# Tokenomics: Dynamic Adoption and Valuation

Lin William Cong† Ye Li§ Neng Wang‡

*PRELIMINARY. COMMENTS WELCOME.*

First Draft: February 4, 2018
This Draft: March 25, 2018

**Abstract**

We provide a dynamic model of cryptocurrencies and tokens that serve as means of payment among (blockchain-based) platform users. Introducing tokens capitalizes future growth because the expected technological progress and popularity of the platform render tokens an attractive store of value, inducing further adoption. We derive the unique equilibrium in continuous-time formulation, and characterize, in addition to the contemporaneous complementarity of users' adoption decisions, an inter-temporal feedback from the interaction between user-base dynamics and token price. The token price depends on user base, platform productivity, agents' transaction needs, and their expectation of token appreciation. We also show that native tokens not only accelerate adoption but also moderate user-base fluctuation to enhance welfare. Our model sheds light on the broad issue of asset pricing with user-base externalities.

**JEL Classification: C73, F43, E42, L86**

**Keywords:** Blockchain, Cryptocurrency, Digital Currency, ICOs, FinTech, Network Effect, Platforms, Tokens.

†University of Chicago Booth School of Business. E-mail: will.cong@chicagobooth.edu
§Ohio State University. E-mail: li.8935@osu.edu
‡Columbia Business School and NBER. E-mail: neng.wang@columbia.edu

# 1 Introduction

Blockchain-based cryptocurrencies and tokens have taken the world by storm. According to CoinMarketCap.com, the entire cryptocurrency market capitalization has also grown from around US$20 billion to around US$600 billion over last year, with active trading and uses;[1] virtually unknown a year ago, ICOs are also now more celebrated and debated than the conventional IPOs, raising 3.5 billion in more than 200 ICOs in 2017 alone, according to CoinSchedule. However, it is far from clear if cryptocurrency would completely escape regulation or replace conventional money, especially given the large volatility involved. There lacks no critics of the development of cryptocurrency, at least Bitcoin, in both the industry and academia.[2]. ICOs are also facing quagmires regarding its legitimacy and distinction from security issuance.[3] In the recent hearing on Capital Markets, Securities, and Investment Wednesday, March 14, 2018, the regulators appear rather divided, if not outright "confused", on the future of cryptocurrencies, digital currencies, ICOs, and Blockchain development.

In order to draw a line between reckless speculation and financial innovation, and understand how cryptocurrency impact fiat money or whether tokens should be regulated like securities, it is important to first understand how cryptocurrency or tokens derive their value. What fundamentals drive their pricing and volatility? How do they interact with the endogenous user adoption and evolution of the blockchain ecosystem and virtual economy? What are the new economic insights about asset pricing we can glean from the development of cryptocurrency or tokens? From token pricing, what can we learn about platform or user-base valuation in general?

Motivated by these questions and the debates in both industry and academia, we develop the first dynamic model of virtual economy with endogenous user adoption dynamics and a native cryptocurrency/token (henceforth generically referred to as "coin") that facilitates transactions and business operations (e.g., smart contracting) on a blockchain. We anchor coin valuation on the fundamental progress of blockchain technology, and demonstrate how coins derive value both as a medium of exchange and as a store of value. Our model highlights that coins front-load user-base growth in the future: agents' expectation of technological progress and popularity of the blockchain system translates into expected coin price appreciation, which makes coins an attractive store of value and in turn induces more agents to buy coins and join the ecosystem.

[1]For example, many retailers in Japan already accept Bitcoins (e.g., Holden and Subrahmanyam (2017)).
[2]Rogoff (2017) and Shiller (2017) are notable representatives.
[3]See, for example, "Token Resistance," The Economist, November 11th, 2017.

Specifically, we consider a continuous-time economy with a unit mass of agents who differ in their needs to conduct transactions on the blockchain. We broadly interpret transaction as including not only typical money transfer (e.g., on the bitcoin blockchain) but also signing smart contracts (e.g., on the Ethereum blockchain). Accordingly, we model agents' gain from blockchain transaction as a flow utility that depends on agent-specific transaction needs, the current state of blockchain technology, and very importantly, the size of blockchain community. The larger the community is, the more surplus can be realized through trades among agents on the blockchain. In our models, agents make a two-step decision: (1) whether to incur a cost to meet potential trade counterparties; (2) how many coins to hold, which depends on both blockchain trade surplus and the expected future coin price. And, through the impact on community size, agents' decision exerts externalities on each other. An expectation of price appreciation leads to stronger demand for coins, and more agents joining the blockchain community.

The very requirement that agents must hold coins to conduct transactions is consistent with many existing applications. Coins are the required medium of exchange for transactions and business operations on blockchain platforms, either by protocol design or by the fact that they offer higher convenience yield relative to alternative currencies. In fact, contrary to the general perception, most "utility tokens" issued through ICOs are not "corporate coupons" that are used to redeem products or services from the issuing company, but instead are the required means of payment for products and services from other blockchain users.

Here we highlight that the benefits of using such coins increases in the size of blockchain user base. As a result, coin price reflects the future growth of the community, and becomes higher, if the expected user-base growth is stronger. Taking a step back, when the platform technology is forecast to improve, inducing more agents to join the community, the consequent expectation of coin price appreciation feeds into agents current decision to join the community and hold coins. Therefore, the existence of coins as a native currency not only serves for technological purposes as practitioners argue, but more importantly, advances the growth of user base through agents' expectation of future technological progress, larger user base, and higher coin price. The model equilibrium features an intertemporal complementarity of user base – expectation of more users in the future feeds into more users today. Nevertheless, we show there exists a unique non-degenerate Markov equilibrium under usual conditions of continuous-time formulation.

We compare blockchain ecosystems with and without coins, and show that those with coins see their user base grow faster when the underlying technology is expected to improve over time, resulting in a higher welfare. Akin to many equilibrium models that feature interaction between financial markets and the real economy, the financial side of our model is the endogenous price of coins, while the real side is the user base, which determines the benefits of individual agents who trade on the blockchain. Coin price affects user base through agents' expectation of the future, but at the same time, user base affects coin price through both a higher flow utility from trade surplus and through a stronger demand for coins when more people participate. We show that this feedback loop not only impacts the growth of user base and coin price, but also affects the volatility of both. Specifically, introducing native currency can lower user-base volatility.

Our model sheds light on the pricing of means of payment in peer-to-peer networks that are the defining features of many virtual economies. Many private digital currencies have been set up in association with platforms whether payment-focused or not: Linden dollar for the game Second Life, WoW Gold for the game World of Warcraft, Facebook Credits, Q-coins for Tencent QQ, Amazon coins, to name a few.[4] The Blockchain technology gives platforms unprecedented flexibility and commitment power in introducing native currencies and designing their attributes, yet we lack a valuation framework. Our model offers a pricing formula and reveals how introducing native currencies benefit users and accelerate their adoption. Our framework potentially applies to a wide range of applications, such as email protocols and online social network. More generally, our framework can be applied to asset pricing and macro models with network externality. When more agents invest in certain assets either now or in future, everyone benefits from the increase of investor base.

**Literature Review.** Our paper first contributes to the emerging literature on FinTech, especially on blockchains and distributed-ledger systems. Among studies on the application and economic impact of the technology, Harvey (2016) briefly surveys the mechanics and applications of crypto-finance, especially Bitcoin.[5] Yermack (2017) evaluates the potential impacts of the blockchain technology on corporate governance. Cong and He (2018) emphasize

[4]Even before the heated debate on cryptocurrencies, economists, and commentators were already raising questions such as "Could a gigantic nonsovereign like Facebook someday launch a real currency to compete with the dollar, euro, yen and the like?" (Yglesias (2012)). Gans and Halaburda (2015) provides an insightful introduction on how payment systems and platforms are related.

[5]For a brief introduction to blockchains and ICOs, see Nanda, White, and Tuzikov. (2017a,b). Other papers on more specialized applications include: Catalini and Gans (2016) point out the blockchain technology can reduce the cost of verification and the cost of networking. Malinova and Park (2016) study the design of the mapping between identifiers and end-investors and the degree of transparency of holdings in a blockchain-based marketplace. Khapko and Zoican (2017) argue that blockchain allows for flexible settlement of trades, and the optimal time-to-settle trades off search costs and counter-party risk, creating vertical differentiation.

information distribution in generating decentralized consensus, with implications on industrial organization. Several studies analyze crypto-currency mining games (e.g., Nakamoto (2008), Eyal and Sirer (2014), and Biais, Bisiere, Bouvard, and Casamatta (2017)) and miners' compensation and organization (e.g., Easley, O'Hara, and Basu (2017), Huberman, Leshno, and Moallemi (2017), and Cong, He, and Li (2018)).

Our paper takes the functionality of the technology as given and focuses on the valuation of cryptocurrencies and tokens and the user adoption dynamics. Closely related is Athey, Parashkevov, Sarukkai, and Xia (2016) which emphasizes agents' belief on binary technology quality, but does not model technology evolution and user-base externality. Gans and Halaburda (2015) is among the earliest studies on virtual currencies within a platform, while Ciaian, Rajcaniova, and Kancs (2016) discusses price formation for Bitcoins. Fernández-Villaverde and Sanches (2016) and Gandal and Halaburda (2014) examine the competition among privately issued money or cryptocurrency and efficiency.

Several contemporaneous studies analyze initial coin offerings (ICOs) and pricing of cryptocurrencies. Sockin and Xiong (2018) study cryptocurrency valuation and ICO in a two-period setting, where cryptocurrency is indivisible and serve as membership certificate that agents hold to be matched with trading counterparties. Li and Mann (2018) study staged coin offerings with coordination issues. Catalini and Gans (2018) study ICOs with tokens as coupons for redeeming products and services from the issuing company. Both Li and Mann (2018) and Catalini and Gans (2018) further argue that ICOs help aggregate dispersed private information.

Instead of focusing on information aggregation or financing through coin offerings, we emphasize the role of cryptocurrencies and crypto-tokens as means of payment in decentralized virtual economy, which fits most token white papers observe in practice.[6] We differ also in allowing endogenous and divisible holdings of coins, and considering both the static and dynamic complementarity among users. While other studies typically focus on equilibrium multiplicity, we are the first to pin down the value of tokens and dynamic user adoption because diminishing returns to user-base complementarity combined with continuous sample path of token price yields a unique equilibrium.

Also related are discussions on the design of cryptocurrencies/tokens and platforms. Gans and Halaburda (2015) highlight the link between research on platforms and payments systems

[6] In a companion paper, Cong, Li, and Wang (2018), we embed our pricing framework into a study of ICOs as a financing innovation, emphasizing tokens' role as means of payments (as opposed to membership certificate or product/service coupons) among users and accelerator of technology/platform development when held by dispersed contributors.

literature, and discuss platform-currency design. Chiu and Wong (2015) take a mechanism design approach to discuss how e-money such as bitcoin and PayPal help implement constrained efficient allocations. Chiu and Koeppl (2017) find that cryptocurrency systems such as Bitcoin can improve efficiency by relying more on money growth than transaction fees, or by adopting alternative consensus protocols such as the proof-of-stake. Balvers and McDonald (2017) discuss a blockchain-based global currency that can be used to achieve an ideal currency stable in terms of purchasing power. By providing a dynamic pricing framework, we directly tie the protocol-based design on coin supplies to coin valuation and user adoption. The framework can therefore be used to evaluate various design objectives.

We organize the remainder of the article as follows. Section 2 provides the institutional background on crypto-currency and crypto-tokens. Section 3 sets up the model, characterizes the dynamic equilibrium, and discusses model implications. Section 4 concludes.

# 2 Institutional Background

In this section, we briefly introduce the development of the blockchain technology, and then clarify various concepts associated with cryptocurrency , which are not mutually exclusive and constantly evolving. Importantly, we highlight two salient features shared among the majority of cryptocurrencies, tokens, and platform currencies: first, they are used as means of payment by design ("monetary embedding"); second, their typical application scenarios exhibit some forms of network effect ("user-base externality"). Our model in Section 3 aims to capture these defining features of a large class of cryptocurrencies and tokens to price them and characterize their interactions with user adoption.

