= \lambda\Phi_0 \int_0^\infty e^{-\lambda\Phi_0 x}dx - \lambda\Phi_0 \int_0^\infty \left(e^{-\lambda(\Phi_0+\phi_0)x}\right) dx \\ &= \lambda\Phi_0 \left(\frac{e^{-\lambda\Phi_0 x}}{-\lambda\Phi_0}\right)\Bigg|_0^\infty - \lambda\Phi_0 \left(\frac{e^{-\lambda(\Phi_0+\phi_0)x}}{-\lambda(\Phi_0+\phi_0)}\right)\Bigg|_0^\infty = 1 - \frac{\Phi_0}{\Phi_0+\phi_0}. \end{aligned}$$

■

Lemma 6 *Let* $M_n = \min\{Y_i : i \in I \setminus \{0\}\}$ *and* $\Phi_0 = \sum_{i=1}^n \phi_i$. *For each* $i \in I$, *suppose that cumulative distribution function for* Y_i *is* $F_{\phi_i}(y) = 1 - e^{-\lambda\phi_i x}$. *Then, for every* $t \in \mathbb{R}$

$$\Pr(Y_0 - t \leq M_n | Y_0 > t) = \Pr(Y_0 \leq M_n - t | M_n > t) = \frac{\phi_0}{\phi_0 + \Phi_n}$$

and

$$\mathbb{E}\left[\min\{Y_0 - t, M_n\} | Y_0 > t\right] = \mathbb{E}\left[\min\{Y_0, M_n - t\} | M_n > t\right] = \frac{1}{\lambda(h + \Phi)}.$$

Proof. First, observe that

$$\Pr\left(Y_0 - t \leq M_n \middle| Y_0 > t\right) = \int_0^\infty \Pr\left(Y_o \leq t + y \middle| Y_0 > t \wedge M_n = y\right) f_n(y)dy.$$

Therefore, $\Pr\left(Y_0 - t \leq M_n \middle| Y_0 > t\right) = \frac{\phi_0}{\phi_0+\phi_n}$ since

$$\int_0^\infty \left(\frac{F_{\phi_0}(t+y) - F_{\phi_0}(t)}{1 - F_{\phi_0}(y)}\right) f_n(y)dy = \int_0^\infty \left(\frac{e^{-\phi_0\lambda t} - e^{-\phi_0\lambda(t+y)}}{e^{-\phi_0\lambda t}}\right) f_n(y)dy$$
$$= 1 - \int_0^\infty e^{-\phi_0\lambda y}\left(\phi_n\lambda e^{-\phi_n\lambda y}\right)dy = 1 - \phi_n\lambda\int_0^\infty e^{-\lambda y(\phi_o+\phi_n)}dy = \frac{\phi_0}{\phi_0+\phi_n}.$$

Similarly, observe that

$$\Pr\left(Y_0 \leq M_n - t \middle| M_n > t\right) = \int_0^\infty \Pr\left(Y_o \leq M_n - t \middle| M_n > t \wedge Y_0 = y\right) f_{\phi_0}(y)dy.$$

Therefore, $\Pr\left(Y_0 \leq M_n - t \middle| M_n > t\right) = \frac{\phi_0}{\phi_0+\phi_n}$ since

$$\int_0^\infty \Pr\left(y + t \leq M_n \middle| M_n > t\right) f_{\phi_0}(y)dy = \int_0^\infty \left[1 - Pr\left(M_n \leq y + t \middle| M_n > t\right)\right] f_{\phi_0}(y)dy$$
$$= 1 - \int_0^\infty \frac{F_{\phi_n}(y+t) - F_{\phi_n}(t)}{1 - F_{\phi_n}(t)} f_{\phi_0}(y)dy = 1 - \int_0^\infty \frac{e^{-\lambda\phi_n t} - e^{-\lambda\phi_n(t+y)}}{e^{-\lambda\phi_n t}} f_{\phi_0}(y)dy$$
$$= 1 - \int_0^\infty \left(1 - e^{-\lambda\phi_n y}\right) f_{\phi_0}(y)dy = \int_0^\infty e^{-\lambda\phi_n y}\left(\phi_0\lambda e^{-\lambda\phi_0 y}\right)dy = \phi_o\lambda\left(\frac{1}{\lambda(\phi_n+\phi_0)}\right).$$

Now,

$$E\left[\min\left\{Y_0 - t, M_n\right\} \middle| Y_0 > t\right] = \int_0^\infty \left[\int_t^\infty \frac{\min\left\{Y_0 - t, m\right\}}{1 - F_{\phi_0}(t)} f_{\phi_0}(y|M_n = m)dy\right] f_{\phi_n}(m)dm,$$

where $f_{\phi_0}(y|M_n = m)$ denotes the probability density function of Y_0 at y conditional on $M_n = m$. Given Y_0 and M_n are independent random variables, $f_{\phi_0}(y|M_n = m) = f_{\phi_0}(y)$.

