The public blockchain ecosystem:

An empirical analysis *

Felix Irresberger† Kose John‡ Peter C. Mueller§ Fahad Saleh¶

Abstract

This paper provides an empirical overview of the largely unexplored public blockchain ecosystem. Our overview highlights that only a few blockchains dominate the ecosystem although no single blockchain, not even Bitcoin, dominates uniformly. We explain our empirical findings with a simple theoretical framework that establishes three key economic attributes - adoption, scale, and security - as the determinants of blockchain user utility. We examine each blockchain along those dimensions empirically. Comparing across these attributes, we establish whether a blockchain could be optimal relative to all other blockchains for some user type. Applying that comparison yields that only a few blockchains could be optimal for some user type. Our results thus explain why only a few blockchains dominate the broader blockchain ecosystem and further provide an empirical framework from which to evaluate progress within the blockchain ecosystem.

Keywords: Blockchain, Cryptoasset, Cryptocurrency, Scale, Security, Adoption, DeFi
JEL Classification: C0, G0, O3

*We thank Carol Alexander, Carsten Bienz, Franz Hinzen, Engin Iyidogan, Laura Liu, William Mann, Katya Malinova, Raghu Rau, Ioanid Roşu, Larry Wall, Baozhong Yang, David Yermack, Peter Zimmerman, Xun Zhong, and participants at the Bergen Fintech Conference, Northern Finance Association Annual Meeting, Toronto Fintech Conference, Cryptocurrency Research Conference, Paris Webinar on Financial Technology and Crypto, 2nd Yushan Conference, and seminars at Durham University, McGill University, Sussex University, and University of Leeds for valuable comments.

†Durham University. Email: felix.irresberger@durham.ac.uk

‡Corresponding author: New York University, Stern School of Business; 44 West 4th Street, Suite 9-190, New York, New York 10012; Telephone: (212) 998-0337; Email: kjohn@stern.nyu.edu

§University of Oklahoma. Email: pmueller@ou.edu

¶Wake Forest University. Email: salehf@wfu.edu

1 Introduction

There exist hundreds of public blockchains, but the economics literature has studied only Bitcoin in depth. While each individual blockchain platform might not be worthy of study, it is unclear whether there are blockchains other than Bitcoin that deserve attention. The key purpose of this paper is to examine the blockchain universe to identify which elements might be worthy of study from an economic perspective. Our main finding is that there exists an exclusive set of blockchains, which we term the *blockchain frontier*, that could generate the highest user utility among all blockchains for some user type. Crucially, no single blockchain is optimal for all user types, and most blockchains are not optimal for any user type. Our blockchain frontier excludes those blockchains that are not optimal for any user type, thereby highlighting those public blockchains most relevant from an economic welfare perspective.

We begin in Section 2 with a broad overview of the public blockchain ecosystem. Immediately, it becomes clear that the universe of blockchains consists of many small platforms unlikely to be of broad economic significance. Nonetheless, there is also clear evidence of an evolution since Bitcoin's birth in 2009. In particular, we document an explosion in the launching of platforms that are fundamentally different from Bitcoin, many of which possess nontrivial market capitalization. As an example, the number of blockchains employing protocols different than Bitcoin to generate agreement on ledger contents, commonly referred to as consensus, far outnumber those using the same protocol as Bitcoin. It is noteworthy that Bitcoin remains the largest blockchain in terms of market capitalization, but it is also important to recognize that Bitcoin does not dominate across all relevant economic quantities. Of particular note, Bitcoin has processed far fewer transactions than several other blockchain platforms. Moreover, Bitcoin possesses narrow functionality so that it has limited relevance for important blockchain applications such as Decentralized Finance (DeFi). As a whole, our empirical overview unveils a few dominant blockchain platforms but no monolithic leader, not even Bitcoin. To understand these empirical patterns and the economic relevance of individual blockchains more deeply, we turn to a theoretical framework.

