BANK OF ENGLAND

Staff Working Paper No. 855

Blockchain structure and cryptocurrency prices

Peter Zimmerman

February 2020

BANK OF ENGLAND

Staff Working Paper No. 855
Blockchain structure and cryptocurrency prices

Peter Zimmerman[1]

Abstract

I present a model of cryptocurrency price formation that endogenizes both the financial market for coins and the fee-based market for blockchain space. A cryptocurrency has two distinctive features: a price determined by the extent of its usage as money, and a blockchain structure that restricts settlement capacity. Limited settlement space creates competition between users of the currency, so speculative activity can crowd out monetary usage. This crowding-out undermines the ability of a cryptocurrency to act as a medium of payment, lowering its value. Higher speculative demand can reduce prices, contrary to standard economic models. Crowding-out also raises the riskiness of investing in cryptocurrency, explaining high observed price volatility.

Key words: Blockchain, cryptocurrency, global games, price volatility.

JEL classification: D4, E42, G13.

(1) Bank of England. Email: peter.n.zimmerman@gmail.com

This paper does not necessarily reflect the views of the Bank of England. I am grateful to Pat Akey, Carol Alexander, Arash Aloosh, Christophe Aymanns, Andrew Burnie, Sabrina Buti, Johan Cassel, Xavier Freixas, Rodney Garratt, Thomas Geelen, Bige Kahraman, Lukas Kremens, Alex Montag, Alan Morrison, Walt Pohl, Fahad Saleh, Joel Shapiro, Donghwa Shin, Rhiannon Sowerbutts, Jan Starmans, Oren Sussman, Mungo Wilson, and Xingtan Zhang, as well as conference participants at Anglia Ruskin University, Bergen Fintech Conference, Cambridge Centre for Alternative Finance, Cleveland Fed-OFR Financial Stability Conference, Crypto Valley, Dublin City University, Edinburgh Business School, EuroFIT 2018 at UCL, European Finance Association Doctoral Tutorial, Northern Finance Association, and University of Sussex, and seminar participants at Amsterdam Business School, Bank of England, Bank for International Settlements, Copenhagen Business School, Federal Reserve Bank of Cleveland, Federal Reserve Board of Governors, Lancaster University Management School, Monash University, University of New South Wales, University of North Carolina at Chapel Hill (Kenan-Flagler), University of Oxford (Saïd), Queen Mary University of London, University of Sydney, and University of Toronto (Rotman). All errors are my own.

The Bank's working paper series can be found at www.bankofengland.co.uk/working-paper/staff-working-papers

Bank of England, Threadneedle Street, London, EC2R 8AH
Email enquiries@bankofengland.co.uk

ISSN 1749-9135 (on-line)

1. INTRODUCTION

During 2017, the price of bitcoin increased from around $1,000 to a peak of nearly $20,000. This rise was accompanied by a surge in cryptocurrency market trading, leading to congestion in the system and settlement delays. For example, in January 2018, a major Bitcoin conference stopped accepting bitcoin for its tickets, because it was not working well as a means of payment (Choudhury, 2018).

Congestion occurs because the blockchain – a list of all transactions which have occurred in the cryptocurrency – has limited capacity. For example, Bitcoin allows for a maximum of only around seven transactions per second.[1] This makes it more limited than non-blockchain payments systems like Visa or Mastercard, which each handle thousands of transactions per second. This congestion problem arises due to the blockchain structure, and is not limited to Bitcoin. For example, delays on the Ethereum platform in December 2017 were exacerbated by an online trading game.

In this paper, I show blockchain congestion leads to novel interactions between cryptocurrency speculation, monetary usage, and prices. By competing for limited blockchain space, speculators impose an externality on monetary users that we do not see with other forms of money. In my model, cryptocurrency is a means of payment with no intrinsic value. Instead, its value depends on the extent to which it is used as money. Speculation congests the blockchain, reducing the moneyness of cryptocurrency, and impacting its price. This suggests a novel relationship between speculative and transactional usage of cryptocurrencies: an increase in speculative demand can lower the price of the asset, rather than raise it, as standard economics models would predict.

In my model, there two types of strategic agent: households, who derive some value from using cryptocurrency as a means of payment, and speculators, who trade cryptocurrency on an exchange using private information. The value of cryptocurrency depends on its monetary usage, so speculators' trading decisions are based on their beliefs about households' actions, rather than any fundamental. Households choose whether to use cryptocurrency or cash to purchase consumption goods. Using cryptocurrency earns a non-pecuniary payoff, which is increasing in the total number of households that use it. This payoff occurs because cryptocurrency is embedded with a technology that makes it potentially superior to cash as a medium of payment. For example, cryptocurrency

[1] In this paper, I follow convention by writing "Bitcoin" to denote the network, and "bitcoin" to denote the currency unit, and similarly for other cryptocurrencies.

may be easy to use and secure relative to cash, or households may value the lack of reliance on authorities such as central or commercial banks. However, the congestion problem means cryptocurrency transactions can be subject to costly delays. And congestion is worse when more agents use cryptocurrency.

Households and speculators observe signals about the strength of the technology, and thus the size of the payoff from using cryptocurrency. A threshold equilibrium emerges, in which households use cryptocurrency, and speculators buy it, if and only if the technology is sufficiently strong. A high signal means households are more likely to use cryptocurrency as money, which implies a high value. However, as trading requires blockchain space, the presence of speculators raises the threshold at which households are willing to use cryptocurrency. When speculators 'crowd out' households in this way, cryptocurrency becomes less useful as money and its value falls. The crowding-out effect has important implications for price formation. Normally, a rise in demand should result in a higher price for a good. However, that is not necessarily the case for cryptocurrency. A rise in speculative demand can crowd out monetary usage, reducing the price of the asset.

The model also explains why observed price volatility is much higher for cryptocurrencies than for conventional assets. A lower supply of blockchain space — or a larger number of speculators — means cryptocurrency becomes less useful as money, and so the threshold for usage rises. A higher threshold means it is less likely that cryptocurrency has a high price. Just as the volatility of outcomes of a fair-priced lottery is increasing in the odds of winning that lottery, a higher usage threshold makes the outcome of cryptocurrency prices more volatile. The more congested the blockchain, the more volatile the price. Table 1 compares volatility of returns of major cryptocurrencies to those of selected NASDAQ stocks.[2] For some stocks, the most turbulent days in their histories are akin to an average day in the cryptocurrency markets.

I show the effect of congestion on volatility is magnified when markets are less liquid. This is true even if the number of informed speculators is endogenous. Cryptocurrency markets are characterized by low liquidity, with trading fragmented across a large number of unregulated exchanges, and so this effect can further explain the high levels of realized price volatility.

[2]These stocks each have a similar market cap to Bitcoin, around $150bn at the time of writing.

Table 1. **Comparison of daily volatility of returns for cryptocurrencies and selected technology stocks. Volatility is defined as 30-day rolling backward-looking window of standard deviation of daily returns of USD prices, measured in percentage points. Data for cryptocurrencies are from Coin Metrics, and those for stocks are from Yahoo! Finance. Series run from the date indicated until September 30, 2019.**

Asset	From	Observations	Mean	Median	Maximum
Bitcoin	Aug 17, 2010	3332	4.44	3.64	17.30
Litecoin	May 2, 2013	2343	5.91	4.78	29.46
Ether	Sep 7, 2015	1485	6.02	5.30	13.68
Intel	Mar 17, 1980	9985	2.04	1.91	7.51
Cisco	Feb 16, 1990	7476	2.05	1.85	6.99
Nvidia	Jan 22, 1999	5220	3.02	2.52	12.27
Netflix	May 23, 2002	4383	2.98	2.76	10.82
PayPal	Jul 06, 2015	1082	1.52	1.44	3.14

These results arise because of two distinctive characteristics of cryptocurrencies. First, because a cryptocurrency is a monetary asset with no fundamental value, its value is governed by its usage as a means of payment. Second, limited settlement space means that users are in competition with one another. Interaction between these two characteristics makes the price sensitive to the blockchain capacity and to the number of speculators.

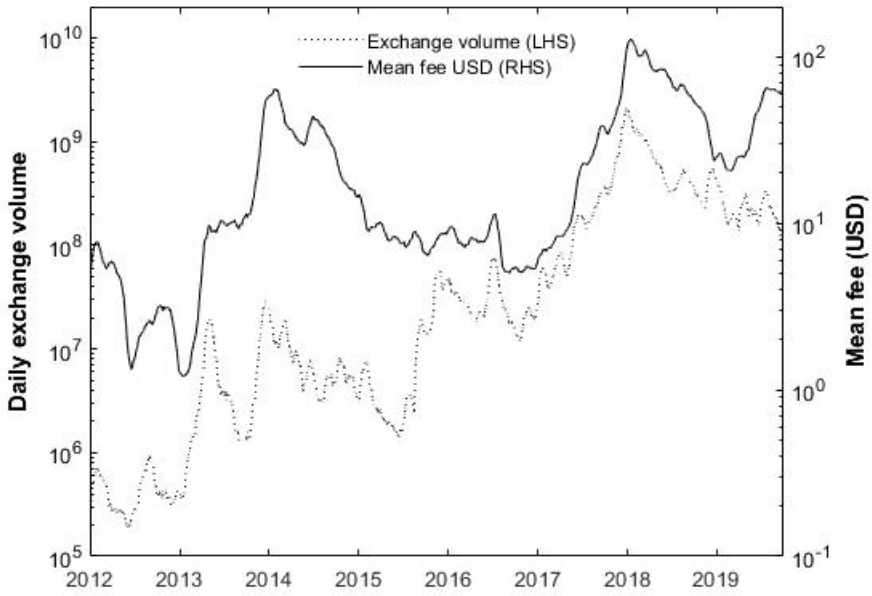
To my knowledge, this paper is the first to endogenously model both the financial market for cryptocurrency and the market for blockchain space, and to explore the interactions between them. The initiator of a transaction can offer a fee, paid in cryptocurrency, to whichever miner includes her payment in a block. This fee allows users to mitigate settlement risk. Miners prioritize transactions with the highest fees, so the market for blockchain space resembles a sealed-bid all-pay auction, where the agents bid for space sold by the miners. The market for blockchain space can exacerbate the crowding-out effect. This is because, when cryptocurrency is more valuable, households become reluctant to spend it on fees. Instead, they prefer to hoard it and endure slower settlement times. I call this a 'digital gold' effect: when cryptocurrency is more valuable, agents view it as an asset to store, rather than money to spend.

In my final set of results, I relax the assumption that agents' signals are perfect, and introduce noisy private signals about the technology. I solve for the agents' equilibrium strategies by adapting global games techniques. These techniques are commonly used when the payoff to an agent from taking an action is increasing in the number of other agents that take the same action, but that is

not always the case in this model. For example, if a household believes others use cryptocurrency and pay high mining fees, then she may prefer not to use cryptocurrency at all. I show that a threshold equilibrium exists nonetheless if signal noise is small, and is unique in the limit as noise tends to zero. In this equilibrium, the link between blockchain congestion and volatility still holds.

There is evidence that speculative activity does indeed have an impact on blockchain congestion. Figure 1 shows that, during the peaks of speculative activity in autumn 2013 and 2017, and more recently in summer 2019, mining fees shot up, making it more expensive to use Bitcoin to make payments. On December 24, 2017, the mean fee paid per transaction was equivalent to $162, suggesting that Bitcoin users were willing to pay non-trivial sums for settlement priority.

Figure 1. Bitcoin daily exchange trading volume (LHS) and mean fee per transaction, in USD (RHS), December 3, 2011 – September 30, 2019. Data are from `blockchain.info` and are plotted in log-scale, daily over a 30-day backward-looking moving average.



These surges in trading activity occur despite the fact that few retailers accept Bitcoin as a means of payment.[3] Carney (2018) and Krugman (2018) argue that, because monetary usage is so low, high levels of speculative activity are suggestive of a bubble. However, there is evidence that cryptocurrency prices do respond to news about their prospects as monetary instruments, so speculation is at least somewhat rational.[4] My paper shows that a high degree of speculative activity

[3]For an up-to-date list, see `https://99bitcoins.com/bitcoin/who-accepts/`.
[4]See Biais, Bisière, Bouvard, Casamatta, and Menkveld (2018).

and price volatility is consistent with low payments usage in a rational expectations equilibrium. The crowding-out effect may explain why we have so far seen much more speculative trading of cryptocurrencies than monetary usage.

My results suggest that price volatility may fall and payments usage increase if, in the future, a greater volume of speculation could be carried out outside the blockchain. Recent developments such as the evolution of cash-settled derivatives markets[5] or the introduction of the Lightning Network could have profound consequences.[6] However, hedging and settlement ultimately have to occur on-chain, albeit netted, so blockchain congestion will continue to affect pricing and usage.

The remainder of the paper is arranged as follows. The next Section reviews the most relevant literature. Section 2 provides an overview of the key features of cryptocurrency that are useful for understanding the model, including blockchain technology, the trading environment, and the use of cryptocurrency as money. Section 3 sets up the model. Section 4 shows there is a unique equilibrium, and explores how speculative trading affects price formation and volatility. Section 5 examines a variant of the model in which agents have imperfect information about the cryptocurrency technology. Section 6 concludes, with a discussion of how the results may be verified empirically. All proofs are in the Appendix.

1.1 *Relevant literature*

This paper is related to a wide literature on the role of cryptocurrencies as a monetary asset, some of which posit alternative explanations for the high level of volatility. Yermack (2013) and Saleh (2018) suggest that, because many cryptocurrencies have a fixed supply schedule, demand shocks cannot be absorbed by adjusting quantity, and so feed through to price. Gandal, Hamrick, Moore, and Oberman (2018) demonstrate that elevated bitcoin price volatility in 2013 may have been due to price manipulation on the Mt. Gox exchange. Several papers show there can be multiple equilibria,

[5] At the time of writing, the Chicago Mercantile Exchange (CME) is the only major exchange offering cash-settled Bitcoin futures. The Chicago Board Options Exchange suspended its own Bitcoin futures market in 2019. The Intercontinental Exchange (ICE) has recently opened a physically-settled futures market. At the time of writing, the total open interest in CME Bitcoin futures is only around $163 million, compared to a total bitcoin market cap of about $150 billion.

[6] The Lightning Network is a secondary layer on top of the existing payments network to facilitate small payments without creating blockchain congestion. See Divakaruni and Zimmerman (2020).

and argue volatility could be a result of uncertainty about which equilibrium will emerge (Biais et al., 2018; Pagnotta, 2018; Schilling and Uhlig, 2019). However, these papers cannot explain why cryptocurrencies experience volatility so much higher than other assets that exist in fixed supply, that are prone to market manipulation, or that exhibit network effects. My model focuses on the technological attributes of cryptocurrencies that makes them different to traditional assets. In my model, there is a unique equilibrium, and volatility emerges due to the unique characteristics of blockchain technology.

A number of papers examine price formation for cryptocurrencies. Ciaian, Rajcaniova, and Kancs (2016) use variants of Fisher's (1911) equation of exchange to propose supply and demand functions, and so determine a unique exchange rate between cryptocurrency and fiat money. Athey, Parashkevov, Sarukkai, and Xia (2016) derive a price for cryptocurrency in a model where users are uncertain about whether the technology will fail. Bolt and van Oordt (2019) introduce a speculative element, so that the equilibrium price is determined by investors' desire to maximize their portfolio values. Again, these approaches do not incorporate the technological factors that distinguish cryptocurrencies from other monetary instruments. The main contribution of my paper is to explore how these technological differences affect pricing.

My paper also relates to a newly developing literature on the fee-based market for blockchain space. The most closely related papers are Huberman, Leshno, and Moalleni (2017) and Easley, O'Hara, and Basu (2019), which both use queueing theory to assess the effect of blockchain congestion on fees and waiting times. As in my model, agents in these papers pay fees in order to achieve timely settlement. In contrast to my model, neither paper features a financial market with endogenous price formation. Hautsch, Scheuch, and Voigt (2018) study the limits to arbitrage between cryptocurrency exchanges that arise due to settlement latency. In this model, neither prices nor fees are micro-founded, and the reduction in latency from a given mining fee is assumed to be fixed, rather than endogenized as in my model.

There is a long literature on the determinants of usage and price of monetary assets, too extensive to review here. One particularly relevant paper is Kiyotaki and Wright (1989), which shows that it is possible for an intrinsically useless asset to be used as money, so long as it is liquid

and agents are willing to accept it. This idea informs the monetary role that cryptocurrency plays in my paper, although the details of my model are quite different.

2. INSTITUTIONAL FEATURES OF CRYPTOCURRENCIES

This Section outlines technical features of cryptocurrencies that are key to my model. These motivate the modeling choices that I make. In particular, I discuss the limited capacity of the blockchain, the trading environment, and the utility of cryptocurrency as money. Readers who are familiar with these topics may wish to go straight to the description of the model in Section 3.

At the time of writing, the website `coinmarketcap.com` lists over 2,000 different cryptocurrencies. The descriptions in this Section, and the results in the rest of the paper, are relevant for any cryptocurrency that settles on its own blockchain, so long as that blockchain has finite capacity. This includes all of the major cryptocurrencies such as Bitcoin, Bitcoin Cash, Ethereum, and Litecoin. The paper may be less relevant for tokens that use a shared blockchain, including most Initial Coin Offerings (ICOs).[7]

2.1 *Blockchain technology*

A cryptocurrency is a digital asset with no physical form. Ownership is recorded on a decentralized ledger called a *blockchain*, which is maintained by a global network of computer *nodes*. The ledger is public, so anybody with a computer and Internet access can download the software, become a node, and join the network. Owners of cryptocurrency store it using software called a *wallet*. A private key is needed to access the contents of a wallet. Only the owner of a wallet has the key and, without it, any attempt to make a transaction will be rejected by the nodes.

When one person — let us call her 'Alice' — wants to send currency to another person — 'Bob' — she notifies the network.[8] Her payment is then put into the *mempool*, which is a set of pending payments that have not yet been added to the ledger. The transfer of ownership of a coin

[7] At the time of writing, at least 82% of the total cryptocurrency market capitalization consists of coins that settle on their own blockchains, according to data from `coinmarketcap.com`.

[8] If Alice is a node, she can do this directly. Otherwise, she notifies her wallet provider, which is a node that intermediates her access to the network.

is finalized only when the corresponding payment is removed from the mempool and added to the blockchain. For this to happen, it must be included in a new *block*, which is a record of transactions that are grouped together and permanently appended to the blockchain.

New blocks are created at a random rate, and can contain only a limited number of payments. For example, a Bitcoin block contains up to 1 megabyte of data, which is typically sufficient for around 4,000 transactions.[9] If a payment cannot be incorporated into a block, it must remain in the mempool and wait for the next block.

Limits on blockchain capacity are the result of a deliberate design choice, which trades off security against payment efficiency. Each time a block is added to the blockchain, all nodes must update their own local version of it. If they do not have time to do this before the next block is created, there may be disagreement about the true state of the blockchain (Hinzen, John, and Saleh, 2019). Increasing the block size, or the block creation rate, can therefore mean a less efficient verification process. A larger block size would also increase the technical requirements for becoming a node, making the network less secure.[10] Attempts have been made to adjust Bitcoin's core code and increase blockchain capacity, but so far no proposal has been able to achieve the required consensus among the developer community (Morgan, 2017).

Some nodes choose to work on adding new blocks to the blockchain; these are called *miners*. Every so often, a miner is selected to create a new block, and can choose mempool transactions to put into it. Suppose that, among all potential miners, 'Minnie' is selected to mine the next block. Alice can incentivize Minnie to include her payment by attaching a fee, denominated in cryptocurrency, when she submits her payment instruction to the mempool. If Minnie includes Alice's payment in her block, she receives this fee. The fee system is a market mechanism for the assignment of priority. Since Minnie will rationally prioritize the payments with highest fees, she is effectively operating an auction.

Once a payment has been submitted to the mempool, the fee cannot be recovered, even if the

[9]The determinants of the size of an individual payment in bytes tend to be technical in nature, and not related to the factors of interest in this model. For example, one key determinant is the number of 'inputs' to the transaction. These are the number of separate previous payments to the payer that, collectively, constitute the source of the crypto she is now paying out.

[10]See Clifford (2017). Budish (2018) examines miners' trade-off between using their computing power to maintain the blockchain and to attack it.

payment is later canceled. The fee mechanism is akin to an all-pay auction operated by Minnie, with voluntary participation. Alice can make her payment to Bob cancellable if she flags the transaction as 'replace by fee'. If she does this then, while the payment is in the mempool, she can submit a second transaction that sends the same exact same coins to herself, but with a higher fee attached. Minnie will then prioritize the second transaction. Once it is added to the blockchain, the first transaction becomes invalid because the same coins cannot be spent twice. However, Alice must then pay the higher fee.

