frontiers in Blockchain

ORIGINAL RESEARCH
published: 06 May 2021
doi: 10.3389/fbloc.2021.443966

Monetary Dynamics With Proof of Stake

*Nicola Dimitri**

Department of Political Economy and Statistics, University of Siena, Siena, Italy

In recent years blockchain consensus mechanisms based on Proof of Stake gained increasing attention as an alternative to Proof of Work, which requires high energy consumption. In its original version Proof of Stake hinges on the idea that, for a user, the likelihood to confirm the next block is positively related to the amount of currency units held in the wallet, and possibly also on the time length which the money has been unspent for. In a simple framework with risk neutral users we provide some early insights on the monetary equilibrium of Proof of Stake based platforms. In particular, we find that the aggregate demand and supply of currency may not coincide, which implies that users could hold suboptimal quantities of the currency. Furthermore, we also discuss how symmetric stationary states of the system could be implausible. As a consequence, a long run uniform distribution of money would seem unlikely unless appropriate measures are introduced.

Keywords: Proof of Stake, blockchain, cryptocurrency, money demand, monetary equilibrium

OPEN ACCESS

Edited by:
Claudio J. Tessone,
University of Zurich, Switzerland

Reviewed by:
Francesco Tiezzi,
University of Camerino, Italy
Patrick Lehner,
Zurich University of Applied Sciences, Switzerland
Florian Spychiger,
ZHAW School of Management and Law, Center for Organizational Viability,
in collaboration with reviewer PL

***Correspondence:**
Nicola Dimitri
dimitri@unisi.it

Specialty section:
This article was submitted to Non-Financial Blockchain, a section of the journal Frontiers in Blockchain

Received: *04 January 2019*
Accepted: *16 March 2021*
Published: *06 May 2021*

Citation:
Dimitri N (2021) Monetary Dynamics With Proof of Stake. Front. Blockchain 4:443966. doi: 10.3389/fbloc.2021.443966

INTRODUCTION

The publication of the Satoshi Nakamoto paper (2008), introducing Bitcoin, spurred remarkable activity and interest on cryptocurrencies. A distinguishing feature of Bitcoin, as well as of other currencies, is its consensus mechanism and type of incentive provided to the *miners*, the nodes who have the *right* and *responsibility* for confirming currency transactions in the next block of the chain. To gain such *right* miners need to exhibit the so-called *proof of work* (PoW), which requires solving a cryptopuzzle. There is no strategy to find a solution to such puzzle, which for this reason needs to be solved by computational *brute force*. Consequently, the likelihood to solve the puzzle increases with a miner's computational power, and the Bitcoin protocol is set in such a way that the difficulty to find a solution is adjusted periodically to keep, on average, a block confirmation about every 10 min. As a reward, and cost compensation, for the mining activity the Bitcoin protocol provides a given number of *newly mined* currency units, so called *coinbase*. Moreover, because of block space limitation, users may offer transaction fees to miners as an incentive to prioritize confirmation of their transaction in the next block. Therefore, due to the intense mining competition and computational activity, this type of PoW turned out to be very energy demanding. As a result, in recent years a concern increased on this massive electricity consumption, which being exclusively dedicated to solving cryptopuzzles is considered as a waste.

Hence, alternatives to PoW were proposed in order to save on electricity consumption. One such criterion is the so called *Proof of Stake* (PoS), originally introduced by King and Nadal (2012), also in combination with PoW (Bentov et al., 2014, 2017) and currently used, or planned to use, by a number cryptocurrrencies (Halaburda and Sarvary, 2016; Gilad et al., 2017;

Buterin and Griffith, 2019; Chen and Micali, 2019; Nguyen et al., 2019; Wang et al., 2019; Nijsse and Litchfield, 2020; Saleh, 2020; Xiao et al., 2020; Rijsberger et al., 2021). In its early version (Vasin, 2014), PoS was based on the idea that *rights* to confirm the next block of transactions depend on two elements, which jointly form the so called *coinage*.

First the number of currency units held in one's wallet and, second, the length of time that such units were unspent by the user. The likelihood for a node to be selected to confirm the next block depends on the combination of these two elements. In particular, suppose m_t is the number of currency units held by a user at time t and l_t the average length of time such units remained unspent in his wallet. Then, broadly speaking, for a user the probability to be *drawn* to confirm the next block of transactions is given by $\frac{m_t l_t}{M_t L_t}$, where $m_t l_t$ is the total time length that units have been unspent in the individual's wallet (coinage) while $M_t L_t$ is the overall time period that the total number M_t of units in the system were unspent in the users' wallets.