Our theoretical framework, put forth in Section 3, establishes that a blockchain user's welfare depends critically upon three characteristics of the blockchain: adoption, scale, and security. User utility increases in each of these characteristics. Adoption refers to the number of active users on the same blockchain platform equipped to engage in an economic interaction of interest. For example, if Alice would like to exchange assets without an intermediary, then her utility would increase in the number of active users that could serve as her counterparty as more such users would yield improved liquidity. More generally, a larger active user base improves the likelihood of finding a suitable counterparty in any economic interaction so that adoption increases transaction surplus and thereby enhances user utility. Scale refers to the rate at which transactions are added to the blockchain. We demonstrate that a higher scale enables not only more expeditious processing but also endogenously lower transaction fees, thereby enhancing user utility. Security refers to the likelihood that a transaction could be reversed. In practice, counterparties impose delays in settlement to compensate for such security risks. Consequently, higher security blockchains generate

higher user utility because higher security implies lower settlement delays.

We empirically implement our theoretical framework in Section 4. Specifically, we compare existing blockchains on the dimensions of adoption, scale, and security. We find that Bitcoin is the most widely adopted among users seeking simple payments, but Bitcoin does not lead on any other dimensions. Of particular note, Bitcoin's lack of functionality renders it without any active user base for all economic interactions beyond payments. Consequently, Bitcoin has no economic value for users interested in activities such as DeFi transactions, gaming, gambling or data storage. We find that Ethereum leads by a wide margin on DeFi and narrowly over EOS on gaming. TRON leads all other platforms, even Ethereum, with regard to data storage and gambling applications. While Bitcoin, Ethereum and TRON all lead on some aspect of adoption, none lead with regard to scale. The EOS blockchain leads with regard to scale which enables EOS to provide quick transaction processing at low costs relative to all other blockchain platforms. All of the referenced blockchains lag behind on security when compared to Stellar, which is the most secure blockchain.

The purpose of our theoretical model and its empirical implementation is to identify those blockchains that fit within the blockchain frontier. As discussed, the blockchain frontier excludes any blockchain that cannot provide the highest utility among all blockchains for any user type. To identify this set of blockchains, we invoke one of our theoretical results from Section 3, which establishes that a blockchain is in the frontier if and only if it is not dominated by any other blockchain on several pairwise comparisons involving the key blockchain characteristics of adoption, scale, and security. Applying the aforementioned comparisons, we find a blockchain frontier consisting of seven blockchains. The set includes all five of the previously referenced blockchains that lead on some characteristic: Bitcoin, Ethereum, TRON, EOS and Stellar. It also includes Binance Coin and Bitcoin Satoshi's Vision.

As our theory demonstrates, a blockchain that leads on adoption for users with any particular economic purpose (e.g., payments, DeFi, etc.) is necessarily part of the blockchain frontier. Intuitively, this follows because a user who is insensitive to wait times values only the transaction surplus from her economic interaction, and that transaction surplus depends exclusively on finding a suitable counterparty. Consequently, such a user finds whichever blockchain leads on adoption with respect to her economic purpose to be optimal for her. This means that Bitcoin is best for a user desiring to conduct a simple purchase or sale so long as the user is sufficiently insensitive to wait times. Similarly, a wait insensitive user desiring to conduct a financial transaction without an intermediary (i.e., a DeFi transaction) would prefer Ethereum to all other blockchains, and a wait insensitive user desiring to engage in decentralized data storage would prefer TRON to all other blockchains. Accordingly, Bitcoin, Ethereum and TRON are part of the blockchain frontier.

A blockchain that leads on scale also necessarily enters the blockchain frontier. Intuitively, users that are highly sensitive to waiting prefer the highest scale blockchain. Such users tend to be those that are interested in applications that involve a large number of actions such as some gaming applications. Each action in a game on a blockchain typically requires a transaction for that action. Thus, some gaming applications involve frequent transactions, and frequent transactions necessitate

quick and cheap processing for each individual transaction. In turn, as we demonstrate in Section 3, the highest scale blockchain most appropriately suits these needs as it not only provides quick processing of transactions but also endogenously generates low transaction costs. As noted, EOS leads on scale and thus is necessarily also part of the blockchain frontier. It is also noteworthy that EOS attracts a high level of gaming activity potentially because its scale makes it well suited for such activities.