Therefore, $E\left[\min\left\{Y_0 - t, M_n\right\} \middle| Y_0 > t\right] = 1/\lambda(\phi_0 + \phi_n)$ since it equals

$$\begin{aligned}
&\int_0^\infty \left[\int_t^{(m+t)} \frac{(y-t) f_{\phi_0}(y)}{1 - F_{\phi_0}(t)} dy + \int_{m+t}^\infty \frac{m f_{\phi_0}(y)}{1 - F_{\phi_0(t)}} dy \right] f_{\phi_n}(m) dm \\
&= \int_0^\infty \left[\frac{(y-t) F_{\phi_0}(y)}{1 - F_{\phi_0}(t)} \Big|_t^{m+t} - \int_t^{m+t} \frac{F_{\phi_0}(y)}{1 - F_{\phi_0}(t)} dy + \int_{m+t}^\infty \frac{m f_{\phi_0}(y)}{1 - F_{\phi_0}(t)} dy \right] f_{\phi_n}(m) dm \\
&= \int_0^\infty \left\{ \frac{m F_{\phi_0}(t+m) + m\left[1 - F_{\phi_0}(m+t)\right]}{1 - F_{\phi_0}(t)} - \int_t^{m+t} \left(\frac{1 - e^{-\lambda y \phi_0}}{1 - F_{\phi_0(t)}} \right) dy \right\} f_{\phi_n}(m) dm \\
&= \int_0^\infty \left[\frac{m - \left(y + \frac{e^{-\lambda y \phi_0}}{\lambda \phi_0} \right) \Big|_t^{m+t}}{1 - F_{\phi_0}(t)} \right] f_{\phi_n}(m) dm = \int_0^\infty \left[\frac{-\left(\frac{e^{-\lambda \phi_0 (m+t)} - e^{-\lambda \phi_0 t}}{\lambda \phi_0} \right)}{e^{-\lambda \phi_0 t}} \right] f_{\phi_n}(m) dm \\
&= \frac{1}{\lambda \phi_0} - \int_0^\infty \frac{e^{-\lambda \phi_0 m} \left(\lambda \phi_n e^{-\lambda \phi_n m} \right)}{\lambda \phi_0} dm = \frac{1}{\lambda \phi_0} - \frac{\phi_n}{\phi_0} \int_0^\infty e^{-\lambda m (\phi_0 + \phi_n)} dm \\
&= \frac{1}{\lambda \phi_0} - \frac{\phi_n}{\phi_0} \frac{e^{-\lambda m (\phi_n + \phi_0)}}{(-1)\lambda(\phi_n + \phi_0)} \Big|_0^\infty = \frac{1}{\phi_0 \lambda} + \frac{-\phi_n}{\phi_0 (\phi_0 + \phi_n) \lambda} = \frac{1}{\lambda \phi_0} \left[1 - \frac{\phi_n}{\phi_0 + \phi_n} \right].
\end{aligned}$$

Similarly,

$$E\left[\min\left\{Y_0, M_n - t\right\} \middle| M_n > t\right] = \int_0^\infty \left[\int_t^\infty \frac{\min\left\{y, M_n - t\right\}}{1 - F_{\phi_n}(t)} f_{\phi_n}(m | Y_0 = y) dm \right] f_{\phi_0}(y) dy,$$

where $f_{\phi_n}(m|Y_0 = y)$ denotes the probability density function of M_n at m conditional on $Y_0 = y$. Given Y_0 and M_n are independent random variables, $f_{\phi_n}(m|Y_0 = y) = f_{\phi_n}(m)$.