When creating a new block, a miner also receives a certain number of newly minted units of the currency, called the *coinbase reward*. At the time of writing, a Bitcoin miner receives 12.5 new bitcoins per block mined, in addition to the fees attached to any payments taken from the mempool. The total supply of Bitcoin is fixed at 21 million, with the last coin expected to be mined around the year 2140. To achieve this, the coinbase reward halves every 210,000 blocks — roughly every 4 years — until all coins have been issued. Thus, as the system matures, coinbase rewards become a less important part of the incentive system for miners, and the fees become correspondingly more important. Nakamoto (2008), the original white paper that introduced Bitcoin, explains that this predictable and limited supply schedule is designed to eliminate the risk of currency debasement when a monetary authority controls supply. Easley et al. (2019) show that fees necessarily become a more important part of the system as it develops.

At the time of writing, over 270 cryptocurrency exchanges exist (see `coinmarketcap.com`). Typically, an exchange operates double auctions with bids and asks, and charges a commission on trades (see, e.g., Böhme, Christin, Edelman, and Moore, 2015). Trades on an exchange are generally settled off-chain. The exchange simply debits the paying member's account and credits the receiver, without recording anything on the blockchain. Off-chain settlement improves delivery times and eliminates fees, at the cost of delaying finality and creating counterparty credit risk between the receiving member and the exchange. But a speculator who wishes to move cryptocurrency off an exchange — for example, to a wallet or another exchanges — must do so via the blockchain.

2.2 *Cryptocurrencies as money*

Cryptocurrency has no intrinsic or fundamental value and does not generate any cash flows. Like other monetary assets without a fundamental value such as token currency, the long-term value of cryptocurrency depends on the extent to which it is used as a medium of payment.[11]

The technology behind cryptocurrency may make it superior to other forms of money as a means of payment, at least for some users. The original motivation behind the development of Bitcoin was to create a decentralized currency that avoids dependence on monetary authorities or commercial banks for the verification of transactions (Nakamoto, 2009). Such an asset allows for transactions to be made over the Internet anonymously and privately, just as notes and coins allow in the offline world. The demand for monetary privacy is often associated with criminal or illicit activity, but legitimate users may require it too. For example, privacy can protect users from fraud and spam mail (Bech and Garratt, 2017). Markets with decentralized money may be more complete, as an individual money issuer cannot prohibit access (Pagnotta, 2018).

Other potential advantages of cryptocurrencies are the lack of intermediary fees (Athey et al., 2016); the record-keeping advantages of blockchain (Fernández-Villaverde, 2018); a superior convenience yield (Cochrane, 2018); and the ability of coin holders to participate in the crypto economy, for example, writing smart contracts, investing in ICOs, and trading on cryptocurrency exchanges that do not accept fiat currency (e.g. Sockin and Xiong, 2018). My model is agnostic about precisely why agents may find cryptocurrency a superior means of payment. Any of the features listed here would suffice.

3. MODEL SETUP

I present a model in which the price of a cryptocurrency is endogenously determined by the extent to which it is used as a means of payment. There is a large number of technologically adept households, who can choose to buy a consumption good using either cryptocurrency, which I call 'crypto' for brevity, or a conventional currency, which I refer to as 'cash'. Crypto has technological

[11] See Kiyotaki and Wright (1989) for a model of intrinsically useless monetary assets. I assume here that speculative bubbles cannot be maintained for an indefinite period.

features that make it potentially superior to cash as a means of payment. The technology in my model can be readily interpreted as delivering any of the other potential benefits listed in Section 2.2. There is also a number of speculators, who can profit from trading crypto. Speculators do not obtain the households' non-pecuniary payoff from using it, but instead use their private information to trade profitably against uninformed noise traders. In Section 5, I examine an extension where households receive imperfect signals about the strength of the technology.

Unlike in conventional trading models, speculation is not driven by news about a fundamental value, because crypto has none in this model. Instead, speculation is driven by beliefs about the actions of households, which then affect the value of crypto. However, as speculation requires blockchain space, it can reduce the value of crypto to households. This novel feedback effect is the key insight of my paper.

3.1 *Households and speculators*

There are three periods, labeled T_0, T_1 and T_2. At T_0, all agents are born and take decisions. Consumption occurs at times T_1 and T_2, and then the game ends. There are three assets in the economy: crypto, cash, and a consumption good, which also serves as a numéraire. Crypto and cash are monetary assets that have no consumption value, but can be exchanged for consumption goods at T_1 or T_2.

At time T_0, a unit mass of *households* and a mass $M \geq 0$ of *speculators* is born. All agents are risk-neutral. Each agent has access to a large endowment of crypto and cash, and seeks to maximize her utility from consumption over the two periods, T_1 and T_2. Agents discount over time, so that consumption at the later period T_2 is subject to a discount factor $\rho \in (0, 1)$.

Households aim to stagger consumption over time in the following way: each prefers to consume no more than one unit of the consumption good at T_1, while any amount can be consumed at T_2. Given consumption of $c_1, c_2 \geq 0$ units of consumption good at times T_1, T_2 respectively, a household's total utility from consumption is:

$$u_H(c_1, c_2) \;=\; \min\{c_1, 1\} + \rho c_2. \tag{1}$$

At T_0, each household can choose whether to use crypto or cash to purchase a unit of consumption good for delivery at T_1. She then uses the remainder of her wealth to consume at T_2.

Speculators have a different objective. At T_0, each speculator has an opportunity to place a market order on an exchange for one unit of crypto. He then uses all of his wealth to purchase consumption goods. A speculator's utility is simply equal to the amount of consumption goods he is able to acquire, discounted over time. Given consumption of $c_1, c_2 \geq 0$ at times T_1, T_2 respectively, a speculator's payoff is:

$$u_S(c_1, c_2) \;=\; c_1 + \rho c_2. \tag{2}$$

The restriction on a household's early consumption given in Equation (1) makes her choice meaningful. If a household could consume unlimited amounts at T_1, it would clearly be optimal to spend her entire endowment of crypto and cash immediately, and there would be no strategic choice to make. For a speculator, strategic choices are based on trading decisions, not consumption timing, so such a restriction is not necessary. For simplicity, I allow speculators to consume freely.[12]

Household i's decision about her means of payment is denoted $y_i \in \{0, 1\}$, where $y_i = 0$ if she pays in cash, and $y_i = 1$ if she pays in crypto. Define y to be the total mass of households that use crypto:

$$y \;=\; \int_0^1 y_i \;\mathrm{d}i. \tag{3}$$

At T_1, total crypto usage y is publicly revealed.[13]

Definition 1 (Crypto payments technology). *Crypto embeds a technology that makes it potentially superior to cash as a means of payment for households. The strength of this technology is a real-valued random variable R, drawn by nature at the beginning of the game from a distribution function $B(R)$ with positive measure over the whole of $\mathbb{R}$. $B(R)$ is continuous and strictly increasing in R. The value of R is revealed to all households and speculators at T_0. A household that uses crypto earns a non-monetary payoff $Rg(y)$, where $g(y) > 0$ is strictly increasing in $y \in [0, 1]$, in*

[12] Dang, Gorton, Holmström, and Ordoñez (2017) use a similar utility function to my households. Imposing an early consumption constraint on speculators would not affect their optimal trading decisions, so all of the results in the model will still go through. The main difference would be that speculators may pay lower mining fees.

[13] I follow the literature in assuming that y is well-defined under Lebesgue integration. This is not an innocuous assumption, as the set $\{i : y_i = 1\}$ is not guaranteed to be Lebesgue-measurable. See Judd (1985) and Uhlig (1996) for an explanation of the problem and possible remedies.

addition to the consumption payoff in Equation (1).

The non-monetary payoff $Rg(y)$ is the utility of using crypto as a means of payment, relative to cash. This payoff consists of two components. First, the strength of the technology R reflects the technological superiority of crypto relative to cash as a means of payment, as described in Section 2.2. For example, crypto may have a higher convenience yield than cash, or allow greater privacy when making payments.

Second, for any household, the benefit from using crypto is higher when it is used by a greater number of other households y. The function $g(y)$ can be thought of as the strength of *network effects*. A steeper function $g(y)$ means stronger strategic complementarities between households. These strategic complementarities tend to arise naturally in monetary models, because a monetary instrument is more attractive when other agents use it too.[14]

Crypto has no underlying cash flows or intrinsic value. Its real value is given by a function $v(y)$; that is, it can be used to purchase consumption goods at a rate of $v(y)$ units of consumption good per unit of crypto. This value is endogenously determined by the number of households y who use it at T_1, and is strictly increasing in y, with $v(0) = 0$ and $v(1) = V > 0$. The realization of $v(y)$ becomes publicly known at T_1, when y is revealed.[15] The value of cash is normalized to 1; i.e. one unit of the consumption good always costs one unit of cash. This is justified by the assumed existence of a central bank that is able to fix the value of cash in real terms.

Unlike households, speculators do not derive any non-pecuniary benefit from paying with crypto. For speculators, the crypto technology has no intrinsic utility. Instead, each speculator seeks to maximize trading gains, based on his observation of the strength of the crypto technology R at T_0. He can choose to place a buy or sell order for one unit of crypto, or not to trade at all. Speculator j's order is denoted $x_j \in \{-1, 0, 1\}$, representing a sell order, no order, and a buy order respectively. The limit on trade size is simply to prevent speculators from placing arbitrarily large trades.[16]

[14]See, for example, Kiyotaki and Wright (1989). Other network effects may exist for cryptocurrencies — for example, Pagnotta (2018) argues that greater usage incentivizes mining, which helps secure the network and further boosts its value. For simplicity, in this paper $g(y)$ is exogenously given rather than micro-founded.

[15]My model is agnostic about the functional form of $v(y)$, so long as it is an increasing function. For example, Fisher's equation of exchange implies a linear relationship (Fisher, 1911). Network models would tend to predict a convex relationship (Cong, Li, and Wang, 2018). The transactions demand for money theory predicts a square-root relationship between money usage and demand (Baumol, 1952; Tobin, 1956).

[16]This is consistent with papers such as Glosten and Milgrom (1985). Because the focus of this paper is on the

Prices in the market are set by a market maker.[17] The market maker has large endowments of both crypto and cash, and balances the crypto market by absorbing excess demand. She is subject to competitive pressure, due to a free entry condition, that ensures she makes zero expected profits. The market maker does not receive any signal about R, but she can observe the total order flow $z = x + u$, where:

$$x = \int_0^M x_j \ \mathrm{d}j \tag{4}$$

is the total size of the informed order flow and u is a random noise trading term, realized at T_0 and independent of the total informed order x.[18] Noise trading follows a uniform distribution $u \sim U[-\ell, \ell]$, where $\ell > M$ is a liquidity parameter. The greater the value of ℓ, the noisier the market maker's signal, and so the better able speculators are to disguise their private information. The market maker sets a price $p(z)$ equal to the posterior mean of the value of crypto, conditional on her information z. In the context of this model, noise traders can be interpreted as crypto holders who sell because they need to raise cash immediately (for example, to pay a counterparty that will not accept crypto, such as a tax authority). Alternatively, they may be interpreted as traders who wish to buy regardless of the current price, because they anticipate that crypto may be significantly more expensive in future and so wish to hedge against that risk.[19]

The distinction between households and speculators is a modeling choice designed to separate the monetary and speculative motives for usage, so the impact of speculation can be examined by varying the number of speculators M. The model can easily be adjusted to allow households to speculate, without fundamentally changing the results. A household that observes a high value of R would use crypto to make her payment and, believing other households are also using crypto, would choose to buy more. A household that observes a low value would use cash, and sell crypto.

effect of the blockchain structure and mining fees, rather than market microstructure, the trading environment is kept deliberately simple. There already exists an extensive literature around order sizes and their effect on pricing and liquidity; see Foucault, Pagano, and Roell (2013) for an overview.

[17] Most cryptocurrency exchanges do not have designated market makers, but many do provide monetary incentives to liquidity providers. My model abstracts from this, assuming a simple free entry model of market-making.

[18] Again, I assume x is well-defined under Lebesgue integration. See footnote 13.

[19] Many in the cryptocurrency trading community subscribe to the philosophy of HODL ("hold on for dear life"): one should not sell even when the price is falling, because eventually cryptocurrency will be widely used as money and much more valuable than it is now. As their motives are long-term, they do not require urgent settlement. Yet another way to rationalize the market maker's signal noise is via market fragmentation (Makarov and Schoar, 2019). The order flow on one exchange may represent only a small amount of total trading across the market, meaning an imperfect signal. Under this interpretation, the market maker would lose money to the informed speculators, and would require some kind of subsidy to be willing to continue business.

As each household is infinitesimal, she cannot strategically influence the price.

3.2 *Blockchain settlement*

The payoffs of both households and speculators depend on the timing of their consumption. This is formalized through the concept of a ledger.

Definition 2 (Ledger). *A ledger is a record of all transactions settled in a given monetary medium. There are two ledgers, one associated with crypto (called the 'blockchain') and one with cash. A transaction must be recorded on the relevant ledger before a consumption good can be delivered.*

The cash ledger is updated instantaneously, so any good purchased at T_1 can be consumed immediately.[20] However, the crypto ledger — that is, the blockchain — has a finite capacity at T_1, denoted by the random variable N, so that only a measure N of crypto payments can be settled by T_1. At T_2, all remaining transactions are added to the blockchain.

Definition 3 (Mempool). *The mempool is the set of all crypto transactions that are attempted at T_0. A household i has a transaction in the mempool if $y_i = 1$. A speculator j has a transaction in the mempool if $x_j = 1$.*

Each crypto transaction is assumed to take up the same amount of blockchain space (see footnote 9). If the mempool has measure greater than the blockchain capacity N, then some crypto transactions are not added to blockchain until T_2. These agents' consumption is delayed. If a household uses crypto and learns at T_1 that her payment will not be delivered, I assume there is not enough time to change her mind, make a cash payment, and have the good delivered by T_1. Therefore, once an agent chooses an action at T_0, she is committed.

Blockchain capacity is not public information at T_0, so a household faces greater uncertainty about consumption timing when she uses crypto than when she uses cash. She trades this uncertainty off against the potential benefit from the superior technology. The realization of blockchain

[20] The cash ledger is maintained by a monetary authority or commercial bank who can verify transactions and update the ledger without delay. Alternatively, if cash consists of physical tokens (e.g., notes and coins, or commodity money), then the ledger can be conceptualized as the physical allocation of tokens across agents, so delivery occurs as soon as tokens change hands.

capacity does not directly affect the long-term value of crypto $v(y)$, which depends on the total number of households y who use crypto, not on when consumption occurs.

Trades are settled across exchange accounts, and so do not need to be recorded on the blockchain. But any trading gain from buying crypto can be crystallized only once the newly purchased crypto is used to buy consumption goods. To make such a purchase, the speculator must move the crypto via the blockchain, just like a household. If his transaction is not added to the blockchain at T_1, then his consumption is delayed to T_2, and his payoff is discounted by a factor ρ. Sell orders are more straightforward. Each speculator is assumed to already have his crypto placed in an account at the exchange, so it can be sold and his account credited with cash without requiring blockchain space. Any buyer may, of course, encounter problems in trying to realize the trading gain, and that will be reflected in the price paid.

Blockchain capacity is denoted by N and is governed by a parameter λ, called the block rate.

Definition 4 (Block rate). *For a given λ, the block rate is a parameter $\lambda \in \mathbb{R}$. The blockchain capacity N available during period T_1 has cumulative distribution function $Z_\lambda(n)$ with support on $n \in [0, \infty)$, and the following properties:*

1. ***Feasibility of zero blockchain capacity:*** *$Z_\lambda(0) > 0$.*
2. ***Monotonicity and continuity in*** *n: For any $\lambda \in \mathbb{R}$, $Z_\lambda(n)$ is continuously differentiable and strictly increasing over $n \in [0, \infty)$. This implies the existence of a well-defined inverse function $Z_\lambda^{-1} : [Z_\lambda(0), Z_\lambda(1)] \to [0, \infty)$.*
3. ***First-order stochastic dominance in*** *λ: For any $n \in [0, \infty)$, $Z_\lambda(n)$ is strictly decreasing in λ.*

Definition 4 provides a realistic description of block capacity. Bitcoin blocks, for example, arrive approximately as a Poisson process (Nakamoto, 2008) so, in any finite period of time, there is a non-zero probability that no new block is created. This is ensured by the first property $Z_\lambda(0) > 0$, which implies a point mass at $N = 0$. The second property captures the fact that payments vary in size according to exogenous factors (see footnote 9), and ensures that a household always benefits from any marginal improvement in her priority. The third property ensures that high values of the

block rate λ tend to imply high blockchain capacity N. This makes the block rate λ a key variable of interest in the model, as it parameterizes the blockchain settlement constraint.

I impose an additional condition on the relationship between blockchain capacity $Z_\lambda(n)$ and network effects $g(y)$. Assumption 1 states that, as households switch from using cash to crypto and speculators switch from selling to buying, the benefit of an increase in network strength $g(1)/g(0)$ is at least as great as the increase in blockchain congestion $Z_\lambda(1+M)/Z_\lambda(0)$. This means, on average, the strategic complementarities between crypto users exceed the strategic substitutes.

Assumption 1 (Strategic complementarities stronger than strategic substitutes).

$$\frac{Z_\lambda(0)}{Z_\lambda(1+M)} \geq \frac{g(0)}{g(1)}. \tag{5}$$

An agent can hedge against the risk of a low realization of blockchain capacity N by offering a mining fee when she submits her crypto payment to the mempool. Her payment is then prioritized over any other crypto payment with a lower fee.

Definition 5 (Mining fees). *A fee $f \geq 0$ is an additional amount of crypto attached by an agent to a payment at the time it is submitted to the mempool. The fee must be paid whether or not the transaction is added to the blockchain at T_1.*

When creating a new block, miners always select the N mempool transactions that have the largest fees attached. If two or more payments have equal fees, priority is assigned at random. As miners' actions are trivial, it is not necessary to model them explicitly as strategic agents.

Fees are denoted in units of crypto and must be paid in crypto. Negative fees are not possible, but there is no upper limit. Unconfirmed transactions in the mempool cannot be canceled once submitted, so the fee is forfeit regardless of the outcome.[21]

A speculator's fee is financed from his buy order, and so reduces his potential trading gains.[22]

[21] As explained in Section 2.1, a household is able to cancel her payment but cannot recover the fee. She would never do this, because by assumption she cannot change her mind once N is realized. A model with an alternative technology that allows fees to be cancellable would not have qualitatively different findings from this model, though payoffs would certainly be higher.

[22] Alternatively, a speculator could finance the fee from his endowment, but it is straightforward to see that would never be optimal. Paying a fee f from the order means there is an amount $1-f$ subject to blockchain delivery risk. Paying it from the endowment means the full amount 1 is subject to this risk, making the speculator worse off.

Because of the cost of fees and the risk of settlement delay, the expected value of a unit of crypto held at the exchange lies somewhere betwen $v(y)$ and $\rho v(y)$. It is useful to distinguish between two notions of value: crypto held on the exchange and crypto held off it.

Definition 6 (On-exchange value of crypto). *The on-exchange value of crypto is the expected utility associated with holding one unit of crypto at the exchange. Given a fee f_j, expected utility is:*

$$\hat{K}(f_j; R) \;=\; (1-f_j)\mathbb{E}\Big[v(y)\Big(\mathbb{1}\{\textit{delivered by } T_1\} + \rho\mathbb{1}\{\textit{not delivered by } T_1\}\Big) \;\Big|\; R, f_j\Big], \quad (6)$$

and the on-exchange value is $K(R) = \max_{f_j \geq 0} \hat{K}(f_j; R)$. The off-exchange value of crypto is $v(y)$.

The market maker uses a pricing rule $p : \mathbb{R} \to [0, \infty)$ based on her beliefs about the on-exchange value, given the information contained in the order flow z:

$$p(z) \;=\; \mathbb{E}\Big[K(R)\Big|z\Big]. \quad (7)$$

We can now write down agents' expected payoffs. A household's total expected payoff if she uses crypto, given R and a choice of fee f_i, is:

$$\mathbb{E}\Big[Rg(y) + \mathbb{1}\{\text{delivery}\} + \rho\mathbb{1}\{\text{non-delivery}\} - \rho v(y) f_i - \rho \;\Big|\; R, f_i\Big]. \quad (8)$$

The first term in Equation (8) is household i's expected non-pecuniary benefit from using crypto. The second term is the consumption payoff when the payment settles at T_1 and the household consumes early. The third term is the consumption payoff when the payment does not settle at T_1 and the household consumes late. The fourth term is the cost of the fee, in terms of foregone consumption at T_2. A unit of crypto paid as a fee to a miner means the household must forego $v(y)$ units of consumption at T_2.

The final term $(-\rho)$ in Equation (8) is the opportunity cost of making the payment. Because y is public knowledge at T_1, the value $v(y)$ of crypto is publicly known. The household agrees with the seller of the consumption good that a fair price is $1/v(y)$ units of crypto, which is worth 1 in

real terms. Making the payment thus means one unit less consumed at T_2, which costs ρ in real terms.[23]

Using cash would deliver the same payoff as crypto if there were no non-pecuniary bonus, no fee, and certain delivery by T_1. The payoff from cash is thus $1-\rho$. Given a household's signal R_i and fee f_i, I write $\pi_H(f_i; R_i)$ for the difference between her expected payoff from using crypto (given in Equation (8)), and that from using cash $(1-\rho)$:

$$\pi_H(f_i; R) \;=\; Rg(y) \;-\; (1-\rho)\mathbb{P}\Big[\text{non-delivery}\Big|R, f_i\Big] \;-\; \rho f_i v(y). \tag{9}$$

The first term in Equation (9) is the household's non-pecuniary benefit from using crypto. The second term is the expected opportunity cost of delayed consumption. The third term is the opportunity cost of paying a fee, in terms of foregone consumption. Note that a household's choice of fee f_i affects the probability of delivery, but does not affect y, which is a deterministic function of R given beliefs about other households' strategies.

