ON BUBBLES IN CRYPTOCURRENCY PRICES*

Maarten R.C. van Oordt†

Vrije Universiteit Amsterdam

Tinbergen Institute

October 30, 2024

Abstract

This paper develops a tractable model for cryptocurrency prices to assess how cryptocurrencies relate to concepts such as bubbles, Ponzi-schemes and digital gold. Investors in the baseline equilibrium hold coins to sell them at a profit to future users. In a bubble equilibrium, investors hold the cryptocurrency because they expect its price to appreciate merely due to future investment inflows. The net investment inflows required to sustain a bubble equilibrium are smaller for cryptocurrencies with less new issuance, higher growth in transactional demand, a lower required return and a lower level of transactional demand. Investors in a cryptocurrency with non-negative money growth must experience Ponzi-scheme equivalent payoffs in the aggregate in a bubble equilibrium. Cryptocurrencies that experience negative issuance as they burn transaction fees may generate positive aggregate cash flows to investors even if their price path follows a bubble trajectory.

Keywords: Asset pricing, Bitcoin, crypto assets, exchange rates, rational bubble

JEL Classification Numbers: E41, F31, G12.

*I am grateful to Andrea Canidio, Albert J. Menkveldt, Dirk Niepelt, Yenan Wang, and participants in a seminar at Vrije Universiteit Amsterdam for helpful comments and suggestions.

†Email: m.van.oordt@vu.nl. Phone: +31-20-598-1578. Address: De Boelelaan 1105, 1081HV Amsterdam, The Netherlands.

I. Introduction

The terminology employed to describe cryptocurrencies like Bitcoin is notably diverse. Skeptics have called Bitcoin *the mother of all bubbles* (Roubini, 2018) and *a Ponzi-scheme* (Welch, 2017; Carstens, 2018). Enthusiasts have called it *the flagship of a new asset class* (Harvey et al., 2021) and *digital gold* (Popper, 2016; Fink, 2024). These expressions arise from underlying beliefs about the characteristics of cryptocurrencies and their (dis)connection to price trends. The purpose of this paper is to articulate how underlying beliefs regarding the properties of cryptocurrencies and their prices relate to the use of terms such as bubbles, Ponzi-schemes and digital gold. We do so by investigating the various possible price trajectories of cryptocurrencies in a consistent theoretical framework.

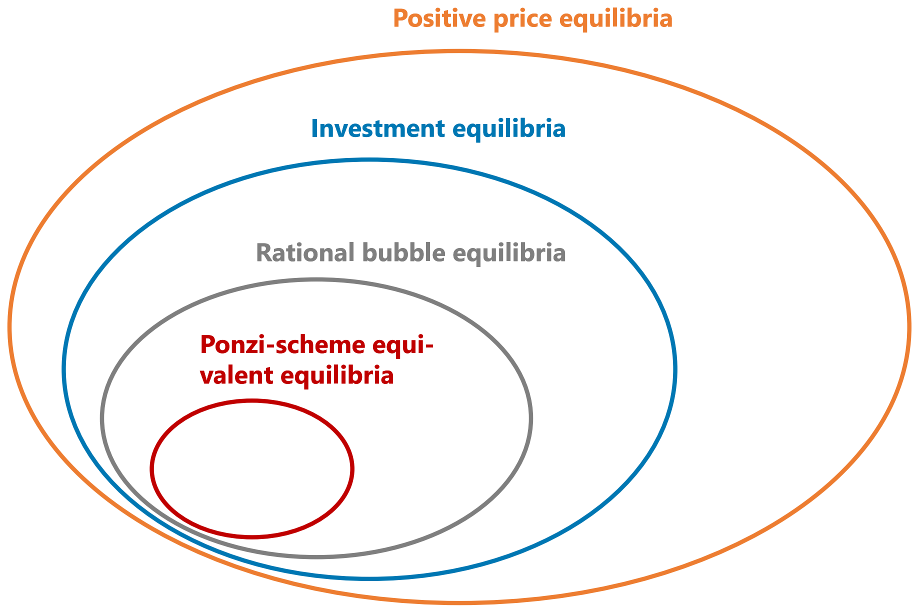
The present paper develops a deliberately simple but general model for cryptocurrency prices that allows for classical rational bubble equilibria in the sense of Blanchard (1979), Blanchard and Watson (1982) and Tirole (1982, 1985).[1] Cryptocurrencies in the model differ from securities in that they pay no dividends and that they experience a certain dollar-amount of user demand, for example, to facilitate payments. We use the model to characterize the various possible equilibrium paths for the exchange rates of cryptocurrencies.

[1]The concept of rational bubbles in asset prices has been described as fundamentally flawed because such bubbles are said to eventually outgrow all other wealth in the world. However, theory predicts that the expected return of an asset of which the price contains a rational bubble component equals the required return in equilibrium, as is the case for all other financial assets. Suppose all financial assets were to face the same required return and a rational bubble were present in the price of a single asset. Then the value of that bubble asset as a share of total financial wealth would be constant in expectation (abstracting from capital distributions, new issuance, the emergence of new financial assets, etc). Moreover, if the bubble asset faced a below-average required return, e.g., because investors perceive the asset as an insurance for bad states of the world, then its share in total financial wealth would be diminishing in expectation.

A snapshot of the possible equilibrium price paths is provided in Figure 1. Depending on the properties of the cryptocurrency, there may be equilibria where exclusively users choose to hold cryptocurrency as well as investment equilibria where some agents hold the cryptocurrency purely for financial gain. In the investment equilibrium that correspond to the baseline equilibrium, the investors hold tokens to sell them at a profit to future users in anticipation of an increase in user demand. The other investment equilibria are so-called rational bubble equilibria. In a rational bubble equilibrium, investors expect ongoing appreciation driven by future investment inflows rather than user demand. Such bubble equilibria can display a payoff equivalence to Ponzi-schemes in that investors lose in the aggregate by investing in such cryptocurrencies if the bubble persists, but, perhaps surprisingly, they do not have to be. Whether investors lose in the aggregate depends on characteristics of a cryptocurrency such as future issuance as well as whether investors perceive it as digital gold.

The analysis begins by determining the equilibrium exchange rate path that we will refer to as the baseline equilibrium. The baseline equilibrium is characterized by an exchange rate that is driven by either user demand or investor demand, or both. Investors in the baseline equilibrium choose to temporarily hold the cryptocurrency only if they anticipate sufficiently high growth in user demand and sufficiently low money growth. Otherwise, solely users will hold the cryptocurrency. Even though initially it may be mainly investors who hold the cryptocurrency, they do expect to sell their coins at a profit to users in the future. The current exchange rate in the baseline equilibrium depends on the peak level of the user demand per coin rather than the user demand over the entire lifetime of the cryptocurrency. Any exchange rate lower than the baseline equilibrium cannot reflect an equilibrium.

Figure 1: Possible Equilibria for the Exchange Rates of Cryptocurrencies



Note: This Euler diagram shows the nested relationships among various sets of equilibrium price trajectories for cryptocurrencies. The areas are not meant to accurately reflect the prevalence of equilibria in practice.

The paper also derives bubble equilibrium paths for the exchange rates of cryptocurrencies that are reminiscent of classical rational bubbles in security prices. The exchange rate of a cryptocurrency on a bubble equilibrium path is higher than that on the baseline equilibrium path. A bubble equilibrium path is characterized by investors who hold the cryptocurrency solely due to anticipated exchange rate appreciation, without the exchange rate appreciation being driven by an expected increase in user demand. Rather, investors expect the exchange rate to appreciate due to expected future increases in investment demand.

We analyze the net investment inflows implied by various equilibrium paths for the prices of cryptocurrencies. Sustaining a bubble equilibrium for a cryptocurrency requires an ongoing flow of investment of which the level depends on various aspects. The required inflow of investors' funds will be temporarily lower, or even turn negative, whenever there is growth in underlying user demand. The required inflow of investors' funds to a sustain a bubble equilibrium increases in the issuance of new cryptocurrency units and the return required by investors. The required inflow to sustain a bubble equilibrium also increases in the *level* of user demand because users need fewer cryptocurrency units for their purposes as their value continues to appreciate. The share of the coins held by users on a bubble equilibrium path tends to decrease over time, although temporary fluctuations may occur.

To study the equivalence between Ponzi-schemes and cryptocurrencies, we postulate a condition that we refer to as a Ponzi-scheme equivalence condition. This condition requires the equivalence between the cash flows of investors in a cryptocurrency and investors in a Ponzi-scheme. A Ponzi-scheme is an operation where the organizers pay returns to earlier investors from funds put into the scheme by later investors, who are then paid from funds contributed by even later investors, while the organizers skim off the scheme. An individual investor may profit from joining a Ponzi-scheme provided that the scheme continues, but the future cash flows of investors in the aggregate are characterized by a negative present value if the scheme persists. Similarly, the Ponzi-scheme equivalence condition requires the future *aggregate* cash flows of investors from investing in the cryptocurrency to have a negative present value.

The analysis shows that a cryptocurrency does not satisfy the Ponzi-scheme equivalence condition if its exchange rate path follows the baseline equilibrium. The cash outflows that investors experience when they acquire cryptocurrency in the baseline equilibrium will be balanced by expected cash inflows from selling cryptocurrency to users in the future. A cryptocurrency of which the exchange rate follows the baseline equilibrium path does not share the feature with Ponzi-schemes that future cash flows for investors have a negative present value in the aggregate.