Therefore, $E\left[\min\left\{Y_0, M_n - t\right\} \middle| M_n > t\right] = 1/\lambda(\phi_0 + \phi_n)$ since it equals

$$
\begin{aligned}
&\int_0^\infty \left[\int_t^{y+t} \frac{(m-t)f_{\phi_n}(m)}{1-F_{\phi_n}(t)}dm + \int_{y+t}^\infty \frac{y f_{\phi_n}(m)}{1-F_{\phi_n(t)}}dm\right] f_{\phi_0}(y)dy \\
&= \int_0^\infty \left[\frac{(m-t)F_{\phi_n}(m)}{1-F_{\phi_n}(t)}\bigg|_t^{y+t} - \int_t^{y+t} \frac{F_{\phi_n}(m)}{1-F_{\phi_n}(t)}dm + y\int_{m+t}^\infty \frac{f_{\phi_n}(m)}{1-F_{\phi_n}(t)}dm\right] f_{\phi_0}(y)dy \\
&= \int_0^\infty \left\{\frac{yF_{\phi_n}(y+t) + y\left[1-F_{\phi_n}\left(y+t\right)\right]}{1-F_{\phi_n}(t)} - \int_t^{y+t}\left(\frac{1-e^{-\lambda\phi_n m}}{1-F_{\phi_n(t)}}\right)dm\right\} f_{\phi_0}(y)dy \\
&= \int_0^\infty \frac{y - \left(m + \frac{e^{-\lambda\phi_n m}}{\lambda\phi_n}\right)\Big|_t^{y+t}}{1-F_{\phi_n}(t)} f_{\phi_0}(y)dy = \int_0^\infty \frac{-\left(e^{-\lambda\phi_n(y+t)} - e^{-\lambda\phi_n t}\right)}{\lambda\phi_n e^{-\lambda\phi_n t}} f_{\phi_0}(y)dy \\
&= \frac{1}{\lambda\phi_n} - \int_0^\infty \frac{e^{-\lambda\phi_n y}}{\lambda\phi_n}\lambda\phi_0 e^{-\lambda\phi_0 y}dy = \frac{1}{\lambda\phi_n} - \frac{\phi_0}{\phi_n}\int_0^\infty e^{-\lambda(\phi_n+\phi_0)y}dy \\
&= \frac{1}{\lambda\phi_n} - \frac{\phi_0}{\phi_n}\frac{e^{-\lambda m(\phi_0+\phi_n)}}{(-1)\lambda(\phi_n+\phi_0)}\bigg|_0^\infty = \frac{1}{\phi_n\lambda} + \frac{-\phi_0}{\phi_n(\phi_0+\phi_n)\lambda} = \frac{1}{\lambda\phi_n}\left[1 - \frac{\phi_0}{\phi_0+\phi_n}\right] \\
&= \frac{1}{\lambda(\phi_0+\phi_n)}.
\end{aligned}
$$

■

Lemma 7 *Function $\pi_{RA}(z_h)$ is strictly increasing and strictly concave in h for all $h \geq 0$. Function $\pi_{HI}(z_h)$ is strictly increasing and strictly concave in h for all h such that $z_h \geq R/r$. Also, $\pi_{RA}(R/r) = \pi_{HI}(R/r)$ and*

$$\pi'_{RA}(R/r) = \frac{1}{(1+R/r)^2} < \frac{1}{(1+R/r)^2}\frac{1+2R/r}{1+R/r} = \pi'_{HI}(R/r). \tag{24}$$

Proof. From definition of $\pi_{\mathtt{RA}}(z)$ in lemma 1, it trivially follows that $\pi'_{\mathtt{RA}}(z_h)z'_h = \frac{1/n\bar{h}}{(1+z_h)^2} > 0$ and $\pi''_{\mathtt{RA}}(z_h)(z'_h)^2 = \frac{-2/(n\bar{h})^2}{(1+z_h)^3} < 0$ so that $\pi_{\mathtt{RA}}(z_h)$ is strictly increasing and strictly concave in h for all $h > 0$. From definition of $\pi_{\mathtt{HI}}(z)$ in lemma 1, it follows that