A blockchain leading on security does not imply its inclusion in the blockchain frontier. This is because counterparties internalize security risks and compensate for those risks by imposing settlement delays upon users. As we demonstrate in Section 3, those settlement delays depend not only upon the blockchain's security but also upon the rate at which blocks are added to the blockchain. In particular, less secure blockchains incur higher settlement delays to compensate for the lack of security. However, our results establish that a given level of security implies a settlement delay of a particular number of blocks to be added to the blockchain, not a specific amount of time. In turn, since users incur disutility with respect to wait times rather than the number of blocks, user disutility associated with settlement delays depends also on the block rate of a blockchain.

While a blockchain leading on security does not imply its inclusion into the blockchain frontier, a blockchain generating the lowest settlement delay does imply such inclusion. Binance Coin exhibits the lowest settlement delay and is therefore a part of the blockchain frontier. Binance Coin is used heavily in trading with the Binance cryptocurrency exchange. The low settlement delay is especially advantageous for users interacting frequently with a cryptocurrency exchange since the low settlement delay enables such users to trade frequently without lengthy interruptions.

Stellar and Bitcoin Satoshi's Vision are also part of the blockchain frontier. These blockchains feature in the frontier because they perform well on several of the key blockchain characteristics of adoption, scale and security. This overall performance is sufficient such that no single blockchain induces a higher utility than either of them across all user types and hence enables both to enter the blockchain frontier.

Related Literature Our paper joins a growing literature on blockchain economics that began with Harvey (2016) and Yermack (2015, 2017). Chen, Cong, and Xiao (2019) provide an overview of that literature. Li, Shin, and Wang (2019), Liu and Tsyvinski (2020), Liu, Tsyvinski, and Wu (2019), Makarov and Schoar (2019), Shams (2020), Griffin and Shams (2020) and Härdle, Harvey, and Reule (2020) study the asset pricing dimensions of cryptoasset markets. In contrast, we focus on the economic features of the underlying blockchain. We empirically analyze consensus protocols, a topic that has been extensively studied in theoretical terms. Most studies consider PoW. Prominent studies of PoW include Arnosti and Weinberg (2018), Basu, Easley, O'Hara, and Sirer (2018), Budish (2018), Chiu and Koeppl (2018), Biais, Bisière, Bouvard, and Casamatta (2019), Chiu and Koeppl (2019), Benetton, Compiani, and Morse (2019), Easley, O'Hara, and Basu (2019), Hinzen, John, and Saleh (2020), Huberman, Leshno, and Moallemi (2019), Saleh (2019), Alsabah and Capponi (2020), Cong, He, and Li (2021a), and Pagnotta (2020). Prominent studies

of PoS include Irresberger (2019), Rosu and Saleh (2021), and Saleh (2021).

This paper proceeds as follows. Section 2 details the major consensus protocols and provides a descriptive analysis of the public blockchain ecosystem. Section 3 puts forth our theoretical framework, while Section 4 implements that framework empirically. Section 5 describes the blockchain frontier resulting from our empirical analysis. Section 6 concludes.

2 The public blockchain ecosystem: An overview

This section provides a descriptive analysis of the public blockchain ecosystem, a necessary precondition for a careful study of the broader blockchain universe. We document the existence of hundreds of public blockchains, the consensus protocols they use, and a stark heterogeneity in relevance, as indicated by market capital and blockchain usage. We first give an overview of consensus protocols and then provide evidence on the current state of ecosystem with respect to them. Our results highlight and motivate the need for an economic framework to explain the success of very few blockchains within the ecosystem.

2.1 Institutional background on consensus protocols

A blockchain is an electronic ledger that is distributed across a network of agents referred to as validators.[1] Blockchain validators differ from blockchain users in that users submit transactions for processing on the blockchain, whereas validators determine whether those transactions achieve settlement. Blockchain users generally submit transactions via a native platform currency that we hereafter refer to as the native cryptoasset.[2] For the blockchain to be useful for users, there must be a process by which submitted transactions achieve settlement. By definition, a transaction is considered settled on the blockchain only if the validators agree on the transaction being entered on the blockchain. Accordingly, agreement among validators, known as *consensus*, is a key concern for any blockchain. Each blockchain attempts to resolve that concern via a set of rules for updating the blockchain known as a *consensus protocol*. Such protocol is a technical feature that is often used to distinguish between different blockchain designs. For this study, we partition the space of consensus protocols into five groups: (1) PoW, (2) PoS, (3) Hybrid PoW/PoS, (4) DPoS, and (5) Nonstandard protocols. The remainder of this subsection provides a brief description of each category.