Therefore, since for a user what matters is the product $m_t l_t$, the same *coinage* value could be obtained for example by keeping few units in the wallet for a long period and the rest for a very short time, or keeping all the units unspent for some *intermediate* length of time. In case only the number of units would matter then $l_t = 1$, and a user's likelihood to be selected becomes $\frac{m_t}{M_t}$.

A simple, though very important, implication of such criterion is the following. Paying/receiving currency units may be seen to have a double effect on the user's welfare. The first could be defined as a *direct* effect, given by the possibility to buy/sell assets, goods and services. The second may be called an *indirect* effect, given by the externality on the probability of being selected to confirm the next block and receive a reward. For example, suppose a user pays and receives the same amount of money, say 1 currency unit, at some date. If this is the only variation in her wallet then while the overall amount of money remains the same, the total length of time that money in the wallet has been unspent for typically decreases or, at best, remains unaltered. Indeed, while the paid currency unit must have been in the wallet for at least one period of time, the unit received by the individual has been in her wallet for one period only. While such transaction induces no *direct* effect it does have a, typically, negative *indirect* effect since it decreases the probability for being selected to confirm the next block. The above considerations suggest that, with *coinage* based PoS, users may find it profitable to first spend those units which have been in the wallet for a shorter period of time, and then those which have been held for a longer period (Vasin, 2014). Indeed, by doing so they minimize the negative externality induced by the payment. In case time length does not matter then the direct effect only would be at work.

Since the early proposals, a main concern with PoS has been its security and the possibility of attacks such as malicious forking and double spending (Houy, 2014; BitFury Group, 2015; Narayanan et al., 2016; Kiayias et al., 2017; Brown-Cohen et al., 2018; Fan and Zhou, 2018; Deirmentzoglou et al., 2019). In this paper we focus instead on the system monetary dynamics with PoS, that is on understanding how users may behave in terms of money holding and, based on this, how the whole monetary system would characterize and evolve. More specifically, we shall be interested in asking if PoS implies a monetary equilibrium of the system, where aggregate currency demand and supply coincide. Moreover, we'll investigate if PoS leads to a concentration or instead to a more uniform distribution of money, across users, with no dominating positions.

There is a recent, growing, literature on the economic dynamics of PoS based platforms. In particular, Fanti et al. (2019) and Wang et al. (2020) compare the long run behavior of alternative reward rules, more specifically a constant reward rule vs. a geometric reward rule in terms of their asymptotic effect on the users' shares of currency. Saleh (2020) discusses the role of the reward to generate consensus in a PoS economy, while Rosu and Saleh (2021) enquire the dynamics of shares of currency holdings when users can choose between a risky cryptocurrency and a safe, alternative, asset.

As anticipated, in this paper we shall also be interested in the long run behavior of currency shares held by users. However, our work differs from the above contributions along two main dimensions. The first is an explicit consideration of the money utility, to buy and sell assets, goods and services, which is taken into account when modeling the preferences of a representative agent. That is money, in a PoS economy, may not be only accumulated by users but also transferred to other users, in exchange of goods/services, etc. Secondly, based on this, we investigate the existence of a monetary equilibrium for the whole economy, by considering aggregate demand and supply of the currency.

The model that we present in the paper takes inspiration from the early PoS ideas, and it does not exactly coincide with currently circulating proposals. In a comprehensive recent survey Ferdous et al. (2020) discuss the large variety of PoS consensus procedures adopted by different cryptocurrencies. Because of such wide range of proposals, it perhaps would be too ambitious to have an all-encompassing model capturing the economics of all of them. This is the main reason why we decided to focus on the very initial, fundamental, versions of PoS which, in any case, remain key to any subsequent proposal. An additional reason for our choice is because we only focus on economic aspects and do not discuss security related issues against attacks, etc., which motivated many of the more recent PoS models.

In particular it differs from Casper, the Ethereum proposal (Buterin and Griffith, 2019) in that we do not analyze the possibility that coins are slashed from the wallet of a block validator, in case of untruthful validation. The Algorand version of PoS (Gilad et al., 2017; Chen and Micali, 2019) also differs from ours since we do not consider committees for validating transactions. PeerCoin (King and Nadal, 2012) and BlackCoin (Vasin, 2014) cryptocurrencies adopt hybrid PoW and PoS models, and so also differ from our framework. NxT coin is in turn partly different because we do not introduce transactions fees, rather newly minted coin units only as a reward for confirming new blocks. We also do not consider participation costs. Despite all such differences, we believe that our model

may capture some economic fundamentals of PoS and we hope that it could represent a useful benchmark to gain some relevant insights, also on several of its variations.