$$
\begin{aligned}
\pi'_{\mathtt{HI}}(z_h)z'_h &= \frac{\partial}{\partial z_h}\left(\frac{z_h^3 + 3z_h^2 + (1-R/r)z_h}{(1+z_h)^3}\right)\frac{1}{n\bar{h}} \\
&= \frac{(1+z_h)^3(3z_h^2+6z_h+(1-R/r)) - 3(1+z_h)^2(z_h^3+3z_h^2+(1-R/r)z_h)}{n\bar{h}(1+z_h)^6} \\
&= \frac{(1+z_h)(3z_h^2+6z_h+(1-R/r)) - 3(z_h^3+3z_h^2+(1-R/r)z_h)}{n\bar{h}(1+z_h)^4} \\
&= \frac{2(2+R/r)z_h - R/r + 1}{n\bar{h}(1+z_h)^4} \geq \frac{(3+2R/r)R/r+1}{n\bar{h}(1+z_h)^4} > 0,
\end{aligned}
$$

and, therefore, $\pi_{\mathtt{HI}}(z_h)$ is strictly increasing in h when $z_h \geq R/r$. Conditions $\pi_{\mathtt{RA}}(R/r) =$

$\pi_{\texttt{HI}}(R/r)$ and (24) are easily verified by evaluating functions $\pi_{\texttt{RA}}(z)$, $\pi_{\texttt{HI}}(z)$, $\pi'_{\texttt{RA}}(z)$ and $\pi'_{\texttt{HI}}(z)$ at $z = R/r$. In order to verify that $\pi_{\texttt{HI}}(z_h)$ is strictly concave in h when $z_h \geq R/r$, observe that

$$\begin{aligned}
\pi''_{\texttt{HI}}(h)(z'_h)^2 &= \frac{\partial}{\partial z_h}\left(\frac{2(2+R/r)z_h - R/r + 1}{(1+z_h)^4}\right)\frac{1}{(n\bar{h})^2} \\
&= \frac{2(2+R/r)(1+z_h)^4 - 4(1+z_h)^3[2(2+R/r)z_h - R/r + 1]}{(n\bar{h})^2(1+z_h)^8} \\
&= \frac{2(2+R/r) + 2(2+R/r)z_h - 8(2+R/r)z_h + 4(R/r-1)}{(n\bar{h})^2(1+z_h)^5} \\
&= 6\frac{R/r - (2+R/r)z_h}{(n\bar{h})^2(1+z_h)^5} \leq 6(R/r)\frac{1-(2+R/r)}{(n\bar{h})^2(1+z_h)^5} = 6\frac{-(R/r)(1+R/r)}{(n\bar{h})^2(1+z_h)^5} < 0,
\end{aligned}$$

where the inequality is implied by $z_h \geq R/r$. ■

Lemma 8 *Let* $f(x) = \sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}} - \left(1 + \frac{r}{2x}\right)$. *Then,* $f'(0) = 0$ *and* $f'(x) < 0$ *for all* $x > 0$. *Also,* $f(d+R) = 0$ *and* $\lim_{x\to 0^+} f(x) = (d+R)/r$.

Proof. In effect,

$$\begin{aligned}
f'(x) = \frac{d}{dx}\left\{\sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}} - \left(1+\frac{r}{2x}\right)\right\} &= \frac{\left(\frac{r}{2}\right)^2\left(\frac{-2}{x^3}\right) + \frac{(d+r+R)(-1)}{x^2}}{2\sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}}} + \frac{r}{2x^2} \\
&= \frac{r}{2x^2}\left[1 - \frac{r^2 + 2x(d+r+R)}{2rx\sqrt{\left(\frac{r}{2x}\right)^2 + \frac{d+r+R}{x}}}\right] = \frac{r}{2x^2}\left[1 - \frac{r^2+2x(d+r+R)}{r\sqrt{r^2+4x(d+r+R)}}\right].
\end{aligned}$$

Define $y(x) = \sqrt{r^2 + 4x(d+r+R)}$ so that $y(x) > y(0) = r$ for all $x > 0$. Then, $y(x)^2 - r^2 = 4x(d+r+R)$ and

$$\begin{aligned}
f'(x) = \frac{r}{2x^2}\left(\frac{ry(x) - r^2 - [y(x)^2 - r^2]/2}{ry(x)}\right) &= \frac{2ry(x) - 2r^2 - y(x)^2 + r^2}{4x^2 y(x)} \\
&= \frac{2ry(x) - r^2 - y(x)^2}{4x^2 y(x)} = (-1)\frac{(r-y(x))^2}{4x^2 y(x)} \leq 0,
\end{aligned}$$