A speculator's expected payoff is simply:

$$\pi_S(x_j, f_j; R) \;=\; x_j\Big(\hat{K}(f_j; R) - \mathbb{E}[p(z)|R]\Big). \tag{10}$$

The payoff π_S is defined relative to the benchmark of submitting no order; in other words, the payoff from not submitting an order is normalized to zero.

3.3 *Equilibrium concept*

The events over the three time periods as follows:

1. At time T_0, the strength of the technology $R \sim B(R)$ is determined by nature. Each agent observes R. Each household i chooses a payment medium $y_i \in \{0, 1\}$ and, if $y_i = 1$, a fee $f_i \geq 0$. Each speculator j chooses an order $x_j \in \{-1, 0, 1\}$ and, if $x_j = 1$, a fee $f_j \geq 0$. The market maker observes total order flow $z = x + u$ and sets the price $p(z)$.

[23] Strictly speaking, this argument may not be valid when $v(y) = 0$, so a problem could arise in the event that $y = 0$ and a countable number of households use crypto. But this event can never occur, as I assume households strictly prefer to use cash if it yields exactly the same expected payoff as crypto (Definition 7).

2. At time T_1, y is publicly revealed and the long-term value of crypto $v(y)$ is determined. The amount of block space $N \sim Z_\lambda(n)$ is determined by nature. The N crypto payments that have the highest fees attached are added to the ledger, as are all cash payments. Any household that had her payment added to the ledger can consume. Any speculator that placed a buy order and had his payment added to the ledger can exchange it for consumption goods.
3. At time T_2, all remaining crypto payments are added to the ledger. Consumption occurs and the game ends.

An equilibrium is defined as follows.

Definition 7 (Symmetric equilibrium). *A household's strategy is a pair of decision functions* $\eta_H : \mathbb{R} \to [0,1]$ *and* $\phi_H : [0,\infty) \times \mathbb{R} \to [0,1]$. *A speculator's strategy is a pair* $\eta_S : \{-1,0,1\} \times \mathbb{R} \to [0,1]$ *and* $\phi_S : [0,\infty) \times \mathbb{R} \to [0,1]$. $\eta_S(x_j; R)$ *describes a distribution function on* $\{-1,0,1\}$ *given* R, *while* $\phi_H(f; R)$ *and* $\phi_S(f; R)$ *describe distribution functions on* f *given* R. *An equilibrium is a quintuple* $(\eta_H, \phi_H, \eta_S, \phi_S, p)$ *such that:*

- *if a household believes all other households use strategies* (η_H, ϕ_H), *all speculators use strategies* (η_S, ϕ_S), *and the market maker has a pricing rule* $p(z)$, *then her optimal strategy is* (η_H, ϕ_H);
- *if a speculator believes all households use strategies* (η_H, ϕ_H), *all other speculators use strategies* (η_S, ϕ_S), *and the market maker has a pricing rule* $p(z)$, *then his optimal strategy is* (η_S, ϕ_S);
- *the pricing rule* $p(z)$ *satisfies Equation* (7).

If using crypto or cash yield the same expected payoff for a household, she chooses to use cash. If buying or selling yield the same expected payoff for a speculator, he chooses to sell.

The solution concept is Bayesian Nash equilibrium. Because all households are identical to one another, and likewise for speculators, attention is restricted to symmetric equilibria. The tie-breaking criteria are imposed to simplify the results; nothing substantial hinges on them.[24]

[24] The set of R where agents are indifferent between different actions will have measure zero. Because a speculator has an information advantage over the noise traders, he can always trade profitably, and so will never choose not to trade. Therefore, there is no need to specify which action he would choose if not trading (i.e. $x_j = 0$) earns the same expected payoff as a trading action.

Households have strategic complementarities with respect to each others' actions, so in general there can be multiple equilibria. It is useful to impose a refinement that yields a unique equilibrium for each R, so that the model can be used to make predictive statements about prices, trading, and blockchain usage. I use payoff-dominance; in Section 5, I consider an alternative refinement, in which the game is perturbed and embedded in a game of incomplete information.

Assumption 2 (Payoff-dominance for households). *For any R, if there are multiple equilibria, agents coordinate on the one that maximizes* $\max_{f \geq 0} \pi_H(f; R)$.

Payoff-dominance is a common refinement used for coordination games with multiple equilibria (see, for example, Carlsson and van Damme, 1991). It is often justified by assuming households can engage in pre-game communication, or even tacit bargaining, that allows them to coordinate on the equilibrium that is jointly optimal for them. Pre-game communication by speculators would not cause households to deviate from this equilibrium, because no commitment by speculators is credible. For example, if a group of speculators promised not to place buy orders, in order to encourage households to use crypto more often, there would be no incentive for those speculators to stick to that promise. In other words, in any subgame perfect equilibrium with an initial round of communication, the speculators' messages will be treated as babble.

4. RESULTS

4.1 *Equilibrium*

I start by proving the following two simple but useful results. Lemma 1 states that, in any pure strategy equilibrium, households and speculators have matching strategies. Speculators buy if and only if households use crypto, and sell if and only if households use cash. Lemma 2 provides some auxiliary results for fee strategies.

Lemma 1 (Households and speculators employ the same non-fee strategies). *For any R, exactly one of the following is true: either $\eta_H(R) = 1$ and $\eta_S(1; R) = 1$, or $\eta_H(R) = 0$ and $\eta_S(-1; R) = 1$. No other outcome is possible, and each of these two events occurs with non-zero*

probability. Conditional on $\eta_H(R) = 1$ and $\eta_S(1; R) = 1$, neither agents' fee strategies nor $K(R)$ depend on R.

The proof is in the Appendix (Section 7.1). Households use crypto when R is high and use cash when R is low, so the off-exchange value of crypto $v(y)$ is uncertain. The market maker is strictly less informed than speculators about the on-exchange value, and so trading is always profitable. If households use cash, the value of crypto is low, and speculators sell. Conversely, if households use crypto, it is valuable, and speculators buy. The marginal benefit or cost of fees depends on y but does not depend directly on R so, conditional on $y = 1$, agents' strategies do not depend on R.

Lemma 2 (Fee strategies). *For any R, let $\mathcal{F}_{\mathcal{H}}$ and $\mathcal{F}_{\mathcal{S}}$ be the supports of households' and speculators' fee strategies respectively. Suppose the union of these sets $\mathcal{F}_{\mathcal{H}} \cup \mathcal{F}_{\mathcal{S}}$ is non-empty. Then it is bounded with infimum equal to zero, and essentially convex; i.e. it differs from the open interval defined by its boundaries by a set of measure zero. Neither households nor speculators employ strategies with point masses; i.e. for any R, both $\phi_H(f; R)$ and $\phi_S(f; R)$ are continuous in f.*

The proof is in the Appendix (Section 7.2). The Lemma seems technical but is intuitive. The smallest fee paid must be zero, because there is no reason to pay to have the lowest priority. There are no point masses because, if an agent believes a mass of other agents all pay the same fee, then it would be strictly better to pay slightly more. There cannot be an interval missing within the support, because then it cannot be optimal to play a fee at the supremum of that interval.

Armed with Lemmas 1 and 2, the main result follows.

Proposition 1 (Equilibrium with financial market). *There is a unique equilibrium in pure strategies. All agents play a switching strategy with a threshold R^*:*

- *If $R \leq R^*$, then $\eta_H(R) = 0$ and $\eta_S(-1; R) = 1$.*
- *If $R > R^*$, then $\eta_H(R) = 1$ and $\eta_S(1; R) = 1$.*

The threshold R^*, on-exchange value of crypto $K(R)$, and fee strategies are given by three mutually exclusive cases:

1. *If* $\rho V \geq 1 + (1-\rho)(Z_\lambda(1+M) - Z_\lambda(M) - Z_\lambda(0))$*, the threshold is given by:*

$$R^* \;=\; (1-\rho)\frac{Z_\lambda(1+M)}{g(1)}. \tag{11}$$

Households' fees are randomly chosen from an interval containing zero, and speculators' fees from an interval lying above the households' fee support. When $R > R^*$*, on-exchange value is given by:*

$$K \;=\; \Big(V - \frac{1-\rho}{\rho}\big(Z_\lambda(1+M) - Z_\lambda(M)\big)\Big)\Big(1 - (1-\rho)Z_\lambda(M)\Big). \tag{12}$$

2. *If* $\rho V \leq 1 - (1-\rho)Z_\lambda(1)$*, the threshold is:*

$$R^* \;=\; \frac{1-\rho}{g(1)}\Big(Z_\lambda(1) + \rho V\frac{Z_\lambda(1+M) - Z_\lambda(1)}{1-(1-\rho)Z_\lambda(1)}\Big). \tag{13}$$

Speculators' fees are randomly chosen from an interval containing zero, and households' fees from an interval lying above the speculators' fee support. When $R > R^*$*, on-exchange value is given by:*

$$K \;=\; V\Big(1 - (1-\rho)Z_\lambda(1+M)\Big). \tag{14}$$

3. *Otherwise,* R^* *is given by Equation* (11)*. The support of households' fees consists of a pair of disjoint intervals containing zero. The support of speculator's fees is nested between those intervals. When* $R > R^*$*, on-exchange value is given by:*

$$K \;=\; \Big(V - \frac{1-\rho}{\rho}\big(Z_\lambda(1+M) - Z_\lambda(h)\big)\Big)\Big(1 - (1-\rho)Z_\lambda(h)\Big), \tag{15}$$

where $h \in [0,1]$ *is the unique solution to:*

$$Z_\lambda(h+M) + Z_\lambda(h) \;=\; Z_\lambda(1+M) - \frac{\rho V - 1}{1-\rho}. \tag{16}$$

When $R \leq R^*$*, on-exchange value is zero. In all three cases,* R^* *is decreasing in the block rate* λ *and network effects* $g(1)$*, and increasing in the number of speculators* M*. The market maker sets*

price $p(z)$:

$$p(z) = \begin{cases} 0, & \text{if } z \leq -\ell + M, \\ (1 - B^*)K, & \text{if } -\ell + M < z < \ell - M, \\ K, & \text{if } z \geq \ell - M, \end{cases} \tag{17}$$

where $B^* = B(R^*)$ is the probability that the threshold is not exceeded.

The full proof in the Appendix (Section 7.3) provides explicit expressions for the fee functions.

Under payoff-dominance, switching strategies are households' unique best response to the speculators' strategies implied by Lemma 1, so a threshold equilibrium emerges.

A threshold equilibrium arises because, for given speculators' strategies, households' payoffs from using crypto are increasing in R. By Lemma 1, speculators' optimal strategies are determined purely by their beliefs about households' strategies. Therefore crypto usage is non-decreasing in R, and the unique payoff-dominant strategy is a switching strategy. If Assumption 1 did not hold, there would be values of R with no equilibrium in pure strategies. The model can be solved but, in general, threshold equilibria would not emerge, and there might be cases where higher R leads to less crypto usage, which is unintuitive.

The three cases described in Proposition 1 arise because the parameters affect how much households value crypto relative to speculators. When V is high, the real cost to a household of spending crypto on a mining fee is high, because more consumption is foregone at T_2. However, the value of V does not directly affect the speculators' payoffs, because a change to V affects both the trading gain and the price paid in equal proportion. Therefore, when V is high, speculators tend to be willing to pay higher fees than households (case 1), and when V is low the converse is true (case 2). Case 3 represents an intermediate case in which households randomize between paying lower and higher fees than speculators. In Equation (16), h is the proportion of households that pay higher fees than speculators, which is a decreasing function of V. When $h = 0$, we have case 1, and when $h = 1$, we have case 2.

4.2 *Prices and the crowding-out effect*

When $R > R^*$ and crypto is valuable, its on-exchange value K depends on the cost of moving it off-exchange to obtain consumption goods. This cost depends on speculators' beliefs about blockchain congestion and other users' fees. For example, when the discount factor ρ is low, the cost of late settlement is higher, and K is lower.[25]

A decrease in the block rate λ or an increase in the number of speculators M make the blockchain more congested. But the effect of this on K is not monotonic. This is because fees, in general, are not monotonic in congestion. To see why, note that as λ becomes very large, there is less competition for blockchain space, and so agents don't need to pay high fees. And, as $\lambda \to -\infty$, agents believe their crypto payments are unlikely to be settled early in any case, and so paying a fee is a waste. It is for intermediate values of λ that paying a fee is most worthwhile: blockchain capacity must be scarce enough that priority is worth paying for, but not so scarce that fees are a waste of money. The effect of changes in M are similarly nuanced.

Worse congestion (lower λ or higher M) affects the on-exchange value of crypto via two channels:

a. **Moneyness:** For a given level of fee, as congestion increases, speculators are more likely to have consumption delayed, and so the on-exchange value K falls.

b. **Household displacement:** As congestion increases, households believe that crypto payments are less likely to be settled early, and so they reduce their fees. This means speculators' payments are relatively more likely to settle early, and K increases.

The moneyness channel is a direct effect, and always exists. For the household displacement channel to operate, speculators must have priority over at least some households. This occurs if speculators are paying high fees relative to households; i.e. cases 1 and 3. When households pay higher fees than speculators (case 2), speculators cannot displace them. In this case, K is monotonically increasing in λ and decreasing in M, so congestion unambiguously reduces the on-exchange value of crypto.

There is a novel relationship between speculative demand and the price of crypto. The moneyness channel means an increase in informed demand M can reduce the price of crypto, contrary

[25] In the remainder of the paper, I abuse notation slightly and use K as shorthand to denote the on-exchange value of crypto conditional on $R > R^*$.

to our usual economic intuition. This is because speculative demand takes up blockchain space and reduces transactional demand. I call this novel result the **crowding-out effect**. This effect runs contrary to the usual intuition in the market microstructure literature, where the asset has an exogenously-determined fundamental value, and the price is monotonically increasing in the market maker's observed order flow (e.g. Kyle, 1985; Glosten and Milgrom, 1985) For a cryptocurrency, in contrast, the value depends on monetary usage, which is itself affected by speculative behavior. Price formation for cryptocurrencies is therefore qualitatively different from that for standard assets, and even from that for other forms of money.

There are two distinct characteristics of cryptocurrency that give rise to the crowding-out effect. First, the monetary nature of a cryptocurrency means its value is endogenously determined by the amount of usage. Second, the blockchain infrastructure causes speculative activity to have a negative impact on the value. Together, these features generate an interaction between speculative activity and price that is absent from traditional assets.

To illustrate how the crowding-out effect affects price formation, consider the following small change to the model. Let the number of speculators $M \in [0, \infty)$ be a random variable. At T_0, the value of M is realized by nature and observed by all agents, including the market maker. They then choose optimal strategies as described in Proposition 1. To simplify things, take $\ell \to M$, so that the market maker can perfectly infer informed demand x, and assume $V \leq 1$, so that we are in case 2 described in Proposition 1.

The market maker sets the following price as a function of informed demand x:

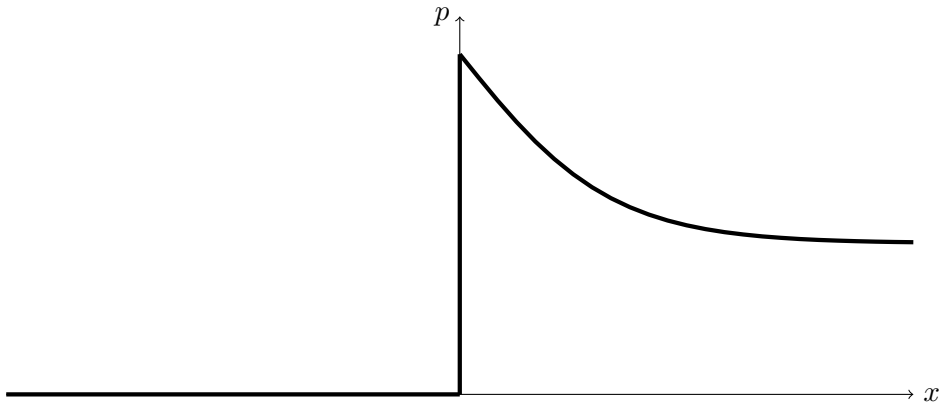
$$p(x) = \begin{cases} 0, & \text{if } x < 0, \\ V(1 - B^*)(1 - (1 - \rho)Z_\lambda(1)), & \text{if } x = 0, \\ V(1 - (1 - \rho)Z_\lambda(1 + x)), & \text{if } x > 0. \end{cases} \tag{18}$$

When $x < 0$, the market maker infers $R \leq R^*$ and crypto has value 0. When $x > 0$, she infers crypto is valuable and sets a price equal to the on-exchange value. The case $x = 0$ occurs if and only if $M = 0$, in which case the market maker uses the prior mean of the price.

Figure 2 illustrates the pricing function for a given level of speculative demand x. The price is

strictly increasing only at $x = 0$, and decreases over $x > 0$. As $x \to \infty$, it asymptotes to ρV, which is the lowest possible value of K.

Figure 2. Illustration of downward-sloping pricing function. Excess market demand is x, and market maker's price is p. Higher speculative demand can crowd out monetary usage of crypto and reduce the price.



The graph is downward-sloping for $x > 0$ because of the moneyness channel. A larger number of speculators congests the blockchain, and making it harder to move crypto off-chain. This reduces the on-exchange value. Limited blockchain capacity is crucial to this result. If blockchain capacity were unlimited (i.e. if $Z_\lambda(n) = 0$ for all finite n) then the on-exchange value would always be equal to V, and the pricing function would be non-decreasing everywhere.

In cases 1 and 3, the pricing function can be locally increasing over $x > 0$, because of the household displacement channel. But it will certainly be decreasing asymptotically. In both cases, as $x \to \infty$, $K(R) \to V(1 - (1 - \rho)Z_\lambda(1 + x))$ for all $R > R^*$. This is the same price as in case 2, so the asymptotic behavior is the same.

If noise trading were higher ($\ell > M$), the market maker would no longer be able to perfectly discern whether $R > R^*$ or $R \leq R^*$. A plot of M against expected price would resemble a smoothed version of Figure 2. The function could increase for low positive values of x, but would still be decreasing asymptotically.

4.3 *Comparative statics of the threshold and price volatility*

Proposition 1 establishes that the threshold for crypto usage R^* is always decreasing in the block rate λ and increasing in the number of speculators M. When λ is low or M high, blockchain

congestion is worse, and so households either have to pay high fees or endure late consumption. They therefore require a larger non-pecuniary payoff $Rg(1)$, and thus a higher realization of R, to be willing to use crypto.

This negative feedback channel from the financial market to households is novel and, to my knowledge, does not occur with other assets. It may explain why crypto has been slow to be adopted as money: a glut of speculative activity (higher M) has crowded out monetary usage (higher R^*).

The threshold equilibrium outcome means we can think of an investment in crypto as a lottery with two outcomes. Consider the limit $\ell \to M$. With probability one, crypto takes one of only two values, 0 or K. The probability that it is zero is $B^* = B(R^*)$, so a fair price for playing this lottery is $(1-B^*)K$, which is the expected value of a unit of crypto before R is observed. The gross return on a lottery ticket is then either zero (with probability B^*) or $1/(1-B^*)$. The volatility of these returns is increasing in B^*: the riskiness of a fair-priced lottery with high odds is higher than that of a fair-priced lottery with low odds. When $\ell > M$, returns are less volatile but the same intuition applies. To formalize this notion, I define price volatility to be the standard deviation of the gross return on a unit of crypto.

Definition 8 (Price volatility). *Price volatility is:*

$$\Gamma \;:=\; \frac{\sqrt{\mathbb{V}[p(z)]}}{\mathbb{E}[p(z)]}. \tag{19}$$

This is well-defined, so long as $\mathbb{P}[p(z)=0] < 1$.

The case $\mathbb{P}[p(z)=0] = 1$ is rather trivial, since it implies $y = 0$ and crypto is never used.

Proposition 2 (Price volatility increases as block rate falls). *Given a threshold equilibrium with threshold* R^**, price volatility* Γ *is:*

$$\Gamma \;=\; \sqrt{\frac{M}{\ell}\Big(\frac{B^*}{1-B^*}\Big)}. \tag{20}$$

where $B^* = B(R^*)$*, the probability that* R *is below the threshold. When* $0 < B^* < 1$*, volatility is*

strictly increasing in the threshold R^*, and is therefore decreasing in block rate λ and increasing in the number of speculators M.

The proof is in the Appendix (Section 7.4).