**Blockchain, Cryptocurrency, and Token**. The advent in FinTech and sharing economy is largely driven by the increasing preference for forming peer-to-peer connections that are instantaneous and open, which is transforming how people interact, work together, consume and produce. Yet financial systems are rather centralized, arranged around a set of key players such as asset managers, banks, and payment and settlement institutions. Blockchain-based applications are part of an attempt to create a peer-to-peer financial architecture, reorganizing the society into a set of decentralized networks of human interactions. By providing decentralized consensus, blockchains allow peers unknown to and distant from one another to interact, transact, and contract without relying a centralized trusted third party. The technology can potentially better prevents single point of failure, and even reduce concentration of market power, but still face many challenging issues.[7] In this paper, we emphasize the economics, rather than technical aspects, of the blockchain technology and its functionalities.

Even though not always necessarily required, a majority of blockchain applications entail the use of cryptocurrencies and tokens. There is a lack of clarity, if not general confusion, on the myriad of terms and references such as cryptocurrencies, altcoins, appcoins, tokens, e.t.c.. A lot of these concepts are not mutually exclusive and are starting to be used interchangeably.

Cryptocurrencies are cryptography-secured digital or virtual currencies. Bitcoin represents the first widely-adopted decentralized cryptocurrency, and popularized the concept. Besides Bitcoin, over 1000 different "altcoins" (stand for for alternative cryptocurrency coins, alternative to Bitcoin) have been introduced over the past few years and many central banks are actively exploring the area for retail and payment systems.[8] Many altcoins such as Litecoin and Dogecoin are variants (forks) from Bitcoin, with mofidications to the original open-sourced protocol to enable new features. Others such as Ethereum and Ripple created their own Blockchain and protocol to support the native currency. Cryptocurrencies are typically regarded as payment-focused and primarily associated with their own independent blockchain. In these payment and settlement applications as exemplified by Bitcoin and Ripple, cryptocurrencies obviously act as means of payment on their respective blockchain platforms.

Meanwhile, Blockchain-based crypto-tokens have also gained popularity. In what is known as Initial Coin Offerings (ICO), entrepreneurs sell "tokens" or "AppCoins" to dispersed investors around the globe.[9] Tokens are representations of claims on issuers' cashflow,

[7]Although Bank of England governor Mark Carney dismissed Bitcoin as an alternative curency, he recognized that the blockchain technology benefits data management by improving resilience by "eliminating central points of failure" and enhancing transparency and auditability while expanding what he called the use of "straight-through processes" including with smart contracts. In particular, "Crypto-assets help point the way to the future of money". See, e.g., beat.10ztalk.com. For various applications of the technology, we refer the readers to Harvey (2016) and Yermack (2017), and for smart contracting, Cong and He (2018).

[8]For example, People's Bank of China aims to develop a digital currency system; Bank of Canada and Singapore Monetary Authority use blockchain for interbank payment systems; Deutsche Bundesbank works on prototype of blockchain-based settlement systems for financial assets; in a controversial move, the government of Venezuela became the first federal government to issue digital currency and announced on Feb 20, 2018 the presale of its "petro" cryptocurrency — an oil-backed token as a form of legal tender that can be used to pay taxes, fees and other public needs.

[9]While the first ICO in 2013 raised a meager $ 500k and sporadic activities over the next two years. 2016 saw 46 ICOs raising about $ 100m and according to CoinSchedule, in 2017 there were 235 Initial Coin Offerings. The year-end totals came in over $3 billion raised in ICO. In August, 2017, OmiseGO (OMG) and

rights to redeem issuers' products and services, or medium of exchange among blockchain users. They usually operate on top of an existing blockchain infrastructure to facilitates the creation of decentralized applications.[10] Some tokens derive their value from the company's future cashflow, and thus, serve a function similar to securities (thus termed "security tokens"). They are well-understood and are not our focus. The vast majority of ICOs that launched in 2016 and 2017 were "utility tokens", which include many of the highest-profile projects: Filecoin, Golem, 0x, Civic, Raiden, Basic Attention Token (BAT), and more.

Many media reporters, practitioners, regulators, and even academics often analogize utility tokens to "corporate coupons", which allow consumers to redeem products or services from the service provider. While some tokens are indeed corporate coupons, it is thus far neglected that the majority of them are not.[11] As we illustrate using some of the aforementioned tokens shortly, utility tokens are often the required means of payment to pay peer users for certain products or services, or represent certain opportunities to provide blockchain services for profit as in the case of "stake tokens". Precisely here lies the key innovation of the blockchain technology: allowing peer-to-peer interactions in decentralized networks, as opposed to designing and auctioning coupons issued by centralized product/service providers – an old phenomenon economists understand relatively well (e.g., pay-in-kind crowdfunding).

In this paper, we focus on the common features shared by cryptocurrencies and utility tokens that serve essentially the role of means of payment among blockchain users. We thus use "tokens", "cryptocurrencies", e.t.c., interchangeably and often collectively refer to them as "coins". Next, we highlight these unique features of the blockchain technology that render the economics of coins introduction and valuation quite distinct from what we already know in the literature of monetary economics and asset pricing.

**Monetary Embedding.** Many blockchain-based decentralized networks introduce native currencies that agents need to hold for transactions – a phenomenon we call "monetary embedding". In the following, we elaborate on the rationales behind such phenomenon and relate them to the issue of money velocity, setting the stage for our formal analysis in Section 3.

---

Qtum passed a US$1 billion market cap today, according to coinmarketcap.com, to become the first ERC20 tokens built on the Ethereum network and sold via an ICO to reach the unicorn status.

[10]By "on top of" a blockchain, we mean that one can use smart contract templates, for example on the Ethereum or Waves platform, to create tokens for particular applications, without having to create or modify codes from other blockchain protocols.

[11]We should be very clear about this distinction because not only the valuation framework differs, but legal and regulatory implications differ as well.

First, in the virtual economy, potential users are likely from around the globe, using fiat money issued by and subject to specific countries' legal and economic influences. Transacting in a uniform currency is simply more convenient, free from the transaction costs of currency exchange. For example, it is cheaper to make international payments and settlements using Ripples (XRP) on the Ripple network. Even though Ethereum platform allows other App-Coins and cryptocurrencies (provided that they are ERC-20 compatible), many transactions and fundraising activities are still carried out using Ethers (ETH) because of its convenience and popularity (i.e., widely accepted by Ethereum users).

Second, from a theoretical perspective, it is advantageous to adopt a standard unit of account in the ecosystem because it mitigates the risks of asset-liability mismatches when they are denominated in different units of account (Doepke and Schneider (2017)). This is particularly relevant on a blockchain platform designed for smart contracting. Some argue that the lack of trust in an online space, very much due to the anonymity of participants, implies that trade has to be quid pro quo, so a means of payment is required (Kiyotaki and Wright (1989)).

Then why not just use US dollars or other existing currencies as settlement media? This leads to the third rationale: native currency helps to incentivize miners, validators, and users to contribute to the stability, functionality (provision of decentralized consensus), and prosperity of the ecosystem. For example, for blockchain applications where decentralized consensus is achieved through the mechanism of "proof-of-stake", the ownership of native currency entitles platform users to generate decentralized consensus; to profit from providing validation services, OmiseGo tokens (OMG) are required as proof of stakes on the OmiseGo blockchain; similarly, Bitcoins and Filecoins are used to reward miners for block creations in the consensus processes. If a blockchain application is developed without native currency but is based upon other cryptocurrencies, then the incentive of users is no longer directly linked to the blockchain in question and varies with the price of these other cryptocurrencies. Practitioners are very well aware of this issue, as Strategic Coin explains in its BAT token launch research report.[12]

Fourth, introducing native currency allows the issuer to collect seigniorage, especially through initial offer coin offering (ICO). In contrast to sovereigns who cannot easily commit to a money supply rule, blockchain developers can commit to an algorithmic rule of coin

[12]BAT serves as a medium exchange between users, advertisers, and publishers who participate in the Brave browser ecosystem. Advertisers purchase ads using BAT tokens, which are then distributed among both publishers and browser users as compensation for hosting the ads and viewing them, respectively.

supply, and therefore, create certain degree of scarcity. Provided that users need to hold coins to transact on the platform, a positive coin price can arise in an equilibrium, and such value is collected by the developers at ICO, reflecting a form of monopoly rent – the fact that users can only conduct some activities on a particular blockchain platform translates into a high price of its native currency, and more ICO revenues to the developer.

These rationales motivate us to focus on platforms with native coins. But let us take a step back and ask why cryptocurrency may have a determinant value in the first place. In principle, if one wants to transact on a blockchain platform, one can exchange dollars for its native currency, and make a transfer on the blockchain, and then immediately, the payee may exchange the native currency back into dollars. If the whole process happens instantaneously, i.e., the velocity of native currency is infinity, then there does not exist a net demand for native currency, so there exists an equilibrium of zero dollar price and equilibria with any positive level of price of native currency. Therefore, we need to pin down a positive demand, so together with a algorithmically controlled supply, coin price can be determined. This brings us to the second aspect of monetary embedding: agents actually need to hold the coins to profit from on-chain activities. This is indeed the case in practice for at least three reasons.

First, a demand may arise because decentralized miners or service providers ("keepers") may have to hold the native currencies to earn the right to serve the system. Proof-of-Stake protocols typically fall in this category. These tokens are sometimes referred to as work tokens or staking tokens, and notable implementations include Keep (off-chain private computation), Filecoin (distributed file storage), Truebit (off-chain computation), Livepeer (distributed video encoding), and Gems (decentralized mechanical Turk). To enforce some sort of mechanism to penalize workers who fail to perform their job to some pre-specified standard, work tokens have to be held. For example, in Filecoin, service providers contractually commit to storing some data with 24/7 access and some minimum bandwidth guarantee for a specified period of time. During the contract term, service providers must "escrow" some number of Filecoin, which can be automatically slashed (taken away) should they fail to perform the service.

Second, blockchains enable the use of smart contracts—digital contracts allowing terms contingent on decentralized consensus that are typically self-enforcing and tamper-proof through automated execution. Smart contracts typically automate transfer of tokens once certain contingencies are triggered (e.g., default), which in turn requires that the corresponding amount of cryptocurrencies must be "escrowed" during the episode that the contingencies can be triggered.[13] In other words, agents hold cryptocurrency as collateral.[14]

Third, because the generation of decentralized consensus takes time, there is a technical limit on how quickly transactions can be validated and recorded. While many protocols such as the Lightening Network and Ethereum process transactions significantly faster than Bitcoin (seconds versus 10-11 minutes), the decentralized nature of the validation means it always takes some amount of time to ensure robustness and synchronization of the consensus. During such confirmation time, cryptocurrency cannot be liquidated by either party of the transfer.

In line with these considerations, our model assumes that agents, who want to enjoy a trade surplus on the blockchain, hold its cryptocurrency for at least an instant. This holding period is important. No matter how short it is, it exposes the owner of cryptocurrency to the fluctuation of its price, so that users of the platform care not only the surplus from conducting trade with peer users but also the future coin price, which in turn depends on further user base. Next, we discuss user-base externality, another key feature of decentralized network that our model captures.

**User-Base Externality** One of the key aspects of platform economics is user-base externality – when more people join the platform, individuals enjoy more surplus through interacting with other users because it is easier to find a trade partner. "Trade" here can be very general, encompassing selling products and services and signing a long-term financing contracts. According to CoinSchedule, 34.5% of the ICO-financed projects over the past two years focus on infrastructure. While the other top categories included trading and investing at 13.7%, finance at 10.2%, payments at 7.8%, data storage also at 7.8%, and drugs and healthcare at 5.5%, amongst dozens of other industry categories. Regardless the ICO category, these projects share user-base externality as a common attribute, and in terms of user adoption, exhibit a S-shaped development curve – the growth of user base feeds on itself. User-base externality has been well recognized as one of the defining features of P2P platforms, sharing economy, and various decentralized systems.

In the area of blockchain applications, the utility of using cryptocurrencies (in fact, any

[13] Balvers and McDonald (2017) also argues that automated collateral in terms of tokens can help stabilize the purchasing power of cryptocurrency, a point very related to our emphasize on a positive crytocurrency demand.