We study a very simple and *pure* PoS economy, that is with no PoW hybridization. In analogy with Bitcoin, confirmation of a new block of transactions entitles the selected user to a reward, represented by some newly minted coins. However, entitlement to confirm a block is based on the number of currency units held by an individual in her wallet, rather than on solving a cryptopuzzle. For this reason, a PoS framework would basically eliminate the distinction between miners and users, which characterizes Bitcoin.

In a simple dynamic model with risk neutral agents, a main finding of the paper is that aggregate money supply and demand may not coincide, and so the system could not always be in equilibrium. For this reason, money allocation across individuals might be suboptimal. We also discuss how symmetric stationary equilibrium states are unlikely to take place in the system, which implies that a long run uniform distribution of currency units may be implausible. Indeed, in our model a stationary symmetric equilibrium can exist only if the quantity of money in the system does not grow, which would require incentives other than money reward for block confirmation to sustain the system functioning.

The paper is structured as follows. In section "The Model Fundamentals" we introduce the model fundamentals. In section "Optimal Currency Holdings and the System Monetary Equilibrium" we discuss users' optimal money holding and the system monetary equilibrium while section "Conclusion" concludes the paper.

THE MODEL FUNDAMENTALS

Suppose i, with $i = 1, 2, .., n$, is the generic user in the system and that $t = 0, 1, 2, \ldots$, stands for the time index. We suppose the number of users to be time independent, although it would be simple to extend the model to a time varying number of users.

Consider now the time period between two consecutive dates, t and $t + 1$, and assume the following. *At the beginning* of that period we define m_{it} to be the number of currency units held at t by user i, in her wallet. Hence

$$M_{tb} = \sum_{i=1}^{n} m_{it} \tag{1}$$

is the total quantity of money held in the economy at the *beginning* of the period.

Moreover suppose s_{it} and z_{it} are, respectively, the number of currency units the user spends and receives between t and $t + 1$. Hence $x_{it} = s_{it} - z_{it}$ represents her net expenses in that period, before the random drawing for next block confirmation has taken place. Below we see that x_{it} is a choice variable in our model for the user, but that its *desired* level may differ from the *actual* level due to market constraints and money availability in the system.

We do not allow for borrowing and, for this reason, $0 \leq m_{it} - x_{it}$ is a necessary condition to avoid double spending. We also require the number of units held by a user to satisfy $m_{it} - x_{it} \leq M_{te}$, where M_{te} is the total quantity of money that users holds at the *end* of the period, before the random drawing, defined as

$$M_{te} = \sum_{i=1}^{n} (m_{it} - x_{it}) \tag{2}$$

Therefore, if $\sum_{i=1}^{n} x_{it} \neq 0$ then $M_{tb} \neq M_{te}$. Namely, at the end of the period users in the economy may hold more/less money, as a whole, than what they had at the beginning of the same period. As we shall see below, this depends on whether or not the desired level of x_{it} is satisfied. It is worth anticipating that this point will be further elaborated below, when discussing Eq. (7).

Henceforth, we shall define $M_t = M_{te}$ and refer to it as the quantity of money in the system at time t.

Furthermore, suppose $l_{it} = 1, .., t$ is the average time length that currency units $m_{it} - x_{it}$ have been unspent for, in player $i's$ wallet. More explicitly if l_{ijt} is the time period during which currency unit j, with $j = 1, .., (m_{it} - x_{it})$, has not been spent by i, then l_{it} is given by

$$l_{it} = \sum_{j=1}^{(m_{it} - x_{it})} \frac{l_{ijt}}{(m_{it} - x_{it})} \tag{3}$$

Therefore, $(m_{it} - x_{it})l_{it}$ is the total length of time that $i's$ currency units have not been spent for, that is her *coinage* at time t, before the next block of transactions at time $(t + 1)$ is confirmed.

It is worth observing that the same level of coinage $(m_{it} - x_{it})l_{it}$ could be obtained by keeping few currency units unspent for some time or, for example, by holding most units unspent for a short time.

Finally, the following expression stands for the total time that the whole set of currency units in the system has been unspent for.

$$M_t L_t = \sum_{i=1}^{n} (m_{it} - x_{it})l_{it} \tag{4}$$

where, as above, M_t is the total number of currency units, money held by users, in the system at the end of the period, just before the random draw is performed, and L_t the average period of time that each unit has not been spent for.

Finally, suppose at $(t + 1)$ a user is selected to confirm the next block, receiving as reward a number $r_t \geq 0$ of *newly minted* currency units.

We suppose that the total quantity of money M_t in the system evolves with time according to two different assumptions.

Exogenous, Supply Driven, Quantity of Money

In this case we assume the total quantity of money to be *exogenously* determined by the platform, regardless of whether or not such quantity corresponds to the desired, aggregate, demand for money by the users. As a consequence, aggregate monetary supply and demand may differ and, due to this, the economy may not be in a monetary equilibrium. That is, the quantity of money

held by users may be larger or smaller than what they consider to be optimal for them.