Proof-of-Work PoW was first introduced by Dwork and Naor (1992) as a method to disincentivize spam emails. PoW then gained broad attention when Nakamoto (2008) employed it as the consensus protocol for Bitcoin. PoW was also the most prominent consensus protocol adopted by early public blockchain alternatives to Bitcoin, such as Litecoin and Dogecoin. Currently, the two largest blockchains, as measured by the market value of their native cryptoassets, Bitcoin and

[1] For Bitcoin and similar blockchains, these validators are referred to as miners.

[2] For example, Bitcoin has a native cryptoasset called bitcoin, and Ethereum has a native cryptoasset called ether. Some blockchains, such as Ethereum, also allow for other assets to be exchanged on the platform.

Ethereum, employ PoW. Under PoW, participating in the process of validating new blocks requires solving a computational puzzle. Nakamoto (2008) argues that the computational complexity of this puzzle makes it difficult to change the contents of the ledger which in turn helps generate consensus.[3] In subsequent work, however, Biais et al. (2019) argue that persistent disagreement can arise on PoW blockchains. PoW has further been criticized on the grounds of requiring excessive amounts of resources. Mora, Rollins, Taladay, Kantar, Chock, Shimada, and Franklin (2018) provide empirical evidence in favor of that claim and establish that the PoW structure generates an exorbitant energy expenditure. These and other concerns associated with PoW (see, e.g., Hinzen et al. 2020) have spurred researchers on a quest to uncover alternative protocols.

Proof-of-Stake PoS constitutes one of the early alternatives to PoW. King and Nadal (2012) provide the first PoS proposal. PoS overcomes PoW's need for exorbitant energy expenditure by removing PoW's computationally complex puzzle from the consensus process. The first pure PoS protocol was employed on the Nxt blockchain in 2013. Under PoS, agents are randomly conferred the authority to validate the next block. The likelihood of being chosen depends on an agent's "stake" which refers to an agent's overall holdings of the native cryptoasset.[4]

Hybrid PoW/PoS Some blockchains have attempted to combine both PoW and PoS protocols in an effort to capture the benefits of both protocols. The first such hybrid consensus protocol was utilized on the Peercoin blockchain in 2012. Since then, dozens of other blockchains have followed this approach. Prominent Hybrid blockchains include Dash and Decred. Both blockchains employ PoW to validate blocks, but grant governance rights to agents based on their stake in the native cryptoasset. Such governance rights can include the right to vote on changes to the protocol or confirmation of the validity of blocks.

Delegated Proof-of-Stake Both PoW and pure PoS blockchains have faced criticism for their alleged inability to process transactions quickly. A variant of PoS protocols known as Delegated Proof-of-Stake (DPoS) arose in response to this criticism. DPoS was first introduced by Daniel Larimer, the eventual founder of the blockchain EOS. Under DPoS, a fixed number of delegates, also called "witnesses," validate new blocks. Holders of the native cryptoasset vote for delegates. Similar to PoS, the number of votes is assigned in proportion to holdings of the native cryptoasset. The relatively small and fixed number of delegates reduces the validating agent network size compared to traditional PoS protocols. This small network size, in theory, allows for faster transaction rates, as fewer agents have to converge on a common version of the ledger.

Nonstandard protocols Research on new consensus protocols is an active field. Numerous proposed blockchain protocols starkly differ from the protocols described above. We group these

[3]For further context regarding PoW, the interested reader can consult Biais et al. (2019).
[4]For further context regarding PoS, the interested reader can consult Saleh (2021).

protocols and refer to them as Nonstandard protocols. Within this group, no single protocol is widely used. The most prominent public blockchains within this category are Ripple and Stellar.

2.2 Empirical evidence on public blockchains

To provide an overview of the public blockchain ecosystem, we use cross-sectional data from cryptoslate.com on hundreds of public blockchains as of February 21, 2021.