Any cryptocurrency with non-negative money growth and nonzero user demand that follows a bubble equilibrium satisfies the Ponzi-scheme equivalence condition whenever its exchange rate path follows a bubble equilibrium. Sustaining a bubble equilibrium for such a cryptocurrency requires a sustained investment inflow that continuously drives up the exchange rate without investors ever profiting *in the aggregate* by cashing out their cryptocurrency holdings. Satisfying the aggregate user demand requires a decreasing number of coins as the exchange rate continuous to increase in the bubble equilibrium. Investors face cash outflows in the aggregate because they continue to accumulate cryptocurrency by purchasing increasingly expensive units held by cryptocurrency users. The present value of future aggregate cash flows to investors is negative even though the expected return of participating in the bubble equilibrium for individual investors satisfies their required return due to a persistent expected appreciation of the exchange rate.

For cryptocurrencies with *negative money growth*, the relationship between bubble equilibrium paths and the Ponzi-scheme equivalance condition is more nuanced. Cryptocurrencies may face negative money growth, for example, because transaction fees that are paid with the cryptocurrency are partly burned (e.g., Ethereum). We show that, depending on the parameters, cryptocurrencies with negative money growth can exhibit bubble equilibrium paths without satisfying the Ponzi-scheme equivalence condition. Investors may benefit both individually and in the aggregate from investing in such a cryptocurrency, even if the cryptocurrency's exchange rate follows a bubble equilibrium path. The net cash inflow for investors in both the baseline equilibrium and a bubble equilibrium come from purchases made by users who replenish their balances to desired levels. A cryptocurrency with negative money growth on a bubble path is less likely to satisfy the Ponzi-scheme equivalence condition if it experiences higher user growth or if the money growth is more negative. Moreover, it is less likely to satisfy the Ponzi-scheme equivalence condition if investors have a lower required return for holding the cryptocurrency. A lower required return could be the consequence of investors perceiving a cryptocurrency as a digital gold that acts as an insurance for particularly bad states of the world.

The remainder of this paper is organized as follows. Section II discusses related literature. Section III introduces the model. Sections IV and V and characterize, respectively, the baseline equilibrium and the bubble equilibria. Section VI analyzes how investor flows in the different equilibria relate to the Ponzi-scheme equivalence condition. Section VII generalizes the results regarding investment flows in bubble equilibria and their relationship to investors' payoffs in Ponzi-schemes to a model where user demand responds to the expected return on holding the cryptocurrency. Section VIII provides concluding remarks. Proofs are in the appendix.

II. Related Literature

The present paper builds upon a fast-growing theoretical literature on the exchange rates of cryptocurrencies (Athey et al., 2016; Bakos and Hałaburda, 2022; Biais et al., 2023; Chiu and Koeppl, 2022; Cong et al., 2021, 2022; Garratt and Van Oordt, 2023; Gryglewicz et al., 2021; Lee and Parlour, 2022; Sockin and Xiong, 2023a,b). User demand in those models is driven by users who derive either transactional or utility benefits from holding the cryptocurrency. Some models for cryptocurrencies also explicitly incorporate the demand by forward-looking investors to analyze the dynamics of cryptocurrency prices (Bolt and

Van Oordt, 2020; Canidio, 2023; Garratt and Van Oordt, 2022, 2024; Karau and Moench, 2023; Malinova and Park, 2023; Prat et al., 2024; Wei and Dukes, 2021). The theoretical environments in those papers, with two exceptions, do not allow for the classical rational bubble equilibria driven by expectations of investor as explored by, among others, Blanchard (1979), Blanchard and Watson (1982) and Tirole (1982, 1985).[2]

The aforementioned exceptions of theoretical studies that allow for rational bubble equilibria are the noteworthy studies by Wei and Dukes (2021) and Canidio (2023). Wei and Dukes (2021) focus on the impact of rational bubble equilibria on user adoption in an environment where the required return equals zero. They find that bubble equilibria may accelerate adoption of a cryptocurrency by regular users. Canidio (2023) shows that rational bubble equilibria can raise the revenue of issuing tokens beyond the level of selling products directly using fiat currency even in an environment with exogenous product demand. Differently from those studies, we focus on the investor inflows that are necessary to a sustain rational bubble equilibria. Our environment permits for nonzero required returns, which allows us to compare the relationship between the present value of investors net inflows for various potential price equilibria and Ponzi-schemes. The comparison reveals among others that bubble equilibria may exhibit payoffs to investors that are in the aggregate equivalent to Ponzi-schemes, but do not necessarily have to.

Brunnermeier et al. (2020) study bubbles on government bonds in a general equilibrium model that also includes an intrinsically useless alternative asset, which they refer to as a cryptocoin (but which could be any intrinsically useless asset). The alternative asset in their model faces no user demand and, hence, differs from that in the aforementioned papers which

[2] See the chapter by Brunnermeier and Oehmke (2013) for an excellent survey of the bubble literature.

model the cryptocurrency price as a function of user demand stemming from transactional or utility benefits. In the present paper, the baseline equilibrium price of such a zero user demand asset would be zero and, hence, any positive price of such an asset would fully reflect a bubble component, which is in line with terminology used by Brunnermeier et al. (2020).

The volatile and explosive price trajectories of cryptocurrencies also have been a popular subject in the empirical literature (Yermack, 2015). The search query for "Bitcoin AND Bubble" on Google Scholar returns no less than 27,000 results. Cheah and Fry (2015) and Cheung et al. (2015) apply the methodology of Phillips et al. (2015) to detect explosive paths on Bitcoin prices. Later studies vary in terms of statistical methods and data. Chaim and Laurini (2019), Geuder et al. (2019) and Cretarola and Figà-Talamanca (2020) apply alternative statistical methods on the price series of Bitcoin and Ethereum. Hafner (2020) considers a larger set of cryptocurrencies using a method that allows for time-varying volatility. Li et al. (2022) find that media attention is associated with higher future returns when bitcoin prices follow a bubbly price trajectory. Enoksen et al. (2020) relate trading and transaction volume to explosive price trajectories when analyzing a variety of cryptocurrencies. Corbet et al. (2018) assesses the explosiveness of nonprice series such as the Bitcoin block size and mining power. Lambrecht et al. (forthcoming) collect experimental evidence on whether the limited new issuance can fuel price bubbles in proof-of-work cryptocurrencies. The theoretical results in the present paper offer valuable insights into factors that may render cryptocurrencies more or less susceptible to explosive price paths in empirical data or experiments. These factors are discussed in greater detail in the concluding remarks.

III. Model

The model is in the tradition of the classical rational bubble models by Blanchard (1979) and Blanchard and Watson (1982). Those models are partial equilibrium models that build off from two main attributes: A rational expectations asset market model and a market-clearing condition. The rational expectations asset market model defines when investors are willing to hold an asset. We adapt their setup to build a tractable model for bubbles in cryptocurrency prices.

Time is discrete and denoted by $t = 0, 1, 2, ...$ We denote the exchange rate of the cryptocurrency in terms of dollars at time t by S_t. The exogenous number of units of the cryptocurrency at time t is denoted by $M_t > 0$. The demand for a cryptocurrency consists of investment demand and utility demand.

The aggregate number of cryptocurrency units held purely for investment purposes is denoted by $Z_t \geq 0$. We impose a non-negativity constraint on the investment position reflecting the fact that investors in the aggregate cannot bring additional units into existence, even though individual investors could maintain long or short positions. Investment demand is determined by what is known as a simple rational expectations asset market model. Let $r > 0$ denote the required return on capital for investment holdings in the cryptocurrency. Investor behaviour is governed by the following assumption.

Assumption 1 (Rational expectations market model) *Investors adjust their investment holdings such that, for any t where $Z_t > 0$,*

$$\mathbb{E}_t\left(S_{t+1}\right) = (1+r)S_t. \tag{1}$$

Moreover, investors do not hold the asset, so that $Z_t = 0$, whenever $\mathbb{E}_t\left(S_{t+1}\right) < (1+r)S_t$.

The $\mathbb{E}_t$-notation is used as short-hand for the expectation conditional upon the information set available at time t, which is assumed to be common to all agents.[3]

Assumption 1 reflects the idea that risk-neutral investors would purchase more of a cryptocurrency if the expected return were higher than the required return. Purchases by investors would drive up the current exchange rate until (1) holds true, after which there are no incentives for investors to further adjust their holdings. If the expected return were less than the required return, then selling pressure by rational investors would put downward pressure on the current exchange rate. The investors would continue to sell until either (1) holds true or $Z_t = 0$.

The user demand in terms of dollars is denoted by $X_t^{\$} \geq 0$. The path of the user demand in terms of dollars is assumed to be exogenous, in line with the typically exogenous dividend path in the classical literature on rational bubbles in securities prices.[4] The model is agnostic regarding the source of the user demand. The primary interpretation of the user demand

[3]The information set Ω_t contains at least the sequences $(M_t, M_{t+1}, M_{t+2}, ...)$ and $(X_t^{\$}, X_{t+1}^{\$}, X_{t+2}^{\$}, ...)$ as well as the current and past values of the exchange rate S_t and the past information set Ω_{t-1}. For more rigorous notation; see, e.g., Blanchard (1979) and Tirole (1982).