Hence we suppose that the total quantity of money M_t evolves according to the following dynamics.

$$M_{t+1} = M_t + r_t = M_0 + \sum_{k=0}^{t} r_k \text{ with } t = 0, 1, 2, 3, .. \quad (5)$$

where M_t is decided at each date by the platform. If $r_t = r$ then

$$M_{t+1} = M_0 + (t+1)\, r \quad (6)$$

Therefore, M_t grows with time unless $r_t = 0$, for all $t \geq T \geq 0$

Endogenous, Demand Driven, Quantity of Money

Alternatively, we also consider the possibility that the total quantity of money in the system mostly determined, *endogenously*, by the aggregate money demand. That is, at each date the quantity M_t perfectly adjusts to the users' demand, while only the reward r_t is predetermined by the platform. In this case

$$M_t = M_{te} = \sum_{i=1}^{n} (m_{it} - x_{it}) \quad (7)$$

where, as we shall see below, x_{it} are optimal for the users. More explicitly, we assume the platform injects money in the system, or withdraws money from the system, according to M_t as defined in Eq. (7). That is, we imagine the platform can perfectly equalise the quantity of money to the aggregate demand.

Monetary transactions could affect the likelihood of being selected since, as well as affecting the amount of money held by users, they will typically impact on the average period that currency units have been unspent for in the wallet.

We can now specify the relevant timing of decisions and events.

At time $t = 0$, at the *beginning* of the first time period, m_{i0} is the money held by user i and so

$$M_{0b} = \sum_{i=1}^{n} m_{i0} \quad (8)$$

is the total money in users' wallet. In the model we consider m_{i0} as given and do not discuss how it is determined. At the *end* of the period, however, before the first random draw for confirming the initial block, $m_{i0} - x_{i0}$ is the money held by user i, hence

$$M_0 = M_{0e} = \sum_{i=1}^{n} (m_{i0} - x_{i0}) \quad (9)$$

is the quantity of money in the system at $t = 0$.

Finally, at $t = 1$ the user knows whether she's selected to confirm the first block. Therefore, from the perspective of date $t = 0$, the number of units m_{i1} held by the user at time $t = 1$ is a (conditional to m_{i0}) random variable defined as follows

$$m_{i1} = \begin{cases} m_{i0} - x_{i0} + r_0 & \text{if } m_{i0} - x_{i0} > 0 \text{ with probability } \frac{(m_{i0} - x_{i0}) l_{i0}}{M_0 L_0} \\ m_{i0} - x_{i0} & \text{if } m_{i0} - x_{i0} > 0 \text{ with probability } 1 - \frac{(m_{i0} - x_{i0}) l_{i0}}{M_0 L_0} \\ 0 & \text{if } m_{i0} - x_{i0} = 0 \end{cases} \quad (10)$$

Hence, before $t = 1$ the user decides $m_{i0} - x_{i0}$, and so l_{i0}. Based on $(m_{i0} - x_{i0}) l_{i0}$, still before date $t = 1$, with probability $\frac{(m_{i0} - x_{i0}) l_{i0}}{M_0 L_0}$ the individual is selected to confirm the next block and to receive r_0 newly minted currency units otherwise, if not selected, receives 0 units.

In general, based on the above timing and *conditional* to having chosen $m_{it} - x_{it}$, *before* selecting the node to confirm the next block, the number of currency units owned by individual i at time $t + 1$ is a random variable defined as

$$m_{i(t+1)} = \begin{cases} m_{it} - x_{it} + r_t & \text{if } m_{it} - x_{it} > 0 \text{ with probability } \frac{(m_{it} - x_{it}) l_{it}}{M_t L_t} \\ m_{it} - x_{it} & f\ m_{it} - x_{it} > 0 \text{ with probability } i \quad 1 - \frac{(m_{it} - x_{it}) l_{it}}{M_t L_t} \\ 0 & \text{if } m_{it} - x_{it} = 0 \end{cases} \quad (11)$$

To simplify notation, henceforth subscript i will be removed. It follows that the conditional expectation on the number of units $E_t(m_{t+1}|m_t) = E(m_{t+1})$, held by the generic individual i at time $(t + 1)$ is

$$E(m_{t+1}) = \begin{cases} m_t - x_t + \frac{r_t (m_t - x_t) l_t}{M_t L_t} & \text{if } m_t - x_t > 0 \\ 0 & \text{if } m_t - x_t = 0 \end{cases} \quad (12)$$

As an illustration suppose, for example, that $m_t = 10$, $x_t = 3$, $r_t = 1$, $l_t = 2$, $M_t = 100$ and $L_t = 4$. Then

$$E(m_{t+1}) = 7 + \frac{14}{400} = 7.035 \quad (13)$$

with the probability of being selected to confirm the next block being equal to 0.035, slightly higher than 3% .