[14] While this is similar to the traditional third-party escrow accounts, what it implies is that the coins are locked up with at least one contracting party. Arguably, blockchains and smart contracting also help solve issues related to non-exclusive contracts, through the use of native tokens to fully keep track of the collateral and escrow.

currency) goes up when more people use them. In other areas, examples also include social networks and payment networks such as Facebook, Twitter, WeChat, PayPal, and OmiseGO. User-base externality is particularly important in the early stage of adoption. Evans and Schmalensee (2010) show that achieving a critical mass is crucial in platform business. For example, Unikrn with UnikoinGold is the decentralized token for betting on e-sports and gambling, and Augur, a decentralized prediction market, both required a critical user base to take off.

That said, such models with user-base externality is often static, yet inter-temporal user-base externality is prevalent and can be even more important. The fact that a larger user base today helps improve the technology tomorrow, and a larger anticipated user base tomorrow encourages greater investments today are examples of how user-base externality can play an inter-temporal role. Filecoin the data storage network, Dfinity the decentralized cloud service, marketplace such as overstock (and its ICO), and infrastructure projects such as Ethereum and LITEX all exhibit user-base externality in both contemporaneous and inter-temporal fashions, as our model highlight.

Our model in the next Section incorporates monetary embedding and user-base externality, both of which are defining characteristics of blockchain-based decentralized applications. The insights gleaned can potentially inform us what is likely to happen for other sharing economy applications such as UBER and AirBnB to introduce native currencies. In fact, consistent with our model, when Tencent QQ introduced Q-coin, a case to which our model is applicable, many users and merchants quickly started accepting them even outside the QQ platform (mapped to increase in system trade surplus in our model), tremendously accelerating adoption and coin valuation.[15]

# 3 The Model

## 3.1 Model setup

**Preferences and off-blockchain environment.** Consider a continuous-time economy with a unit mass of risk-neutral agents. There are generic goods that serve as numeraire ("dollar"), and a storage technology that delivers a return of $r$ per unit of time, which

[15] Annual trading volume reached billions of RMB in late 2000s and the government has to intervene. See articles *China bars use of virtual money for trading in real goods* and *QQ: China's New Coin of the Realm?* (WSJ).

represents off-blockchain investment opportunities. We allow agents to borrow off-blockchain to obtain leverage for investments in cryptocurrency or crypto-tokens (generically referred to as "coin"), in which case the off-blockchain investment is negative and agents pay interest rate $r$. The assumption of risk neutrality reflects the current status of cryptocurrency as a relatively small asset class whose fluctuation is largely orthogonal to the aggregate economy and financial markets. We may interpret the model as specified under the risk-neutral measure.

A representative agent $i$ maximizes the following expected utility function under rational expectation:

$$\mathbb{E}\left[\int_{t=0}^{\infty} e^{-rt} dc_{i,t}\right],$$

where $c_{i,t}$ is agent $i$'s *cumulative* consumption up to $t$.

**Blockchain activities.** The blockchain has a productivity $A_t$ that follows an exogenous, autonomous diffusion process

$$dA_t = A_t \mu_t^A dt + A_t \sigma_t^A dZ_t,$$

where the Brownian shock, $dZ_t$, is the only source of aggregate uncertainty in this model. $A_t$ could be breakthroughs in cryptography and distributed-ledger technology, it could also be driven by regulatory changes or major systemic shifts in agents' preferences.[16]

A representative agent $i$ chooses the units of coins carried forward, denoted by $k_{i,t}$, taking as given the current market price of coin, $P_t$. We conjecture that the equilibrium dynamics of $P_t$ follows a diffusion process,

$$dP_t = P_t \mu_t^P dt + P_t \sigma_t^P dZ_t, \tag{1}$$

which agents take as given under rational expectation. Later, once we clear the coin market, we confirm this equilibrium conjecture. Throughout this paper, we use capital letters for aggregate and price variables that individuals take as given, and lower-case letters for individual variables.

By holding $k_{i,t}$ units of coin, agent $i$ obtains a flow of goods, which we interpret as certain types of *trade surplus* that can only be achieved on the blockchain by transacting in

[16] In 2017 and 2018, China and Korea have introduced various measures to ban/restrict cryptocurrency trading and ICOs, which are widely considered as a negative shock to the usage of cryptocurrencies that triggered widespread price declines.

its native tokens or cryptocurrencies, i.e., coins. Specifically, let $y_{i,t}$ denote the cumulative trade surplus at time $t$, so the trade surplus over the next instant $dt$ is

$$dy_{i,t} = (P_t k_{i,t})^{1-\beta} \left(N_t A_t e^{u_{i,t}}\right)^{\beta} dt, \tag{2}$$

which contains the common productivity $A_t$ and an idiosyncratic productivity $u_{i,t}$.

This flow can be thought of as a convenience yield in the case of transaction cryptocurrency (e.g., Bitcoin) or production flow from entrepreneurial projects in case of smart-contracting cryptocurrency (e.g., Ether). For a more concrete interpretation, consider a merchant who sells products on the blockchain, accepting cryptocurrency or coins as means of payment. A defining feature of blockchain technology is that the transfer of coins is confirmed by decentralized consensus. Decentralized consensus is crucial to prevent double-spending problem, that is a coin being paid to multiple parties simultaneously. To reach centralized consensus takes time. For example, it takes approximately one hour on the Bitcoin blockchain.[17] Therefore, our blockchain merchant effectively holds coins paid by customers during the confirmation period, and is exposed to the risk of coin price fluctuation. When the trade is confirmed, the merchant may exchange coins for dollars or continue to hold coins as a store of value.

For an example of smart contracting, consider an entrepreneur who signs a smart contract with investors and accepts cryptocurrency as means of payment. The transfer of coins from investors to the entrepreneur takes time because a decentralized consensus has to be reached. By the time this transfer is confirmed, an entrepreneur may use coins to purchase goods and services needed for her project or exchange coins for dollars and invest dollars into the project. During the confirmation period, an entrepreneurs is exposed to the risk of coin price fluctuation.

In both examples, the party who accepts cryptocurrency as means of payment enjoys a trade surplus (sales profit and project NPV) but bears the risk of coin price change. Therefore, a crypto payee becomes effectively a holder of coins for at least the confirmation period, which in our continuous-time setting lasts for $dt$.

Noticeably, trade surplus depends on $N_t$, the total number (measure) of agents that decide to join the blockchain network (i.e., $k_{i,t} > 0$, to hold some coins). This term captures a form strategic complementarity or network externality, capturing the ease to find trading

[17] An implicit rule in the Bitcoin community is that a transfer of Bitcoin is confirmed when six blocks are added to the chain after the trade. Every block takes approximately ten minutes to be added (or "mined").

or contracting counterparties in a large community of blockchain users.

We assume that to join the blockchain community and obtain this trade surplus, an agent has to incur a cost equal to $\chi dt$. This cost can be of the cognitive nature. For example, during a period of heightened media attention, it is easier to gather information about potential usages of the blockchain system and what needs to be prepared for a transaction on the blockchain. It can also represent efforts in trading on the blockchain, or writing small contracts, or simply carrying out entrepreneurial activities on-chain. Importantly, agents can easily abstain from participating in the ecosystem any time and save the cost. This feature reflects the reality that in a decentralized blockchain-based system, switching between on-chain and off-chain is rather frictionless. When $\mu_t^A > 0$, i.e., the blockchain productivity grows over time, overwhelming the participation cost $\chi$, and everyone joins the community. We are interested in the initial adoption dynamics and its interaction with coin price.

Let $w_{i,t}$ denote a representative agent $i$'s wealth at time $t$, which has the following law of motion

$$\begin{aligned} dw_{i,t} &= -dc_{i,t} + (w_{i,t} - P_t k_{i,t})\, r dt + \underbrace{(P_t k_{i,t})^{1-\beta} \left(N_t A_t e^{u_{i,t}}\right)^{\beta} dt}_{\text{blockchain trade surplus}} \\ &\quad + \underbrace{(P_t k_{i,t}) \left[\mu_t^P dt + \sigma_t^P dZ_t\right]}_{\text{capital gain of coin holdings}} - \underbrace{\mathbb{I}_{\{k_{i,t}>0\}} \chi dt}_{\text{participation cost}} . \end{aligned}$$

Agents with low $u_{i,t}$ may not find it profitable to join the blockchain community at time $t$ under this participation cost. The heterogeneity in $u_{i,t}$ makes the determination of community size non-trivial. Without such heterogeneity in the cross section, $N_t$ is either equal to zero (no one joins the community). To solve the equilibrium $N_t$, we need to track the whole distribution of $u_{i,t}$. For simplicity, we assume that $u_{i,t}$ follows the Ornstein-Uhlenbeck process

$$du_{i,t} = -\mu^U u_{i,t} dt + \sigma^U dZ_{i,t}^U,$$

where $Z_{i,t}^U$ is an idiosyncratic, standard Brownian motion. The parameters $\phi$ and $\sigma$ are common among agents. And we set the initial cross-section distribution of $u_{i,0}$ equal to the stationary solution of the corresponding Fokker–Planck equation, i.e., with the following probability density

$$g(u) = \sqrt{\frac{\theta}{\pi}} e^{-\theta u^2} \text{ (where } \theta = \mu^U / \left(\sigma^U\right)^2 \text{)},$$

so that the cross-section distribution of $u_{i,t}$ does not vary over time. The stationary distribution has mean equal to zero and standard deviation equal to $1/\sqrt{2\theta}$. or one (all agents join the community).

The interpretation of $u_{i,t}$ depends on the interpretation of blockchain trade surplus. For example, if we have in mind a payment blockchain such as Bitcoin, a high value of $u_{i,t}$ reflects agent $i$'s urge to conduct a transaction using native coins, which can be a legal transfer of money across country borders or for the purchase of illegal products or services; if the trade surplus arises from smart contracting for business operations that are only possible on the blockchain, $u_{i,t}$ reflects the standard productivity of entrepreneurial project; if the trade surplus derives from decentralized data storage or computation (Filecoin or Dfinity), $u_{i,t}$ reflects the secure and fast accessibility of data and computation power for specific tasks.

## 3.2 Dynamic Equilibrium

**Optimal coin holdings.** We focus on Markov equilibria and first study agents' decision to hold coins. A representative agent $i$ has three state variables, $w_{i,t}$, $u_{i,t}$, and $A_t$. Under risk-neutrality, we conjecture the value function takes the following form:

$$v_{i,t} = w_{i,t} + F\left(u_{i,t}, A_t\right). \tag{3}$$

As will be shown later, $F\left(u_{i,t}, A_t\right)$ is the present value of blockchain trade surplus. Under this value-function conjecture, we can write the HJB equation of agent $i$ as follows.

$$\begin{aligned} r v_{i,t} dt \quad = \quad & w_{i,t} r dt + \max_{k_{i,t}} \left\{ \left(P_t k_{i,t}\right)^{1-\beta} \left(N_t A_t e^{u_{i,t}}\right)^{\beta} dt - \chi dt + \right. \\ & \left. \left(P_t k_{i,t}\right) \mu_t^P dt - P_t k_{i,t} r dt \right\} \mathbb{I}_{\{k_{i,t}>0\}} + \\ & \frac{\partial F\left(u_{i,t}, A_t\right)}{\partial u_{i,t}} \left(-\mu^U u_{i,t}\right) dt + \frac{\partial F\left(u_{i,t}, A_t\right)}{\partial A_t} \mu_t^A A_t dt + \\ & \frac{1}{2} \frac{\partial^2 F\left(u_{i,t}, A_t\right)}{\partial u_{i,t}^2} \left(\sigma^U\right)^2 dt + \frac{1}{2} \frac{\partial F\left(u_{i,t}, A_t\right)}{\partial A_t} \left(\sigma_t^A\right)^2 A_t^2 dt + \frac{\partial F\left(u_{i,t}, A_t\right)}{\partial u_{i,t} \partial A_t} \sigma^U \sigma_t^A A_t dt. \end{aligned}$$

Note that since the marginal value of wealth is equal to one, consumption drops off from the HJB equation – consuming one unit of goods adds one unit of flow utility but also decreases the value function by one through the reduction in wealth. We will confirm this conjecture of value function after we characterize more features of the Markov equilibrium.