where the last inequality is strict for all $x > 0$. ■

B Numerical strategy

Consider first the benchmark model without double spending, developed in subsection 2.1. We have $E\left(1/n, r/R\right) = 1 + n^2 z_{h_{\texttt{HI}}} - (n+1)^2 \pi_{\texttt{HI}}\left(z_{h_{\texttt{HI}}}\right)$, since

$$E\left(1/n, r/R\right) = 1 - \frac{\pi_{\texttt{HI}}\left(z_{h_{\texttt{HI}}}\right) - (\rho/2r) n\bar{h} z_{h_{\texttt{HI}}}}{\pi_{\texttt{RA}}\left(1/n\right) - (\rho/2r)\bar{h}} = 1 - \frac{\pi_{\texttt{HI}}\left(z_{h_{\texttt{HI}}}\right) - \frac{n^2}{(n+1)^2} z_{h_{\texttt{HI}}}}{\frac{1/n}{1+1/n} - \frac{n}{(n+1)^2}}.$$

Thus, computing $E(1/n, r/R)$ for a given $(1/n, r/R)$ resumes to computing $z_{h_{\texttt{HI}}}$ which is implied by $h_{\texttt{HI}} \in \arg\max_{h \geq n\bar{h}R/r}\{2r\pi_{\texttt{HI}}(z_h) - \rho h\}$. Maximization problem to be solved can be rewritten as

$$\max_{h \geq n\bar{h}R/r}\{2r\pi_{\texttt{HI}}(z_h) - \rho n\bar{h} z_h\} = 2r \max_{z \geq R/r}\left\{\pi_{\texttt{HI}}(z) - \frac{n^2}{(n+1)^2} z\right\}.$$

Then, $z_{h_{\texttt{HI}}} \in \arg\max_{z \geq R/r}\left\{\pi_{\texttt{HI}}(z) - \frac{n^2}{(n+1)^2} z\right\}$. This optimization problem is solved using the bisection method in order to find a root for the corresponding first-order necessary condition for optima. Because the objective function is concave for $z \geq R/r$ (see lemma 7), this numerical strategy delivers $z_{h_{\texttt{HI}}}$.

Now, consider the model with double spending possibility, developed in subsection 3.1. Observe that $E^w_{\texttt{k}}(1/n, r/R, d/r) = 1 + n^2 z_{h^w_k} - \frac{(n+1)^2}{A_w(d/r)} \pi^w_k(z_{h^w_k})$, since

$$E^w_{\texttt{k}}(1/n, r/R, d/r) = 1 - \frac{\pi^w_k(z_{h^w_k}) - (\rho/2r) n\bar{h} z_{h^w_k}}{A_w(d/r)\pi^w_{\texttt{RA}}(1/n) - (\rho/2r)\bar{h}} = 1 - \frac{\pi^w_k(z_{h^w_k}) - \frac{n^2}{(n+1)^2} A_w(d/r) z_{h^w_k}}{\left(\frac{1}{n+1} - \frac{n}{(n+1)^2}\right) A_w(d/r).}$$

Then, computing $E^w_{\texttt{k}}(1/n, r/R, d/r)$ for a given $(1/n, r/R, d/r)$ resumes to computing $z_{h_{\texttt{k}}}$, which is implied by $h_{\texttt{k}} \in \arg\max_{h \geq 0}\{2r\pi_{\texttt{k}}(z_h) A_w(d/r) - \rho h\}$. This optimization problem can be rewritten as

$$\max_{h \geq 0}\{2r\pi^w_{\texttt{k}}(z_h) A_w(d/r) - \rho n\bar{h} z_h\} = 2r \max_{z \geq 0}\left\{\pi^w_{\texttt{k}}(z) - z\frac{n^2}{(n+1)^2} A_w(d/r).\right\}$$

Then, $z_{h_{\texttt{k}}} \in \arg\max_{z \geq 0}\left\{\pi_{\texttt{k}}(z) - z\frac{n^2}{(n+1)^2} A_w(d/r)\right\}$. This optimization problem is solved using the bisection method in order to find a root for the corresponding first-order necessary condition for optima. The search for a root is restricted to $z \geq \hat{z}$ such that $\pi''_{\texttt{k}}(\hat{z}) = 0$. Because $\pi''_{\texttt{k}}(\hat{z})$ is decreasing everywhere, this search delivers the only interior local maximum. The implied value for the objective function is then compared to the value function at the corner solution $z = 0$. The candidate solution that reaches a higher objective is $z_{h_{\texttt{k}}}$.