For our analysis, we distinguish public blockchains from cryptoassets. Each public blockchain could possess multiple cryptoassets, but each public blockchain typically has only one native cryptoasset, which is created at the inception of the blockchain.[5] Cryptoslate.com lists a total of 2,400 different cryptoassets. Approximately one third of this set is made up of native cryptoassets with an aggregate market capitalization of ca. $1,594 billion, and two thirds consist of tokens with a total market capitalization of $203 billion. We subsequently focus on the 783 native cryptoassets corresponding to a unique public blockchain.[6]

Figure 1 plots native asset market capitalization (on a log-scale) against blockchain announcement dates for the full cryptoslate.com sample. The majority of public blockchains carries little to no value in terms of market capitalization. Half of all blockchains (400) exhibit a market capitalization of its native asset below $1 million or carry no value (e.g., as it is not traded on exchanges or has been abandoned). There are a total of 344 blockchains with native asset market capitalizations between $1 million and $1 billion, and only 39 with market capitalization above $1 billion. The latter group consists not only of older blockchains like Bitcoin, which may have a first-mover's advantage, but also of newer blockchains, such as EOS, TRON or Binance Coin.

To distinguish between different types of blockchains, we divide the large number of public blockchains into groups based on the consensus protocol they employ. Table 1 characterizes the public blockchain ecosystem by consensus protocol in terms of raw counts over time until the end of 2020. Bitcoin was the first blockchain launched in 2009 and employs PoW as a consensus protocol. Over the years, many other public blockchains have employed PoW as their consensus protocol, the most prominent ones being Litecoin (LTC), launched in 2011, Ethereum (ETH), launched in 2014, or Bitcoin blockchain forks such as Bitcoin Cash (BCH) and Bitcoin Satoshi's Vision (BSV), launched in 2017 and 2018, respectively. Alternative protocols such as PoS or Hybrid PoW/PoS started to gain significantly in numbers starting from 2014 onwards. Although

[5] As an example, Ethereum has the native asset ether (ETH) but allows for the creation of many other nonnative assets, such as Basic Attention Token (BAT) or Maker (MKR). Nonnative assets are generally referred to as tokens and have been extensively studied within the initial coin offerings (ICO) literature (see, e.g., Malinova and Park 2018, Chod and Lyandres 2019, Davydiuk, Gupta, and Rosen 2019, Gan, Tsoukalas, and Netessine 2020, Lee, Li, and Shin 2019, Lyandres, Palazzo, and Rabetti 2019, Howell, Niessner, and Yermack 2020, Li and Mann 2020, and Liu, Sheng, and Wang 2020).

[6] To identify all native cryptoassets, we cross-check the information given by cryptoslate.com with the existence of a block explorer and perform additional background research on the history of the blockchain in case the project was abandoned over time. Whenever the announcement date of a blockchain is not disclosed on cryptoslate.com, we take the timestamped date of the genesis block as the announcement date of the blockchain. We also cross-check the information on the consensus protocol employed by a blockchain disclosed on cryptoslate.com with additional web searches.

Figure 1: Blockchain announcement dates and native asset market capital.

This figure shows a scatterplot of blockchains' native asset market capital (log-scale) against blockchain announcement dates. Data are obtained from cryptoslate.com as of February 21, 2021. Whenever the announcement date of a blockchain is not disclosed on cryptoslate.com, we take the timestamped date of the genesis block as the launch date of the blockchain.