The first-order condition is that if $k_{i,t} > 0$,

$$(1-\beta)\, P_t^{1-\beta} \left( \frac{N_t A_t e^{u_{i,t}}}{k_{i,t}} \right)^{\beta} + P_t \mu_t^P = P_t r.$$

Rearranging the equation, we have the following proposition

**Proposition 1.** *Given the common and individual blockchain productivities, i.e., $A_t$ and $u_{i,t}$ respectively, an agent's optimal holdings of coins is given by*

$$k_{i,t} = \frac{N_t A_t e^{u_{i,t}}}{P_t} \left( \frac{1-\beta}{r-\mu_t^P} \right)^{\frac{1}{\beta}}. \tag{4}$$

*It has the following properties. (1) $k_{i,t}$ increases and is proportional to $N_t$. (2) $k_{i,t}$ decreases in the current coin price $P_t$. (3) $k_{i,t}$ increases in $A_t$ and $u_{i,t}$. (4) $k_{i,t}$ increases in the expected coin price appreciation, $\mu_t^P$.*

Agents hold more coin when the common productivity or their agent-specific productivity is high, and also when the community is larger because it is easier to conduct trades in the ecosystem. Equation (4) also reflects the investment motive to hold coins, that is $k_{i,t}$ increases in the expected coin price appreciation, $\mu_t^P$.

**Community size.** The maximized flow surplus from accessing the blockchain community can be solved under the optimal coin holdings:

$$max_{k_{i,t}} \left\{ (P_t k_{i,t})^{1-\beta} (N_t A_t e^{u_{i,t}})^{\beta} dt - \chi dt + (P_t k_{i,t})\, \mu_t^P dt - P_t k_{i,t} r dt \right\} \mathbb{I}_{\{k_{i,t}>0\}} \tag{5}$$

$$= \left\{ N_t A_t e^{u_{i,t}} \beta \left( \frac{1-\beta}{r-\mu_t^P} \right)^{\frac{1-\beta}{\beta}} - \chi \right\} \mathbb{I}_{\{k_{i,t}>0\}}$$

Apparently, if

$$N_t A_t e^{u_{i,t}} \beta \left( \frac{1-\beta}{r-\mu_t^P} \right)^{\frac{1-\beta}{\beta}} < \chi, \tag{6}$$

agent $i$ chooses not to join the blockchain community and does not hold any coins, i.e., $k_{i,t}$. Rearranging the equation, we can solve $\underline{u}_t$, the lower bound of $u_{i,t}$ such that agents with idiosyncratic productivity lower than $\underline{u}_t$ choose not to join the community.

**Proposition 2.** *At time $t$, agents with $u_{i,t} \geq \underline{u}_t$ join the blockchain community, while those* *with $u_{i,t} < \underline{u}_t$ choose not to, where $\underline{u}_t$ is given by*

$$\underline{u}_t = \underline{u}\left(N_t; A_t, \mu_t^P\right) = -\ln\left(N_t\right) + \ln\left(\frac{\chi}{A_t\beta}\right) - \left(\frac{1-\beta}{\beta}\right)\ln\left(\frac{1-\beta}{r-\mu_t^P}\right), \tag{7}$$

*which increases in the community size $N_t$. Let $G(\cdot)$ denote the cumulative probability function of stationary cross-section distribution of $u_{i,t}$. The community size is*

$$N_t = 1 - G\left(\underline{u}_t\right). \tag{8}$$

We note that $N_t = 0$ is always an equilibrium if $\mu_t^P \leq r$. In such a case, blockchain trade surplus is zero. Also, $P_t = 0$ (and $N_t = 0$) is an equilibrium, because the dollar value of a coin transfer is zero, so no trade can be done on the blockchain. We do not consider such degenerate equilibrium, and focus on the case where $N_t > 0$ and $P_t > 0$. Later on, we will show that in the space of $\mathbb{C}^1$, we have a unique Markov equilibrium.

In Proposition 2, $N_t$ increases in $\mu_t^P$. This is the key economic mechanism we emphasize in this paper: the expected coin appreciation reflects future $A_t$ growth, through which coins advances the benefits from the future growth in $A_t$, and thereby, increases the current value $N_t$. This is the direct effect of capitalizing on future growth.

There also exists an indirect effect that reflects a form of intertemporal complementarity in $N_t$. As $A_t$ grows, $N_t$ grows accordingly because more agents find it profitable to join the ecosystem by paying the cost $\chi$. A higher future value of $N_t$ leads to a higher future price of coin, which is a typical cash flow effect since $N_t$ directly enters into the flow surplus of agents' coin holdings. A higher future coin price feeds back into a higher value of $N_t$ right now through the expected price appreciation $\mu_t^P$.

Given the current common productivity $A_t$ and agents' expected price appreciation $\mu_t^P$, there may be multiple values of $N_t$ that satisfy Equations (7) and (8). To address the issue of multiplicity, consider the properties of a *response* function $R\left(n; A_t, \mu_t^P\right)$ that maps a hypothetical value of $N_t$, say $n$, to the measure of agents who choose to join the community after knowing $N_t$:

$$R\left(n; A_t, \mu_t^P\right) = 1 - G\left(\underline{u}\left(n; A_t, \mu_t^P\right)\right), \tag{9}$$

The equilibrium $N_t$ is the interaction between the $45^o$ line and the response curve as shown in the left panel of Figure 1. Note that given $A_t$ and $\mu_t^P$, $\underline{u}\left(n; A_t, \mu_t^P\right)$ approaches infinity, and

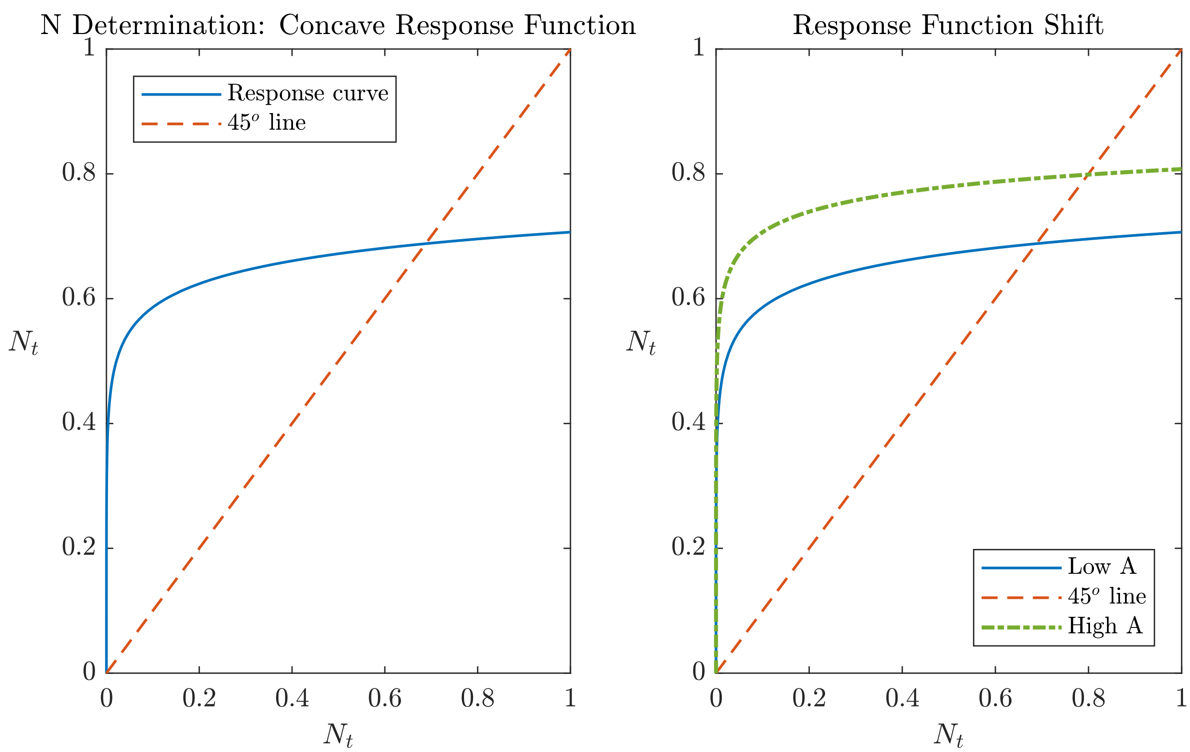


Figure 1: The Determination of Community Size.

$R\left(n; A_t, \mu_t^P\right)$ approaches zero, as $n$ approaches zero. Therefore, the response curve originates from zero. We have a unique equilibrium of positive $N_t$ if and only if the response curve crosses the $45^o$ line once in the range of $(0, 1]$, which is proved in the appendix. Figure 1 illustrates the equilibrium determination given $A_t$ and $\mu_t^P$, which we take as a snapshot of the dynamic equilibrium with time-varying productivity and expectation of price change.

**Proposition 3.** *Given $A_t$ and $\mu_t^P$, $N_t$ in Proposition 2 is unique because the response function only crosses the $45^o$ once.*

As we show later, continuous-time price path can pin down a unique evolution of price (also seen in Glasserman and Nouri (2016)). Combining diminishing returns to contemporaneous user-base externality with continuous-time formulation thus allows us arrive at a unique non-degenerate equilibrium. Note that zero price and adoption always constitute an equilibrium.

**Coin pricing formula.** We consider a fixed supply of coins, $\overline{M}$.[18] The market clearing

[18]This is consistent with many ICOs that fix the supply of tokens. Because resources for business operations on-chain are all discussed in real terms, we can simply normalize $\overline{M}$ to 1 due to money neutrality.

condition is

$$\overline{M} = \int_{u_{i,t} \geq \underline{u}_t} k_{i,t} di,$$

Substituting the optimal coin holdings of individual agents, we have the following proposition for coin pricing.

**Proposition 4.** *The coin market clear condition offers a coin price formula:*

$$P_t = \left(\frac{A_t}{\overline{M}}\right) \underbrace{N_t}_{user\ base} \left(\frac{1-\beta}{r - \underbrace{\mu_t^P}_{price\ appreciation}}\right)^{\frac{1}{\beta}} \underbrace{\left(\int_{\underline{u}_t}^{\infty} e^u \sqrt{\frac{\theta}{\pi}} e^{-\theta u^2} du\right)}_{average\ participant\ productivity}, \tag{10}$$

The coin pricing formula has the following properties. First, it increases in $N_t$, the size of blockchain user base – the larger the ecosystem is, the high trade surplus individual participants can realize by holding coins. From an asset pricing perspective, our model is the first to provide a theoretical foundation for the valuation-to-user base ratio that is commonly used in the technology industry, especially for firms whose customer base feed on network effects. Rearranging the equation, we can solve the coin price-to-user base ratio

$$\frac{P_t}{N_t} = \left(\frac{A_t}{\overline{M}}\right) \left(\frac{1-\beta}{r - \underbrace{\mu_t^P}_{price\ appreciation}}\right)^{\frac{1}{\beta}} \underbrace{\left(\int_{\underline{u}_t}^{\infty} e^u \sqrt{\frac{\theta}{\pi}} e^{-\theta u^2} du\right)}_{average\ participant\ productivity},$$

which increases in the blockchain productivity, expected price appreciation, and the average agent-specific productivity of participants, while decreases in the supply of coins, $\overline{M}$. Note that, as previously emphasized, agent-specific productivity can be broadly interpreted to capture agents' heterogeneous demand for transactions on blockchain. A higher $u_{i,t}$ means agent $i$ obtains more utility (in the form of goods equivalent) from blockchain trade. It worth emphasizing that the asset we price is a blockchain coin, not equity stakes of firms.

**The Markov equilibrium.** The coin pricing formula suggests that there exists a Markov equilibrium with $A_t$ being the only aggregate state variable. Note that aggregate wealth is not an aggregate state variable. This is due to the fact that we are not clearing the goods market – agents can incur negative consumption – and a storage technology is always available for agents to transfer wealth over time. These assumptions are reasonable because the coin market is relative small and orthogonal to the whole economy. It is hard to argue for what happens in the cryptocurrency markets has material impact on the aggregate consumption and pricing kernel. As a result of these assumptions, $A_t$ is the only aggregate state variable of the Markov equilibrium.