Limited blockchain capacity creates a volatility channel that we do not see with traditional assets. As the block rate λ falls, volatility rises. This is because the threshold for crypto usage rises, and so the lottery becomes a riskier gamble. The same occurs if the number of speculators M rises. Again, the result relies on two distinctive features of cryptocurrency: a value that is determined by the extent of monetary usage rather than a fundamental, and limited settlement space due to finite blockchain capacity.

Proposition 2 can explain why price volatility is so much higher for cryptocurrencies than for other assets, as shown in Table 1. While alternative explanations — such as a fixed supply schedule, market illiquidity, or high levels of uncertainty — may contribute, they do not relate to the specific technological characteristics of cryptocurrency, and so cannot explain why other assets tend to have much lower levels of volatility.

A benchmark non-blockchain asset can be viewed as one with infinite blockchain capacity ($Z_\lambda(n) = 0$ for all n), so its volatility is given by Equation (20) with $B^* = B(0)$. Assuming, as is likely, that markets believe that crypto is more likely to be worthless than valuable ($B^* > \frac{1}{2}$), then price volatility is convex in B^* and increases without limit as $B^* \to 1$. Thus, when congestion is severe, volatility can be orders of magnitude higher for cryptocurrencies than for other types of asset.

The relationship between volatility and congestion in Proposition 2 relies on the fact that $v(0) = 0$. This simply means that, if nobody uses crypto, it is worthless. That is a reasonable assertion in the case of cryptocurrency, which has no fundamental value beyond its usefulness as a means of payment, and does not generate cash flows. However, the volatility result may fail to hold for a blockchain token that represents a claim on a real asset, as some initial coin offerings (ICOs) do.[26]

The expression for price volatility contains a term $\sqrt{(M/\ell)} \in [0, 1]$. I call this the *illiquidity*

[26] To be precise, Proposition 2 holds so long as $(1 - B^*)V > B^* v(0)$, so a more general result can be easily established.

factor. When the illiquidity factor is close to 1, trading is more informative and the market maker's price is more sensitive to the market order. When the illiquidity factor is low, the price is less sensitive.[27] Illiquidity magnifies the effect of blockchain congestion on volatility, while liquidity mitigates it. Given the fragmented and unregulated trading landscape for cryptocurrencies (Makarov and Schoar, 2019), this effect can help explain high observed price volatility. Of course, illiquidity can boost volatility for other reasons not considered in this paper (e.g. Gandal et al., 2018), but this analysis suggests there is a novel channel between illiquidity and volatility in cryptocurrency markets that does not operate for other assets.

The definition of price volatility is, essentially, the inverse of the Sharpe ratio of a portfolio containing only crypto and cash. Proposition 2 might be taken to suggest that cryptocurrencies should have lower Sharpe ratios than that of other asset classes. The evidence is not clear on that. For example, Liu and Tsyvinski (2018) find that the Sharpe ratios of major cryptocurrencies are similar to those of stocks at a monthly frequency, but are higher at lower frequencies. This could be due to speculators updating their beliefs about the technology R over time. If they become more optimistic, then B^* falls and the Sharpe ratio rises. This dynamic cannot be captured in my static model.

Finally, we can define the volatility of the on- and off-exchange values:

$$\frac{\sqrt{\mathbb{V}[K(R)]}}{\mathbb{E}[K(R)]} = \sqrt{\frac{B^*}{1-B^*}} = \frac{\sqrt{\mathbb{V}[v(y)]}}{\mathbb{E}[v(y)]} \tag{21}$$

This is the volatility faced by a perfectly informed agent, and is equal to price volatility when $\ell = M$. As before, the volatility is decreasing in λ and increasing in M. This shows that the effect of congestion on volatility is not dependent on the microstructure — or even the existence — of a financial market. Even if there were only households ($M = 0$), the volatility of the crypto value would be still decreasing in the block rate λ.

[27] The illiquidity factor can be likened to Kyle's lambda, which similarly measures price impact using the ratio of informed to noise trading (Kyle, 1985).

4.4 *Welfare*

In this Section, I examine the conditions under which crypto adoption is optimal, and whether the equilibrium outcome achieves optimality. Welfare is defined to be aggregate utility in the economy. Fees have no direct impact on welfare, since they are simply a transfer of wealth from households and speculators to miners. Similarly, trading is a zero-sum game, because any profits made by speculators are exactly matched by losses borne by noise traders. Therefore welfare is equal to the aggregate payoff of all households before fees are paid. This can be interpreted as a measure of how well the households' chosen form of money works for society. It suggests the payoff-dominant allocation may differ from the socially optimal allocation.

Given a realization of technology strength R and equilibrium strategies, welfare is:

$$\hat{\Omega}(R) \;=\; y\Big(Rg(y) \;-\; (1-\rho)\mathbb{P}[\text{household's crypto payment does not settle at } T_1]\Big). \tag{22}$$

The first term in Equation (22) is households' aggregate non-pecuniary bonus from using crypto. The second term is the aggregate cost of settlement delays.

Proposition 3 (Welfare). *In equilibrium, when $R \leq R^*$, welfare is equal to zero. When $R > R^*$, welfare is equal to:*

$$\Omega(R;h) \;=\; Rg(1) - (1-\rho)\int_0^h Z_\lambda(n)\,dn - (1-\rho)\int_{h+M}^{1+M} Z_\lambda(n)\,dn, \tag{23}$$

where h is the proportion of households who pay higher fees than speculators. In case 1, $h = 0$; in case 2, $h = 1$; and in case 3, h is the unique solution to Equation (16)*.*

Welfare under the equilibrium allocation is increasing in the strength of the technology R, in network effects $g(1)$, and in h. It is non-increasing in value of crypto V.

The proof is in the Appendix (Section 7.5). The second term is the expected cost of waiting for the h households that pay higher fees than speculators, while the third term is the cost for the $1-h$ households that pay lower fees. As h is decreasing in V, the result follows.

Welfare is increasing in h: when more households are served before speculators, there is a greater

benefit to using crypto, and welfare is higher. Therefore, fees do affect welfare to the extent that they affect the relative priority of households and speculators.

Welfare is non-increasing in the value of crypto V. This is because high V makes fees more expensive for households, but not speculators. As V increases, households prefer to hoard crypto rather than spend it on fees. As a result, households become increasingly outbid by speculators, and welfare is lower. I call this propensity to hoard crypto, rather than use it for fees, the **digital gold effect**. Higher V makes households more inclined to view crypto as a store of value than as a medium of exchange. There is an apparent paradox: crypto is only valuable if it is used as a medium of exchange, but if it is valuable then households prefer to hoard it. This suggests that there may be a limit on the extent to which crypto will ever be used as a means of payment.

Welfare is sensitive to V only in case 3. In cases 1 and 2, households' fees are either entirely above speculators' or entirely below, so their priority relative to speculators is not sensitive to V. However, in case 2, expected welfare $\mathbb{E}[\Omega(R;1)]$ is decreasing in V, because the threshold for crypto usage R^* is increasing in V. This is again due to the digital gold effect. In case 2, households pay higher fees than speculators. When V increases, the real cost of these fees is higher, and welfare falls as a result.

Surprisingly, welfare can be decreasing in the block rate λ or increasing in the number of speculators M, because h is non-monotonic in these parameters. It might be expected that lower congestion would make households better off and thus improve welfare. But, in case 3, households can respond to worsening congestion by increasing fees, in order to outbid speculators and be served first. This increases h and so is welfare-positive.

Finally, I compare welfare under the equilibrium allocation to that chosen by a benevolent social planner. This provides a benchmark for the effect of congestion on welfare.

Definition 9 (First- and second-best). *For a given R, the first-best allocation is the number of crypto users $y \in [0,1]$ that maximizes welfare $\hat{\Omega}(R)$. The second-best allocation is the number of crypto users $y \in \{0,1\}$ that maximizes welfare.*

As trading brings no benefits to welfare, a benevolent social planner would clearly opt to prohibit

speculators from placing trades. Given R, the planner chooses y to maximize welfare:

$$\hat{\Omega}(y;R) \;=\; y\Big(Rg(y) - (1-\rho)Z_\lambda(y)\Big). \tag{24}$$

The value of y that maximizes welfare may lie in the interior $(0,1)$. Therefore an equilibrium in pure strategies may not, in general, deliver first-best. To assess the welfare properties of a threshold equilibrium, I use the second-best allocation as a benchmark. A social planner constrained to the second-best chooses $y=1$ if $\hat{\Omega}(1;R) > \hat{\Omega}(0;R)$, which is equivalent to:

$$R \;>\; (1-\rho)\frac{\int_0^1 Z_\lambda(n)\mathrm{d}n}{g(1)} \;:=\; R^*_{2B}. \tag{25}$$

The constrained social planner employs a threshold strategy, choosing $y=1$ if $R > R^*_{2B}$, and $y=0$ if $R \leq R^*_{2B}$. As with the thresholds obtained in Proposition 1, R^*_{2B} is decreasing in λ and $g(1)$.

Clearly $R^*_{2B} < R^*$, so households in the decentralized equilibrium strategy use crypto less often than is socially optimal. The social planner would prefer more crypto usage. This occurs because fees paid to miners are costly to households, but neutral for society. Households cannot coordinate with each other and agree to pay miners zero fees; there is always an incentive to deviate, pay a small positive fee, and achieve priority.[28] If the block rate λ becomes so large that $Z_\lambda(1) = 0$, or so small that $Z_\lambda(0) = 1$, then the motivation to pay for blockchain space falls to zero and the thresholds R^* and R^*_{2B} converge at $M = 0$.

The fee system is socially costly. Having to pay miners reduces households' incentives to take socially optimal actions. Society may be better off if blockchain space were simply allocated randomly. If that could be implemented at zero cost, the second-best could be achieved. However, a fee-based system could improve upon a random allocation if there were heterogeneity between households. Suppose, for example, households differed in their discount factors. Then households who value urgency would pay higher fees and be prioritized in the allocation of blockchain space. This may be more efficient than a random allocation, so long as mining fees are not too high.[29]

[28] Miners are not strategic, so there is no tacit bargaining mechanism by which households can be persuaded to take account of their interests. Therefore the payoff-dominant equilibrium is optimal for the households, but not for society at large.

[29] In addition, in a model where security is a concern, the fee-based system could produce higher welfare if it incentivized miners to secure the network.

4.5 *Endogenous speculators*

Until now, I have treated the number of speculators M as an exogenous parameter. In reality, the number of entrants to a market is a function of the cost of entry. Usually, economic theory predicts that a higher cost of entry means fewer entrants. However, in this model, the relationship is not monotonic, because entrants can actually make trading more profitable.

Suppose there is a large mass of uninformed speculators, who have no information about R. At T_0, each can choose to pay an upfront cost $\beta > 0$ to observe R and become informed. We can think of this as the price of acquiring a sufficiently good understanding of blockchain technology to understand whether the computer code underlying crypto makes it a good means of payment. A speculator who does not pay β, and thus does not observe R, will never trade, because he will be no more informed than the market maker. We can now think of M as the number of speculators who choose to pay β and become informed.

Proposition 4 (Endogenous entry). *Let $\beta > 0$ be the cost of entry to speculators. Then the equilibrium number of informed speculators $\hat{M}$ is a value of M satisfying:*

$$2\Big(1 - \frac{M}{\ell}\Big)B^*(1 - B^*)K \;\; = \;\; \beta, \tag{26}$$

where B^* and K are themselves functions of M, as described in Proposition 1. $\hat{M}$ can be locally increasing or decreasing in the cost of entry β, and in the number of noise traders ℓ.

The proof is in the Appendix (Section 7.6). The left-hand side of Equation (26) is a speculator's expected payoff from speculation. The terms $B^*(1 - B^*)$ and K can be increasing or decreasing in M, so the slope of $\hat{M}$ can be locally positive or negative with respect to any of the parameters. For example, suppose $B^* < \frac{1}{2}$, so that the market maker believes crypto is likely to be valuable. An increase in M reduces monetary usage of crypto, so the market maker becomes less certain about its value. This can make trading more profitable. And, if the household displacement effect described in Section 4.2 is sufficiently strong, then higher M can increase the on-exchange value of crypto K, raising trading profitability.

We can compare this to a similar asset that does not have a blockchain capacity constraint. Suppose $Z_\lambda(n) = 0$ for all finite n. Then the speculator's payoff is $2(1 - M/\ell)B_0(1 - B_0)V - \beta$, where $B_0 = B(0)$. This is everywhere decreasing in M and increasing in ℓ, and so $\hat{M}$ is decreasing in β and increasing in ℓ, as we might expect. For this non-blockchain asset, the amount of informed trading M affects profitability only by revealing private information to the market maker, and this channel is weaker when there is a high amount of noise trading (for example, Kyle, 1985). That channel is present in this model too, but may be dominated by other effects.

There is no limit to the number of potential solutions to Equation (26), so in some cases $\hat{M}$ may not be uniquely determined. This non-determinacy could contribute to the volatility of the price. Suppose, for example, that before the game starts the players know only β, and form a prior about M based on the multiple feasible solutions to Equation (26). Uncertainty about crypto usage and price will be greater in this scenario, relative to a benchmark in which the free entry condition has only one solution.

5. IMPERFECT INFORMATION

I now relax the assumption that agents observe perfect signals about the technology R. Instead, agents observe a private signal equal to R plus some error. I show that, as these errors become small, households employ a strategy arbitrarily close to a switching strategy, and greater congestion still leads to higher volatility.

Private signals can be rationalized as follows. The computer code behind the cryptocurrency is public and free to view.[30] However, it is not easy to understand such complex code, and so the agents differ in their interpretations. For example, some may believe that crypto is good at preserving anonymity of users, while others may fear that it is not. Each agent therefore receives a noisy signal about R, and does not know what signals other agents received. However, she knows each signal represents a perturbation from the true value of R. If she receives a high signal, she can infer not only that R is likely to be high, but that other agents are likely to observe high signals too. This information is useful to agents because of strategic interactions in their payoffs.

[30] This is an important characteristic of any truly decentralized currency: any user can read the code herself rather than rely on intermediaries.

I solve the model using global games techniques. Carlsson and van Damme (1991) explain how small perturbations in the signal can be viewed as a refinement of a game with perfect information. Morris and Shin (2003) explore various aspects of global games, while Goldstein and Pauzner (2005) adapt the techniques to a model of bank runs. Typically, agents in these models have strategic complementarities between their actions. If such agents receive private noisy signals about a fundamental, it can be shown that there is a unique equilibrium, and this is a threshold equilibrium. However, in my model, the agents do not necessarily have strategic complementarities. Although there are strategic complementarities between households' choices of payment medium, there are strategic substitutes in their choices of fees. For example, if a household believes that others use crypto and pay high fees, then she may prefer to use cash. This means multiplicity of equilibria can occur, because fees are not pinned down by anything fundamental. Instead, optimal fee actions only depend on beliefs about other players' actions, making it possible for alternative equilibria to be sustained. Nevertheless, I show that, under certain conditions, a threshold equilibrium can still emerge when signal noise is small.

5.1 *Setup*

The technology R is drawn according to the improper uniform density on the entire real line. For simplicity, I consider a model with only households (i.e. $M = 0$). Given R, each household i receives a signal $R_i \sim U[R - \sigma, R + \sigma]$, where $\sigma > 0$ is called the *signal noise*. Conditional on R, signal errors are independently and identically distributed. Having observed her signal, each household chooses between crypto and cash and, if she uses crypto, a fee. The events over the three time periods are otherwise the same as before. A household's payoff from using crypto, given a signal R_i, is now a random variable, because she does not know the exact value of R. Let $\hat{\pi}_H(f_i; R_i)$ be her expected payoff from using crypto and paying a fee of f_i, relative to using cash. Then:

$$\hat{\pi}_H(f_i; R_i) \;=\; \mathbb{E}\Big[Rg(y)\Big|R_i\Big] \;-\; (1-\rho)\mathbb{P}\Big[\text{non-delivery}\Big|R_i, f_i\Big] \;-\; \rho f_i \mathbb{E}\Big[v(y)\Big|R_i\Big], \tag{27}$$

which is simply the result of applying the expectations operator $\mathbb{E}[\cdot|R_i]$ to Equation (9). Once again, the solution concept is Bayesian Nash equilibrium, and attention is restricted to symmetric equilibria. An equilibrium can be defined as follows:

Definition 10 (Equilibrium with imperfect information). *A strategy is a pair of decision functions $\eta_H : \mathbb{R} \to [0,1]$ and $\phi_H : [0,\infty) \times \mathbb{R} \to [0,1]$. An equilibrium is a strategy pair such that, when a household believes:*

- *any household that observes signal R_j uses crypto with probability $\eta_H(R_j)$, and*
- *any household that observes R_j, conditional on using crypto, pays fees using the distribution function $\phi_H(f; R_j)$,*

then her optimal strategy is to use crypto with probability $\eta_H(R_i)$ and, conditional on using crypto, pay a fee drawn from the distribution function $\phi_H(f; R_i)$, where R_i is her own signal.

I strengthen Assumption 1 to ensure that, at every point as more households use crypto, strategic complementarities strengthen faster than strategic substitutes.

Assumption 3 (Strategic complementarities stronger than substitutes over y). *For every $y \in [0,1]$, $g(y)/Z_\lambda(y)$ is strictly increasing in y.*

Assumption 3 says that, as a marginal household moves from using cash to crypto, network effects (represented by the function $g(y)$) increase more rapidly than blockchain congestion ($Z_\lambda(y)$). This means, as the number of households that use crypto increases, the non-pecuniary payoff from using crypto rises faster than the cost of blockchain congestion. If all households believe others use switching strategies then, at the threshold, as y increases from 0 to 1, a marginal household is better off and increases her crypto usage. Thus crypto is used above the threshold, cash is used below it, and a threshold equilibrium emerges. Assumption 3 ensures strategic complementarities are stronger than strategic substitutes at every possible belief about $y \in [0,1]$. Assumption 1 merely ensures this at the extremes $y = 0$ and $y = 1$, which is not sufficient to ensure the existence of a threshold equilibrium when there is imperfect information.

5.2 *Equilibrium*

Proposition 5 (Equilibrium in global games). *Suppose the technology R follows the improper uniform density on the real line, and each household i receives a signal $R_i \sim U[R-\sigma, R+\sigma]$. Then:*

1. *There exists $\bar{\sigma} > 0$ such that, for all $\sigma < \bar{\sigma}$, there is an equilibrium in which all households employ a switching strategy. A household with signal R_i uses crypto if $R_i > R_\sigma^\dagger$ and uses cash if $R_i \leq R_\sigma^\dagger$, where:*

$$R_\sigma^\dagger \;=\; (1-\rho)\frac{\int_0^1 Z_\lambda(s)\,ds}{\int_0^1 g(s)} \;+\; \sigma\Big(1 - \frac{2\int_0^1 sg(s)\,ds}{\int_0^1 g(s)\,ds}\Big). \tag{28}$$

2. *For any $\delta > 0$, there exists $\sigma_\delta > 0$ such that, for all $\sigma < \sigma_\delta$, any equilibrium strategy must satisfy $\eta_H(R_i) = 0$ for all $R_i \leq R_\sigma^\dagger - \delta$ and $\eta_H(R_i) = 1$ for all $R_i > R_\sigma^\dagger + \delta$.*

The proof is in the Appendix (Section 7.7). The threshold $R_\sigma^\dagger$ is the value of R_i at which $\hat{\pi}_H(f; R_i) = 0$ under equilibrium fee strategies. A marginal household that observes a signal exactly equal to $R_\sigma^\dagger$ applies a Laplacian prior (Morris and Shin, 2003), meaning she adopts beliefs in which y follows a uniform distribution over $[0, 1]$. When σ is low, the second term in Equation (28) is small in magnitude. Assumption 3 guarantees that, for this marginal household, an increase in the number of crypto users y causes strategic complementarities to strengthen more than the strategic substitutes. This means the marginal household's payoff is increasing in y at $R_\sigma^\dagger$, so a switching strategy is optimal.

The threshold $R_\sigma^\dagger$ converges to a finite limit as $\sigma \to 0$. Assumption 3 implies this limit is strictly higher than the threshold under payoff-dominance described in Proposition 1. Therefore, imperfect information implies lower welfare than perfect information, at least for low values of σ. This is because a marginal household. who observes a signal at the threshold, cannot be sure how many of her peers use crypto. In contrast, in the perfect information case, the marginal household knows all other households observe the same signal, making coordination easier, and implying higher welfare.

Proposition 5 ensures the existence of a threshold equilibrium for sufficiently small σ, and establishes that, as the signal noise $\sigma \to 0$, any equilibrium approaches the threshold equilibrium. However, it does not ensure uniqueness when $\sigma > 0$. This lack of uniqueness for $\sigma > 0$ is typical

in global games models where agents' payoffs depend on a fundamental state, rather than on their private signals.[31] Nevertheless, in some models, uniqueness can occur when $\sigma > 0$. One crucial characteristic of such models is that agents have global strategic complementarities: as the number of agents that take an action increases, an agent's payoff from taking that same action goes up.[32] That is not the case in the current model. For example, when a household believes R is less than zero, then her payoff π_H from using crypto is certainly decreasing in y.