[4]The assumption regarding the exogenous user demand is unconventional. As a starting point, the assumption helps in terms of tractability by creating a dichotomy between user demand and investment demand. Section VII relaxes this assumption to a more conventional and realistic setting where the level of user demand is allowed to respond to the expected rate of appreciation. Changing the assumption is inconsequential for what are arguably the most novel results in this paper (Theorem 1, Propositions 4, 5 and 6 and Corollary 1).

is the transactional demand for a cryptocurrency that is used as a means of payments but not as a unit of account (Bolt and Van Oordt, 2020; Prat et al., 2024). If individuals use a cryptocurrency to make payments for a total dollar-amount of $T_t^\$$ dollars, and if the cryptocurrency units used to making payments have an average velocity of V_t^*, then this implies a transactional demand of $X_t^\$ = T_t^\$/V_t^*$ dollars.[5] In this interpretation, the level of transactional demand would depend on technology and preferences regarding means of payment. In certain cases, a cryptocurrency is used as the exclusive means of payment to transact on a particular platform, in which case the platform's revenue performance would be an important driver of the transactional demand (Cong et al., 2021; Gryglewicz et al., 2021). An alternative interpretation of the user demand is the utility demand that originates from benefits associated with tokens other than making payments. Tokens may serve as a membership credential that grants access to a particular platform (Bakos and Hałaburda, 2022).

The market-clearing condition requires the total value of all units to reflect the combined value of units held to satisfy user demand and the units held purely for investment purposes.

Assumption 2 (Market-clearing condition) *For any t, we have that*

$$M_t S_t = X_t^\$ + Z_t S_t. \tag{2}$$

The final assumption reflects the idea that users can always dispose of cryptocurrency without incurring any costs, a process that is sometimes referred to as *burning* cryptocurrency.

[5] See Bolt and Van Oordt (2020) for more details; here, we intentionally use the same notation.

Assumption 3 (Free disposal) *Individuals can dispose of cryptocurrency units at no cost so that* $S_t \geq 0$ *for any* t.

The model setup is closed with the following equilibrium definition.

Definition 1 *An equilibrium path for the exchange rate is defined as any path* $\mathbb{E}_0(S_0), \mathbb{E}_0(S_1), \mathbb{E}_0(S_2), ...$ *that satisfies Assumptions 1-3 for given sequences* $(M_0, M_1, M_2, ...)$ *and* $(X_0^\$, X_1^\$, X_2^\$, ...)$.

An attentive reader may have noticed that the framework does not impose a transversality condition on the exchange rate. The model does not impose any requirement that the present value of the future exchange rate converges to zero as the horizon extends to infinity. The model permits outcomes where $\lim_{t\to} \mathbb{E}_0(S_t)/(1+r)^t \neq 0$. This is on purpose. Eliminating such outcomes with a transversality condition would rule out rational bubble equilibria a priori, and prevent us from studying the characteristics of such equilibria.

IV. Baseline Equilibrium

It will be convenient to rewrite the market clearing condition in the form of an equation for the exchange rate.

Lemma 1 *At any time* t *where* $Z_t < M_t$,

$$S_t = \frac{X_t^\$}{M_t - Z_t}. \tag{3}$$

The equation reflects the intuitive notion that a higher exchange rate may follow from higher user demand (i.e., transactional demand or utility demand), a lower number of issued tokens, or a higher investment demand. The lemma also implies a hypothetical reference level for the exchange rate in the absence of any investment demand defined as $X_t^{\$}/M_t$. This reference level does not need to correspond to an equilibrium level for the exchange rate. Investors may have incentives to purchase units of the cryptocurrency if they anticipate a sufficiently strong appreciation of the exchange rate. Nonzero investment demand would raise the exchange rate above the hypothetical reference level.[6]

Traditional rational bubble models for asset prices typically derive an equilibrium with a fundamental value that reflects the present value of expected cash flows. The fundamental value in such models reflects the floor for the equilibrium value of the asset if negative price bubbles are ruled out (in our model, they are ruled out because of Assumption 3). A fundamental value in the sense of the present value of discounted cash flows does not apply directly to cryptocurrencies that do not pay dividends. However, we can derive a similar floor for the equilibrium exchange rate path of cryptocurrencies. We refer to this path as the baseline equilibrium path.

To find the floor for the equilibrium exchange rate of cryptocurrencies, we first define $\tau(1)$ as the time at which the discounted value of the hypothetical reference level without

[6] It is worth noting that, if one were to have empirical data on the number of tokens that are not held to satisfy user demand, one could calculate the value of the hypothetical reference level from the actual exchange rate and the total number of coins as $X_t^{\$}/M_t = S_t(M_t - Z_t)/M_t$. In general, precise empirical data on Z_t are not available since it requires knowledge about motives for token ownership. Proxies for Z_t based on blockchain data do exist, such as the share of coins held in *dormant* addresses (i.e., that do not transact for an extended period) or the amount of coins held in the largest addresses. Such proxies suggest that a substantial share of holdings for major cryptocurrencies does not involve user demand (Garratt and Van Oordt, 2023, Figure 2). This implies that the current value of the hypothetical reference for those cryptocurrencies must be substantially below their current exchange rates.

investors, $X_t^{\$}/M_t$, is maximized, i.e.,

$$\tau(1) =: \inf \operatorname*{argmax}_{t\in\mathbb{N}} \frac{X_t^{\$}/M_t}{(1+r)^t}. \tag{4}$$

The $\mathbb{N}$ corresponds to all positive integers including zero. The derivation of the baseline equilibrium requires $\tau(1)$ to be finite which is true as long as the growth rate of user demand per coin stabilizes at a level that is less than the required return at some point in the future. If there are multiple $t \in \mathbb{N}$ that maximize the argument, then the infimum-operator ensures that $\tau(1)$ corresponds to the time at which the maximum occurs first. At $t = \tau(1)$, we repeat the same procedure to define $\tau(2)$ as the next point in time that maximizes the discounted value of the reference level for the exchange rate. Repeating this procedure yields the sequence $(\tau(1), \tau(2), \tau(3), ...)$ that corresponds to the points in time where the future discounted value of $X_t^{\$}/M_t$ is maximized from the perspective of, respectively, time $t = (\tau(0), \tau(1), \tau(2), ...)$ where $\tau(0) = -1$ by convention. Formally, the values of $\tau(n)$ for $n \in \mathbb{N}$ are defined as

$$\tau(n) =: \inf \operatorname*{argmax}_{t\in\mathbb{N}^{>\tau(n-1)}} \frac{X_t^{\$}/M_t}{(1+r)^t}. \tag{5}$$

Given the sequence $\tau(n)$, we obtain the path for the exchange rate under the baseline equilibrium in the following proposition.

Proposition 1 (Baseline equilibrium) *The lowest possible level of the exchange rate on an equilibrium path for any t such that $\tau(n-1) < t \leq \tau(n)$ is*

$$S_t^* = \frac{X_{\tau(n)}^{\$}/M_{\tau(n)}}{(1+r)^{\tau(n)-t}}.$$

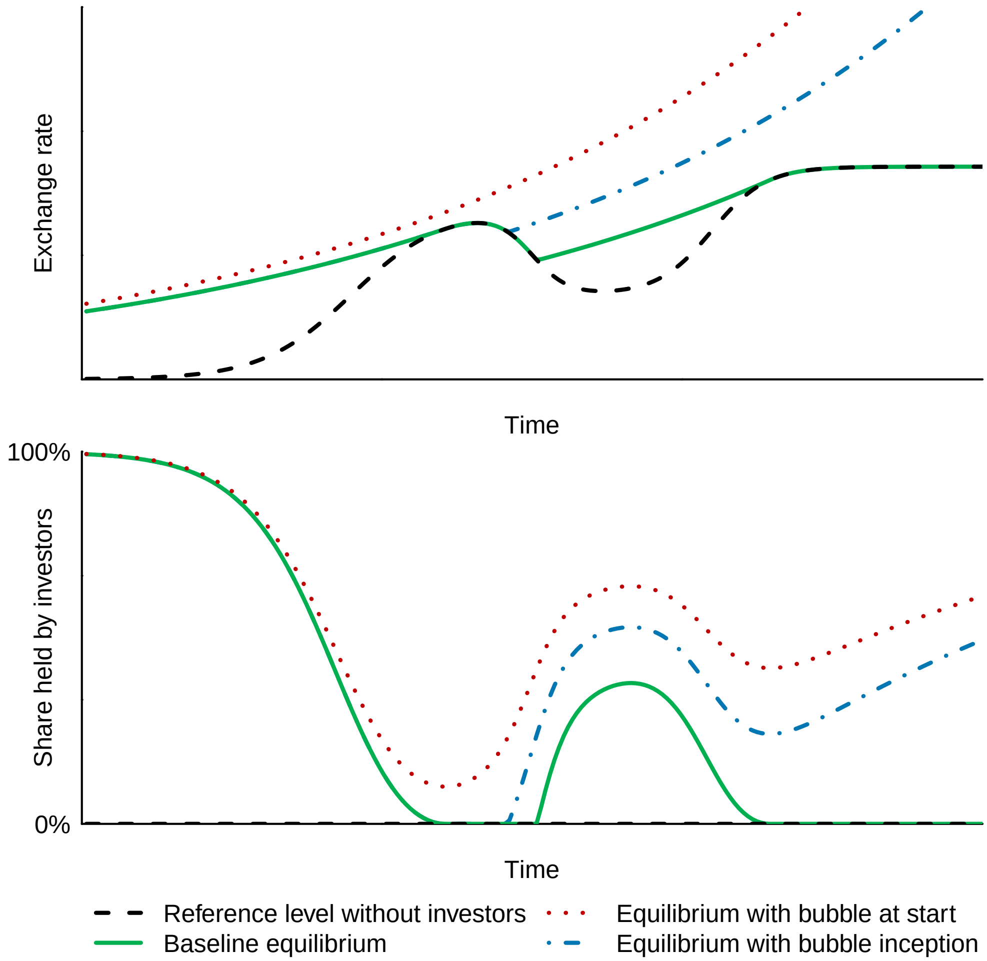
Proof. See Appendix A. ■

The exchange rate on the baseline equilibrium path equals to the reference level $X_t^\$/M_t$ at any $t = \tau(n)$. At such points in time, all cryptocurrency units are held to satisfy user demand and no units are held by investors. If the peak value of the discounted user demand per coin occurs at $t = 0$ (i.e., $\tau(1) = 0$), then we have that the baseline equilibrium is characterized by zero initial investor demand so that the equilibrium corresponds to a positive price equilibrium but not an investment equilibrium in Figure 1. Otherwise, some cryptocurrency units will be held by investors so that the baseline equilibrium corresponds to an investment equilibrium.