**Definition 1.** *For any initial value of $A_0$, the distribution of idiosyncratic productivity $u_{i,t}$ given by the density function $g(u)$, and any endowments of coin holdings among the agents, $\{k_{i,0}, i \in [0,1]\}$, such that*

$$\overline{M} = \int_{i\in[0,1]} k_{i,0} di,$$

*a Markov equilibrium with state variable $A_t$ is described by the stochastic processes of agents' choices and coin price on the filtered probability space generated by Brownian motion $\{Z_t, t \geq 0\}$, such that*

*(1) Agents know and take as given the process of coin price;*

*(2) Agents optimally choose consumption and savings (invested in coins and storage);*

*(3) Coin price adjusts to clear the coin market as in Proposition 4;*

*(4) All variables are functions of $A_t$ that follows an autonomous law of motion given by Equation (3.1) that maps any path of shocks $\{Z_s, s \geq t\}$ to the current state $A_t$.*

This conjecture of Markov equilibrium with state variable $A_t$ is consistent with the equilibrium conditions. For example, by Itô's lemma, $\mu_t^P$ is equal to $\left(\frac{dP_t/P_t}{dA_t/A_t}\right)\mu_t^A + \frac{1}{2}\frac{d^2P_t/P_t}{dA_t^2/A_t^2}\left(\sigma_t^A\right)^2$, which is a univariate function of $A_t$ in the Markov equilibrium. From Proposition 2, we can solve $N_t$, which only only depends on $A_t$ and $\mu_t^P$, and thus, is also a univariate function of $A_t$. Similarly, we can solve $\underline{u}_t$ as a function of $A_t$. These are consistent with Equation (10), the coin pricing formula. Here, all the endogenous aggregate or variables, $P_t$, $\mu_t^P$, $N_t$, and $\underline{u}_t$ only depend on the single state variable $A_t$.

In the Markov equilibrium, we confirm our conjecture of the value function of agent $i$, that is $v_{i,t} = w_{i,t} + F(u_{i,t}, A_t)$. Substituting the optimal coin holdings into the HJB equation, we have

$$\begin{aligned} rF(u_{i,t}, A_t) = \ & \max\left\{0, N_t A_t e^{u_{i,t}}\beta\left(\frac{1-\beta}{r-\mu_t^P}\right)^{\frac{1-\beta}{\beta}} - \chi\right\} + \frac{\partial F(u_{i,t},A_t)}{\partial u_{i,t}}\left(-\mu^U u_{i,t}\right) + \frac{\partial F(u_{i,t},A_t)}{\partial A_t}\mu_t^A A_t \\ & + \frac{1}{2}\frac{\partial^2 F(u_{i,t},A_t)}{\partial u_{i,t}^2}\left(\sigma^U\right)^2 + \frac{1}{2}\frac{\partial F(u_{i,t},A_t)}{\partial A_t}\left(\sigma_t^A\right)^2 A_t^2 + \frac{\partial F(u_{i,t},A_t)}{\partial u_{i,t}\partial A_t}\sigma^U\sigma_t^A A_t. \end{aligned}$$

On the right-hand side of the HJB equation, the first term is a function of $u_{i,t}$ and $A_t$, so overall, the HJB equation translates into a second-order differential equation for $F(u_{i,t}, A_t)$.

A set of natural boundary conditions pin down a unique solution: $\lim_{A_t \to 0} F(u_{i,t}, A_t) = 0$, $\lim_{A_t \to +\infty} F(u_{i,t}, A_t) = +\infty$, $\lim_{u_{i,t} \to 0} F(u_{i,t}, A_t) = 0$, $\lim_{u_{i,t} \to +\infty} F(u_{i,t}, A_t) = +\infty$.

**Proposition 5.** *Using the Feynman-Kac formula, $F(u_{i,t}, A_t)$ can be shown to be exactly the discounted sum of trade surplus on the blockchain, with the discount rate equal to $r$.*

So far, we have shown that once the coin pricing function $P(A_t)$ is known, using Itô's lemma, we can solve for $\mu_t^P$, and then, the optimal coin holdings, $k_{i,t}$ using Proposition 1, and from Proposition 2, we solve the community size, $N_t$, and the lower bound of participants' idiosyncratic productivity, $\underline{u}_t$. Substituting these variables into the coin pricing formula, i.e., Equation (10), we have the right-hand side depends only on $A_t$, $P(A_t)$, and the first and second derivatives of $P(A_t)$ in $\mu_t^P$, $N_t$, and $\underline{u}_t$. So, the coin pricing formula is a second-order ordinary differential equation ("ODE") for $P(A_t)$. By imposing proper boundary conditions, we can solve for $P(A_t)$.[19]

A unique solution of the second-order ODE requires two boundary conditions. The first one is that the limit value of $P(A_t)$ is zero as $A_t$ approaches zero.

$$\lim_{A_t \to 0} P(A_t) = 0. \tag{11}$$

We set the second boundary condition by exploring the asymptotic behavior of the economy. Consider the scenario where $A_t$ approaches infinity. Along the process, $N_t$ approaches one and $\underline{u}_t$ approaches $-\infty$ – when the common productivity is sufficiently high, even agents with low idiosyncratic productivity are willing to join the community. We can solve the integral $\int_{\underline{U}_t}^{\infty} \sqrt{\frac{\theta}{\pi}} e^{u-\theta u^2} du$ as follows.

$$\int_{\underline{u}_t}^{\infty} \sqrt{\frac{\theta}{\pi}} e^{u-\theta u^2} du = e^{\frac{1}{4\theta}} \int_{\underline{u}_t}^{\infty} \sqrt{\frac{\theta}{\pi}} e^{-\theta\left(u-\frac{1}{2\theta}\right)^2} du = e^{\frac{1}{4\theta}} \left[1 - CDF\left(\underline{u}_t | \frac{1}{2\theta}, \frac{1}{\sqrt{2\theta}}\right)\right],$$

so it approaches $e^{\frac{1}{4\theta}}$ as $\underline{u}_t$ approaches $-\infty$ (i.e., everyone joins the community).

**Assumption 1.** *To simplify our analysis, we assume that $A_t$ follows a simple geometric Brownian motion,*

$$dA_t = \mu^A A_t dt + \sigma^A A_t dZ_t, \tag{12}$$

[19]The existence of ODE requires a unique mapping from $A_t$, $P(A_t)$, and $P'(A_t)$ to $P''(A_t)$. The question is given $A_t$ and $P_t$, can we uniquely solve $\mu_t^P$ using the coin pricing formula? Since $\underline{u}_t$ decreases in $\mu_t^P$ (and $N_t$ increases in $\mu_t^P$), the right-hand side of the coin market clearing condition increases in $\mu_t^P$, and we can uniquely pin down $\mu_t^P$ given $A_t$ and $P_t$.

*so in particular, $\mu_t^A = \mu^A$ is a constant.*

By inspecting the coin pricing formula, we know the *asymptote* of $P(A_t)$ as $A_t$ approaches infinite is

$$\overline{P}(A_t) = \left(\frac{A_t}{\overline{\overline{M}}}\right)\left(\frac{1-\beta}{r-\mu^A}\right)^{\frac{1}{\beta}} e^{\frac{1}{4\theta}}, \tag{13}$$

where $N_t$ in the coin pricing formula is replaced by 1 and the last integral replaced by its limit value $e^{\frac{1}{4\theta}}$. Moreover, when $P_t$ is proportional to $A_t$, $\mu_t^P = \mu^A$. Therefore, we have the following boundary condition.

**Lemma 1.** *There exists $\overline{A}$ such that*

$$P\left(\overline{A}\right) = \overline{P}\left(\overline{A}\right) \text{ (value matching) and } P'\left(\overline{A}\right) = \overline{P}'\left(\overline{A}\right) \text{ (smooth pasting).} \tag{14}$$

*For $A_t > \overline{A}$, $P(A_t) = \overline{P}(A_t)$ and $N_t = 1$.*

$\overline{A}$ is the upper bound of $A_t$, above which coin price is equal to $\overline{P}(A_t)$ because $N_t = 1$.

Note that once the coin price function $P(A_t)$ is solved, we know, by Itô's lemma, $\mu_t^P$ as a function of $A_t$, so Equation (11) gives a second-order partial differential equations for $F(u_{i,t}, A_t)$ with the boundary conditions discussed previously. However, to characterize the endogenous variables of interest, such as the community size $N_t$, we do not need to solve out $F(u_{i,t}, A_t)$. The next proposition states the existence and uniqueness of the Markov equilibrium.

**Proposition 6.** *There exists a unique Markov equilibrium with state variable $A_t$ that follows an autonomous law of motion given by Equation (12). Given the coin price function $P(A_t)$, Proposition 2 solves the size of community $N_t$ and the lower bound of participant's idiosyncratic productivity $\underline{u}_t$ and Proposition 1 solves the optimal coin holdings of participants $k_{i,t}$. Substituting these variables into the coin pricing formula, i.e., Equation (10) in Proposition 4, we have a second-order ordinary differential equation that solves the coin price function $P(\cdot)$ under the following boundary conditions of Equation (11) and (14).*

We have exactly three boundary conditions for a second-order ODE and an endogenous boundary $\overline{A}$ that uniquely pin down the solution. Note that the equilibrium is unique in the space of $\mathbb{C}^1$, i.e., continuous and smooth functions, where we finds the ODE solution of $P(A_t)$. Outside $\mathbb{C}^1$, there can be multiple equilibria. Consider a positive coin price at time $t$. Without restricting the price path to be continuous, at $t + dt$, agents can coordinate to a coin price equal to 0. And in the instant after this, agents can coordinate on a positive coin price again. Under the restriction of continuous price path, as long as the initial coin price is positive, we have a unique, non-degenerate equilibrium with positive coin price, and once the dynamics of $P_t$ is given, Proposition 3 states the uniqueness of $N_t$.

**Discussion: an alternative competition boundary.** Many blockchain system accommodates not only its native tokens but also other cryptocurrencies. For example, on Ethereum blockchain, any ERC-20 compatible cryptocurrencies are accepted.[20] In such case, We may consider an alternative upper boundary of $A_t$. Define $\psi$ as the cost of creating a new cryptocurrency that is perfect substitute with the coin we study because it functions on the same blockchain and therefore faces the same common blockchain productivity and agent-specific trade needs. This creates a reflecting boundary at $\overline{A}$ characterized by a value-matching condition and a smooth-pasting condition:

$$P\left(\overline{A}\right) = \psi \text{ and } P'\left(\overline{A}\right) = 0. \tag{15}$$

When coin price increases to $\psi$, entrepreneurs outside of the model will develop a new cryptocurrency that is compatible with the rules of our blockchain system. So, the price level never increases beyond this value. Because it is a reflecting boundary, we need to rule out jumps of coin prices, so the first derivative of $P\left(A_t\right)$ must be zero. Again we have exactly three boundary conditions for a second-order ODE and an endogenous upper boundary that uniquely pins down the solution.

Similarly, we may consider potential competing blockchain systems, and interpret $\psi$ as the cost of creating a new blockchain system and its native coin, which together constitute a perfect substitute for our current system. This creates the same reflecting boundary for coin price. When coin price increases to $\psi$, entrepreneurs outside of the model will build a new system.

**Proposition 7.** *The upper boundary condition is given by Equation (15) in the two following cases: (1) the blockchain system accepts alternative tokens or cryptocurrencies that can be developed at a unit cost of $\chi$; (2) an alternative blockchain system that is a perfect substitute of the current system can be developed at a cost of $\chi$ per unit of its native tokens.*

In this paper, we focus on the asymptotic boundary. While our framework accommo-

[20] ERC-20 defines a common list of rules for all tokens or cryptocurrencies should follow on the Ethereum blockchain.

dates the effect of competition, a careful analysis of crypto industrial organization certainly requires more ingredients, especially those that can distinguish between the entry of multiple cryptocurrencies into one blockchain system and competing blockchain systems.