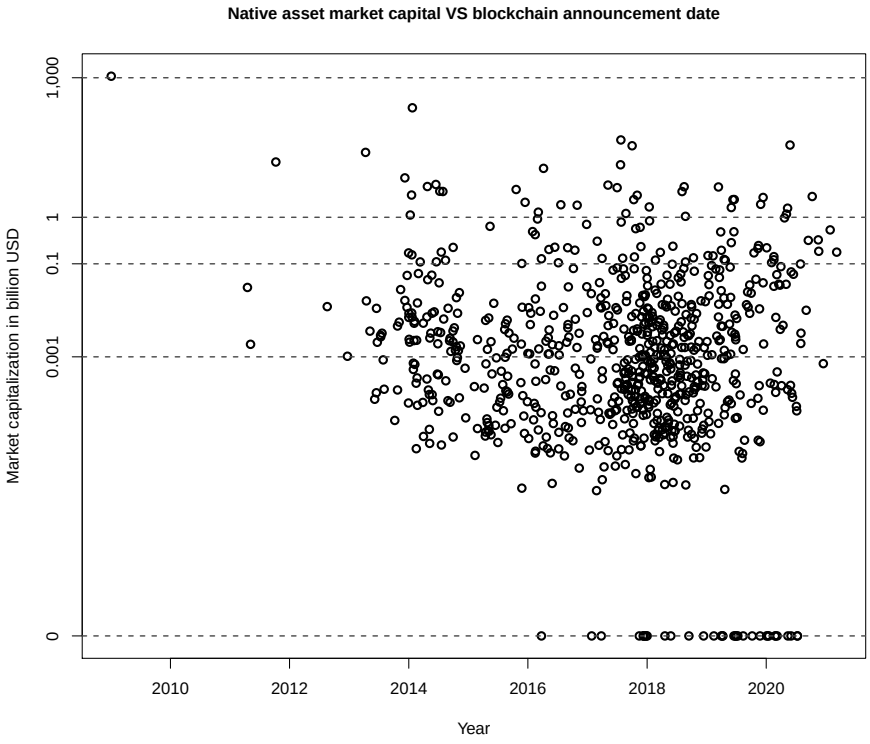


Table 1: Number of newly launched blockchains by consensus protocol

This table presents the public blockchain ecosystem by consensus protocol in terms of raw counts from 2009 to the end of 2020. Data are obtained from cryptoslate.com. Two blockchains from January/February 2021 are omitted in this table for brevity.

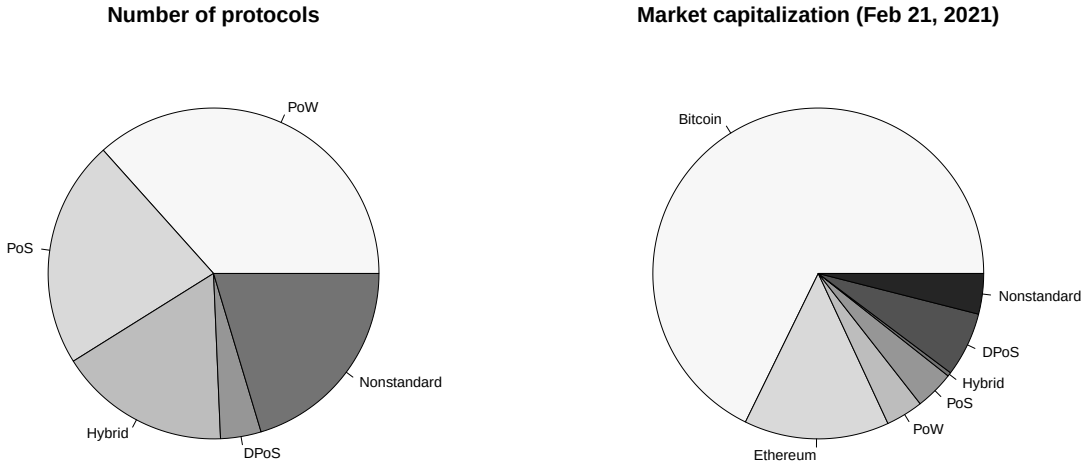
Protocol / Year	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
PoW	1	0	3	1	17	39	28	26	63	72	26	10
PoS	0	0	0	0	0	17	13	14	26	63	30	11
Hybrid	0	0	0	1	4	16	8	23	32	29	10	8
DPoS	0	0	0	0	0	2	1	8	7	3	6	4
Nonstandard	0	0	0	0	2	7	5	14	35	50	30	16
Total (N=781)	**1**	**0**	**3**	**2**	**23**	**81**	**55**	**85**	**163**	**217**	**102**	**49**

nonstandard protocols started with blockchains such as Ripple (XRP) in 2013, we have seen the number of nonstandard blockchains increase dramatically from 2016 to 2018 and the new number of nonstandard and PoW blockchains are comparable in 2019 and 2020, respectively. Although much fewer in numbers compared to other protocols, DPoS blockchains such as EOS (EOS) and TRON (TRX) started to emerge more in 2016 and onwards. PoW no longer dominates as the choice for a blockchain's consensus protocol, but no specific protocol has taken PoW's dominant position; rather, recently launched public blockchains frequently employ alternative protocols.