The solid green line in the upper panel of Figure 2 provides an illustration of the exchange rate path under the baseline equilibrium where the baseline equilibrium corresponds to an investment equilibrium. The dashed black line reflects the exogenous evolution of the hypothetical reference level without investors.[7] The initial exchange rate under the baseline equilibrium is higher than the reference level, because investors hold the tokens in expectation of higher future demand by users. This is reflected by the share of coins held by investors in the bottom panel of the figure. The equilibrium share of coins held by investors can be calculated from the equilibrium exchange rate as $Z_t/M_t = 1 - X_t^\$/(M_t S_t^*)$. Initially, investors hold almost all the coins. The share of coins held by investors converges to zero in the run-up to the next peak in the discounted level of the user demand per coin (i.e., when t approaches the next value in the sequence of $\tau(n)$).

[7]The double-hump shaped path for the reference level in the upper panel of Figure 2 illustrates a scenario with strong initial growth and then a temporary decline in user demand. The path is arbitrary and was generated using a combination of three logistic functions.

Figure 2: Exchange Rate and Investment Share in Equilibrium



The exchange rate of a cryptocurrency in the baseline equilibrium and the fundamental price of a security have crucially different relationships to their underlying values. For a security, the material underlying values are the discounted cash flows over the entire lifetime of the security. The fundamental price is calculated as the *sum* of the discounted cash flows of the security. For a cryptocurrency, the material underlying value is the discounted user demand per coin. The current exchange rate under the baseline equilibrium is determined by the *peak value* of the discounted user demand per coin. This peak value occurs at

$t = \tau(1)$ and, hence, the initial exchange rate at $t = 0$ under the baseline equilibrium equals $(X^{\$}_{\tau(1)}/M_{\tau(1)})/(1+r)^{\tau(1)}$.

Finally, there are direct implications of Proposition 1 for equilibrium existence. The baseline equilibrium requires $\tau(1)$ to be finite. If the lowest possible exchange rate path cannot exist in equilibrium, then no equilibrium can exist. In other words, the existence of *any* equilibrium requires $\tau(1)$ to be finite.[8]

V. Bubble Equilibria

The exchange rate under the baseline equilibrium in Proposition 1 is based on one particular solution of the difference equation in Assumption 1. Also other solutions to the difference equation that reflect equilibria exist. In particular, at $t = 0$, the exchange rate may be higher due to the presence of a rational bubble component that is stacked on top of the baseline equilibrium. Such equilibria with a bubble component from the outset are characterized in the following proposition.

Proposition 2 (Rational bubble equilibrium) *Any path for the expected exchange rate that satisfies*

$$\mathbb{E}_0 S_t = (S^*_0 + B)(1+r)^t$$

for $B \geq 0$ and any $t \in \mathbb{N}$ constitutes an equilibrium path.

[8] An example where this condition does not hold true is that where $X^{\$}_t/M_t$ grows indefinitely at a constant rate $g > r$. This is analogous to the familiar result regarding the nonexistence of the fundamental equilibrium price of a security with a dividend that grows indefinitely at a constant rate $g > r$.

The initial exchange rate in a bubble equilibrium characterized by the proposition consists of two components: The exchange rate under the baseline equilibrium in Proposition 1 plus a non-negative rational bubble component, $B \geq 0$.

An illustration of an equilibrium with a bubble component in the initial exchange rate is provided by the blue dotted line in the upper panel of Figure 2. The exchange rate and the share of cryptocurrency held by investors under this equilibrium are larger than in the baseline equilibrium, and the divergence tends to increase over time. Investors have incentives to hold the cryptocurrency despite of the bubble component because the cryptocurrency is expected to continue to appreciate at a rate that equals the required return on capital. The share of coins held by investors in a bubble equilibrium slowly converges to all coins in circulation as shown by the blue dotted line in the lower panel of Figure 2, even though temporary growth in user demand can lead to a short-term reduction in the share held by investors.

The expected exchange rate of a cryptocurrency on a bubble equilibrium path in Proposition 2 depends on the required return on capital and the initial level of the exchange rate. Proposition 2 permits bubble exchange rate paths that contain random elements – it describes the exchange rate path in terms of expectations. Blanchard and Watson (1982) suggest an intuitive example of a bubble equilibrium where the exchange rate grows at a faster speed than the required return as long as the bubble persists, but where there is a positive probability that the bubble will burst. The expected return on such a stochastic bubble path still equals the required return because the higher rate of appreciation is counterbalanced by the downside risk. Alternative stochastic bubble paths with more complex dynamics are possible too.

The previous proposition covers the case in which there is a rational bubble component from the outset. If there was no rational bubble component from the outset, then a rational bubble component to the price could still commence in the future if the expected return in the baseline equilibrium is sufficiently low. The following proposition characterizes the equilibria that involve the inception of a bubble in cryptocurrency prices.

Proposition 3 (Rational bubble inception) *Suppose $S_t = S_t^*$ for $t = \tau(n)$ given some value $n \in \mathbb{N}$. Then any path for the expected exchange rate that satisfies*

$$\mathbb{E}_{\tau(n)} S_t = (S^*_{\tau(n)+1} + B)(1+r)^{t-\tau(n)-1}$$

for B s.t. $0 \leq B \leq S^*_{\tau(n)}(1+r) - S^*_{\tau(n)+1}$ and all $t > \tau(n)$ constitutes an equilibrium path.

An illustration of an bubble equilibrium path that involves the inception of a bubble in the exchange rate is given by the red dash-dotted line in Figure 2. The exchange rate under the baseline equilibrium is on a downward trajectory when the inception of the bubble occurs, and, hence, expected returns in the baseline equilibrium are less than the required return. This is relevant because the size of the bubble at inception as measured by B is limited in magnitude since the expected return on the cryptocurrency's exchange rate at the moment of inception cannot exceed the required return in equilibrium. The expected return in the baseline equilibrium must be less than the required return in order to allow for the possible inception of a bubble in investor's expectations to exist. Otherwise, the possible inception of the bubble with a nonzero probability would raise the expected return above the required return, which cannot occur in equilibrium.[9]

[9]Proposition 3 extends the seminal result of Diba and Grossman (1987) to cryptocurrencies. Diba and Grossman show that the inception of a rational bubble in security prices cannot occur because, in the absence

VI. Sustaining a Bubble Equilibrium

The previous sections explored the possible equilibrium price paths given Assumptions 1–3. The present section explores the net investment flows that are implied by the equilibrium price paths and their relationship to Ponzi-schemes. The first result is that the following condition must hold true for the expected net investment inflows to sustain the rational bubble equilibria characterized in Propositions 2–3.

Theorem 1 *A rational bubble equilibrium for a cryptocurrency can persist if and only if*

$$\underbrace{\mathbb{E}_t \Delta Z_{t+1} S_{t+1}}_{\substack{\text{Net investment}\\ \text{inflow}}} = \underbrace{\mathbb{E}_t \Delta M_{t+1} S_{t+1}}_{\substack{\text{Value of}\\ \text{newly issued}\\ \text{units}}} - \underbrace{\Delta X^{\$}_{t+1}}_{\substack{\text{New user}\\ \text{demand}}} + \underbrace{r X^{\$}_t}_{\substack{\text{Appreciation}\\ \text{of units held}\\ \text{by users}}}. \tag{6}$$

Proof. See Appendix B. ■

The expression for the net inflow of investors' funds required to sustain a rational bubble consists of three components.[10] The first component is the value of newly issued cryptocurrency units. Newly issued units need to be absorbed by investors to sustain a bubble equilibrium, and, hence, the larger the new issuance the larger the net inflow of investors' funds necessary to sustain a rational bubble. The second component is the change in user

of a bubble, the expected rate of return must equal the expected return. Intuitively, a nonzero probability for the start of a new bubble would raise the expected return of a security above the required return, which cannot occur in equilibrium. Similarly, the inception of a rational bubble in cryptocurrency prices cannot occur whenever the expected rate of return in the baseline equilibrium equals to the required return (that is, whenever investors are willing to hold the cryptocurrency). Differently, in the baseline equilibrium for cryptocurrency prices, there can be periods where the expected return is less than the required return so that users only are willing to hold the coin. By definition, this can be the case when moving from $t = \tau(n)$ to $t = \tau(n) + 1$. The possible inception of a rational bubble at $t = \tau(n) + 1$ does not raise the expected return above the required return provided that the initial expected size of the bubble is limited in size, i.e., B s.t. $0 \leq B \leq S^*_{\tau(n)}(1 + r) - S^*_{\tau(n)+1}$.