### 3.3 Numeric solution

**Parameter values.** We solve the ODE for $P(A_t)$ under the following parameter values. First, we set $\chi$ equal to 1. This parameter is the cost of joining the blockchain community, measured in goods. It serves as a reference point for other parameters. We set $\overline{M}$, the supply of coins, equal to 10 billion. This parameter just has scaling effect on the coin price. About the dynamics of common productivity of blockchain $A_t$, we set $\mu^A = 0.02$ and $\sigma^A = 0.1$, so the instantaneous volatility of $dA_t/A_t$ is 0.01, i.e., half of the instantaneous growth rate. If we consider one unit of time as one month, over a period of one year, the blockchain technology becomes 27% more productivity.

$\beta$ is the parameter that determines the decreasing return to community size in the blockchain trade surplus. When $\beta$ is high, the surplus, which is a flow utility of coins, is more sensitive to $N_t$. While both $N_t$ and $P_t$ approach zero, as $A_t$ approaches zero, at what level of coin price does $N_t$ reaches 1 depends on $\beta$. We set $\beta$ equal to 0.3 so that $N_t$ is equal to 1, and $P(A_t)$ touches its asymptote when $P(A_t)$ is equal to 30 million.

$r$ is set to 5%, roughly in line with the expected return in financial markets. Finally, we set $\theta = 0.01$, so the standard deviation of cross-section distribution of agent-specific blockchain productivity is 7, i.e., seven times the participation cost.

**Coin price dynamics.** The left panel of Figure 2 plots $P_t$ against the state variable $A_t$. It is an increasing function because the more productive the blockchain is, the stronger the demand for its coins, which pushes up coin price.

The right panel of Figure 2 plots the difference between $P(A_t)$ and its upper bound $\overline{P}(A_t)$, i.e, the asymptote of $P(A_t)$. $\overline{P}(A_t)$ is the coin price when everyone has joined the community, or, to relate to our parameters, the participation cost is equal to zero. The difference is small when $A_t$ is low because both are near zero. The wedge widens because $P(A_t)$ grows slower than $\overline{P}(A_t)$ when $A_t$ grows. The benefit of blockchain technology, represented by $A_t$, translates into real trade surplus by multiplying $N_t^{\beta}$. When $N_t$ is low, coin price is less responsive to the growth of $A_t$. However, as the growth of $A_t$ drives up $N_t$, inducing more agents to join the ecosystem, coin price catches up and finally converges to its asymptote, as $N_t$ rises up to 1.

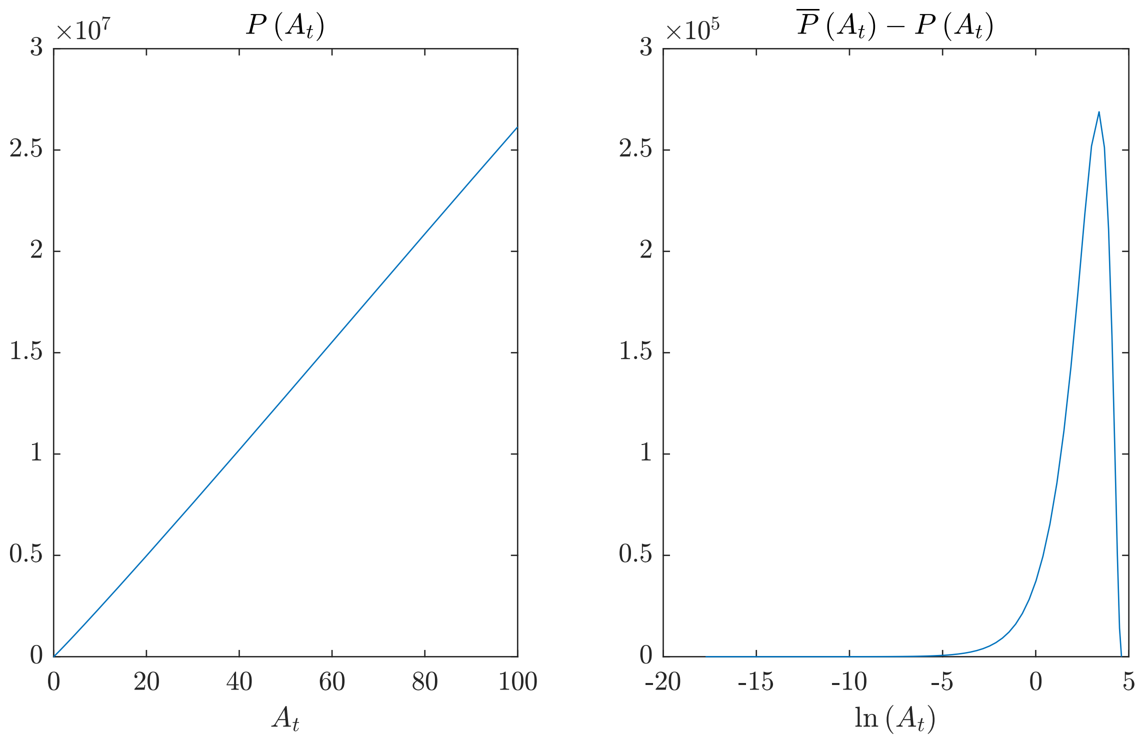


Figure 2: Coin Price.

**Community size.** The solid line in Figure 3 plots the community size $N_t$ against the logarithm of $A_t$. The curve exhibits S-shaped development. When the blockchain technology is not so efficient, the growth of user base in response to technological progress is small. But as $N_t$ increases, the growth of user base feeds on itself – the more agents join the ecosystem, the higher surplus it is from trading on the blockchain. As a result, the growth of $N_t$ speeds up in the interim range of blockchain productivity. User adoption eventually slows down when the pool of new comers get exhausted. This model does not feature population growth, so when more agents join the ecosystem, there are less new comers left to be included in the future when $A_t$ rises up further.

This S-shaped development also helps us understand the dynamics of coin price in the right panel of Figure 2. Initially, the first derivative of $P_t$ with respect to $A_t$ is lower than its asymptote, which happens before the peak of the wedge curve because the *level* of $N_t$ is below 1. However, there is another force working through the *derivative* of $N_t$ with respect to $A_t$. As $A_t$ grows, it directly increases coin price as shown in Proposition 4. It also indirectly increases coin price by increasing $N_t$. This second force eventually dominates, so we see $P_t$ becomes more responsive to variation in $A_t$ than its asymptote, and eventually, the wedge closes in the right panel of Figure 2.

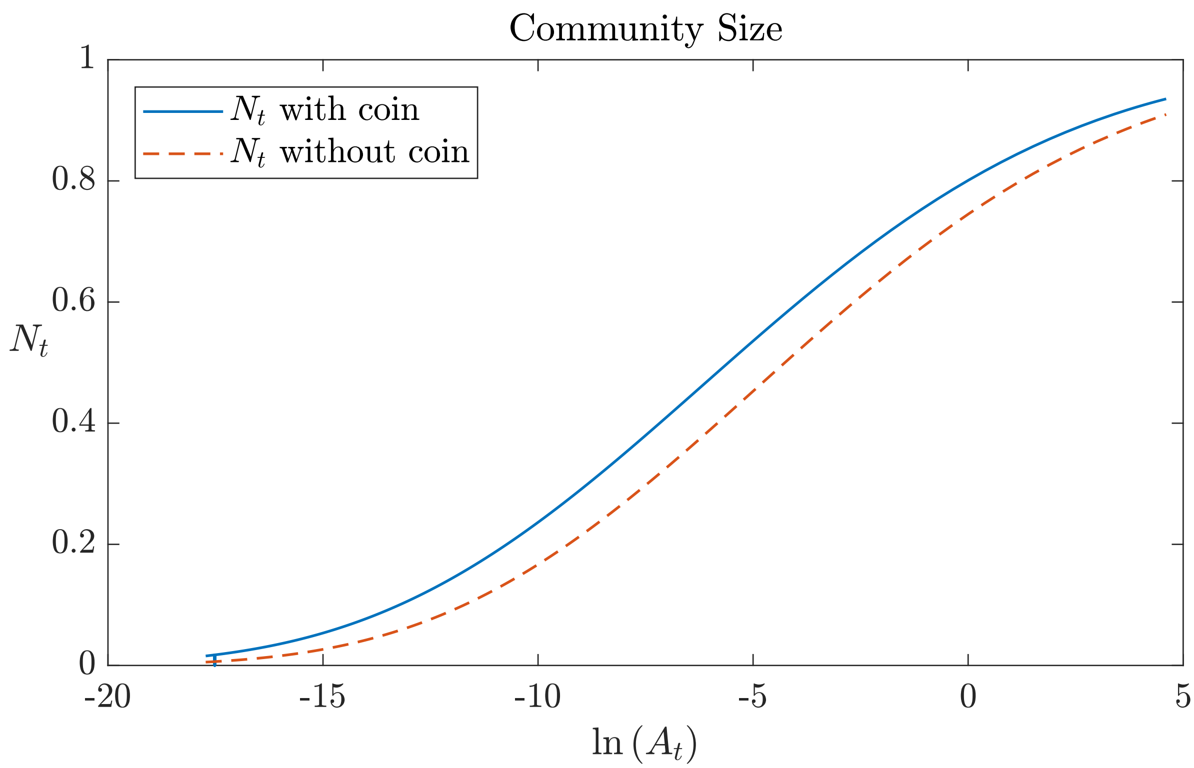


Figure 3: Community Size.

Figure 3 also compares the user adoption with and without coins or blockchain native tokens. The former strictly dominates the latter, but the two eventually converge to one. Why introducing blockchain native tokens speeds up user adoption? Next, we considers an ecosystem without coins, and solve agents' participation decisions.

### 3.4 With or without coin: growth effect and excess volatility

In reality, native tokens can be introduced for various reasons. For example, on the technological side, decentralized consensus is well defined and more easily achieved if the targeted contingency is as simple, for example, as the transfer of native tokens. To record users' transaction record, it is more efficient to unify all transactions under one local currency. For blockchain communities without native tokens, often the case, oracles, a subset of users, are selected to confirm certain contingencies that are relevant for the completion of transactions. This requires more complicated design of blockchain.

In this paper, we focus on a simple effect of introducing native tokens – capitalizing the future growth of technology. When native token or coin is introduced as the local settlement currency, its secondary market trading reflects agents' expectation of future technological progress and price appreciation. We can speed up user adoption because agents join the community not only to enjoy the trade surplus but also the expected appreciation of coin price.

To understand the effect of introducing blockchain native tokens on user adoption, we consider an alternative setup where agents can conduct businesses and enjoy the trade surplus on blockchain without holding coins. Let $b_{i,t}$ denote the dollar value of investment or purchase done on the blockchain. Under the assumption of risk neutrality, the cost of funds is $r$, so agents solve the following profit maximization problem

$$\max_{b_{i,t}} (b_{i,t})^{1-\beta} \left(N_t A_t e^{u_{i,t}}\right)^{\beta} - \chi - b_{i,t} r \tag{16}$$

The first order condition is

$$(1-\beta)\left(\frac{N_t A_t e^{u_{i,t}}}{b_{i,t}}\right)^{\beta} - r = 0. \tag{17}$$

Rearranging the equation, we have

$$b_{i,t} = N_t A_t e^{u_{i,t}} \left(\frac{1-\beta}{r}\right)^{\frac{1}{\beta}}. \tag{18}$$

Substituting the optimal $b_{i,t}$ into the profit function, we have the profit for $k_{i,t} > 0$ equal to

$$N_t A_t e^{u_{i,t}} \beta \left(\frac{1-\beta}{r}\right)^{\frac{1-\beta}{\beta}} - \chi.$$

**Proposition 8.** *In an economy without coins, agents with $u_{i,t} \geq \underline{u}_t^{NC}$ ("NC" for no coin) join the blockchain community, while those with $u_{i,t} < \underline{u}_t^{NC}$ choose not to, where $\underline{u}_t^{NC}$ is given by*

$$\underline{u}_t^{NC} = -\ln(N_t) + \ln\left(\frac{\chi}{A_t \beta}\right) - \left(\frac{1-\beta}{\beta}\right)\ln\left(\frac{1-\beta}{r}\right), \tag{19}$$

*which increases in the community size $N_t$. Let $G(\cdot)$ denote the cumulative probability function of cross-section distribution of idiosyncratic productivity. The community size is*

$$N_t = 1 - G\left(\underline{u}_t^{NC}\right). \tag{20}$$

**The growth effect of coin and feedback effects.** In comparison with Proposition 2, the only difference is that without coin, the price appreciation term, i.e., $\mu_t^P$, drops out in the lower bound of idiosyncratic productivity. Therefore, in states where $\mu_t^P > 0$, a blockchain system with coin has a larger community. The intuition is very simple. Agents hold coins not only to enjoy the trade surplus that is unique to the blockchain technology (utility purchase), but also the coin price appreciation (investment purchase). In a system without coin, the investment-driven demand is shut down.