Expression (12) implies also that when $m_t - x_t > 0$ it is $E(m_{t+1}) > m_t$ if

$$z_t + \frac{r_t (m_t - x_t) l_t}{M_t L_t} > s_t \quad (14)$$

that is when, at $(t + 1)$, the sum of currency units received from other users and those awarded for possible block registration, weighted by $\frac{(m_t - x_t) l_t}{M_t L_t}$, is higher than the number of currency units spent by the individual.

Moreover, for example with an endogenous quantity of money, it is

$$\frac{dE(m_{t+1})}{dm_t} = 1 + \frac{r_t (M_t L_t - (m_t - x_t) l_t) l_t}{(M_t L_t)^2} > 1 \quad \text{for all } m_t - x_t > 0 \quad (15)$$

with

$$lim_{(m_t-x_t)\to 0}\frac{dE(m_{t+1})}{dm_t} = 1 + \frac{r_t l_t}{M_t L_t} > 1 \tag{16}$$

The reason why the above derivatives are larger than one is simple, being due to the positive expected reward for block confirmation.

Furthermore

$$\frac{dE(m_{t+1})}{dl_t} = \frac{r_t(m_t - x_t)(M_t L_t - (m_t - x_t)l_t)}{(M_t L_t)^2} > 0 \quad for\ all\ m_t - x_t > 0 \tag{17}$$

which is also positive.

OPTIMAL CURRENCY HOLDINGS AND THE SYSTEM MONETARY EQUILIBRIUM

In this section we discuss how the relevant monetary quantities of the model are optimally determined by users and, based on them, how the system evolves with time. To simplify the discussion we assume that only the amount of money matters for confirming a block, and so $l_t = 1$. To study demand for money and the monetary equilibrium evolution of the system, for each individual we now introduce preferences through a utility function, which we assume to be time-independent. In choosing x_t a user faces the following, fundamental, trade-off. On the one hand, the larger x_t the higher his welfare while, on the other hand, the lower the probability of being selected to confirm the next block and obtain additional currency units. The reason why we assume the user's welfare to increase with x_t is because we suppose that the larger the expenditure the higher the level of purchased goods/services, and/or financial assets other than the cryptocurrency. This can take place either buying directly by means of the cryptocurrency, or exchanging it with some other currency first.

Though this is what we assume in the work, admittedly it may not be only way to model preferences. Indeed, for example, rather than being increasing with x_t we could assume welfare to increase with $s_t + z_t$, that is with the total amount of currency units exchanged. This would capture the idea that any *in/out* transaction, being voluntary, improves the welfare level of the user. In this case, for example, $x_t = 0$ would not necessarily imply that the user's welfare is stable, since it may be the outcome of *in/out* transactions being positive and equal.

At each date t, a simple utility function capturing the above trade- off can be the following

$$U(x_t, Em_{t+1}) = av(x_t) + b\delta Em_{t+1} \tag{18}$$

with $v' > 0$ and $v'' \leq 0$, where $0 \leq \delta \leq 1$ is the user's discount rate and $a, b \geq 0$ are weights quantifying, respectively, the importance of $v(x_t)$ and Em_{t+1} in the utility function. For example, $a = 0$ means that the user cares only about Em_{t+1} while $b = 0$ implies that only x_t matters. More in general, $\frac{a}{b}$ expresses the relative importance of the two components for the user. Considering Eq. (12) the utility function in Eq. (18) can be written as

$$U(x_t, Em_{t+1}) = av(x_t) + b\delta\left(m_t - x_t + \frac{r_t(m_t - x_t)}{M_t}\right) \tag{19}$$

Since at time t the quantity m_t is a given for the user, once x_t is chosen the random draw for block confirmation will determine, with probability $\frac{(m_t - x_t)}{M_t}$, whether or not the user will receive r_t additional units, finalizing the value of m_{t+1}. Hence, for a single user the only decision variable in Eq. (19) is x_t and, to simplify notation, we can write $U(x_t, Em_{t+1}) = U(x_t)$

For this reason, the user's problem can be formulated as

$$Max_{x_t} U(x_t) \quad subject\ to\ 0 \leq m_t - x_t \leq M_t \tag{20}$$

In what follows we are going to discuss problem (20) by considering both an exogenous and an endogenous M_t, which appears in Eq. (19).