5.3 *Volatility in the imperfect information threshold equilibrium*

Under the threshold equilibrium at $R_\sigma^\dagger$ identified in Proposition 5, I show volatility is decreasing in the block rate λ, so long as σ is sufficiently small. As there is no financial market, I focus on the volatility of off-exchange value $\sqrt{\mathbb{V}[v(y)]}/\mathbb{E}[v(y)]$, as defined in Equation (21).

For tractability, in Proposition 5 I used an imperfect uniform prior for R. But this prior is not suitable for measuring volatility, because $\mathbb{P}[R \leq R_\sigma^\dagger]$ needs to be well-defined. Instead, I use a finite uniform prior for both the technology $R \sim U[R_0, R_1]$, where $R_0 < R_\sigma^\dagger < R_1$. Given this prior, any household's signal R_j given R has distribution $U[-\sigma, \sigma]$ conditional on $\sigma < R < 1 - \sigma$. Similarly, the posterior of R given R_i is distributed $U[-\sigma, \sigma]$, conditional on $\sigma < R_i < 1 - \sigma$.

Proposition 6 (Volatility in imperfect information case). *Suppose R has prior $U[R_0, R_1]$, and each signal has distribution $R_i \sim U[R - \sigma, R + \sigma]$ iid. Suppose all households play switching strategies with threshold $R_\sigma^\dagger$. Then, if $R_0 + 2\sigma < R_\sigma^\dagger < R_1 - 2\sigma$, the volatility of off-exchange crypto value is:*

$$\frac{\sqrt{\mathbb{V}[v(y)]}}{\mathbb{E}[v(y)]} = \sqrt{(R_1 - R_0)\frac{2\sigma \int_0^1 v(y)^2 dy + (R_1 - R_\sigma^\dagger - \sigma)V^2}{(2\sigma \int_0^1 v(y)\, dy + (R_1 - R_\sigma^\dagger - \sigma)V)^2} - 1}. \tag{29}$$

Define $J := \int_0^1 (V^2 + 2Vv(y) - 4\int_0^1 v(y)^2) dy$. If $J > 0$, then, for all $\sigma < (R_1 - R_\sigma^\dagger)V^2/J$, volatility is increasing in $R_\sigma^\dagger$. If $J \leq 0$, volatility is increasing in $R_\sigma^\dagger$ for any σ. Therefore, when σ is sufficiently small, volatility is decreasing in block rate λ.

[31] See Morris and Shin (2003), section 2.2.2.

[32] In Goldstein and Pauzner (2005), uniqueness holds under a weaker condition of 'one-sided strategic complementarities': the payoff is increasing in the number of agents that take the action so long as the payoff is positive. But even that weaker condition does not hold in this paper.

The proof is in the Appendix (Section 7.8). From Equation (28), $R_\sigma^\dagger$ is decreasing in λ, so volatility is decreasing in λ whenever it is increasing in $R_\sigma^\dagger$.

Proposition 6 is an imperfect information analogue of the result established in Section 4.3. It states that, in the equilibrium with threshold $R_\sigma^\dagger$, we recover the result that volatility is decreasing in block rate λ, so long as signal noise σ is not too high. Similarly, volatility is decreasing in the discount factor ρ, and in the strength of network effects. As $\sigma \to 0$, we recover volatility under perfect information given by Equation (21), with $\hat{B}$ replaced by $\mathbb{P}[R \leq R_\sigma^\dagger] = (R_\sigma^\dagger - R_0)/(R_1 - R_0)$.

The Proposition requires $R_\sigma^\dagger$ to lie within (R_0, R_1), the interior of the support of R. This ensures the existence of upper and lower dominance regions. If this condition does not hold, then there cannot be a threshold equilibrium at $R_\sigma^\dagger$. If $R_0 > R_\sigma^\dagger$, then there will instead be an equilibrium in which all households use crypto. If $R_1 < R_\sigma^\dagger$, there will be an equilibrium in which all use cash.

The Proposition imposes two possible upper bounds on the value of σ. First, σ must be small enough that $R_0 + 2\sigma < R_\sigma^\dagger < R_1 - 2\sigma$. This ensures that, for a household i with a signal R_i close to the threshold $R_\sigma^\dagger$, her posterior about R is a simple uniform $U[R_i - \sigma, R_i + \sigma]$ and, conditional on R, her posterior about other households' signals is $R_j \sim U[R - \sigma, R + \sigma]$. If σ were too large, then we would have to worry about the corners of the uniform distributions, making the analysis more complicated.

Second, if $J > 0$, we require $\sigma < (R_1 - R_\sigma^\dagger)V^2/J$. The quantity J measures how slowly $v(y)$ increases over $y \in [0, 1]$. When J is high, volatility increases more gradually with $R_\sigma^\dagger$, and can actually decrease if J is high enough. A low value of σ mitigates this effect, because it makes y increase more quickly with R close to $R_\sigma^\dagger$, since $y = 0$ at $R = R_\sigma^\dagger - \sigma$, and $y = 1$ at $R = R_\sigma^\dagger + \sigma$.

6. CONCLUSION

I make four important contributions to our understanding of the economics of cryptocurrencies. First, I show that the pricing curve for cryptocurrencies can be locally downward-sloping, in contrast to standard economic theory. This is because of the crowding-out effect: increased speculative pressure makes the currency less useful as a means of payment, reducing its value. Second, I identify a driver of price volatility specific to blockchain technology, thus explaining why observed

price volatility is so high for cryptocurrencies compared to other assets. Third, I show that the volatility effect is amplified by market illiquidity, which makes pricing more sensitive to news contained in the market maker's order flow. Fourth, I demonstrate the existence of the digital gold effect: willingness to use cryptocurrency as money is inversely related to its price.

These results rely on two key conditions. First, there is limited blockchain capacity, so users compete for settlement. Second, the value of cryptocurrency depends on its usage as a means of payment. To my knowledge, there is no other traded asset where both of these conditions are true simultaneously. If such an asset existed, we may expect its price to have similar levels of volatility to cryptocurrencies.

I also make two technical contributions. I build a model that endogenizes both the financial market for cryptocurrency, and the fee-based market for blockchain space. And I contribute to the literature on global games by solving a model in which agents can purchase priority via fees.

The model has testable implications. It predicts that anticipated decreases in the block rate (the parameter λ) should be associated with higher price volatility. One way to test this is to exploit a feature of Bitcoin through which its block rate changes in a predictable way in the short run. Miners create new blocks by solving complicated cryptographic problems. If miners increase their computing power (called the 'hash rate'), the rate of new blocks tends to increase. To regulate the long-run supply schedule, the Bitcoin protocol adjusts the difficulty of the problems every 2016 blocks, roughly every two weeks. As hash rate tends to increase over time — due to technological progress — there is typically a drop in hash rate after each adjustment. My model predicts that the price volatility should rise on these days.

My results also have implications for the long-term future of cryptocurrencies. Roy Amara's celebrated law (Amara, 2016) posits that the impact of technological innovations are often overestimated in the short term and underestimated in the long term, so that speculation precedes actual adoption. Amara's law may be particularly true of cryptocurrencies, because short-term speculation can crowd out usage. Hype results in speculative pressure, making cryptocurrency less useful as money and, paradoxically, hampering adoption. In the longer run, as private information is incorporated into the price, the gains from trading decrease, and speculative activity falls. Re-

duced competition for blockchain space then allows cryptocurrency to function better as a means of payment, and to fulfill its potential. My model cannot predict whether cryptocurrencies will eventually be adopted as money, but it does suggest such an outcome would be consistent with the history we have observed so far.

In order to present a closed-form model of cryptocurrency usage and pricing, I have abstracted away from some features that could be worth analyzing further. In particular, I have assumed that the time-frame over which beliefs form about the future value of cryptocurrency is similar to the time-frame over which settlement is delayed. In reality, settlement delays are likely to be of the order of days at most, whereas beliefs about future value will take much longer to form. A multi-period version of the model could provide a more realistic treatment, and allow the long-term value $v(y)$ to be micro-founded. So long as current usage informs beliefs about future usage, the effects I identify in this model will remain.

My model can also be extended to incorporate imperfect information for speculators, as well as households. In the current setting, this may not add much value, because there are no strategic complementarities between an individual speculator's actions and those of any other agent. However, a different setting could give rise to new insights. Suppose, for example, there is a finite number of speculators and households, and speculators' signals are not perfectly correlated with households'. Suppose further that trading is costly (in the sense described in Section 4.5), and households can observe the price posted by the market maker before choosing their actions. Then households may be incentivized to pay low fees and allow speculators priority, to encourage more trading. This would make the price a more accurate signal of R, helping guide households' decisions and improve welfare. This could explain why blockchain usage and fees tend to be driven by speculative trading (as suggested by Figure 1), rather than payments activity.[33]

References

Amara, R., 2016. Oxford essential quotations, 4th edition. *Oxford University Press* http://www.oxfordreference.com/view/10.1093/acref/9780191826719.001.0001/q-oro-ed4-

[33]There is a related literature looking at how speculators generate information that is useful to management. See Edmans, Goldstein, and Jiang (2015).

00018679.

Athey, S., Parashkevov, I., Sarukkai, V., Xia, J., 2016. Bitcoin pricing, adoption and usage: theory and evidence. *SSRN* (2826674).

Baumol, W. J., 1952. The transactions demand for cash: an inventory theoretic approach. *Quarterly Journal of Economics* 66 (4), 545–556.

Bech, M., Garratt, R., 2017. Central bank cryptocurrencies. *BIS Quarterly Review*, 55–70.

Biais, B., Bisière, C., Bouvard, M., Casamatta, C., Menkveld, A., 2018. Equilibrium bitcoin pricing. *SSRN* (3261063).

Böhme, R., Christin, N., Edelman, B., Moore, T., 2015. Bitcoin: economics, technology, and governance. *Journal of Economic Perspectives* 29 (2), 213–38.

Bolt, W., van Oordt, M. R. C., 2019. On the value of virtual currencies. *Journal of Money, Credit and Banking* in press.

Budish, E., 2018. The economic limits of Bitcoin and the blockchain. *National Bureau of Economic Research working paper* (24717).

Carlsson, H., van Damme, E., 1991. Equilibrium selection in stag hunt games. *CentER Discussion Paper* 1991-70.

Carney, M., 2018. The future of money. *Speech* https://www.bankofengland.co.uk/speech/2018/mark-carney-speech-to-the-inaugural-scottish-economics-conference.

Choudhury, S. R., 2018. A Bitcoin conference has stopped taking bitcoin payments because they don't work well enough. *CNBC* https://www.cnbc.com/2018/01/10/bitcoin-conference-stops-accepting-cryptocurrency-payments.html.

Ciaian, P., Rajcaniova, M., Kancs, D., 2016. The economics of bitcoin price formation. *Applied Economics* 48 (19), 1799–1815.

Clifford, J., 2017. Understanding the block size debate https://medium.com/@jcliff/understanding-the-block-size-debate-351bdbaaa38.

Cochrane, J. H., 2018. The Bitcoin market isn't irrational. *Chicago Booth Review* http://review.chicagobooth.edu/finance/2018/article/bitcoin-market-isn-t-irrational.

Cong, L. W., Li, Y., Wang, N., 2018. Tokenomics: dynamic adoption and valuation. *SSRN* (3153860).

Dang, T. V., Gorton, G., Holmström, B., Ordoñez, G., 2017. Banks as secret keepers. *American Economic Review* 107 (4), 1005–1029.

Divakaruni, A., Zimmerman, P., 2020. Ride the Lightning: turning Bitcoin into money. *SSRN* (3514125).

Easley, D., O'Hara, M., Basu, S., 2019. From mining to markets: the evolution of Bitcoin transaction fees. *Journal of Financial Economics* 134 (1), 91–109.

Edmans, A., Goldstein, I., Jiang, W., 2015. Feedback effects, asymmetric trading, and the limits to arbitrage. *American Economic Review* 105 (12), 3766–3797.

Fernández-Villaverde, J., 2018. A crash course in digital monetary economics. *Penn Institute for Economic Research working paper* 18 (23).

Fisher, I., 1911. The purchasing power of money, its determination and relation to credit, interest and crises. The Macmillan Company.

Foucault, T., Pagano, M., Roell, A., 2013. Market liquidity: theory, evidence, and policy. Oxford University Press.

Gandal, N., Hamrick, J. T., Moore, T., Oberman, T., 2018. Price manipulation in the Bitcoin ecosystem. *Journal of Monetary Economics* 95, 86–96.

Glosten, L. R., Milgrom, P. R., 1985. Bid, ask and transaction prices in a specialist market with heterogeneously informed traders. *Journal of Financial Economics* 14 (1), 71–100.

Goldstein, I., Pauzner, A., 2005. Demand–deposit contracts and the probability of bank runs. *Journal of Finance* 60 (3), 1293–1327.

Hautsch, N., Scheuch, C., Voigt, S., 2018. Limits to arbitrage in markets with stochastic settlement latency. *Center for Financial Studies Working Paper* (616).

Hinzen, F. J., John, K., Saleh, F., 2019. Bitcoin's fatal flaw: the limited adoption problem. *SSRN* (3334262).

Huberman, G., Leshno, J., Moalleni, C., 2017. Monopoly without a monopolist: an economic analysis of the Bitcoin payment system. *CEPR discussion paper* (12322).

Judd, K., 1985. The law of large numbers with a continuum of iid random variables. *Journal of Economic Theory* 35 (1), 19–25.

Kiyotaki, N., Wright, R., 1989. On money as a medium of exchange. *Journal of Political Economy* 97 (41), 927–954.

Krugman, P., 2018. Bubble, bubble, fraud and trouble. *New York Times* https://www.nytimes.com/2018/01/29/opinion/bitcoin-bubble-fraud.html.

Kyle, A. S., 1985. Continuous auctions and insider trading. *Econometrica* 53 (6), 1315–1335.

Liu, Y., Tsyvinski, A., 2018. Risks and returns of cryptocurrency. *National Bureau of Economic Research working paper* (24877).

Makarov, I., Schoar, A., 2019. Trading and arbitrage in cryptocurrency markets. *Journal of Financial Economics* in press.

Morgan, D., 2017. The great Bitcoin scaling debate – a timeline. *Hacker Noon* https://hackernoon.com/the-great-bitcoin-scaling-debate-a-timeline-6108081dbada.

Morris, S., Shin, H. S., 2003. Global games: theory and applications. *Econometric Society Monographs* 1, 56–114.

Nakamoto, S., 2008. Bitcoin: a peer-to-peer electronic cash system. *Mimeo.*

Nakamoto, S., 2009. Bitcoin open source implementation of P2P currency. *P2P Foundation* http://p2pfoundation.ning.com/forum/topics/bitcoin-open-source.

Pagnotta, E., 2018. Bitcoin as decentralized money: prices, mining, and network security. *SSRN* (3264448).

Saleh, F., 2018. Volatility and welfare in a crypto economy. *SSRN* (3235467).

Schilling, L., Uhlig, H., 2019. Some simple Bitcoin economics. *Journal of Monetary Economics* 106, 16–26.

Sockin, M., Xiong, W., 2018. A model of cryptocurrencies. *Mimeo.*

Tobin, J., 1956. The interest-elasticity of transactions demand for cash. *Review of Economics and Statistics* 38 (3), 241–247.

Uhlig, H., 1996. A law of large numbers for large economies. *Economic Theory* 8 (1), 41–50.

Yermack, D., 2013. Is Bitcoin a real currency? An economic appraisal. *National Bureau of Economic Research working paper* (19747).

7. APPENDIX: Proofs

7.1 *Proof of Lemma 1*

Define $\mathcal{R}_1 = \{R : \eta_H(R) = 1\}$ and $\mathcal{R}_0 = \{R : \eta_H(R) = 0\}$. I begin by showing these two sets are collectively exhaustive, and are each non-empty. Suppose there exists R such that $0 < \eta_H(R) < 1$. Households must receive the same payoff from crypto and cash. Then, by Definition 7, households all prefer to use cash. But that contradicts $\eta_H(R) > 0$. Thus either $\eta_H(R) = 1$ or $\eta_H(R) = 0$.

A household can do no better than when all other households use crypto and all agents pay a fee of zero, so that she ranks first for priority even with an arbitrarily low fee. Thus her optimal payoff $\pi^*_H(R)$, given a realization of the technology R, is bounded above:

$$\pi^*_H(R) \;\leq\; Rg(1) - (1-\rho)Z_\lambda(0). \tag{A.1}$$

When $R \leq (1-\rho)Z_\lambda(0)/g(1)$, a household will certainly choose to use cash regardless of her beliefs. Thus all such R are members of $\mathcal{R}_0$. As R can take any value in $\mathbb{R}$, we have $\mathbb{P}[R \in \mathcal{R}_0] > 0$.

Similarly, a household can do no worse than ranking last for priority behind all other households and speculators. In such a case, she may as well pay a fee of zero. Thus her optimal payoff is bounded below:

$$\pi^*_H(R) \;\geq\; \min_{y\in[0,1]} \Big\{ Rg(y) - (1-\rho)Z_\lambda(y+M) \Big\}. \tag{A.2}$$

When $R > (1-\rho)\min_y\{Z_\lambda(y+M)/g(y)\}$, then $\pi^*_H(R) > 0$, so a household will certainly choose to use crypto regardless of her beliefs.[34] Thus all such R are members of $\mathcal{R}_1$, and $\mathbb{P}[R \in \mathcal{R}_1] > 0$.

[34]Note it is important here that $g(0) > 0$; otherwise, there can be an equilibrium where crypto is never used for any R.

When $R \in \mathcal{R}_0$, then $y = 0$ and $v(y) = 0$ for sure, so the on-chain value of crypto $K(R)$ is zero. When $R \in \mathcal{R}_1$, then $y = 1$, and each household i chooses a fee f_i to maximize her expected payoff; i.e. she aims to solve the following problem:

$$\max_{f_i \geq 0} \Big\{ Rg(1) - (1-\rho) Z_\lambda \Big(1 - \phi_H(f_i; R) + M(1 - \phi_S(f_i; R)) \Big) - \rho f_i V \Big\}, \tag{A.3}$$

which is equivalent to:

$$\min_{f_i \geq 0} \Big\{ (1-\rho) Z_\lambda \Big(1 - \phi_H(f_i; R) + M(1 - \phi_S(f_i; R)) \Big) + \rho f_i V \Big\}. \tag{A.4}$$

Conditional on $R \in \mathcal{R}_1$, the value of R affects her choice of f_i only to the extent it changes her beliefs about other agents' fees. Similarly, a speculator's expected payoff depends only on his beliefs about the actions of the other agents, and not directly on R. Therefore, conditional on $R \in \mathcal{R}_1$, neither households' nor speculators' fees directly depend on R in equilibrium, and the on-exchange value $K(R)$ is the same for all such R. Write it as $\bar{K}$.

Finally, I show speculators always buy if $R \in \mathcal{R}_1$ and sell if $R \in \mathcal{R}_0$. Whatever strategies speculators employ, total informed order $x \in [-M, M]$. Conditional on x, the market maker observes total order flow $z \sim U[x - \ell, x + \ell]$ where $\ell > M$. With positive probability, the market maker cannot infer whether or not $R \in \mathcal{R}_1$ because, for any value of x, the probability density function of z is always strictly positive over $z \in [M - \ell, -M + \ell]$. This means that a speculator's posterior expected price $\mathbb{E}[p(z)|R]$ always lies in the open interval $(0, \bar{K})$. When $R \in \mathcal{R}_1$, a speculator expects the price to be less than the true on-exchange value $\bar{K}$, and so strictly prefers to buy. When $R \in \mathcal{R}_0$, he expects the price to be higher than the true on-exchange value of zero, and so strictly prefers to sell. The proof is complete.

7.2 *Proof of Lemma 2*

I begin by establishing some notation. From Lemma 1, we know that fees are paid if and only if $\eta_H(R) = 1$ and $\eta_S(1; R) = 1$, so for the remainder of the proof we can assume that is the case. Conditional on that, optimal fees do not depend on the value of R. Define $\mathcal{F}_\mathcal{H}$ to be the support of

households' optimal fee strategies and $\mathcal{F}_{\mathcal{S}}$ to be the support of speculators' optimal fee strategies. Let $\mathcal{F} = \mathcal{F}_{\mathcal{H}} \cup \mathcal{F}_{\mathcal{S}}$ be the union of these supports.

Define $\bar{\phi}_H(f) = 1 - \phi_H(f; R)$ to be the complementary distribution of households' fees, and $\bar{\phi}_S(f) = 1 - \phi_S(f; R)$ the complementary distribution of speculators' fees. Define $\psi(f)$ to be the total measure of agents that offer fees strictly higher than f:

$$\psi(f) \;=\; \bar{\phi}_H(f) \;+\; M\bar{\phi}_S(f). \tag{A.5}$$

$\psi(f)$ is non-increasing in f. As $\phi_H(f; R)$ and $\phi_S(f; R)$ are probability distribution functions, they are right-continuous in f, and so $\psi(f)$ is also right-continuous.