[10] The difference operator Δ applies to the first symbol by convention; e.g., $\Delta Z_{t+1} S_{t+1} = (Z_{t+1} - Z_t) S_{t+1}$.

demand. An increase in user demand reduces the number of units that need to be acquired by investors. A smaller net investment inflow is required to sustain a bubble equilibrium if the user demand expands. The required net inflow may turn negative if the increase in user demand is sufficiently large. The third component stems from the existing user demand for a cryptocurrency. Sustaining a bubble equilibrium path implies a continuous appreciation of the coins held by users resulting in a reduction in the number of coins they need to hold for transactional or utility purposes. Investors need to acquire the coins that users sell to sustain the equilibrium, which number depends on the rate of appreciation which depends in equilibrium on the required return. The required net investment inflow in (6) will be lower if investors require a lower return on investments in the cryptocurrency because they perceive it as a digital gold that provides insurance for bad states of the world.

The condition in Theorem 1 hints that sustaining a bubble exchange rate paths may require a continuous inflow of investors funds like a Ponzi-scheme. A Ponzi-scheme is distinct from a cryptocurrency in the literal sense in that investors can choose to buy or sell them at the prevailing market price, but it could display similarities in that the prolongation of a Ponzi-scheme requires a sustained inflow of aggregate investors' funds like certain equilibria for cryptocurrency prices. We explore the relationship between bubble exchange rate paths and Ponzi-schemes by postulating the following Ponzi-scheme equivalence condition regarding the cash flows for investors.

Condition 1 (Ponzi-scheme equivalance) *The remaining cash flows for investors in the aggregate have a negative present value at some point in time in the future, that is,*

$$-\sum_{i=1}^{\infty} \frac{\mathbb{E}_T \Delta Z_{T+i} S_{T+i}}{(1+r)^i} < 0 \quad \textit{for some} \quad T \geq 0.$$

The condition sums all the expected aggregate cash flows to investors at some point in the future and requires the present value to be negative. The minus-sign in front of the sum accounts for the fact that net sales by investors – cash inflows from the perspective of the investors – correspond to negative values of ΔZ_t. Net purchases – cash outflows for investors – correspond to positive values of ΔZ_t. A cryptocurrency satisfies the Ponzi-scheme equivalence condition for example if its equilibrium exchange rate path requires a continuous inflow of investors funds: This would imply $\Delta Z_t > 0$ for all $t > T$, and, hence, violate Condition 1. The condition requires that there will be some point in time where the remaining discounted cash flows from coin sales by investors will be less than the discounted cost of the remaining coin purchases by investors.

A. Non-negative Money Growth

We first consider aggregate payoffs of investors in bubble equilibria for cryptocurrencies that exhibit non-negative money growth ($\Delta M_t \geq 0$ for any $t > T$). Denote the growth rate of user demand by $g_t = (X_{t+1} - X_t)/X_t$. Consider a cryptocurrency for which the growth stabilizes at some point in the – potentially distant – future such that the user growth rate will be lower than the required return on capital, i.e., $g_t < r$ for any $t > T$ given some T. The following proposition summarizes our result for such cryptocurrencies.

Proposition 4 *Consider a cryptocurrency with non-negative issuance* $\Delta M_t \geq 0$ *and for which the nonzero user demand stabilizes at some distant point in the future such that the growth rate* $g_t < r$ *for any* $t > T$ *given some* $T \geq 0$.

The cryptocurrency satisfies the Ponzi-scheme condition if its exchange rate follows a bubble equilibrium path.

Proof. See Appendix C. ■

The intuition for this result is that an ongoing appreciation of the exchange rate is only sustainable if investors purchase cryptocurrency from users, who need fewer and fewer coins as the exchange rate continues to increase. Sustained user growth can help to alleviate the need for investors to purchase units from users, but this reduction is not sufficient if the growth rate is less than the required return of capital ($g_t < r$). The continuing purchases of cryptocurrency by investors from users ad infinitum imply a negative present value of the remaining aggregate cash flows from the perspective of investors. Despite of the negative cash flows for investors in the aggregate, every individual investor who acquires cryptocurrency in the bubble equilibrium and sells it in the future is expected to earn the required return.

B. Endogenous Negative Money Growth

Some cryptocurrencies exhibit negative money growth. Negative money growth can be a design feature. For example, Ethereum has shown a period of negative money growth after its switch to a mechanism where part of the tokens paid as transaction fees are burned. A hidden source of negative money growth is the coins to which users have lost access permanently.

To illustrate the relationship between the cash flows for investors in Ponzi-schemes and bubble equilibria for cryptocurrencies with negative money growth, we extend the model to allow for a scenario where every period a proportion $f > 0$ of the user demand $X_t^\$$ is burnt as transaction fees (or, alternatively, lost) such that $\Delta M_{t+1} S_{t+1} = -f X_t^\$$.[11] The following proposition states the Ponzi-scheme equivalence result for such a cryptocurrency.

Proposition 5 *Consider a cryptocurrency where every period a fraction of the nonzero user demand $f > 0$ is burnt and for which the growth rate of user demand g is such that $g < r$ for any $t > 0$.*

1. *If $f < r - g$ and the exchange rate follows a bubble equilibrium path, then the cryptocurrency satisfies the Ponzi-scheme equivalence condition.*

2. *If $f > r - g$ and the exchange rate follows a bubble equilibrium path, then the cryptocurrency does not satisfy the Ponzi-scheme equivalence condition.*

Proof. See Appendix D. ■

All bubble equilibria satisfy the Ponzi-scheme equivalence condition if the proportion of the user demand that is burnt every period is less than the difference between the required return and the growth in user demand ($f < r - g$). We find a different result for the situation where the proportion of user demand paid as fees exceeds the difference between the required return and the growth in user demand ($f > r - g$). For such cryptocurrencies, bubble equilibria do not satisfy the Ponzi-scheme equivalence condition. This is why there is a non-empty set of bubble equilibria with payoffs that are not equivalent to Ponzi-schemes in Figure 1.

[11] The expression assumes $\Delta M_{t+1} = -f X_t^\$ / S_{t+1}$. Alternatively, one could assume $\Delta M_{t+1} = -f X_t^\$ / S_t$. This has no impact on Propositions 5 and 6, except that the f in any expression should be replaced by $f/(1 + r)$.

A cryptocurrency for which $f > r - g$ is an interesting scenario from an economic point of view in that the user demand per coin and, hence, the reference level would grow forever at a rate $f + g$ which is greater than the required return r if there weren't any investors. The presence of investors ensures that the exchange rate does not appreciate at a rate higher than the required return in equilibrium. The mechanism functions as follows. Investors who acquire the cryptocurrency drive up the initial exchange rate. The higher initial exchange rate implies that users hold fewer coins, and, hence, burn a smaller number of coins as transaction fees. The number of coins declines at a slower speed resulting in a slower increase in the user demand per coin than in the absence of investors. In equilibrium, the user demand per coin will grow at precisely the same rate as the required return. The remaining cash flows to investors will be positive in such an equilibrium. Users have to purchase tokens from investors to replenish their cryptocurrency balances after burning the transaction fees which generates a positive aggregate cash flow from users to investors.

The following proposition illustrates the equilibrium exchange rate path and the evolution in the share of coins held by investors.

Proposition 6 *Consider a cryptocurrency with no new issuance, with a constant growth rate of user demand $g < r$, and with users who burn a proportion $f > r - g$ of their coins as transaction fees at any t.*

The following exchange rate path constitutes an equilibrium:

$$S_t = (1+r)^t \frac{f}{r-g} \frac{X_0^{\$}}{M_0 - U} \quad \textit{for any} \quad 0 \leq U < M_0. \tag{7}$$

The equilibrium where $U = 0$ corresponds to the baseline equilibrium; any equilibrium where U such that $0 < U < M_0$ corresponds to a bubble equilibrium. The equilibrium share of coins held by investors equals

$$\frac{Z_t}{M_t} = \frac{\frac{f-(r-g)}{f}(M_0 - U)\left(\frac{1+g}{1+r}\right)^t + U}{(M_0 - U)\left(\frac{1+g}{1+r}\right)^t + U}.$$

Proof. See Appendix E. ■

The share of coins held by investors slowly converges to all coins in a bubble equilibrium ($0 < U < M_0$) as was the case for the earlier bubble equilibria where the money issuance was exogenous. The evolution of the share of coins held by investors with the endogenous burning of coins is different for the baseline equilibrium ($U = 0$). Rather than converging to zero as was the case with the exogenous money issuance, the share of coins held by investors is constant: Investors in the baseline equilibrium sell precisely the amount to restore the balance between the shares held by users and investors.

The finding that bubble equilibria do not satisfy the Ponzi-scheme condition if $f > r - g$ does not mean that the net present value of the cash flows for investors of investing in the cryptocurrency will be non-negative in the aggregate. The Ponzi-scheme equivalence condition tests whether the future cash flows for investors have a negative present value in the aggregate. The condition does not consider the initial cost for investors to acquire the coins. If investors were to pay the prevailing market price for their initial position in cryptocurrency at $t = 0$, then the cost of their position would be $S_0 Z_0$. From the proposition, we can then derive the following corollary.