In the former case M_t is the total quantity of money *exogenously* introduced in the system by the platform, and held by users, at time t. As a consequence M_t for the users is independent of their money demand and, treating it as a constant, from Eq. (19) the first order derivative with respect to x_t is given by

$$av'(x_t) - b\delta\left(1 + \frac{r_t}{M_t}\right) \tag{21}$$

In the latter case M_t would be the aggregate *endogenous demand for money*, obtained by summing up the individual monetary demands, just before the random draw. For this reason, now the quantity of money M_t before the random draw is no longer a constant for the users and will be defined by summing up all the individuals' money demand.

Replacing Eq. (19) into Eq. (20) and differentiating it with respect to x_t we obtain the following first derivative

$$av'(x_t) + b\delta\left(-1 + r_t\left(\frac{-M_t + (m_t - x_t)}{M_t^2}\right)\right) \tag{22}$$

Risk Neutral Users

To gain a better understanding of Eq. (21), Eq. (22) and the model functioning consider as an example, $v(x_t) = x_t$ *for all the users*, who because of this are risk neutral. Then Eq. (21) becomes

$$a - b\delta\left(1 + \frac{r_t}{M_t}\right) \tag{23}$$

and it follows that the optimal x_t is given by

$$x_t = \begin{cases} m_t & if \quad \frac{a}{b} > \delta\left(1 + \frac{r_t}{M_t}\right) \\ [-(M_t - m_t), m_t] & if\ \frac{a}{b} = \delta\left(1 + \frac{r_t}{M_t}\right) \\ -(M_t - m_t) & if\ \frac{a}{b} < \delta\left(1 + \frac{r_t}{M_t}\right) \end{cases} \tag{24}$$

Expression (24) suggests that if $v(x_t) = x_t$ *is sufficiently more important* than $E(m_{t+1})$, that is $\frac{a}{b}$ is large enough, then the user will want to hold no money in his wallet before the random draw for confirming the next block. Since we assume identical users, It

follows that this is true for all them and the aggregate demand for money is

$$n\left(m_t - x_t\right) = 0 \tag{25}$$

Hence the system may not be in a monetary equilibrium, since the aggregate demand for money will be equal to 0 while the quantity of money in the economy is $M_t > 0$.

As a consequence, perhaps some users may indeed satisfy their money demand before the random drawing, but not all of them. Likewise, if $\frac{a}{b}$ is sufficiently low then users will find it optimal to hold all the available quantity of money. Hence, for analogous reasons as above, this would also not lead to a monetary equilibrium since the aggregate demand will be nM_t, larger than the aggregate supply of money M_t. Finally, only if the extreme case of $\frac{a}{b} = \delta\left(1 + \frac{r_t}{M_t}\right)$ holds than the economy *may* be in equilibrium.

Suppose now that aggregate money supply completely, and instantaneously, adjusts to the aggregate money demand, and that users know this. From Eq. (22) it follows that the first order condition for the optimal x_t is given by

$$a = b\delta\left(1 + r_t\frac{M_t - (m_t - x_t)}{M_t^2}\right) \tag{26}$$

which, it can be checked, identifies a maximum.

Since we assume identical users it is $n(m_t - x_t) = M_t$ and so

$$M_t - (m_t - x_t) = (n-1)(m_t - x_t) = \frac{(n-1)M_t}{n} \tag{27}$$

Hence, summing up both sides of Eq. (26) over all users we obtain

$$an = nb\delta + b\delta r_t\frac{(n-1)}{M_t} \tag{28}$$

It follows that

$$M_t = \begin{cases} \frac{b\delta r_t(n-1)}{(a-b\delta)n} & if\ \frac{a}{b} > \delta \\ 0 & if\ \frac{a}{b} \leq \delta \end{cases} \tag{29}$$

which represents the aggregate demand for currency units, as well as the aggregate quantity of money in the model. Notice that expression (12) increases with n, r_t and δ. Hence, the higher the discount factor, the more important is the future for the users, the larger is their money demand.

Since preferences are the same across individuals, then Eq. (29) implies

$$m_t - x_t = Max\left(0, \frac{b\delta r_t\,(n-1)}{\left(a - b\delta\right)n^2}\right) \tag{30}$$

and therefore

$$Max(0, m_t - \frac{b\delta r_t\,(n-1)}{\left(a - b\delta\right)n^2}) = x_t \tag{31}$$

To obtain additional insights on the model, consider the following numerical example: $m_0 = 10,\ n = 100, a = b = 1,\ \delta = \frac{1}{2}$ and $r_t = 1$.