Part 1: $\mathcal{F}$ is bounded. Negative fees are infeasible, so clearly $\mathcal{F}$ must be bounded below by zero. If $f > 1$, then $\hat{K}(f; R) < 0$, so speculators never pay fees greater than 1, and $\mathcal{F}_{\mathcal{S}}$ is bounded above. All that remains is to show $\mathcal{F}_{\mathcal{H}}$ is bounded above. As $y = \eta_H(R) = 1$, the payoff to a household from choosing any fee $f \in \mathcal{F}_{\mathcal{H}}$ is bounded above:

$$\pi_H(f; R) \;\leq\; Rg(1) - (1-\rho)Z_\lambda(0) - \rho V f, \tag{A.6}$$

since a household can do no better than when she ranks above all other households. A household only chooses crypto when $\pi_H(f; R) > 0$, so we must have:

$$f \;<\; \frac{Rg(1) - (1-\rho)Z_\lambda(0)}{\rho V}. \tag{A.7}$$

Since optimal fees do not depend on the value of R, $\mathcal{F}_{\mathcal{H}}$ is bounded above by $\inf_{R \in \mathcal{R}_1}\{(Rg(1) - (1-\rho)Z_\lambda(0))/\rho V\}$.

Part 2: Fee strategies do not have point masses. Proof by contradiction. Suppose there is a point mass, so that there exists at least one $f \in \mathcal{F}$ where $\psi(f)$ is not left-continuous. That means there exists at least one fee $f \in \mathcal{F}$ such that $\lim_{\epsilon \to 0^+} \psi(f) - \psi(f - \epsilon) > 0$, where $\epsilon \to 0^+$ denotes convergence to zero from above. Consider the set $\mathcal{F}'$ of all points where $\psi(f)$ is not left-continuous. As $\mathcal{F}'$ is a subset of a bounded set $\mathcal{F}$, it must have a supremum, which I label f'.

Suppose $f' \in \mathcal{F}'$. Let $\mu = \lim_{\epsilon \to 0^+} \psi(f') - \psi(f' - \epsilon) > 0$ be the size of the point mass at f'.

Consider an agent, labeled i, that chooses fee f'. She ranks equally for priority with exactly μ other agents. Blockchain space is allocated randomly among these agents, so the proportion that are prioritized above i is equal to $\psi(f')$ plus a random variable distributed $\sim U[0,\mu]$.

Suppose i is a household, so $f' \in \mathcal{F}_{\mathcal{H}}$. As $\eta_H(R) = 1$, the expected payoff to the household from choosing fee f' is:

$$\pi_H(f';R) \;=\; Rg(1) - (1-\rho)\Big(\frac{1}{\mu}\int_0^{\mu} Z_\lambda(\psi(f')+s)\mathrm{d}s\Big) - \rho V f'. \tag{A.8}$$

Consider any $\epsilon > 0$ satisfying:

$$\epsilon \;<\; \frac{(1-\rho)}{\rho V}\Big(\frac{1}{\mu}\int_0^{\mu} Z_\lambda(\psi(f')+s)\mathrm{d}s - Z_\lambda(\psi(f'))\Big). \tag{A.9}$$

The right-hand side of Equation (A.9) is strictly positive, by the monotonicity property of $Z_\lambda(\cdot)$. We know $f'+\epsilon \notin \mathcal{F}'$, because f' is the supremum of $\mathcal{F}'$. The payoff from choosing fee $f'+\epsilon$ is:

$$\begin{aligned}
\pi_H(f'+\epsilon;R) \;&=\; Rg(1) - (1-\rho)Z_\lambda(\psi(f'+\epsilon)) - \rho V(f'+\epsilon),\\
&\geq\; Rg(1) - (1-\rho)Z_\lambda(\psi(f')) - \rho V(f'+\epsilon),\\
&=\; \pi_H(f';R) + (1-\rho)\Big(\frac{1}{\mu}\int_0^{\mu} Z_\lambda(\psi(f')+s)\mathrm{d}s - Z_\lambda(\psi(f'))\Big) - \rho V\epsilon,\\
&>\; \pi_H(f';R),
\end{aligned} \tag{A.10}$$

by the definition of ϵ. As $f'+\epsilon$ yields a strictly higher payoff for households than f', we must have $f' \notin \mathcal{F}_{\mathcal{H}}$, which is a contradiction. By a similar argument, we can show that, for sufficiently small $\epsilon > 0$, a speculator earns a strictly higher payoff with a fee of $f'+\epsilon$ than with f', so $f' \notin \mathcal{F}_{\mathcal{H}} \cup \mathcal{F}_{\mathcal{S}} = \mathcal{F}$. But this contradicts $f' \in \mathcal{F}' \subset \mathcal{F}$.

Now suppose $f' \notin \mathcal{F}'$. Then, for any ϵ, there exists $f''_\epsilon \in \mathcal{F}'$ such that $f' - \epsilon < f''_\epsilon < f'$. By a similar argument to above, for sufficiently small ϵ, a fee of f' yields a strictly higher payoff than f''_ϵ, for both households and speculators. But this contradicts $\mathcal{F}' \subset \mathcal{F}$.

These results imply $\mathcal{F}'$ is a bounded set with no supremum. It must therefore be empty. There are no point masses in the fee strategies.

Part 3: Infimum of $\mathcal{F}$ is zero. By part 1, $\mathcal{F}$ is bounded below by zero, so it has an infimum

$f_0 \geq 0$. Part 2 implies that any agent's expected payoff is continuous in f, so paying a fee of f_0 must yield the optimal payoff for some agent.

Suppose f_0 yields the optimal payoff for a household. Since no agent pays a fee lower than f_0, and there is no point mass at f_0, we have:

$$\pi_H(f_0; R) \;=\; Rg(1) - (1-\rho)Z_\lambda(1) - \rho f_0 V. \tag{A.11}$$

Deviating to a fee of exactly zero yields:

$$\pi_H(0; R) \;=\; Rg(1) - (1-\rho)Z_\lambda(1) \;=\; \pi_H(f_0; R) + \rho f_0 V. \tag{A.12}$$

This contradicts the optimality of f_0, unless $f_0 = 0$. By a similar argument, f_0 cannot yield the optimal payoff for a speculator unless $f_0 = 0$. Thus the infimum of $\mathcal{F}$ is zero.

Part 4: Essential convexity. Proof by contradiction. Let $\mathcal{F}_C$ be the convex hull of $\mathcal{F}$; i.e. the smallest interval on $\mathbb{R}$ that contains all members of $\mathcal{F}$. By part 1, $\mathcal{F}_C$ is bounded. Suppose there is a set of positive measure $\mathcal{F}''$ such that $\mathcal{F}'' \subset \mathcal{F}_C$ but $\mathcal{F}'' \cap \mathcal{F}$ is empty.

Let f_1 be the infimum of $\mathcal{F}''$, and $f_2 > f_1$ the supremum. Part 2 implies continuity of ψ so, for all $f \in [f_1, f_2]$, $\psi(f)$ is constant and equal to $\psi(f_2)$. By definition of f_2 and $\mathcal{F}''$, for any $\epsilon > 0$, there is a $f'' \in \mathcal{F}$ such that $f_2 < f'' < f_2 + \epsilon$. Then either $f'' \in \mathcal{F}_\mathcal{H}$ or $f'' \in \mathcal{F}_\mathcal{S}$. For a household, choosing f'' yields:

$$\begin{aligned} \pi_H(f''; R) \;&\leq\; Rg(1) - (1-\rho)Z_\lambda(\psi(f_2+\epsilon)) - \rho V f_2, \\ &=\; \pi_H(f_1; R) - (1-\rho)\Big(Z_\lambda(\psi(f_2+\epsilon)) - Z_\lambda(\psi(f_1)\Big) - \rho V(f_2 - f_1). \end{aligned} \tag{A.13}$$

By continuity of ψ, as $\epsilon \to 0$, $\psi(f_2+\epsilon) \to \psi(f_2) = \psi(f_1)$. Thus, for small enough ϵ, $\pi_H(f''; R) < \pi_H(f_1; R)$. Choosing f'' cannot be an optimal strategy for a household, so $f'' \notin \mathcal{F}_H$. By a similar argument, $f'' \notin \mathcal{F}_\mathcal{S}$. Thus $f'' \notin \mathcal{F}$. This means there exists an $\epsilon > 0$ such that no member of $(f_2, f_2+\epsilon)$ is a member of $\mathcal{F}$. But then f_2 is not the supremum of $\mathcal{F}''$, and we have a contradiction.

7.3 *Proof of Proposition 1*

The proof consists of several stages. First, I derive the market maker's pricing rule $p(z)$. Second, I establish some auxiliary results about the intersection between the supports of households' and speculators' fee decisions. In the following stages, I use these results to solve for the fee strategies, the threshold, and the on-exchange value of crypto. Sixth and finally, I show that any equilibrium strategies η_H, η_S must be switching strategies at the same threshold.

Stage 1: Pricing rule. By Lemma 1, either $\eta_H(R) = 1$ or $\eta_H(R) = 0$. Again, define $\mathcal{R}_1 = \{R : \eta_H(R) = 1\}$, and let $\mathcal{R}_0$ be its complement. When $R \in \mathcal{R}_1$, speculators' total order is $x = M$ and, by Lemma 1, the on-exchange value of crypto is some K that does not depend on R. When $R \in \mathcal{R}_0$, $x = -M$ and the on-exchange value of crypto is zero.

The market maker observes $z = x+u$, where $u \sim U[-\ell, \ell]$ and $\ell > M$. If $z \leq -\ell+M$, the market maker infers $R \in \mathcal{R}_0$ with probability 1, and so she sets a price of zero. Similarly, if $z \geq \ell - M$ she infers $R \in \mathcal{R}_1$ and sets a price equal to K. In the intermediate case $-\ell+M < z < \ell-M$, the order flow does not change her prior, so she sets the price equal to the ex ante mean of the on-exchange value $p(z) = K\,\mathbb{P}[R \in \mathcal{R}_1|z]$. When agents employ switching strategies at some R^*, $p(z)$ is given by Equation (17).

Stage 2: Support of fee strategies. When $R \in \mathcal{R}_0$, households use cash and speculators sell, so neither requires blockchain space and there are no fees. Consider the case $R \in \mathcal{R}_1$. Let $\mathcal{F}_\mathcal{H}$ denote the support of households' fee strategies, and let $\mathcal{F}_\mathcal{S}$ denote the support of speculators' fee strategies. By Lemma 1, $\mathcal{F}_\mathcal{H}$ and $\mathcal{F}_\mathcal{S}$ do not depend on the value of R, so long as $R \in \mathcal{R}_1$. The Lemma also ensures both households' and speculators' payoffs are continuous in the fee. This means that, for any limit point f_L of $\mathcal{F}_\mathcal{H}$, a household is indifferent between choosing f_L and choosing any member of $\mathcal{F}_\mathcal{H}$. Thus we can assume that $\mathcal{F}_\mathcal{H}$ contains its limit points; i.e. it is a closed set. If not, we can replace $\mathcal{F}_\mathcal{H}$ by the smallest closed set that contains $\mathcal{F}_\mathcal{H}$. Similarly, we can assume $\mathcal{F}_\mathcal{S}$ is closed.

Suppose $\mathcal{F}_\mathcal{H}$ and $\mathcal{F}_\mathcal{S}$ can both be written as unions of disjoint intervals. In stage 5, I show that this must be the case. I claim the intersection of the supports $\mathcal{L} = \mathcal{F}_\mathcal{H} \cap \mathcal{F}_\mathcal{S}$ is non-empty. This can be proven by contradiction. Suppose the $\mathcal{L}$ is empty. Take an interval $[f_a, f_b] \subset \mathcal{F}_\mathcal{H}$. Then

$f_a, f_b \in \mathcal{F}_\mathcal{H}$ (since $\mathcal{F}_\mathcal{H}$ is closed by assumption) and there exists an $\epsilon > 0$ such that $(f_a - \epsilon, f_a) \notin \mathcal{F}_\mathcal{H}$ and $(f_b, f_b + \epsilon) \notin \mathcal{F}_\mathcal{H}$. We know $\mathcal{F}_\mathcal{S}$ is non-empty and, by assumption, not exactly equal to $\mathcal{F}_\mathcal{H}$. By Lemma 2, $\mathcal{F} = \mathcal{F}_\mathcal{H} \cup \mathcal{F}_\mathcal{S}$ is essentially convex. Thus there must exist a $\delta \in (0, \epsilon)$ such that either $(f_a - \delta, f_a) \subset \mathcal{F}_\mathcal{S}$ or $(f_b, f_b + \delta) \subset \mathcal{F}_\mathcal{S}$. But then either f_a or f_b is a limit point of $\mathcal{F}_\mathcal{S}$, and so must be a member of $\mathcal{F}_\mathcal{S}$, contradicting the assumption that $\mathcal{L}$ is empty.

By Lemma 2, $0 \in \mathcal{F}$, so zero must be a member of at least one of $\mathcal{F}_\mathcal{H}$ and $\mathcal{F}_\mathcal{S}$. I consider each possibility separately, under the assumption that both sets are unions of disjoint intervals. In stage 3, I show the case $0 \in \mathcal{F}_\mathcal{S}$ implies case 2 described in Proposition 1 and, in stage 4, I show $0 \in \mathcal{F}_\mathcal{H}$ implies cases 1 and 3.

Stage 3: Solution when speculators play a fee of zero. Suppose $\mathcal{F}_\mathcal{H}$ and $\mathcal{F}_\mathcal{S}$ can both be written as unions of disjoint intervals, and $0 \in \mathcal{F}_\mathcal{S}$. For any $f \in \mathcal{F}_\mathcal{S}$, speculators are indifferent between a fee of f and a fee of zero, so $\hat{K}(f; R) = \hat{K}(0; R)$; i.e.:

$$V\Big(1 - (1-\rho)Z_\lambda(1+M)\Big) \;=\; V(1-f)\Big(1 - (1-\rho)Z_\lambda(\bar{\phi}_H(f) + M\bar{\phi}_S(f))\Big), \tag{A.14}$$

where $\bar{\phi}_H(f)$ and $\bar{\phi}_S(f)$ are the complementary distribution functions for households' and speculators' fees, respectively, given $R \in \mathcal{R}_1$.

I claim $\mathcal{L} = \mathcal{F}_\mathcal{H} \cap \mathcal{F}_\mathcal{S}$ has exactly one or two members. Stage 2 tells us it has at least one, so I just need to show it cannot have more than two. Suppose it has three or more members. Let f_1, f_2, f_3 be distinct members of $\mathcal{L}$. As f_1 lies in the households' optimal strategy set $\mathcal{F}_\mathcal{H}$, a household's optimal payoff is:

$$\pi^*_H(R) \;= \pi_H(f_1; R) \;=\; Rg(1) - (1-\rho)Z_\lambda\Big(\bar{\phi}_H(f_1) + M\bar{\phi}_S(f_1)\Big) - \rho V f_1. \tag{A.15}$$

As $f_1 \in \mathcal{F}_\mathcal{S}$, I can use Equation (A.14) to obtain:

$$\pi^*_H(R) \;=\; Rg(1) - \frac{(1-\rho)Z_\lambda(1+M) - f_1}{1 - f_1} - \rho V f_1. \tag{A.16}$$

As f_2 and $f_3 \in \mathcal{L}$, Equation (A.16) must also be true when f_1 is replaced by f_2 or f_3. We can

equate the right-hand sides and rearrange to obtain:

$$1 - f_2 \;=\; \frac{1-(1-\rho)Z_\lambda(1+M)}{\rho V(1-f_1)} \;=\; 1 - f_3, \tag{A.17}$$

so $f_2 = f_3$ and $\mathcal{L}$ cannot have three distinct members. Therefore, $\mathcal{L}$ must have exactly one or two members. I consider each case separately. In stage 3A, I show that there can be no equilibrium where there are two members. In stage 3B, I show there is a unique equilibrium where $\mathcal{L}$ has one member, corresponding to case 2, and find conditions for its existence.

Stage 3A: No equilibrium where $\mathcal{L}$ has two members. Proof by contradiction. Suppose $\mathcal{L}$ has two members. As $0 \in \mathcal{F}_\mathcal{S}$, we can write $\mathcal{F}_\mathcal{S} = [0, f_1] \cup [f_2, f_3]$ and $\mathcal{F}_\mathcal{H} = [f_1, f_2]$, for some $0 < f_1 < f_2 < f_3$. I claim the postulated strategies are not consistent with an equilibrium.

Let $h' = M\bar{\phi}_S(f_2)$, the mass of speculators who choose fees higher than the households. A speculator is indifferent between a fee of f_1 and a fee of f_2, so:

$$(1-f_1)\Big(1-(1-\rho)Z_\lambda(1+h')\Big) \;=\; (1-f_2)\Big(1-(1-\rho)Z_\lambda(h')\Big). \tag{A.18}$$

A household is also indifferent between f_1 and f_2, so:

$$(1-\rho)Z_\lambda(1+h') + \rho V f_1 \;=\; (1-\rho)Z_\lambda(h') + \rho V f_2. \tag{A.19}$$

Eliminating $Z_\lambda(1+h')$ in Equations (A.18) and (A.19):

$$1 - \rho V(1-f_1) \;=\; (1-\rho)Z_\lambda(h'). \tag{A.20}$$

As both 0 and $f_2 \in \mathcal{F}_\mathcal{S}$, we have:

$$1-(1-\rho)Z_\lambda(1+M) \;=\; (1-f_2)\Big(1-(1-\rho)Z_\lambda(h')\Big). \tag{A.21}$$

As $f_2 \in \mathcal{F}_\mathcal{H}$, a household cannot be made strictly better off switching from a fee of f_2 to a fee of zero. Thus:

$$(1-\rho)Z_\lambda(1+M) \;\geq\; (1-\rho)Z_\lambda(h') + \rho V f_2. \tag{A.22}$$

Substituting in Equation (A.21) and rearranging gives:

$$\rho V \;\leq\; 1-(1-\rho)Z_\lambda(h'). \tag{A.23}$$

Substituting in Equation (A.20) then implies:

$$\rho V \;\leq\; \rho V(1-f_1), \tag{A.24}$$

which is impossible, as $f_1 > 0$. The postulated strategies are not feasible.

Stage 3B: Equilibrium where $\mathcal{L}$ has a single member (case 2). Suppose $\mathcal{L}$ contains a single member $f_1 > 0$. Since $0 \in \mathcal{F}_\mathcal{S}$, we have $\mathcal{F}_\mathcal{S} = [0, f_1]$ and $\mathcal{F}_\mathcal{H} = [f_1, f_2]$, for some $0 < f_1 < f_2$. I show any such equilibrium corresponds to case 2, as described in the statement of the Proposition.

For all $f \in \mathcal{F}_\mathcal{S}$, speculators are indifferent between a fee of f and a fee of zero, so:

$$1-(1-\rho)Z_\lambda(1+M) \;=\; (1-f)\Big(1-(1-\rho)Z_\lambda(1+M\bar{\phi}_S(f))\Big), \tag{A.25}$$

and we can solve explicitly for speculators' fee strategies:

$$\bar{\phi}_S(f) \;=\; \frac{1}{M}\Big(Z_\lambda^{-1}\Big(\frac{Z_\lambda(1+M)-\frac{f}{1-\rho}}{1-f}\Big)-1\Big), \tag{A.26}$$

for all $f \in \mathcal{F}_\mathcal{S}$, and:

$$f_1 \;=\; (1-\rho)\frac{Z_\lambda(1+M)-Z_\lambda(1)}{1-(1-\rho)Z_\lambda(1)}. \tag{A.27}$$

The on-exchange value of crypto K can be obtained when the speculator pays a fee of zero, giving Equation (14). Households are indifferent between a fee of f_1 and any other $f \in \mathcal{F}_\mathcal{H}$, so:

$$(1-\rho)Z_\lambda(1)+\rho V f_1 \;=\; (1-\rho)Z_\lambda(\bar{\phi}_H(f))+\rho V f. \tag{A.28}$$

Then we can solve explicitly for households' fee strategies:

$$\bar{\phi}_H(f) \;=\; Z_\lambda^{-1}\Big(Z_\lambda(1)-\frac{\rho V}{1-\rho}(f-f_1)\Big), \tag{A.29}$$

for all $f \in \mathcal{F}_{\mathcal{H}}$, and:

$$f_2 \;=\; f_1 + \frac{1-\rho}{\rho V}\Big(Z_\lambda(1) - Z_\lambda(0)\Big). \tag{A.30}$$

When $R \in \mathcal{R}_1$, a household's payoff under the optimal strategy is:

$$\pi_H^*(R) \;=\; Rg(1) - (1-\rho)Z_\lambda(1) - \rho V f_1. \tag{A.31}$$

The optimal payoff is strictly positive whenever $R > R^*$, where:

$$R^* \;=\; \frac{(1-\rho)Z_\lambda(1) + \rho V f_1}{g(1)}, \tag{A.32}$$

which gives Equation (13).

I have shown that there is at most one strategy consistent with this equilibrium. I now need to show this equilibrium exists; i.e. households cannot be made strictly better off by deviating to a strategy in the speculators' optimal fee set $\mathcal{F}_{\mathcal{S}}$, or vice versa.