**Corollary 1.** *Compare a blockchain with and without coin. In states where $\mu_t^P > 0$ ($< 0$), a blockchain with coin has a larger (smaller) user base than the one without.*

Intuitively, if $A_t$ is expected to grow fast (i.e., a larger and positive $\mu^A$), $\mu_t^P$ tends to be positive. Therefore, by introducing a native token that is required to be means of payment, a blockchain system can capitalize future productivity growth in coin price, and thereby, front load the growth of community size. This is the growth effect of introducing coins. Proposition 8 explains why the solid curve, representing a blockchain user base with native tokens, is above the dotted line, representing a blockchain user base without native tokens.

The existence of coins leads to several a feedback loop, the *intertemporal complementarity* the community size. First, by capitalizing future technological progress, coin induces faster growth of user base in the early stage. As the user base is *expected* to expand fast, coin price is expected to increase fast because the flow surplus will become higher for all participants, and thus, all will demand more coins. This expected future increase of coin price in turn feeds into stronger investment-driven demand for coins.

Introducing coins capitalizes future growth, only under the assumption that coin supply is predetermined. If when coin price is high, coin supply increases and coin price declines, then the expected coin price appreciation will be delinked from the prospect of technological progress. A predetermined supply of cryptocurrency is achieved through the decentralized consensus mechanism empowered by blockchain technology. In contrast, traditional monetary policy has commitment problem – monetary authority cannot commit not to supply more money when its currency value is relatively high.

**Excess volatility of community size.** Introducing coins also brings endogenous volatility in the form of coin price fluctuation, denoted by $\sigma_t^P$, the shock loading of $dP_t/P_t$. This endogenous volatility translates into excessive volatility of the community size $N_t$, with "excessive" defined with respect to the system without coin.

To solve the dynamics of $N_t$, we first conjecture that $N_t$ follows a diffusion process in equilibrium

$$dN_t = \mu_t^N dt + \sigma_t^N dZ_t. \tag{21}$$

Strictly speaking, $N_t$ follows a reflected (or "regulated") diffusion process that is bounded below at zero and bounded above at one. We study the interior behavior of $N_t$.

First, we consider the case without coin. Using Itô's lemma, we can differentiate Equation (20), and then, by matching coefficients with Equation (21), we can derive the expressions for $\mu_t^N$ and $\sigma_t^N$:

$$dN_t = -g\left(\underline{u}_t^{NC}\right) d\underline{u}_t^{NC} - \frac{1}{2} g'\left(\underline{u}_t^{NC}\right)\left\langle d\underline{u}_t^{NC}, d\underline{u}_t^{NC}\right\rangle, \tag{22}$$

where $\left\langle d\underline{u}_t^{NC}, d\underline{u}_t^{NC}\right\rangle$ is the quadratic variation of $d\underline{u}_t^{NC}$. Using Itô's lemma, we differentiate Equation (19)

$$\begin{aligned} d\underline{u}_t^{NC} &= -\frac{1}{N_t} dN_t + \frac{1}{2N_t^2}\langle dN_t, dN_t\rangle - \frac{1}{A_t} dA_t + \frac{1}{2A_t^2}\langle dA_t, dA_t\rangle \\ &= -\left(\frac{\mu_t^N}{N_t} - \frac{\left(\sigma_t^N\right)^2}{2N_t^2} + \mu^A - \frac{\left(\sigma^A\right)^2}{2}\right) dt - \left(\frac{\sigma_t^N}{N_t} + \sigma^A\right) dZ_t \end{aligned} \tag{23}$$

Substituting this dynamics into Equation (22), we have

$$\begin{aligned} dN_t = &\left[ g\left(\underline{u}_t^{NC}\right)\left(\frac{\mu_t^N}{N_t} - \frac{\left(\sigma_t^N\right)^2}{2N_t^2} + \mu^A - \frac{\left(\sigma^A\right)^2}{2}\right) - \frac{1}{2} g'\left(\underline{u}_t^{NC}\right)\left(\frac{\sigma_t^N}{N_t} + \sigma^A\right)^2 \right] dt \\ &+ g\left(\underline{u}_t^{NC}\right)\left(\frac{\sigma_t^N}{N_t} + \sigma^A\right) dZ_t, \end{aligned} \tag{24}$$

By matching coefficients on $dZ_t$ with Equation (21), we can solve $\sigma_t^N$.

**Proposition 9.** *In an economy without coins, $N_t$ follows a law of motion given by Equation (24) with the instantaneous standard deviation of $dN_t$ is*

$$\sigma_t^N = \left(\frac{g\left(\underline{u}_t^{NC}\right)}{1 - g\left(\underline{u}_t^{NC}\right)/N_t}\right)\sigma^A. \tag{25}$$

Once coin is introduced, $N_t$ depends on the expected coin price appreciation $\mu_t^P = \mu^P(A_t)$, which is also a univariate function of state variable $A_t$. The dynamics of $\underline{u}_t$ is

$$d\underline{u}_t = -\frac{1}{N_t}dN_t + \frac{1}{2N_t^2}\langle dN_t, dN_t\rangle - \frac{1}{A_t}dA_t + \frac{1}{2A_t^2}\langle dA_t, dA_t\rangle \\ -\left(\frac{1-\beta}{\beta}\right)\left(\frac{1}{r-\mu_t^P}\right)d\mu_t^P - \left(\frac{1-\beta}{\beta}\right)\left(\frac{1}{2\left(r-\mu_t^P\right)^2}\right)\langle d\mu_t^P, d\mu_t^P\rangle \tag{26}$$

By Itô's lemma, $\mu_t^P$ is equal to $\left(\frac{dP_t/P_t}{dA_t/A_t}\right)\mu^A + \frac{1}{2}\frac{d^2P_t/P_t}{dA_t^2/A_t^2}\left(\sigma^A\right)^2$, which is also a univariate function of $A_t$, so in equilibrium, its law of motion is given by a diffusion process

$$d\mu_t^P = \mu_t^{\mu P}dt + \sigma_t^{\mu P}dZ_t. \tag{27}$$

Let $\sigma_t^{\underline{u}}$ denote the diffusion of $\underline{u}_t$. We have

$$\sigma_t^{\underline{u}} = -\frac{\sigma_t^N}{N_t} - \sigma^A - \left(\frac{1-\beta}{\beta}\right)\left(\frac{\sigma_t^{\mu P}}{r-\mu_t^P}\right), \tag{28}$$

which, in comparison with Equation (23), contains an extra term that reflects the volatility of expected coin price change. Note that, similar to Equation (22), we have

$$dN_t = -g\left(\underline{u}_t\right)d\underline{u}_t - \frac{1}{2}g'\left(\underline{u}_t\right)\langle d\underline{u}_t, d\underline{u}_t\rangle, \tag{29}$$

so the diffusion of $N_t$ is $-g\left(\underline{u}_t\right)\sigma_t^{\underline{u}}$. Matching it with the conjectured diffusion $\sigma_t^N$, we can solve $\sigma_t^N$.

**Proposition 10.** *In an economy with coins, $N_t$ follows a law of motion given by Equation (21) with the diffusion term given by*

$$\sigma_t^N = \left(\frac{g\left(\underline{u}_t\right)}{1-g\left(\underline{u}_t\right)/N_t}\right)\left[\sigma^A + \left(\frac{1-\beta}{\beta}\right)\left(\frac{\sigma_t^{\mu P}}{r-\mu_t^P}\right)\right]. \tag{30}$$

Comparing Proposition 9 and 10, we see that introducing coins alters the volatility dynamics of user base through the fluctuation of expected coin price change, i.e., $\sigma_t^{\mu P}$. Having a native currency can either amplify or dampen the shock effect on the size of blockchain community, depending on the sign of $\sigma_t^{\mu P}$. By Itô lemma, $\sigma_t^{\mu P} = \frac{d\mu_t^P}{dA_t}\sigma^A A_t$, so the sign of $\sigma_t^{\mu P}$

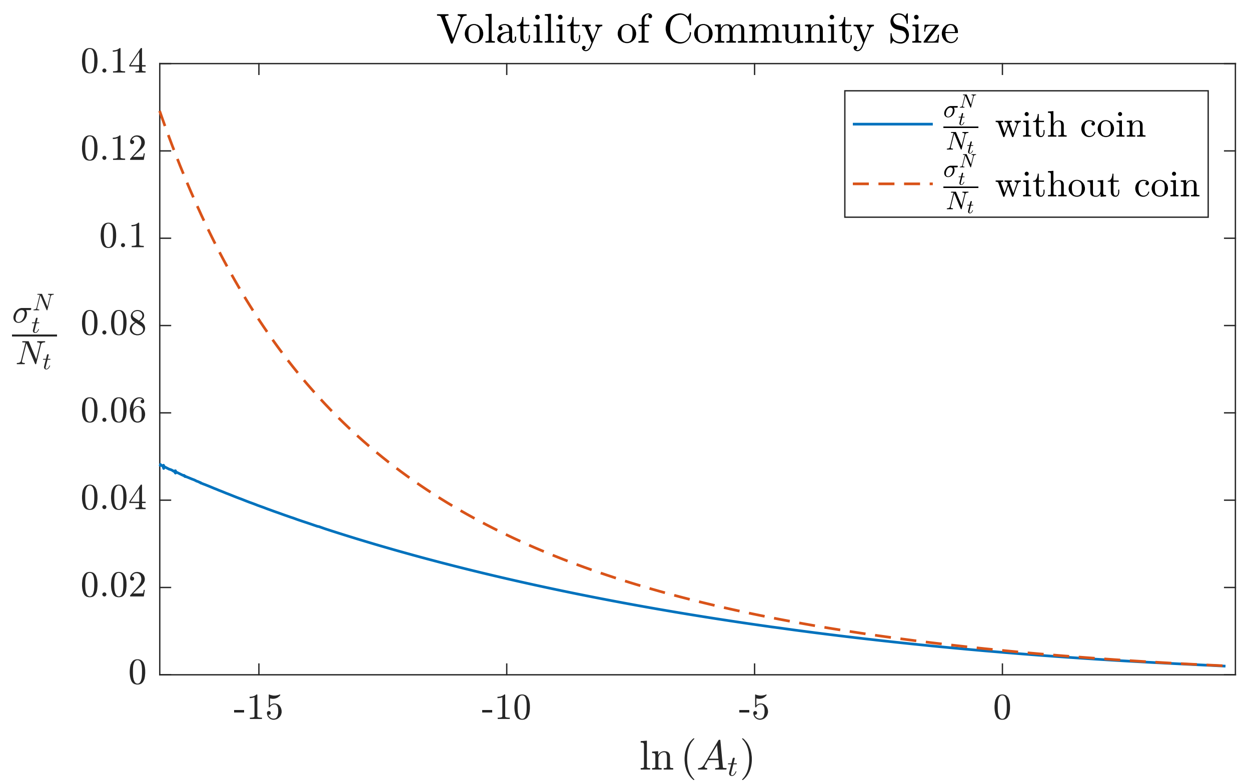


Figure 4: Volatility of Community Size.

depends on whether $\mu_t^P$ increases or decreases in $A_t$. Again, by Itô lemma, $\mu_t^P$ is equal to $\left(\frac{dP_t/P_t}{dA_t/A_t}\right)\mu^A + \frac{1}{2}\frac{d^2P_t/P_t}{dA_t^2/A_t^2}\left(\sigma^A\right)^2$, so the sign of $\sigma_t^{\mu P}$ eventually depends on the third derivative of $P_t$ with respect to $A_t$.