The left panel in Figure 2 shows the distribution of raw counts of consensus protocols. Although

Figure 2: Number of blockchains and market capitalization by consensus protocol.

This figure is a snapshot of the distribution of the raw number of introduced public blockchains by consensus protocol (left) and the native asset market capital share as of February 21, 2021 (right). The full sample consists of 783 blockchains with native cryptoassets listed at cryptoslate.com.

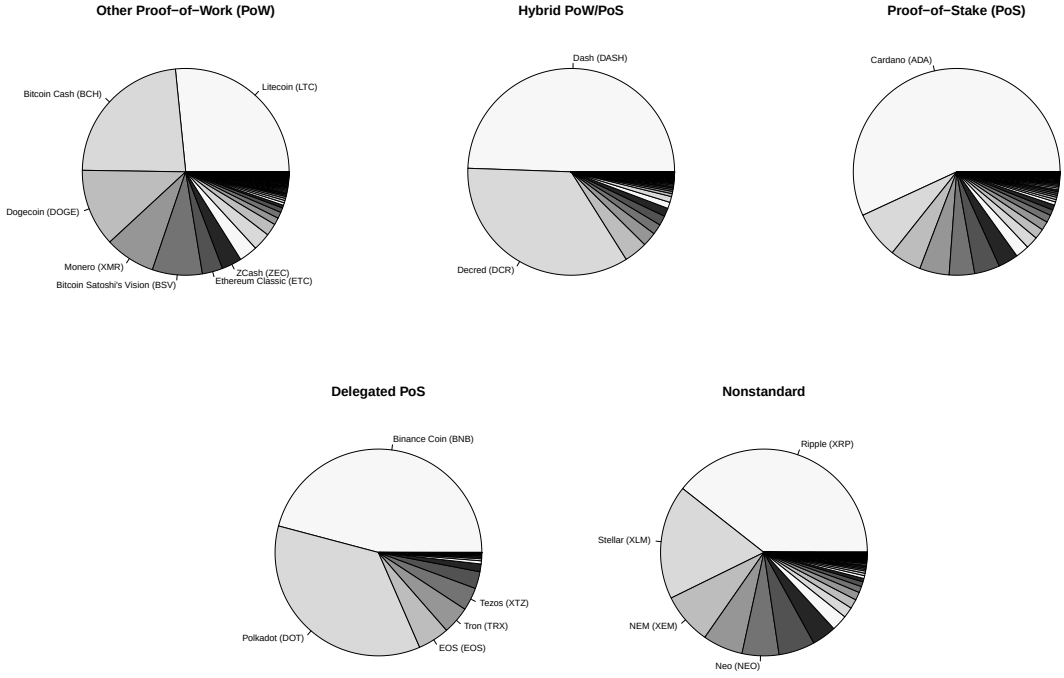


the number of blockchains employing PoW is highest among all protocol groups, alternatives such as PoS, DPoS, and Nonstandard protocols are not far behind. However, if we view the ecosystem through the lens of market capital share, we see a heavily skewed distribution of relevance. The right panel in Figure 2 shows the market share (as of February 21, 2021) of Bitcoin (BTC), Ethereum (ETH), and native cryptoassets of blockchains using PoW, PoS, Hybrid, DPoS, and Nonstandard protocols, respectively. Bitcoin accounts for two thirds of the total market capitalization of the public blockchain ecosystem, while Ethereum captures a 14.2% market share. The remainder of the market capital is divided relatively evenly across other PoW, PoS and Nonstandard protocols. DPoS captures a share of only 1.2% of the native asset market capitalization.

Figure 3 shows the distribution of market shares within each consensus protocol group. Within each group, most of the market capital share is captured by only a handful of blockchains. Other relevant PoW blockchains include Bitcoin Cash (BCH), Bitcoin Satoshi's Vision (BSV), Litecoin

Figure 3: Market capital share within consensus protocol group.

This figure shows native asset market capital share distributions within consensus protocol groups for 783 public blockchains. Data are from cryptoslate.com and are as of February 21, 2021. Major blockchains and their native asset ticker symbol are next to the market capital share. 'Other PoW' excludes Bitcoin (BTC) and Ethereum (ETH).