For households' strategies to be deviation-proof, we must have, for all $f \in \mathcal{F}_{\mathcal{S}}$, $\pi_H(f;R) \leq \pi_H(f_1;R)$; i.e.:

$$(1-\rho)Z_\lambda(1 + M\bar{\phi}_S(f)) + \rho V f \;\geq\; (1-\rho)Z_\lambda(1) + \rho V f_1. \tag{A.33}$$

Substituting in Equation (A.25) and rearranging, we obtain:

$$1 - (1-\rho)Z_\lambda(1) \;\geq\; \rho V(1-f). \tag{A.34}$$

In order for this to be true for all $f \in \mathcal{F}_{\mathcal{S}} = [0, f_1]$, we must have $1 - (1-\rho)Z_\lambda(1) \geq \rho V$.

For speculators' strategies to be deviation-proof, we must have, for all $f \in \mathcal{F}_{\mathcal{H}}$, $\pi_S(1, f; R) \leq \pi_S(1, f_1; R)$; i.e.:

$$(1-f)\Big(1 - (1-\rho)Z_\lambda(\bar{\phi}_H(f))\Big) \;\leq\; (1-f_1)\Big(1 - (1-\rho)Z_\lambda(1)\Big). \tag{A.35}$$

As $\pi_H(f;R) = \pi_H(f_1;R)$, we have $(1-\rho)Z_\lambda(\bar{\phi}_H(f)) + \rho V f = (1-\rho)Z_\lambda(1) + \rho V f_1$, and so the

speculators' no-deviation condition is equivalent to:

$$1-(1-\rho)Z_\lambda(1) \;\geq\; \rho V(1-f), \tag{A.36}$$

for all $f \in [f_1, f_2]$, which is already implied by the no-deviation condition for households. Therefore, these fee strategies describe an equilibrium if and only if $1-(1-\rho)Z_\lambda(1) \geq \rho V$, as required.

Stage 4: Solution when households play a fee of zero. Suppose $\mathcal{F}_\mathcal{H}$ and $\mathcal{F}_\mathcal{S}$ can both be written as unions of disjoint intervals, and $0 \in \mathcal{F}_\mathcal{H}$. Then, when $R \in \mathcal{R}_1$, a household's optimal payoff is:

$$\pi_H^*(R) \;=\; Rg(1)-(1-\rho)Z_\lambda(1+M). \tag{A.37}$$

This is strictly positive for all $R > (1-\rho)Z_\lambda(1+M)/g(1)$, which is the threshold R^* given by Equation (11).

The remainder of stage 4 proceeds along very similar lines to stage 3. Again, I show there are exactly one or two members of $\mathcal{L} \in \mathcal{F}_\mathcal{H} \cap \mathcal{F}_\mathcal{S}$. Stage 2 tells us there is at least one member. Suppose there are at least three distinct members, f_1, f_2, f_3. As households and speculators are indifferent between these fees and a fee of zero, we have, for $f \in \{f_1, f_2, f_3\}$:

$$(1-\rho)Z_\lambda(1+M) \;=\; (1-\rho)Z_\lambda\Big(\bar{\phi}_H(f)+M\bar{\phi}_H(f)\Big)+\rho V f. \tag{A.38}$$

As speculators are indifferent between fees f_1 and f_2, we have:

$$\begin{aligned}(1-f_1)\Big(1-(1-\rho)Z_\lambda\Big(\bar{\phi}_H(f_1)+M\bar{\phi}_H(f_1)\Big)\Big)& \\ =\; (1-f_2)\Big(1-(1-\rho)Z_\lambda\Big(\bar{\phi}_H(f_2)+M\bar{\phi}_H(f_2)\Big)\Big)&.\end{aligned} \tag{A.39}$$

Substituting in the expressions from Equation (A.38) when $f = f_1$ and f_2, we obtain:

$$1-(1-\rho)Z_\lambda(1+M) \;=\; \rho V(1-f_1-f_2). \tag{A.40}$$

But Equation (A.40) is also true with f_2 replaced by f_3. Thus $f_2 = f_3$, and $\mathcal{L}$ can have no more than two members.

As in stage 3, I consider two cases. When $\mathcal{L}$ has exactly one member, we have stage 4A, which corresponds to case 1 described in the Proposition. When $\mathcal{L}$ has exactly two members, we have stage 4B, which corresponds to case 3.

Stage 4A: Equilibrium where $\mathcal{L}$ has a single member (case 1). Write $\mathcal{F}_{\mathcal{H}} = [0, f_1]$ and $\mathcal{F}_{\mathcal{S}} = [f_1, f_2]$, where $0 < f_1 < f_2$. The supports and strategies follow from similar arguments to stage 3B. For all $f \in \mathcal{F}_{\mathcal{H}}$, households are indifferent between a fee of f and zero, so:

$$\bar{\phi}_H(f) \;=\; Z_\lambda^{-1}\Big(Z_\lambda(1+M) - \frac{\rho}{1-\rho}Vf\Big) - M, \tag{A.41}$$

and:

$$f_1 \;=\; \frac{1-\rho}{\rho V}\Big(Z_\lambda(1+M) - Z_\lambda(M)\Big). \tag{A.42}$$

As speculators are indifferent between a fee of f_1 and any other $f \in \mathcal{F}_{\mathcal{S}}$, we have for all $f \in \mathcal{F}_{\mathcal{S}}$:

$$\bar{\phi}_S(f) \;=\; \frac{1}{M}Z_\lambda^{-1}\Big(\frac{(1-f_1)Z_\lambda(M) - \frac{f-f_1}{1-\rho}}{1-f}\Big), \tag{A.43}$$

and:

$$f_2 \;=\; 1 - (1-f_1)\Big(\frac{1-(1-\rho)Z_\lambda(M)}{1-(1-\rho)Z_\lambda(0)}\Big). \tag{A.44}$$

Therefore, if this equilibrium exists, it is unique. The on-exchange value of crypto K is the payoff given a fee of f_1 before subtracting the price, which gives Equation (12).

For any $f \in \mathcal{F}_{\mathcal{S}}$, households cannot be made better off by switching from fee f_1 to f, so:

$$(1-\rho)Z_\lambda(M) + \rho V f_1 \;\leq\; (1-\rho)Z_\lambda\Big(M\bar{\phi}_S(f)\Big) + \rho V f. \tag{A.45}$$

Substituting in Equation (A.43) and rearranging yields:

$$1 - (1-\rho)Z_\lambda(M) \;\leq\; \rho V(1-f). \tag{A.46}$$

This is true for all $f \in \mathcal{F}_{\mathcal{S}} = [f_1, f_2]$ if and only if $1 - (1-\rho)Z_\lambda(M) \leq \rho V(1-f_2)$; i.e.:

$$\rho V \;\geq\; 1 + (1-\rho)\Big(Z_\lambda(1+M) - Z_\lambda(M) - Z_\lambda(0)\Big), \tag{A.47}$$

which is the required condition for case 1. No-deviation for speculators implies, for all $f \in \mathcal{F}_{\mathcal{H}}$:

$$(1-f_1)\Big(1-(1-\rho)Z_\lambda(M)\Big) \;\geq\; (1-f)\Big(1-(1-\rho)Z_\lambda\Big(\bar{\phi}_H(f)+M\Big)\Big). \tag{A.48}$$

Substituting in Equations (A.41) and (A.42) and rearranging yields:

$$\rho V(1-f) \;\geq\; 1-(1-\rho)Z_\lambda(M). \tag{A.49}$$

This is true for all $f \in \mathcal{F}_{\mathcal{H}}$ if and only if $1-(1-\rho)Z_\lambda(M) \leq \rho V(1-f_1)$, which is already implied by the no-deviation condition for households.

Stage 4B: Equilibrium where $\mathcal{L}$ has two members (case 3). In this final case, there exists $0 < f_1 < f_2 < f_3$ such that $\mathcal{F}_{\mathcal{H}} = [0, f_1] \cup [f_2, f_3]$ and $\mathcal{F}_{\mathcal{S}} = [f_1, f_2]$. Define $h = \bar{\phi}_H(f_2) \in (0,1)$ as the mass of households that pay fees higher than every speculator. I shall show there exists an equilibrium of this kind if and only if the condition for neither case 1 nor 2 is satisfied. If the equilibrium exists, it is unique.

As households are indifferent over all $f \in [0, f_1]$, their fee strategies over this range are described by Equation (A.41), with:

$$f_1 \;=\; \frac{1-\rho}{\rho V}\Big(Z_\lambda(1+M)-Z_\lambda(h+M)\Big). \tag{A.50}$$

Households are also indifferent between $0, f_2$ and f_3, so:

$$f_2 \;=\; \frac{1-\rho}{\rho V}\Big(Z_\lambda(1+M)-Z_\lambda(h)\Big), \qquad \text{and} \qquad f_3 \;=\; \frac{1-\rho}{\rho V}\Big(Z_\lambda(1+M)-Z_\lambda(0)\Big). \tag{A.51}$$

Households are indifferent over all $f \in [f_2, f_3]$, so their fee strategies over this range are given by:

$$\bar{\phi}_H(f) \;=\; Z_\lambda^{-1}\Big(Z_\lambda(h)-\frac{\rho V}{1-\rho}(f-f_2)\Big). \tag{A.52}$$

Speculators are indifferent over all $f \in [f_1, f_2]$, so their fee strategies over this range are:

$$\bar{\phi}_S(f) \;=\; \frac{1}{M}\Big(Z_\lambda^{-1}\Big(\frac{(1-f_1)Z_\lambda(h+M)-\frac{f-f_1}{1-\rho}}{1-f}\Big)-h\Big). \tag{A.53}$$

The on-exchange value of crypto K is the payoff to the speculator given a fee of f_2, before subtracting the price. This is given by Equation (15). Thus we have a unique equilibrium, given h. We can solve for h by using the fact that speculators are also indifferent between f_1 and f_2:

$$(1-f_1)\Big(1-(1-\rho)Z_\lambda(h+M)\Big) \;=\; (1-f_2)\Big(1-(1-\rho)Z_\lambda(h)\Big). \tag{A.54}$$

Substituting Equations (A.50) and (A.51) into Equation (A.54) and rearranging, we obtain:

$$\rho V \;=\; 1+(1-\rho)\Big(Z_\lambda(1+M)-Z_\lambda(h+M)-Z_\lambda(h)\Big), \tag{A.55}$$

which is the required condition. As the right-hand side of Equation (A.55) is strictly decreasing in h, it has at most one solution in h.

Suppose Equation (A.55) has no solution in $h \in [0,1]$. This is true if and only if $\rho V < 1-(1-\rho)Z_\lambda(1)$ or $\rho V > 1+(1-\rho)(Z_\lambda(1+M)-Z_\lambda(M)-Z_\lambda(0))$. The first of these inequalities corresponds to case 2 (see stage 3B). The second corresponds to case 1 (see stage 4A). Therefore the three cases are mutually exclusive and cover the entire parameter space. As $h \to 0$, the solution to case 3 approaches that of case 1. As $h \to 1$, it approaches case 2.

Finally, to show this equilibrium exists, we must consider the no-deviation conditions for households and speculators. A household cannot be strictly better off with a fee $f \in (f_1, f_2]$ than with a fee of f_1, so we must have:

$$1-(1-\rho)Z_\lambda(h+M) \;\leq\; \rho V(1-f),\;\; \forall f \in [f_1, f_2]. \tag{A.56}$$

A speculator does not deviate from f_1 to a fee $f \in [0, f_1)$ so long as:

$$1-(1-\rho)Z_\lambda(h+M) \;\leq \rho V(1-f),\;\; \forall f \in [0, f_1], \tag{A.57}$$

and does not deviate from f_2 to a fee $f \in (f_2, f_3]$ so long as:

$$1-(1-\rho)Z_\lambda(h) \;\geq\; \rho V(1-f),\;\; \forall f \in [f_2, f_3]. \tag{A.58}$$

All three of these conditions are guaranteed by Equation (A.55), so this equilibrium exists and is unique. This stage of the proof is complete.

Stage 5: $\mathcal{F}_{\mathcal{H}}$ and $\mathcal{F}_{\mathcal{S}}$ must be unions of disjoint intervals. Suppose one or both of $\mathcal{F}_{\mathcal{H}}$ or $\mathcal{F}_{\mathcal{S}}$ cannot be written as a union of disjoint intervals. Then one or both of these sets has an isolated point: it contains a point that is not a limit point of any sequence contained in that set.

Again, $\mathcal{L} = \mathcal{F}_{\mathcal{H}} \cap \mathcal{F}_{\mathcal{S}}$ cannot be empty. Proof by contradiction. Suppose $\mathcal{L}$ is empty. Consider any isolated point $f' \in \mathcal{F}_{\mathcal{S}}$. As $\mathcal{F}$ is convex and $f' \in \mathcal{F}$, there must be a sequence in $\mathcal{F}$ with limit point f'. This sequence must therefore have a subsequence entirely contained in $\mathcal{F}_{\mathcal{H}}$. The limit of this subsequence is f'. Thus, as $\mathcal{F}_{\mathcal{H}}$ is closed, $f' \in \mathcal{F}_{\mathcal{H}}$, which contradicts the emptiness of $\mathcal{L}$. The same argument works for isolated points in $\mathcal{F}_{\mathcal{H}}$.

Since $\mathcal{F}_{\mathcal{H}} \cup \mathcal{F}_{\mathcal{S}}$ is essentially convex by Lemma 2, any isolated point must be a member of both sets. There are a number of possible such cases, and can all be ruled out on a case-by-case basis, except for some specific values of the parameters. As there are no point masses, isolated points are always chosen with probability zero, so equilibrium strategies will be the same as in one of the cases described in the Proposition. Thus any equilibrium where $\mathcal{F}_{\mathcal{H}}$ or $\mathcal{F}_{\mathcal{S}}$ is the union of disjoint intervals will differ only trivially from an equilibrium where both are.

Writing out all the cases with isolated points is tedious, so I give an example. Suppose $\mathcal{F}_{\mathcal{S}} = [0, f_1]$ and $\mathcal{F}_{\mathcal{H}} = \{f_0\} \cup [f_1, f_2]$, where $0 \leq f_0 < f_1 < f_2$. By the same argument as in case 3B, this can only be an equilibrium when $\rho V \leq 1 - (1-\rho)Z_\lambda(1)$. But households' and speculators' indifference between f_0 and f_1 implies $(1-f_0)\rho V = 1-(1-\rho)Z_\lambda(1)$. In general, this is not possible. An equilibrium can hold only in the special case $\rho V = 1 - (1-\rho)Z_\lambda(1)$, in which case $f_0 = 0$, and all strategies are exactly the same as in case 3B.

Stage 6: Switching strategies. To complete the proof, I need to show the threshold equilibrium at R^* is payoff-dominant over any other equilibrium. As fee strategies are uniquely determined whenever $R \in \mathcal{R}_1$, we can completely describe an equilibrium by specifying a subset of the real numbers $\mathcal{R}_1$. Then $\mathcal{R}_0$ is the complement of $\mathcal{R}_1$. Consider any equilibrium. Given the fee strategies,

a household's expected payoff from using crypto is:

$$\pi_H^*(R) \;=\; \begin{cases} Rg(1) - (1-\rho)Z_\lambda(1+M), & \text{if } R \in \mathcal{R}_1 \text{ and } \rho V > 1 - (1-\rho)Z_\lambda(1), \\ Rg(1) - (1-\rho)\Big(Z_\lambda(1) + \rho V \frac{Z_\lambda(1+M) - Z_\lambda(1)}{1-(1-\rho)Z_\lambda(1)}\Big), & \text{if } R \in \mathcal{R}_1 \text{ and } \rho V \leq 1 - (1-\rho)Z_\lambda(1), \\ Rg(0) - (1-\rho)Z_\lambda(0), & \text{if } R \notin \mathcal{R}_1. \end{cases} \tag{A.59}$$

Consider R^* as defined in the statement of the Proposition. Suppose there is a $R' \leq R^*$ that belongs to $\mathcal{R}_1$. Then $\pi_H^*(R) \leq 0$, and so households would prefer to use cash. $\mathcal{R}_1$ cannot describe an equilibrium. Thus any equilibrium must have $(-\infty, R^*] \subseteq \mathcal{R}_0$.

Now suppose there is a $R'' > R^*$ that belongs to $\mathcal{R}_0$. Then a household that observes $R = R''$ uses cash and earns a payoff of zero. Now consider an alternative equilibrium $\mathcal{R}_1'' := \mathcal{R}_1 \cup \{R''\}$. In this equilibrium, households earn the same payoff at all $R \neq R''$, and a strictly higher payoff at R'', since $\pi_H^*(R'') > 0$ when $R'' \in \mathcal{R}_1$. Therefore any payoff-dominant equilibrium must have $(R^*, \infty) \subseteq \mathcal{R}_1$. Thus we must have $\mathcal{R}_1 = (R^*, \infty)$, and the threshold equilibrium at R^* is the unique equilibrium that survives payoff-dominance.

Finally, I need to show that this threshold equilibrium is indeed an equilibrium. I have already shown that, for all $R \in \mathcal{R}_1$, $\pi_H^*(R) > 0$. For all $R \notin \mathcal{R}_1$, $\pi_H^*(R) \leq R^* g(0) - (1-\rho)Z_\lambda(0)$. By Assumption 1, this is non-positive, so households prefer cash. The proof is complete.

7.4 *Proof of Proposition 2*

Given the pricing rule in Equation (17), the price $p(z)$ has the following distribution:

$$p(z) \;=\; \begin{cases} 0, & \text{with probability } \frac{M}{\ell} B^*, \\ (1-B^*)K, & \text{with probability } 1 - \frac{M}{\ell}, \\ K, & \text{with probability } \frac{M}{\ell}(1-B^*), \end{cases} \tag{A.60}$$

where K is the off-exchange value of crypto given $R > R^*$. This means:

$$\mathbb{E}[p(z)] \;=\; (1-B^*)K, \qquad \mathbb{V}[p(z)] \;=\; \frac{M}{\ell} B^*(1-B^*)K^2, \tag{A.61}$$

which gives the required result for the volatility Γ. Note the expected price given z is equal to the prior mean of the off-exchange value, as the law of iterated expectations implies. As $B^* = B(R^*)$ is increasing in R^*, which is itself decreasing in λ and increasing in M, we have the required comparative statics.

7.5 *Proof of Proposition 3*

Consider the equilibrium described in Proposition 1. When $R \leq R^*$, households use cash, $y = 0$, and so welfare is clearly equal to zero. When $R > R^*$, all households use crypto and $y = 1$. All speculators buy, so there is a mass $1 + M$ of agents that require blockchain space. A mass h of households have top priority (i.e. the first h crypto payments included in a block will belong to households), and a mass $1 - h$ have lowest priority. The speculators occupy priority positions between h and $h + M$.

Consider the realization of blockchain space N. If $0 \leq N \leq h$, then exactly $1 - N$ households have payments fail to settle at T_1. If $h < N \leq h + M$, exactly $1 - h$ households fail to settle. If $h + M < N < 1 + M$, exactly $1 + M - N$ fail to settle, and if $N \geq 1 + M$, then all households are settled at T_1. Given this, welfare is equal to:

$$\begin{aligned}\Omega(R, h) &= Rg(1) \\ &- (1-\rho)\Big(Z_\lambda(0) + \int_0^h (1-n)\mathrm{d}Z_\lambda(n) + \int_h^{h+M} (1-h)\mathrm{d}Z_\lambda(n) + \int_{h+M}^{1+M} (1+M-n)\mathrm{d}Z_\lambda(n)\Big).\end{aligned} \tag{A.62}$$

Integration by parts gives Equation (23). The partial derivatives of Equation (23) with respect to R, $g(1)$, and h are all positive. By Equation (16), h is decreasing in V, and thus so is welfare.

7.6 *Proof of Proposition 4*

With probability $1-B^*$, all speculators observe $R > R^*$ and place buy orders, so $x = M$. According to the pricing rule in Proposition 1, the market maker sets a price of K with probability M/ℓ, and otherwise sets a price of $(1 - B^*)K$. The private value of crypto to a speculator is its on-exchange

value K, so the expected payoff is $(1 - M/\ell)B^*K$.

Similarly, with probability B^*, speculators observe $R \leq R^*$, place sell orders, and the expected payoff is $(1 - M/\ell)(1 - B^*)K$. The expected payoff is therefore given by the left-hand side of Equation (26). The total derivative of this expression with respect to M can have any sign, since B^* is increasing in M, and K can be either increasing or decreasing. Therefore a change in β or ℓ can move $\hat{M}$ in either direction.