Corollary 1 *Consider the equilibria characterized in Proposition 6. The baseline equilibrium (i.e., $U = 0$) is the only equilibrium with a non-negative net present value for investors* *in the aggregate, i.e.,*

$$-S_0 Z_0 - \sum_{t=1}^{\infty} \frac{\mathbb{E}_0 \Delta Z_t S_t}{(1+r)^t} \geq 0.$$

Investors experience positive cash flows in the aggregate in bubble equilibria where $f > r - g$, so the Ponzi-scheme equivalence condition is not satisfied, but the present value of the aggregate cash flows is less than the initial cost of acquiring cryptocurrency in the first period. Despite the negative present value in the aggregate, every individual investor who acquires cryptocurrency and sells it in the future is still expected to earn the required return.

VII. Discussion

A. Endogenous user demand

The user demand in the model is assumed to be inelastic with respect to the expected return on the cryptocurrency. Although this assumption simplifies the model considerably, it ignores how the demand for a means of payment depends on the opportunity cost of holding it. Alternatively, one could consider a reduced-form generalization of the model where the user demand at time t equals $X_t^{\$}(\mathbb{E}_t R_{t+1}) = A(\mathbb{E}_t R_{t+1})\widehat{X}_t^{\$}$. The $\widehat{X}_t^{\$}$ is assumed to be exogenous and the $A(\cdot)$ is a non-negative finite scaling factor that increases in the expected return $\mathbb{E}_t R_{t+1} = \mathbb{E}_t(S_{t+1}/S_t)$ for $\mathbb{E}_t R_{t+1} \geq 0$. The original model can be considered as a special case where $A(\mathbb{E}_t R_{t+1}) = 1$ for any $\mathbb{E}_t R_{t+1}$. The more general specification allows user demand to depend on time-specific fundamental factors as measured by $\widehat{X}_t^{\$}$ as well as the expected rate of appreciation.

The main results regarding the investment flows in bubble equilibria and their relationship to investors' payoffs in Ponzi-schemes extend immediately to the more general specification, provided that $A(1 + r)$ is finite. Theorem 1, Propositions 4, 5 and 6, and Corollary 1 all hold true in the more general model.[12] The reason why the bubble results also hold true in the more general model is straightforward. Investors hold the cryptocurrency in any equilibrium where the exchange rate contains a bubble component, so the expected return must equal the required return in any bubble equilibrium (Assumption 1). Hence, we must have $A(\mathbb{E}_t R_{t+1}) = A(1 + r)$ for all t whenever the cryptocurrency price contains a bubble component in equilibrium, so that the user demand $X_t^{\$}$ becomes a re-scaled version of the underlying fundamental factor $\widehat{X}_t^{\$}$. The user demand takes its maximum possible value because the expected return attains its maximum possible equilibrium value—that is, the required return—in a bubble equilibrium.

The aforementioned generalization of the bubble results is conditional upon $A(1 + r)$ being finite. This requires the user demand for cryptocurrency in dollar terms to be finite even if the opportunity cost of holding cryptocurrency were zero. Although many micro-founded models of money do imply finite real transactional balances if the opportunity cost of holding money converges to zero, this does not hold true for all models. Famously, Tirole (1985, Proposition 7) considers an environment with money-in-the-utility where the marginal benefit of real money balances is strictly positive. In this environment, agents are incentivized to increase their real money balances to infinitely large levels as the opportunity cost approaches zero. Intuitively, a rational bubble in the value of a currency—implying a

[12] The growth rates referred to in those propositions should in the more general model be understood as growth rates of the underlying fundamental $\widehat{X}_t$, i.e., $g_t = (\widehat{X}_{t+1} - \widehat{X}_t)/\widehat{X}_t$. The solution for the baseline equilibrium is more challenging in the general model. The path of the user demand per coin need not be unique in the baseline equilibrium for a given sequence of $\widehat{X}_t^{\$}$.

zero opportunity cost of holding that currency—cannot coexist with that currency being used for transactional purposes in such an environment. The present model would yield a similar impossibility result if we were to assume $A(\mathbb{E}_t R_{t+1}) \to \infty$ as $\mathbb{E}_t R_{t+1} \to 1 + r$. If $A(1 + r)$ is finite, then the bubble results generalize as aforementioned to the setting with the reduced-form endogenous money demand.

The theoretical result that a price bubble may stimulate user demand for a cryptocurrency by reducing the opportunity cost of holding it makes cryptocurrency quite different from a commodity that serves as an input at fixed quantities for other goods or services. Brunnermeier and Oehmke (2013) note that the emergence of a price bubble would make a commodity relatively expensive, so that users would be incentivized to seek for substitutes. In contrast, a higher exchange rate of a cryptocurrency does not directly change the cost of using that cryptocurrency for making payments. Users simply need a smaller quantity of the cryptocurrency to make the same dollar-amount of payments. What does matter to users is the expected rate of appreciation of the cryptocurrency in the bubble equilibrium, which is either higher than or equal to the rate of appreciation in the baseline equilibrium.

VIII. Concluding Remarks

This paper focused on the question how cryptocurrency price paths relate to concepts such as new asset classes, bubbles, Ponzi schemes and digital gold. The analysis reveals how those terms relate to differences in underlying beliefs regarding future peak values of the user demand per coin and discount rates.

High crypto prices can be justified by a high expected peak value in terms of user demand. Describing a cryptocurrency as equivalent to a Ponzi-scheme is not justified if the current price reflects the discounted value of the expected peak value in user demand. This holds true even if the current price seems to be driven mostly by investors' actions rather than user dynamics. Even though investors experience outflows when they acquire cryptocurrency, they expect to profit from selling crypto to users in the future. An observer could easily mistake a high price observed in a baseline equilibrium for a bubble when underestimating the expected peak value in user demand. Moreover, higher prices could be justified by a lower discount rate resulting from investors perceiving cryptocurrency as a digital gold that provides insurance against bad states of the world.

The picture is bleaker if current high prices are the consequence of investors expecting price increases solely due to higher future investor demand, and not due to the expected peak level of future user demand. Such bubble price paths are possible in equilibrium and are associated with a gradually increasing share of coins held purely for investment purposes. The analysis reveals that, for cryptocurrencies with nonnegative money growth, such price paths are associated with Ponzi-scheme equivalent payoffs to investors in the aggregate. Even though individual investors are expected to earn their required return if the bubble persists, they do experience negative cash flows in the aggregate. Finally, investors do not necessarily experience Ponzi-scheme equivalent payoffs in the aggregate if they invest in a bubble equilibrium for a cryptocurrency with negative money growth.

For the empiricist or experimenter, our results provide a theoretical foundation for potential factors that make cryptocurrencies more or less susceptible to explosive price paths. For reasons outside the model, it may seem less plausible that an equilibrium can persist if it requires a high rather than a low net investment inflow over a sustained period of time. Combining such an a posteriori statement with Theorem 1 implies the following predictions: A bubble equilibrium for cryptocurrencies is *less plausible* with (1) *higher new issuance*, (2) *lower growth in user demand*, and (3) *higher existing user demand*. It is noteworthy that user demand acts as a double-edged sword: Growth in user demand reduces the required investment inflow to sustain a bubbly exchange rate path initially, but the existing level of user demand increases the required investment inflow. Finally, the required investment inflow for bubbles is smaller when the required return is lower which typically would be the case if investors perceive a cryptocurrency as a digital gold that acts as an insurance for bad states of the world.

For the theorist, the condition in Corollary 1 may prove useful to rule out rational bubble equilibria if the baseline equilibrium is the object of study. A theorist may be tempted to ruling out bubble equilibria by imposing an alternative condition that limits the asymptotic growth of the exchange rate so that the present value of the future exchange rate converges to zero, akin to a transversality condition. The disadvangage of such a transversality-like condition is that it may rule out both the bubble equilibria *and* the baseline equilibrium as we have seen in the case studied in Proposition 6.[13]

[13]From Eq. (7), it is immediate that the baseline equilibrium condition in Proposition 6 violates the condition $\lim_{t\to\infty} S_t/(1+r)^t = 0$ since $\lim_{t\to\infty} S_t/(1+r)^t > 0$ for $U = 0$ provided that $X_0^{\$} > 0$.

Appendix: Proofs

A. *Proof of Proposition 1*

We first consider t such that $0 < t \leq \tau(1)$.

Suppose $X^{\$}_{\tau(1)} > 0$. Lemma 1 and $Z_{\tau(1)} \geq 0$ imply that any $S_{\tau(1)} < X^{\$}_{\tau(1)}/M_{\tau(1)}$ would be inconsistent with market clearing (Assumption 2). This proves the lower bound for $t = \tau(1)$. Moreover, if $S_{\tau(1)} = X^{\$}_{\tau(1)}/M_{\tau(1)}$, then any level of the exchange rate $S_t(1+r)^{\tau(1)-t} < X^{\$}_{\tau(1)}/M_{\tau(1)}$ for $0 < t < \tau(1)$ would violate Assumption 1. This proves the lower bound for any $0 < t < \tau(1)$. Assumption 3 also holds true on the path since $X^{\$}_{\tau(1)} > 0$ implies $S^*_t > 0$ for $0 < t \leq \tau(1)$, so the path S^*_t in the proposition constitutes an equilibrium for any t such that $0 < t \leq \tau(1)$.