Figure 4 plots $\sigma_t^N$, i.e., the shock loading of $N_t$ growth rate $dN_t/N_t$, and compares the case with and without coin. Under our calibration, $\sigma_t^{\mu P} < 0$, introducing coin reduces the volatility of $N_t$. This volatility reduction effect is more prominent in the early stage of development when $A_t$ and $N_t$ are low.

**Excess volatility of coin price.** The dynamics of community size in turn affects the volatility of coin price. When $\chi = 0$, agents' decision to participate becomes irrelevant. Every agent participates, so $N_t = 1$, and coin price is given by Equation (13) and the ratio of $P_t$ to $A_t$ is a constant. Therefore, the diffusion of coin price, i.e., $\sigma_t^P$, is equal to $\sigma^A$.

A key theme of this paper is the endogenous dynamics of user adoption. When $\chi > 0$, the ratio of $P_t$ to $A_t$ depends on the $\underline{u}_t$, the threshold value of agent-specific blockchain productivity, above which an agent participates. The variation of $N_t$ feeds into $P_t/A_t$, and therefore, amplifies the volatility of coin price beyond $\sigma^A$ which is the level of volatility when

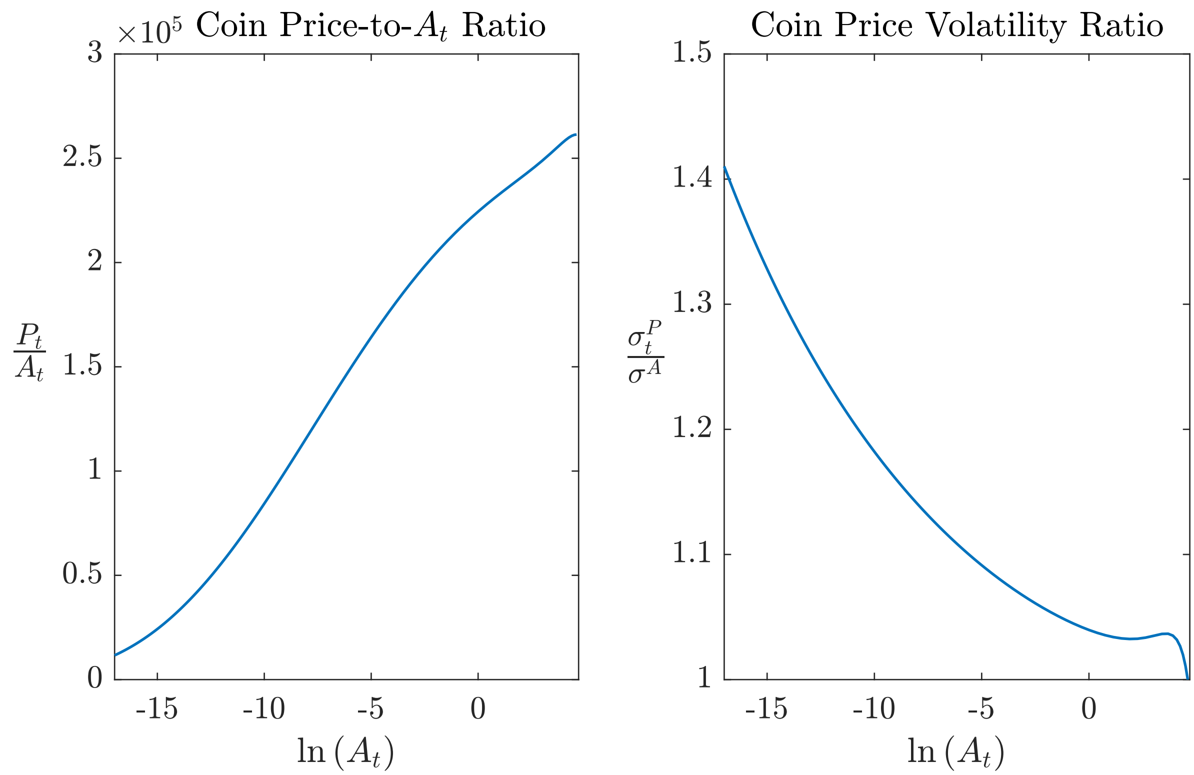


Figure 5: Coin Price-to-Blockchain Productivity Ratio and Volatility.

the issue of user adoption is irrelevant.

The left panel of Figure 5 plots $P_t/A_t$, which follows quite closely the dynamics of $N_t$ shown in Figure 3, exhibiting an S-shaped curve. The right panel of Figure 5 plots the ratio of coin price volatility to $\sigma^A$, which eventually converges to 1 as $N_t$ approaches one and $P_t$ approaches its asymptote. At its height, endogenous user adoption amplifies coin price volatility (or instantaneous standard deviation, to be precise) by more than 40%. A key result of this paper is this the mutual effect between $N_t$ and $P_t$ in both growth and volatility. The volatility of coin price in turn feeds into the volatility of expected coin price change, and the volatility of $N_t$.

# 4 Conclusion

This paper provides the first dynamic pricing model of cryptocurrencies and tokens that serve as medium of exchange among blockchain users. Our model highlights a key benefit of introducing such native currency: when agents expect future technological progress, token price appreciation induces more agents to trade on the blockchain by reflecting such expectation and serving as an attractive store of value. In other words, token capitalizes future growth and speeds up user adoption. We characterize the inter-temporal feedback mechanism that arises through the interaction between user base dynamics and token price. While the growth effect enhances welfare, tokens can either amplify or reduce the volatility of user adoption through price variation. Our model sheds light on the broad issue of asset pricing with user-base externalities.

# Appendix - Proofs

## A.1 Proof of Proposition 3

The first derivative of $R\left(n; A_t, \mu_t^P\right)$ is

$$\frac{dR\left(n; A_t, \mu_t^P\right)}{dn} = -\left(\sqrt{\frac{\theta}{\pi}} e^{-\theta \underline{u}^2}\right) \frac{d\underline{u}}{dn} = \left(\sqrt{\frac{\theta}{\pi}} e^{-\theta \underline{u}^2}\right) \frac{1}{n} \tag{31}$$

Next, we solve the second derivative

$$\begin{aligned} \frac{d^2R\left(n; A_t, \mu_t^P\right)}{dn^2} &= -\left(\sqrt{\frac{\theta}{\pi}} e^{-\theta \underline{u}^2}\right) \frac{2\theta \underline{u}}{n^2} - \left(\sqrt{\frac{\theta}{\pi}} e^{-\theta \underline{u}^2}\right) \frac{1}{n^2} \\ &= -\left(\sqrt{\frac{\theta}{\pi}} e^{-\theta \underline{u}^2}\right) \frac{(2\theta \underline{u} + 1)}{n^2}. \end{aligned} \tag{32}$$

Note that in the expression $\underline{u}$ is pinned down by $n$, and it is a decreasing function of $n$. When $n$ is small, $\underline{u}$ is large, so the response function starts from the origin as a concave curve, and a potential second crossing with the $45^o$ line happens when the response function turns convex and crosses from below as $n$ increases. For the equilibrium $N_t$ to be unique, a necessary and sufficient condition is that the second crossing never happens, i.e., $R\left(1; A_t, \mu_t^P\right) < 1$, i.e., $G\left(\underline{u}\left(1; A_t, \mu_t^P\right)\right) > 0$, or equivalently, $\underline{u}\left(1; A_t, \mu_t^P\right)$ is not equal to negative infinity, which trivially holds as shown in Equation (7).

## A.2 Proof of Proposition 5

Using the FeynmanKac formula, we can show that

$$F\left(u_{i,t}, A_t\right) = \mathbb{E}_t\left[\int_{s=t}^{+\infty} e^{-r(s-t)} \max\left\{0, N_s A_s e^{u_{i,s}} \beta \left(\frac{1-\beta}{r-\mu_s^P}\right)^{\frac{1-\beta}{\beta}} - \chi\right\} ds\right].$$

# References


Athey, Susan, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia, 2016, Bitcoin pricing, adoption, and usage: Theory and evidence, .

Balvers, Ronald J, and Bill McDonald, 2017, Designing a global digital currency, .

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, and Catherine Casamatta, 2017, The blockchain fold theorem, *Preliminary Work in Progress*.

Catalini, Christian, and Joshua S Gans, 2016, Some simple economics of the blockchain, Discussion paper, National Bureau of Economic Research.

——— , 2018, Initial coin offerings and the value of crypto tokens, Discussion paper, National Bureau of Economic Research.

Chiu, Jonathan, and Thorsten V Koeppl, 2017, The economics of cryptocurrencies–bitcoin and beyond, .

Chiu, Jonathan, and Tsz-Nga Wong, 2015, On the essentiality of e-money, Discussion paper, Bank of Canada Staff Working Paper.

Ciaian, Pavel, Miroslava Rajcaniova, and dArtis Kancs, 2016, The economics of bitcoin price formation, *Applied Economics* 48, 1799–1815.

Cong, Lin William, and Zhiguo He, 2018, Blockchain disruption and smart contracts, *Review of Financial Studies. In-principle Acceptance of FinTech Registered Report, Completion of the Paper in Progress.*

——— , and Jiasun Li, 2018, Decentralized mining in centralized pools, .

Cong, Lin William, Ye Li, and Neng Wang, 2018, Tokenomics: Coin offerings and business acceleration, .

Doepke, Matthias, and Martin Schneider, 2017, Money as a unit of account, *Econometrica* 85, 1537–1574.

Easley, David, Maureen O'Hara, and Soumya Basu, 2017, From mining to markets: The evolution of bitcoin transaction fees, .

Evans, David S, and Richard Schmalensee, 2010, Failure to launch: Critical mass in platform businesses, *Review of Network Economics* 9.

Eyal, Ittay, and Emin Gün Sirer, 2014, Majority is not enough: Bitcoin mining is vulnerable, in *International Conference on Financial Cryptography and Data Security* pp. 436–454. Springer.

Fernández-Villaverde, Jesús, and Daniel Sanches, 2016, Can currency competition work?, Discussion paper, National Bureau of Economic Research.

Gandal, Neil, and Hanna Halaburda, 2014, Competition in the cryptocurrency market, .

Gans, Joshua S, and Hanna Halaburda, 2015, Some economics of private digital currency, in *Economic Analysis of the Digital Economy* . pp. 257–276 (University of Chicago Press).

Glasserman, Paul, and Behzad Nouri, 2016, Market-triggered changes in capital structure: Equilibrium price dynamics, *Econometrica* 84, 2113–2153.

Harvey, Campbell R, 2016, Cryptofinance, *Working Paper*.

Holden, Craig W, and Avanidhar Subrahmanyam, 2017, A yen for plastic, *Economics Letters* p. 72.

Huberman, Gur, Jacob Leshno, and Ciamac C. Moallemi, 2017, Monopoly without a monopolist: An economic analysis of the bitcoin payment system, working paper 17-92 Columbia Business School.

Khapko, Mariana, and Marius Zoican, 2017, 'smart' settlement, *Working Paper*.

Kiyotaki, Nobuhiro, and Randall Wright, 1989, On money as a medium of exchange, *Journal of Political Economy* 97, 927–954.

Li, Jiasun, and William Mann, 2018, Initial coin offering and platform building, *Working Paper*.

Malinova, Katya, and Andreas Park, 2016, Market design for trading with blockchain technology, *Available at SSRN*.

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

Nanda, Ramana, Robert F. White, and Alexey Tuzikov., 2017a, Blockchain, cryptocurrencies and digital assets, *Harvard Business School Technical Note* pp. 818–066.

——— , 2017b, Initial coin offerings, *Harvard Business School Technical Note* pp. 818–067.

Rogoff, Kenneth, 2017, Crypto-fools gold?, *Project Syndicate* 9.

Shiller, Robert, 2017, what is bitcoin really worth? don't even ask, *The New York Times* Dec 15.

Sockin, Michael, and Wei Xiong, 2018, A model of cryptocurrencies, .

Yermack, David, 2017, Corporate governance and blockchains, Discussion paper, .

Yglesias, Matthew, 2012, Social cash: Could facebook credits ever compete with dollars and euros?, .