7.7 *Proof of Proposition 5*

Part 1: Existence of threshold equilibrium for $\sigma > 0$. Suppose $\eta_H(R_i) = 1$ for $R_i > R_\sigma^\dagger$ and $\eta_H(R_i) = 0$ for $R_i \leq R_\sigma^\dagger$. Then we can write down the number of crypto users y as a function of R:

$$y(R) \;=\; \frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma} \eta_H(R_j)\mathrm{d}R_j \;=\; \begin{cases} 0, & \text{if } R \leq R_\sigma^\dagger - \sigma, \\ \frac{R - R_\sigma^\dagger + \sigma}{2\sigma}, & \text{if } R_\sigma^\dagger - \sigma < R \leq R_\sigma^\dagger + \sigma, \\ 1, & \text{if } R > R_\sigma^\dagger + \sigma. \end{cases} \tag{A.63}$$

I need to show there exist fee strategies consistent with a threshold equilibrium at $R_\sigma^\dagger$. Consider the following function:

$$C(R_i; f) \;=\; Z_\lambda^{-1}\Big(Z_\lambda(y(R_i - \sigma)) - \frac{\rho}{1-\rho} f v(y(R_i - \sigma))\Big), \tag{A.64}$$

where $R_i \in (R_\sigma^\dagger, R_\sigma^\dagger + 2\sigma)$ and:

$$0 \;\leq\; f \;\leq\; \frac{1-\rho}{\rho} \cdot \frac{Z_\lambda(y(R_i - \sigma)) - Z_\lambda(0)}{v(y(R_i - \sigma))}. \tag{A.65}$$

Write $C'(R_i; f) = \dfrac{\mathrm{d}}{\mathrm{d}R_i} C(R_i; f)$. For a household with signal $R_i > R_\sigma^\dagger$, consider the fee strategies given by the following complementary distribution function:

$$\hat{\phi}_H(f; R_i) \;=\; \begin{cases} 2\sigma C'(R_i; f), & \text{if } R_\sigma^\dagger < R_i < R_\sigma^\dagger + 2\sigma, \\ \hat{\phi}_H(f; R_i - 2\sigma), & \text{if } R_i \geq R_\sigma^\dagger + 2\sigma, \end{cases} \tag{A.66}$$

and support for fees given by an interval $[0, \bar{f}(R_i)]$, where:

$$\bar{f}(R_i) \;=\; \begin{cases} 0, \text{if } R_i \leq R_\sigma^\dagger, \\ \frac{1-\rho}{\rho} \min\Big\{ \frac{Z_\lambda(\tilde{y}) - Z_\lambda(0)}{v(\tilde{y})}, \frac{Z'_\lambda(\tilde{y})}{v'(\tilde{y})} \Big\}, & \text{if } R_\sigma^\dagger < R_i < R_\sigma^\dagger + 2\sigma, \\ \frac{1-\rho}{\rho V}\Big(Z_\lambda(1) - Z_\lambda(0)\Big), & \text{if } R_i \geq R_\sigma^\dagger + 2\sigma, \end{cases} \tag{A.67}$$

where $\tilde{y} = y(R_i - \sigma)$, and $Z'_\lambda(\cdot)$ and $v'(\cdot)$ represent the first derivatives of their respective functions. When $R_i \leq R_\sigma^\dagger$, crypto is not used and no fees are paid. Note that, in the limit as $R_i \to R_\sigma^\dagger$, the supremum of the fee support can be unbounded. Note also that, for any $R_i > R_\sigma^\dagger$, the aggregate distribution of other households' fee strategies is the same, and matches that for the perfect information case described in the proof of Proposition 1.[35]

For a given f, $\hat{\phi}_H(f; R_i)$ can be locally increasing or decreasing in R_i, depending on beliefs about the strategies of neighboring households, and on the relative gradients of $Z_\lambda(\cdot)$ and $v(\cdot)$. Given threshold beliefs, a household with a high signal R_i expects y to be high. She anticipates high demand for blockchain space and so needs to pay a higher fee. On the other hand, she also expects the real value of a fee to be higher, putting downward pressure on the optimal fee (the 'digital gold' effect).

A household's expected payoff from using crypto, given signal R_i and fee f, is:

$$\hat{\pi}_H(f; R_i) \;=\; \frac{1}{2\sigma} \int_{R_i-\sigma}^{R_i+\sigma} \Big(Rg(y(R)) - (1-\rho) Z_\lambda\Big(\frac{1}{2\sigma} \int_{R-\sigma}^{R+\sigma} \hat{\phi}_H(f; R_j) \mathrm{d}R_j \Big) - \rho f v(y(R)) \Big) \mathrm{d}R, \tag{A.68}$$

where $\hat{\phi}_H(f; R_i) = 0$ for any $R_i \leq R_\sigma^\dagger$. Under the posited fee strategies, the household is indifferent between all fees in her support $[0, \bar{f}(R_i)]$. As zero is part of this support, the payoff is given by:

$$\hat{\pi}_H^\dagger(R_i) \;=\; \frac{1}{2\sigma} \int_{R_i-\sigma}^{R_i+\sigma} \Big(Rg(y(R)) - (1-\rho) Z_\lambda(y(R)) \Big) \mathrm{d}R. \tag{A.69}$$

Equation (A.69) is an integral, so a household's expected payoff $\hat{\pi}_H(f; R_i)$ is continuous in her signal R_i. At any threshold $R_\sigma^\dagger$ we must have $\hat{\pi}_H^\dagger(R_i) \leq 0$ for all $R_i \leq R_\sigma^\dagger$, and $\hat{\pi}_H^\dagger(R_i) > 0$ for all

[35] The distribution function $\hat{\phi}_H(f; R_i)$ tends to $Z_\lambda^{-1}(Z_\lambda(1) - \rho V f/(1-\rho))$ as $\sigma \to 0$, which matches the distribution in the perfect information case with $M = 0$. This can be shown by noting that, for $R_\sigma^\dagger < R_i < R_\sigma^\dagger + 2\sigma$, $\hat{\phi}'_H(f; R_i) = \lim_{\sigma \to 0} (\hat{\phi}_H(f; R_i) - \hat{\phi}_H(f; R_i - 2\sigma))/2\sigma = C'(R_i; f)$.

$R_i > R_\sigma^\dagger$. Thus $\hat{\pi}_H^\dagger(R_\sigma^\dagger) = 0$, by continuity.

Consider a household with a signal of exactly $R_\sigma^\dagger$. By Equation (A.63), the payoff is:

$$\begin{aligned}\hat{\pi}_H^\dagger(R_\sigma^\dagger) &= \frac{1}{2\sigma}\int_{R_\sigma^\dagger-\sigma}^{R_\sigma^\dagger+\sigma}\Big(Rg\Big(\frac{R-R_\sigma^\dagger+\sigma}{2\sigma}\Big)-(1-\rho)Z_\lambda\Big(\frac{R-R_\sigma^\dagger+\sigma}{2\sigma}\Big)\Big)\mathrm{d}R,\\ &= \int_0^1\Big((2\sigma s+R_\sigma^\dagger-\sigma)g(s)-(1-\rho)Z_\lambda(s)\Big)\mathrm{d}s,\end{aligned} \tag{A.70}$$

making a substitution $s = (R - R_\sigma^\dagger + \sigma)/2\sigma$. The requirement that $\hat{\pi}_H^\dagger(R_\sigma^\dagger) = 0$ means the value of $R_\sigma^\dagger$ must be given by Equation (28).

Finally, I need to show that no household deviates to a different η_H; i.e. all households prefer cash when $R_i \leq R_\sigma^\dagger$, and prefer crypto when $R_i > R_\sigma^\dagger$. When $R_i > R_\sigma^\dagger + 2\sigma$, $y = 1$ for sure, so Equation (A.69) implies:

$$\begin{aligned}\hat{\pi}_H^\dagger(R_i) &= R_i g(1)-(1-\rho)Z_\lambda(1),\\ &> g(1)\Big(R_\sigma^\dagger+2\sigma-(1-\rho)\frac{Z_\lambda(1)}{g(1)}\Big),\\ &> g(1)\Big((1-\rho)\frac{\int_0^1 Z_\lambda(s)\mathrm{d}s}{\int_0^1 g(s)\mathrm{d}s}+\sigma-(1-\rho)\frac{Z_\lambda(1)}{g(1)}\Big),\end{aligned} \tag{A.71}$$

where the last line comes from Equation (28) and noting $\int_0^1 sg(s)\mathrm{d}s < \int_0^1 g(s)\mathrm{d}s$. By Assumption 3, the final line in Equation (A.71) is strictly positive, so there is no incentive to deviate. Similarly, a household that observes $R_i \leq R_\sigma^\dagger - 2\sigma$ always earns a strictly negative payoff from using crypto.

Now suppose a household observes $R_i \in (R_\sigma^\dagger, R_\sigma^\dagger + 2\sigma]$. Using crypto earns:

$$\hat{\pi}_H^\dagger(R_i) = \frac{1}{2\sigma}\int_{R_i-\sigma}^{R_\sigma^\dagger+\sigma}\Big(Rg(y(R))-(1-\rho)Z_\lambda(y(R))\Big)\mathrm{d}R+\frac{1}{2\sigma}\int_{R_\sigma^\dagger+\sigma}^{R_i+\sigma}\Big(Rg(1)-(1-\rho)Z_\lambda(1)\Big)\mathrm{d}R. \tag{A.72}$$

By Assumption 3, $Rg(y) - (1-\rho)Z_\lambda(y) \leq Rg(1) - (1-\rho)Z_\lambda(1)$ for any $R > 0$. This means that, so long as $R_i > \sigma$:

$$\hat{\pi}_H^\dagger(R_i) \geq \frac{1}{2\sigma}\int_{R_i-\sigma}^{R_i+\sigma}\Big(Rg(y(R))-(1-\rho)Z_\lambda(y(R))\Big)\mathrm{d}R > \hat{\pi}_H^\dagger(R_\sigma^\dagger) = 0, \tag{A.73}$$

so this household has no incentive to deviate to cash. A similar argument applies for $R_i \in [R_\sigma^\dagger -$

$2\sigma, R_\sigma^\dagger$), so long as $R_i > -\sigma$. Thus we simply require $R_\sigma^\dagger > \sigma$; i.e.:

$$\sigma \;<\; \bar{\sigma} \;:=\; (1-\rho)\frac{\int_0^1 Z_\lambda(s)\mathrm{d}s}{\int_0^1 2sg(s)\mathrm{d}s}. \tag{A.74}$$

Part 2: Uniqueness in the limit as $\sigma \to 0$. This part consists of several steps. First, I show there exist lower and upper dominance regions: for sufficiently low (high) R_i, a household always uses cash (crypto), regardless of her beliefs about others' strategies. This means there exists an $\underline{R}$ that is the infimum of all signals where crypto is used, and an $\bar{R} \geq \underline{R}$ that is the supremum of all signals where cash is used. Second, I show that, as $\sigma \to 0$, the infimum of the support of any household's equilibrium fee strategies tends to zero. Third, I show, under Assumption 3, a household that observes signal $\underline{R}$ obtains an expected payoff no better than if her beliefs were described by a Laplacian prior, and this implies $\underline{R}$ approaches $R_\sigma^\dagger$ in the limit as $\sigma \to 0$. Fourth, a similar argument implies $\bar{R} \to R_\sigma^\dagger$ in the limit as $\sigma \to 0$. Finally, I obtain the required result.

Step 2A: Lower and upper dominance regions. I use a very similar argument used in the proof of Lemma 1. A household can do no worse than paying a fee of zero and ranking last for priority behind all other households. Thus:

$$\hat{\pi}_H^*(R_i) \;\geq \min_{y\in[0,1]} \Big\{(R_i-\sigma)g(y) - (1-\rho)Z_\lambda(y)\Big\}, \tag{A.75}$$

and so she will always use crypto, regardless of her beliefs, if $R_i > \sigma + (1-\rho)\min_y\{Z_\lambda(y)/g(y)\}$. Similarly, she will always use cash if $R_i \leq (1-\rho)Z_\lambda(0)/g(1) - \sigma$.

We define $\underline{R}$ to be the infimum of the set of signals where crypto is used, and $\bar{R}$ the supremum of the set of signals where cash is used. The existence of upper and lower dominance regions ensure the existence of $\bar{R}$ and $\underline{R}$ respectively. Clearly, $\underline{R} \leq \bar{R}$.

$$\underline{R} \;=\; \inf\{R_i : \eta_H(R_i) > 0\}, \qquad \bar{R} \;=\; \sup\{R_i : \eta_H(R_i) < 1\}. \tag{A.76}$$

Step 2B: Infimum of support of fee strategies tends to zero. Consider any signal R_i where crypto is used; i.e. $\eta_H(R_i) = 1$. Define $f_0 \geq 0$ to be the infimum of all fees played by a

household that observes R_i and uses an optimal strategy. That is:

$$f_0 \;=\; \inf\{f : \hat{\pi}_H(f; R_i) = \hat{\pi}^*_H(R_i)\}. \tag{A.77}$$

Then, by continuity, a fee of f_0 achieves the optimal payoff, so:

$$\begin{aligned}\hat{\pi}^*_H(R_i) \;=\; & \frac{1}{2\sigma}\int_{R_i-\sigma}^{R_i+\sigma}\Big[Rg\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\mathrm{d}R_j\Big) \\ & -(1-\rho)Z_\lambda\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\hat{\phi}_H(f_0;R_j)\mathrm{d}R_j\Big) - \rho f_0 v\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\mathrm{d}R_j\Big)\Big]\mathrm{d}R,\end{aligned} \tag{A.78}$$

where $\hat{\phi}_H(f; R_j)$ is the cumulative distribution function of fees for a household that observes signal R_j. We can compare this to the payoff from paying a fee of zero. As $\hat{\phi}_H(0; R_j) = 1$ for any R_j where $\eta_H(R_j) = 1$, we have:

$$\begin{aligned}\hat{\pi}^*_H(R_i) - \hat{\pi}_H(0;R_i) \;=\; & \frac{1}{2\sigma}\int_{R_i-\sigma}^{R_i+\sigma}\Big[-\rho f_0 v\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\mathrm{d}R_j\Big) \\ & -(1-\rho)\Big(Z_\lambda\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\mathrm{d}R_j\Big) - Z_\lambda\Big(\frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\hat{\phi}_H(f_0;R_j)\mathrm{d}R_j\Big)\Big)\Big]\mathrm{d}R.\end{aligned} \tag{A.79}$$

The right-hand side of Equation (A.79) tends to a finite limit as $\sigma \to 0$:

$$\lim_{\sigma\to 0}\Big(\hat{\pi}^*_H(R_i) - \hat{\pi}_H(0;R_i)\Big) \;=\; -\rho f_0 V - (1-\rho)\Big(Z_\lambda(1) - Z_\lambda(\hat{\phi}_H(f_0;R_i))\Big) \;\leq\; 0, \tag{A.80}$$

where I have used the fact that $\eta_H(R_i) = 1$. But $\hat{\pi}^*_H(R_i) \geq \hat{\pi}_H(0; R_i)$ by definition of optimality, so we must have $f_0 = 0$ and $\hat{\phi}_H(0; R_i) = 1$. This means that, for any $\epsilon > 0$, there is a $\sigma_\epsilon > 0$ such that, for all $\sigma < \sigma_\epsilon$, any optimal payoff in an equilibrium satisfies:

$$0 < \hat{\pi}^*_H(R_i) \;<\; \epsilon + \hat{\pi}_H(0;R_i). \tag{A.81}$$

Step 2C: Difference between $\underline{R}$ and $R^\dagger_\sigma$ tends to zero. Given R, the number of crypto users can be written:

$$y(R) \;=\; \frac{1}{2\sigma}\int_{R-\sigma}^{R+\sigma}\eta_H(R_j)\mathrm{d}R_j. \tag{A.82}$$

For any $R \in [\underline{R} - \sigma, \underline{R} + \sigma]$, we have:

$$y(R) \;\leq\; \frac{R - \underline{R} + \sigma}{2\sigma}, \tag{A.83}$$

since no households with signals $R_j \leq \underline{R}$ use crypto. This means a household with signal $\underline{R}$ will believe y is lower than if she held Laplacian beliefs, in which case y would be given by Equation (A.63) with $R^\dagger_\sigma$ replaced by $\underline{R}$.

Suppose a household receives a signal exactly equal to $\underline{R}$. Using Equation (A.81), for any $\epsilon > 0$, there is a $\sigma_\epsilon > 0$ such that, for all $\sigma < \sigma_\epsilon$:

$$\hat{\pi}^*_H(\underline{R}) \;<\; \epsilon + \frac{1}{2\sigma}\int_{\underline{R}-\sigma}^{\underline{R}+\sigma} \Big(Rg(y) - (1-\rho)Z_\lambda(y)\Big)\mathrm{d}R. \tag{A.84}$$

Using expression (A.83), together with the fact $g(y)/Z_\lambda(y)$ is increasing for all y, we have:

$$\begin{aligned}
\hat{\pi}^*_H(\underline{R}) - \epsilon \;&<\; \frac{1}{2\sigma}\int_{\underline{R}-\sigma}^{\underline{R}+\sigma} \Big(Rg\Big(\frac{R-\underline{R}+\sigma}{2\sigma}\Big) - (1-\rho)Z_\lambda\Big(\frac{R-\underline{R}+\sigma}{2\sigma}\Big)\Big)\mathrm{d}R, \\
&=\; \int_0^1 \Big((\underline{R} - s + 2\sigma s)g(s) - (1-\rho)Z_\lambda(s)\Big)\mathrm{d}s, \\
&=\; (\underline{R} - R^\dagger_\sigma)\int_0^1 g(s)\mathrm{d}s,
\end{aligned} \tag{A.85}$$

so long as $\underline{R} - \sigma > 0$. As $\underline{R} \geq (1-\rho)Z_\lambda(0)/g(1)$, a sufficient condition is $\sigma < (1-\rho)Z_\lambda(0)/g(1)$.

By definition, $\underline{R}$ is arbitrarily close to some R_i where crypto is used, and arbitrarily close to some other signal where cash is preferred. Thus, by continuity, $\hat{\pi}^*_H(\underline{R}) = 0$. This means that, for any $\epsilon > 0$, there is a $\sigma'_\epsilon = \min\{\sigma_\epsilon, (1-\rho)Z_\lambda(0)/g(1)\} > 0$ such that, for all $\sigma < \sigma'_\epsilon$:

$$\underline{R} \;>\; R^\dagger_\sigma - \frac{\epsilon}{\int_0^1 g(s)\mathrm{d}s}. \tag{A.86}$$

Step 2D: Difference between $\bar{R}$ and $R^\dagger_\sigma$ tends to zero. A very similar argument to step 2B can be employed for $\bar{R}$. A household who observes a signal $\bar{R}$ believes y is at least as large as it would be under a Laplacian prior. Thus, for any $\epsilon > 0$, there is a $\sigma''_\epsilon > 0$ such that, for all $\sigma < \sigma''_\epsilon$:

$$\bar{R} \;<\; R^\dagger_\sigma + \frac{\epsilon}{\int_0^1 g(s)\mathrm{d}s}. \tag{A.87}$$

Step 2E: Actions approach threshold equilibrium at $R_\sigma^\dagger$. Steps 2C and 2D imply, for any $\delta > 0$, there is a $\sigma_\delta > 0$ such that, for all $\sigma < \sigma_\delta$:

$$\bar{R} - \delta \;\; < \;\; R_\sigma^\dagger \;\; < \;\; \underline{R} + \delta. \tag{A.88}$$

By definition of $\underline{R}$ and $\bar{R}$, $\eta_H(R_i) = 0$ for all $R_i \leq \underline{R}$ and $\eta_H(R_i) = 1$ for all $R_i > \bar{R}$. This is the required result.

7.8 *Proof of Proposition 6*

Given the realization of the technology R, the number of crypto users is given by Equation (A.63). Then the expected value of crypto is:

$$\begin{aligned} \mathbb{E}[v(y)] &= \frac{1}{R_1 - R_0}\Big(\int_{R_\sigma^\dagger - \sigma}^{R_\sigma^\dagger + \sigma} v\Big(\frac{R - R_\sigma^\dagger + \sigma}{2\sigma}\Big)\mathrm{d}R \;\; + \;\; \int_{R_\sigma^\dagger + \sigma}^{R_1} V \mathrm{d}R\Big), \\ &= \frac{1}{R_1 - R_0}\Big(2\sigma \int_0^1 v(y)\mathrm{d}y \;\; + \;\; (R_1 - R_\sigma^\dagger - \sigma)V\Big), \end{aligned} \tag{A.89}$$

and the variance is:

$$\mathbb{V}[v(y)] \;\; = \;\; \frac{1}{R_1 - R_0}\Big(2\sigma \int_0^1 v(y)^2 \mathrm{d}y \;\; + \;\; (R_1 - R_\sigma^\dagger - \sigma)V^2\Big) \;\; - \;\; \mathbb{E}[v(y)]^2. \tag{A.90}$$

Then volatility is given by Equation (29). Since volatility is positive by definition, it is increasing in $R_\sigma^\dagger$ if and only if its square is increasing; i.e. if and only if:

$$(R_1 - R_\sigma^\dagger)V^2 > \sigma J, \tag{A.91}$$

where J is given in the statement of the Proposition. If $J \leq 0$, then this is true for any σ. Otherwise, it is true so long as $\sigma < (R_1 - R_\sigma^\dagger)V^2/J$. As $R_\sigma^\dagger$ is itself decreasing in λ (because $Z_\lambda(n)$ is decreasing in λ for all n), this is the required result.