Repeating the argument for $n = 2, 3, ...$ provides the proof for any t such that $\tau(n-1) < t \leq \tau(n)$.

The special case where $X^{\$}_{\tau(1)} = 0$ implies $X^{\$}_t = 0$ for any $t \in \mathbb{N}$, so that $\tau(n) = n$. In this case, the path described in the proposition implies $S_t = X^{\$}_t/M_t = 0$ for any t, which is the lowest possible level of the exchange rate that does not violate Assumption 3.

B. *Proof of Theorem 1*

From Lemma 1, we have

$$\mathbb{E}_t(\Delta S_{t+1}) = \mathbb{E}_t\left(\frac{X^{\$}_{t+1}}{M_{t+1} - Z_{t+1}} - \frac{X^{\$}_t}{M_t - Z_t}\right).$$

Moreover, since investors are willing to hold cryptocurrency on a bubble equilibrium path, we have $\mathbb{E}_t(\Delta S_{t+1}) = rS_t$ from Assumption 1. Combining both expressions gives

$$rS_t = \mathbb{E}_t\left(\frac{X^{\$}_{t+1}(M_t - Z_t) - X^{\$}_t(M_{t+1} - Z_{t+1})}{(M_{t+1} - Z_{t+1})(M_t - Z_t)}\right),$$

and, since $S_t = X^{\$}_t/(M_t - Z_t)$,

$$\begin{aligned}
rX^{\$}_t &= \mathbb{E}_t\left(\frac{X^{\$}_{t+1}(M_t - Z_t) - X^{\$}_t(M_{t+1} - Z_{t+1})}{(M_{t+1} - Z_{t+1})}\right), \\
&= \mathbb{E}_t\left(\frac{X^{\$}_{t+1}(M_t - Z_t) - X^{\$}_{t+1}(M_{t+1} - Z_{t+1}) + \Delta X^{\$}_{t+1}(M_{t+1} - Z_{t+1})}{M_{t+1} - Z_{t+1}}\right), \\
&= \mathbb{E}_t\left(S_{t+1}(M_t - Z_t) - S_{t+1}(M_{t+1} - Z_{t+1}) + \Delta X^{\$}_{t+1}\right), \\
&= -\mathbb{E}_t \Delta M_{t+1} S_{t+1} + \mathbb{E}_t \Delta Z_{t+1} S_{t+1} + \Delta X^{\$}_{t+1}.
\end{aligned}$$

Rearranging the last line gives the expression for $\mathbb{E}_t \Delta Z_{t+1} S_{t+1}$ in the proposition.

C. *Proof of Proposition 4*

Aggregating the relationship for the net inflows from investors in Theorem 1 for all $t > T$ with discounting and iterating expectations back to $t = T$ gives

$$\sum_{i=1}^{\infty} \frac{\mathbb{E}_T \Delta Z_{T+i} S_{T+i}}{(1+r)^i} = \sum_{i=1}^{\infty} \frac{\mathbb{E}_T \Delta M_{T+i} S_{T+i}}{(1+r)^i} + \sum_{i=1}^{\infty} \frac{-\Delta X^{\$}_{T+i} + rX^{\$}_{T+i-1}}{(1+r)^i}. \tag{8}$$

Using $M_{T+i} \geq 0$ (non-negative money growth) and $\Delta X_{T+i} = (1+g_{T+i})X^{\$}_{T+i-1} - X^{\$}_{T+i-1} = g_{T+i}X^{\$}_{T+i-1}$ gives

$$\sum_{i=1}^{\infty} \frac{\mathbb{E}_T \Delta Z_{T+i} S_{T+i}}{(1+r)^i} \geq \sum_{i=1}^{\infty} \frac{rX^{\$}_{T+i-1} - g_{T+i}X^{\$}_{T+i-1}}{(1+r)^i}, \tag{9}$$

$$\geq 0, \tag{10}$$

where the last inequality holds because $g_t < r$ for all $t \geq T$. The present value of the net cash inflows from investors is larger than zero which is the same as saying that that present value of the remaining cash flows is negative from the perspective of investors.

D. Proof of Proposition 5

If a fraction f of the coins paid as transaction fees by users are burned, and if there is no further issuance of coins, then $\mathbb{E}_T \Delta M_{T+i} S_{T+i} = -fX^{\$}_{T+i-1}$. Then, from (8), we have

$$\begin{aligned}
\sum_{i=1}^{\infty} \frac{\mathbb{E}_T \Delta Z_{T+i} S_{T+i}}{(1+r)^i} &= \sum_{i=1}^{\infty} \frac{-fX^{\$}_{T+i-1} - gX^{\$}_{T+i-1} + rX^{\$}_{T+i-1}}{(1+r)^i}, \\
&= \frac{r-f-g}{1+g} \sum_{i=1}^{\infty} \frac{(1+g)^i}{(1+r)^i} X^{\$}_T, \\
&= \frac{r-f-g}{r-g} X^{\$}_T.
\end{aligned}$$

This value can be both positive and negative, depending on the level of the transaction fees. If $f < r - g$, then the present value of the future cash flows to investors is negative, so that the Ponzi-scheme equivalence condition is satisfied for any equilibrium where coins continually appreciate at an expected rate r (i.e., bubble equilibria in this case). If the fees

$f > r - g$, then the present value of the remaining cash flows to investors would be positive, so that the Ponzi-scheme equivalence condition is not satisfied in an equilibrium where coins continuously appreciate at an expected rate r (i.e., the equilibria described by Proposition 6 in this case).

E. *Proof of Proposition 6*

Market clearing (Assumption 2) requires that, for any $t \geq T$,

$$S_{t+1} = \frac{X_{t+1}^{\$}}{M_{t+1} - Z_{t+1}} = \frac{(1+g)X_t^{\$}}{M_t - fX_t^{\$}/S_{t+1} - Z_{t+1}} = \frac{(1+f+g)X_t}{M_t - Z_{t+1}}.$$

The rational expectation market model (Assumption 1) requires

$$\mathbb{E}_t \frac{S_{t+1}}{S_t} = (1+f+g)\mathbb{E}_t \frac{M_t - Z_t}{M_t - Z_{t+1}} = (1+r).$$

For non-stochastic Z_{t+1}, one can rewrite this condition into the following difference equation for the speculative position

$$Z_{t+1} = M_t - \frac{1+f+g}{1+r}(M_t - Z_t) = \frac{1+f+g}{1+r} Z_t - \frac{f+g-r}{1+r} M_t.$$

Similarly, we derive the number of cryptocurrency units as

$$M_{t+1} = M_t - fX_t/S_{t+1} = M_t - \frac{f}{1+f+g}(M_t - Z_{t+1}) = \frac{1+g}{1+f+g} M_t + \frac{f}{1+f+g} Z_{t+1}.$$

Plugging in the difference equation for Z_{t+1} yields the difference equation for the existing number of currency units as

$$M_{t+1} = \frac{f}{1+r} Z_t + \frac{1+r-f}{1+r} M_t.$$

Thus, we have the system of difference equations

$$\begin{pmatrix} Z_{t+1} \\ M_{t+1} \end{pmatrix} = \begin{bmatrix} \frac{1+f+g}{1+r} & -\frac{f+g-r}{1+r} \\ \frac{f}{1+r} & \frac{1+r-f}{1+r} \end{bmatrix} \begin{pmatrix} Z_t \\ M_t \end{pmatrix}, \tag{11}$$

with distinct and real eigenvalues $(\lambda_1, \lambda_2) = \left(\frac{1+g}{1+r}, 1\right)$, and eigenvectors $v_1 = \left(\frac{f+g-r}{f}, 1\right)$ and $v_2 = (1, 1)$. The system has the following solution

$$\begin{pmatrix} Z_{t+i} \\ M_{t+i} \end{pmatrix} = C \begin{bmatrix} \frac{f+g-r}{f} \\ 1 \end{bmatrix} \left(\frac{1+g}{1+r}\right)^i + U \begin{bmatrix} 1 \\ 1 \end{bmatrix} 1^i. \tag{12}$$

From the solution of M_{t+i} for $i = 0$, we solve $C = M_t - U$, so that we find the generic solution

$$\begin{aligned} Z_{t+i} &= \frac{f+g-r}{f} (M_t - U) \left(\frac{1+g}{1+r}\right)^i + U, \\ M_{t+i} &= (M_t - U) \left(\frac{1+g}{1+r}\right)^i + U. \end{aligned}$$

What values of U correspond to valid equilibria? Note that $\lim_{i \to \infty} (Z_{t+i}, M_{t+i}) = (U, U)$. Hence, a valid equilibrium requires $U \geq 0$: Otherwise, Z_{t+i} and M_{t+i} would converge to negative numbers. Similarly, a valid equilibrium also requires $M_t > U$. Any solution with a value of U such that $0 \leq U < M_t$ corresponds to a valid equilibrium.