Then from Eq. (31) it follows that $m_0 - x_0 = \frac{9}{100}$ and therefore $x_0 = 9.91$. That is, users' net expenditures will count for 99.1% of their initial money holdings, while the remaining sum will be kept in their wallet, counting for the random draw to confirm the next block. In this case the aggregate quantity of money, before the random drawing for confirming the first block, is given by the aggregate money demand and to $M_0 = 0.91$, hence much lower than $nm_0 = 100$, the amount of money initially introduced in the system.

The Symmetric Stationary Equilibrium States of the System

To further investigate the system evolution, in what follows we briefly discuss the symmetric stationary *equilibrium* states (SSES) of system (12), with exogenous money supply. The SSES we consider is particularly restrictive since we shall require users' monetary holding to satisfy the following notion of time independence $E(m_t) = m_t = m$. That is, our stationarity condition implies that m_t would stop being a random variable, which is admittedly a strong request. We shall see that the findings are consistent with such a demanding assumption.

Additionally, at our SSES we shall require that the remaining quantities are also time independent: hence $l_t = l$, $r_t = r$, $s_t = s$, $z_t = z$ and $\frac{m_t l_t}{M_t L_t} = \frac{1}{n}$.

Based on the above assumptions, the following holds

Proposition *Suppose* $r = 0$. *If* $m_0 = 0$ *only SSES with* $m > 0$ *is the only SSES. Suppose* $r = 0$: *if* $M_0 = M = M_t$ *then the only SSES with* $m > 0$ *is* $m = \frac{M}{n}$, $s = z$, *and* $l = L$.

Proof Assume $r > 0$ and $m_0 = 0$; then from Eq. (12) it follows that $m_t = 0$ for all $t = 1, 2, \ldots$. Suppose now $m_0 > 0$; then, from Eq. (12) the condition for a SSES $m > 0$ becomes

$$E\left(m\right) = m = m - s + z + \frac{r}{n} \tag{32}$$

Hence Eq. (32) implies $s = \frac{r}{n} + z$. However, since $r > 0$ then $M_t = M_{t-1} + r > M_{t-1}$ which, as said, entails that M_t is increasing, due to r additional currency units introduced in the system at each date. But in equilibrium $M_t = (m_t - x_t)n$ while a SSES requires $M_t = (m - x)n$, which is impossible since M_t increases with t while $(m - x)n$ is constant, with respect to t.

Assume now $r = 0$; then, again, from Eq. (32) it follows that $s = \frac{r}{n} + z = z$. Finally, since $\frac{ml}{ML} = \frac{1}{n}$ and $M = mn$ it follows that $l = L$ which concludes the proof.

The above proposition suggests that the only possibility for a system to exhibit a symmetric stationary equilibrium state, assuming exogenous money supply, the population of users to be constant and according to our definition of SSES, is to have a constant amount of money in the economy, and so no reward for block confirmation. This, however, may raise an issue with the provision of the right incentives to the users for blocks confirmation. Based on these considerations, our types of SSES seem to be rather implausible states of the system.

CONCLUSION

In the paper we considered a basic framework to gain some early insights on the monetary dynamics of PoS based platforms. In a simplest model where, for risk neutral users, the likelihood to confirm the next block depends only on the amount of currency held in the wallet we find that, with an exogenous quantity of money, aggregate demand and supply of currency may not coincide. For this reason, some users could be unable to hold in their wallet the desirable quantity of money. This might be due to the money supply evolving according to a rule predefined by the platform, which may not necessarily coincide with the aggregate demand of money.

Indeed, the model considers symmetric users, that is with exactly the same preferences, which suggests that with exogenous money a monetary equilibrium may require users with heterogenous, rather than homogeneous, preferences. Finally, according to our definition, symmetric stationary equilibrium states of the system do not seem plausible, because they either require users to hold no money in their wallet or provide no currency reward for confirming a block. Despite its simplicity we believe the model may present some interesting insights underlying the economic functioning of a system based on PoS.

DATA AVAILABILITY STATEMENT

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

AUTHOR CONTRIBUTIONS

The author confirms being the sole contributor of this work and has approved it for publication.

REFERENCES

Bentov, I., Gabizon, A., and Mizrahi, A. (2017). Cryptocurrencies without proof of work. *arXiv [Preprint]*. Available online at: https://arxiv.org/abs/1406.5694 (accessed January 31, 2019).

Bentov, I., Lee, C., Mizrahi, A., and Rosenfeld, M. (2014). Proof of activity: extending Bitcoin's proof of work via proof of stake. *ACM Sigmetr.* 42, 34–37. doi: 10.1145/2695533.2695545

BitFury Group (2015). *Proof of Stake Versus Proof of Work*. Amsterdam: BitFury Group.