The floor for the equilibrium exchange rate corresponds to the case where $U = 0$, so that $Z_t = M_t(f + g - r)/f$, and $S_t = (X_t/M_t)(f/(r - g))$. Any values of U such that $0 < U < M_t$ corresponds to equilibrium exchange rate paths with higher levels. The share of coins held by speculators can be calculated for all equilibria as

$$\frac{Z_{t+i}}{M_{t+i}} = \frac{\frac{f+g-r}{f}(M_t - U)\left(\frac{1+g}{1+r}\right)^i + U}{(M_t - U)\left(\frac{1+g}{1+r}\right)^i + U}.$$

This number converges to one for all equilibria corresponding to $U > 0$. Hence, these equilibria exhibit a similar pattern in investment holdings as bubble equilibria. If $U = 0$, then the share held by speculators will be constant at $(f + g - r)/f$.

F. *Proof of Corollary 1*

From the proof of Proposition 5, we have

$$-\sum_{i=1}^{\infty} \frac{\mathbb{E}_0 \Delta Z_{t+i} S_{t+i}}{(1+r)^i} = \frac{f+g-r}{r-g} X_0^{\$}. \tag{13}$$

Moreover, from Proposition 6 and its proof, we have

$$\begin{aligned} -S_0 Z_0 &= -\left(\frac{f}{r-g}\frac{X_0^{\$}}{M_0 - U}\right)\left(\frac{f+g-r}{f}(M_0 - U) + U\right), \\ &= -\frac{f+g-r}{f} X_0^{\$} - U\left(\frac{f}{r-g}\frac{X_0^{\$}}{M_0 - U}\right). \end{aligned} \tag{14}$$

Summing (13) and (14) gives for the net present value

$$-S_0 Z_0 - \sum_{i=1}^{\infty} \frac{\mathbb{E}_0 \Delta Z_{t+i} S_{t+i}}{(1+r)^i} = -U \left(\frac{f}{r-g} \frac{X_0^{\$}}{M_0 - U} \right).$$

The only value of U such that $0 \leq U < M_0$ for which the net present value is non-negative is $U = 0$. This value of U corresponds to the baseline equilibrium.

References

S. Athey, I. Parashkevov, V. Sarukkai, and J. Xia. Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. *Working Paper*, 2016.

Y. Bakos and H. Hałaburda. The Role of Cryptographic Tokens and ICOs in Fostering Platform Adoption. *Information Systems Research*, 33(2):1368–1385, 2022.

B. Biais, C. Bisière, M. Bouvard, C. Casamatta, and A. Menkveld. Equilibrium Bitcoin Pricing. *Journal of Finance*, 78(2):967–1014, 2023.

O.J. Blanchard. Speculative Bubbles, Crashes and Rational Expectations. *Economics Letters*, 3(4):387–389, 1979.

O.J. Blanchard and M.W. Watson. Bubbles, Rational Expectations and Financial Markets. *NBER Working Paper*, 982, 1982.

W. Bolt and M.R.C. Van Oordt. On the Value of Virtual Currencies. *Journal of Money, Credit and Banking*, 52(2):835–862, 2020.

M.K. Brunnermeier and M. Oehmke. Bubbles, Financial Crises, and Systemic Risk. *Handbook of the Economics of Finance*, 2:1221–1288, 2013.

M.K. Brunnermeier, S. Merkel, and Y. Sannikov. The Fiscal Theory of the Price Level with a Bubble. *CEPR Discussion Paper*, 14680, 2020.

A. Canidio. Financial Bubbles in Infinitely Repeated Auctions with Tokens. *American Economic Review: Papers and Proceedings*, 113:263–267, 2023.

A. Carstens. Money in the Digital Age: What Role for Central Banks? *Guest Lecture at Goethe University (February, 6)*, 2018. URL https://www.bis.org/speeches/sp180206.htm.

P. Chaim and M.P. Laurini. Is Bitcoin a Bubble? *Physica A: Statistical Mechanics and its Applications*, 517:222–232, 2019.

E.-T. Cheah and J. Fry. Speculative Bubbles in Bitcoin Markets? An Empirical Investigation into the Fundamental Value of Bitcoin. *Economics Letters*, 130:32–36, 2015.

A. Cheung, E. Roca, and J.-J. Su. Crypto-currency Bubbles: An Application of the Phillips-Shi-Yu (2013) Methodology on Mt. Gox Bitcoin Prices. *Applied Economics*, 47(23):2348–2358, 2015.

J. Chiu and T.V. Koeppl. The Economics of Cryptocurrencies: Bitcoin and Beyond. *Canadian Journal of Economics*, 55(4):1762–1798, 2022.

L.W. Cong, Y. Li, and N. Wang. Tokenomics: Dynamic Adoption and Valuation. *Review of Financial Studies*, 34(3):1105–1155, 2021.

L.W. Cong, Y. Li, and N. Wang. Token-Based Platform Finance. *Journal of Financial Economics*, 144(3):972–991, 2022.

S. Corbet, B. Lucey, and L. Yarovaya. Datestamping the Bitcoin and Ethereum Bubbles. *Finance Research Letters*, 26:81–88, 2018.

A. Cretarola and G. Figà-Talamanca. Bubble Regime Identification in an Attention-Based Model for Bitcoin and Ethereum Price Dynamics. *Economics Letters*, 191:108,831, 2020.

B.T. Diba and H.I. Grossman. On the Inception of Rational Bubbles. *Quarterly Journal of Economics*, 102(3):697–700, 1987.

F.A. Enoksen, C.J. Landsnes, K. Lučivjanská, and P. Molnár. Understanding Risk of Bubbles in Cryptocurrencies. *Journal of Economic Behavior & Organization*, 176:129–144, 2020.

L. Fink. BlackRock CEO Larry Fink: I believe Bitcoin is a Legit Financial Instrument. *CNBC Interview (July, 15)*, 2024. URL https://www.youtube.com/watch?v=K4ciiDyUvUo&t=100s.

R.J. Garratt and M.R.C. Van Oordt. Entrepreneurial Incentives and the Role of Initial Coin Offerings. *Journal of Economic Dynamics and Control*, 142:104171, 2022.

R.J. Garratt and M.R.C. Van Oordt. The Crypto Multiplier. *Bank for International Settlements Working Paper*, 1104, 2023.

R.J. Garratt and M.R.C. Van Oordt. Crypto Exchange Tokens. *Bank for International Settlements Working Paper*, 1201, 2024.

J. Geuder, H. Kinateder, and N.F. Wagner. Cryptocurrencies as Financial Bubbles: The Case of Bitcoin. *Finance Research Letters*, 31:179–184, 2019.

S. Gryglewicz, S. Mayer, and E. Morellec. Optimal Financing with Tokens. *Journal of Financial Economics*, 142(3):1038–1067, 2021.

C.M. Hafner. Testing for Bubbles in Cryptocurrencies with Time-Varying Volatility. *Journal of Financial Econometrics*, 18(2):233–249, 2020.

C.R. Harvey, A. Ramachandran, and J. Santoro. *DeFi and the Future of Finance*. John Wiley & Sons, Inc, Hoboken, New Jersey, 2021.

S. Karau and E. Moench. Is It Really Mine? Mining Shocks and their Effects on Bitcoin Valuations. *Working Paper*, 2023.

M. Lambrecht, A. Sofianos, and Y. Xu. Does Mining Fuel Bubbles? An Experimental Study on Cryptocurrency Markets. *Management Science*, forthcoming.

J. Lee and C.A. Parlour. Consumers as Financiers: Consumer Surplus, Crowdfunding, and Initial Coin Offerings. *Review of Financial Studies*, 35(3):1105–1140, 2022.

Y. Li, W. Zhang, A. Urquhart, and P. Wang. The Role of Media Coverage in the Bubble Formation: Evidence from the Bitcoin Market. *Journal of International Financial Markets, Institutions and Money*, 80:101,629, 2022.

K. Malinova and A. Park. Tokenomics: When Tokens Beat Equity. *Management Science*, 69(11):6568–6583, 2023.

P.C.B. Phillips, S.-P. Shi, and J. Yu. Testing for Multiple Bubbles: Historical Episodes of Exuberance and Collapse in the S&P 500. *International Economic Review*, 56(4):1043–1078, 2015.

N. Popper. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*. HarperCollins, 2016.

J. Prat, V. Danos, and S. Marcassa. Fundamental Pricing of Utility Tokens. *Working Paper*, 2024.

N. Roubini. Crypto is the Mother of All Scams and (Now Busted) Bubbles. *Testimony for the Hearing of the US Senate Committee on Banking, Housing and Community Affairs On "Exploring the Cryptocurrency and Blockchain Ecosystem" (October)*, 2018.

M. Sockin and W. Xiong. Decentralization through Tokenization. *Journal of Finance*, 78 (1):247–299, 2023a.

M. Sockin and W. Xiong. A Model of Cryptocurrencies. *Management Science*, 69(11): 6684–6707, 2023b.

J. Tirole. On the Possibility of Speculation under Rational Expectations. *Econometrica*, 50 (5):1163–1181, 1982.

J. Tirole. Theories of Speculation. *MIT Department of Economics Working Paper*, 402, 1985.

Y. Wei and A. Dukes. Cryptocurrency Adoption with Speculative Price Bubbles. *Marketing Science*, 40(2):241–260, 2021.

I. Welch. Bitcoin Is an Energy-Wasting Ponzi Scheme. *Blog at Zócalo Public Square (October 20)*, 2017. URL https://tinyurl.com/4a4cyvv5.

D. Yermack. Is Bitcoin a Real Currency? An Economic Appraisal. In D.L.K. Chuen, editor, *Handbook of Digital Currency*, pages 31–43. Elsevier, 2015.