Brown-Cohen, J., Narayanan, A., Psomas, C.-A., and Weinberg, S. (2018). Formal barriers to longest-chain proof-of-stake protocols. *arXiv [Preprint]*. Available online at: https://arxiv.org/abs/1809.06528? (accessed March 31, 2019).

Buterin, V., and Griffith, V. (2019). Casper the friendly finality gadget. *arXiv [Preprint]*. Available online at: https://arxiv.org/abs/1710.09437 (accessed January 10, 2020).

Chen, J., and Micali, S. (2019). Algorand. *Theoret. Comp. Sci.* 177, 155–183. doi: 10.1016/j.tcs.2019.02.001

Deirmentzoglou, E., Papakyriakopoulos, G., and Patsakis, C. (2019). A survey on long-range attacks for proof of stake protocols. *IEEE Access* 7, 28712–28725. doi: 10.1109/access.2019.2901858

Fan L., and Zhou H. (2018). *A Scalable Proof-of-stake Blockchain in the Open Setting*. Available online at: http://eprint.iacr.org/2017/656 (accessed February 15, 2021).

Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., and Wang, G. (2019). "Compounding of wealth in proof-of-stake cryptocurrencies," in *Financial Cryptography 2019*, Vol. 11598, eds I. Goldberg and T. Moore (Berlin: Springer), 42–61. doi: 10.1007/978-3-030-32101-7_3

Ferdous, S., Chowdury, M., Hoque, M., and Colman, A. (2020). Blockchain consensus algorithms: a survey. *arXiv [Preprint]*. Available online at: http://arxiv.org/abs/2001.07091 (accessed February 15, 2021).

Gilad, Y., Hemo, R., Micali, S., Vlachos, G., and Zeldovich, N. (2017). *Algorand: Scaling Byzantine Agreements for Cryptocurrencies, SOSP'17*. Shanghai: SOSP.

Halaburda, H., and Sarvary, M. (2016). *Beyond Bitcoin*. London: Palgrave McMillan.

Houy, N. (2014). It will cost you nothing to 'kill' a proof-of-stake crypto-currency. *Econ. Bull.* 34, 1038–1044.

Kiayias, A., Russell, A., David, B., and Oliynykov, R. (2017). "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proceedings of the Annual International Cryptology Conference*, (Springer), 357–388. doi: 10.1007/978-3-319-63688-7_12

King, S., and Nadal, S. (2012). *PPCoin: Peer-to-peer Cryptocurrency with Proof-of-stake*.

Narayanan, A., Bonneau, J., Felten, E., Miller, A., and Goldfeder, S. (2016). *Bitcoin and Cryptocurrency Technologies*. Princeton, NJ: Princeton University Press.

Nguyen, C., Hoang, D., Nguyen, D., Niyato, D., Nguyen, H., and Dutkiewicz, E. (2019). Proof-of-Stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access* 7, 85727–85745. doi: 10.1109/access.2019.2925010

Nijsse, J., and Litchfield, A. (2020). A taxonomy of blockchain consensus methods. *Cryptography* 4:32. doi: 10.3390/cryptography4040032

Rijsberger, D., Szalachowki, P., Ke, J., Li, Z., and Zhou, J. (2021). LaKSA: a probabilistic proof-of-stake protocol. *arXiv [Preprint]*. Available online at: https://arxiv.org/abs/2006.01427#:~{}:text=LaKSA%20can%20support%20large%20numbers,on%20its%20implementation%20and%20evaluation (accessed February 15, 2021).

Rosu, I., and Saleh, F. (2021). Evolution of shares in a proof of stake cryptocurrency. *Manag. Sci.* 67, 661–672. doi: 10.1287/mnsc.2020.3791

Saleh, F. (2020). Blockchain without waste: proof of stake. *Rev. Financial Stud.* 34, 1156–1190. doi: 10.1093/rfs/hhaa075

Vasin, P. (2014). *Blackcoin's Proof of Stake Protocol V2*. Available online at: https://Blackcoin.Co/Blackcoin-Pos-Protocol-v2-Whitepaper (accessed January 31, 2019).

Wang, W., Hoang, D., Xiong, Z., Niyato, D., Wang, P., Hu, P., et al. (2019). A survey on consensus mechanisms and mining management in blockchain networks. *IEEEAccess* 7, 22328–22369. doi: 10.1109/access.2019.2896108

Wang, Y., Yang, G., Bracciali, A., Leung, H., Tian, H., Ke, L., et al. (2020). Incentive compatible and anti-compounding of wealth in proof-of-stake. *Inform. Sci.* 530, 85–94. doi: 10.1016/j.ins.2020.03.098

Xiao, Y., Zhang, N., Lou, W., and Hou, Y. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* 22, 1432–1465. doi: 10.1109/comst.2020.2969706

Conflict of Interest: The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.