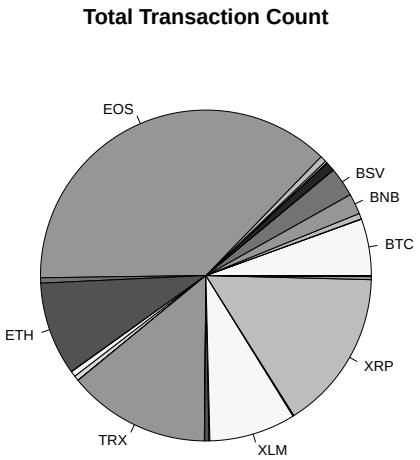
(LTC), Monero (XMR) and Dogecoin (DOGE), which together capture over 75% of the market capital attributed to PoW blockchains (excluding Bitcoin and Ethereum). Within PoS, Cardano (ADA) captures over half of the market capital; within the Hybrid group, DASH (DASH) and Decred (DCR) are the most relevant. DPoS is highly dominated in terms of market capitalization by Binance Coin (BNB) and Polkadot (DOT), with EOS (EOS), Tezos (XTZ), and TRON (TRX) together capturing less than a quarter of all market capitalization in this protocol group. The most important nonstandard blockchain is Ripple (XRP), with Stellar (XLM) being a distant second.

For the remainder of the paper, we restrict our empirical analysis to the set of blockchains with daily time-series of network characteristics (e.g., number of on-chain transactions, active addresses, block counts) available on coinmetrics.io. This subsample is small in numbers but already represents the majority of the overall public blockchain universe (ca. 99% of market capital of *native cryptoassets* and 88.6% of *all* cryptoassets, including tokens, listed on cryptoslate.com). The sample blockchains' names and announcement year, market capitalization and the sum of all transaction counts since inception are documented in Table 2.

Finally, we consider blockchain usage as another economic quantity of interest. Figure 4 shows the share of transactions on each blockchain since its inception. Bitcoin (BTC), the oldest PoW

Figure 4: Total transaction count by blockchain.

This figure shows the distribution of total native asset transaction count for 27 major blockchains from the coinmetrics.io sample up until February 21, 2021. Blockchains with major transaction count shares are annotated with their native asset ticker symbol.



blockchain with by far the highest market capitalization, contributes to only 5.5% of all transactions. Ethereum (ETH) captures only 9.1% of the total transaction count. The vast majority of the total transaction count is attributable to EOS and TRON, two blockchains with DPoS protocols. However, Ripple (XRP), a nonstandard blockchain, captures around 15.7% of all transactions.

Table 2: coinmetrics.io blockchain sample.

This table lists all blockchain names, their symbol, announcement year, native asset market capitalization in billions USD, and native asset total transaction count since inception. Network data are from coinmetrics.io. Market capitalization is based on quantities obtained as of February 21, 2021. Consensus protocols are divided into Proof-of-Work (PoW), Proof-of-Stake (PoS), Hybrid, Delegated Proof-of-Stake (DPoS), and Nonstandard.

Blockchain	**Symbol**	**Market cap** (in USD billions)	**Transaction count** (in millions)	**Year**
PoW				
Bitcoin	BTC	1080.00	617.55	2009
Ethereum	ETH	225.78	1019.50	2014
Litecoin	LTC	15.45	59.13	2011
Bitcoin Cash	BCH	13.46	61.30	2017
Dogecoin	DOGE	7.04	67.68	2013
Bitcoin SV	BSV	4.54	320.55	2018
Ethereum Classic	ETC	1.86	58.18	2016
ZCash	ZEC	1.82	6.84	2016
Digibyte	DGB	1.12	20.73	2014
Bitcoin Gold	BTG	0.57	1.75	2017
Verge	XVG	0.42	4.66	2016
Vertcoin	VTC	0.05	2.66	2017
Hybrid				
Dash	DASH	3.01	96.52	2014
Decred	DCR	2.10	8.60	2015
PoS				
Cardano	ADA	34.50	4.24	2017
WAVES	WAVES	1.29	47.49	2016
PIVX	PIVX	0.10	1.20	2015
DPoS				
Binance Coin	BNB	46.00	225.07	2017
Polkadot	DOT	35.75	11.01	2020
EOS	EOS	4.93	4184.65	2017
TRON	TRX	4.34	1554.38	2017
Tezos	XTZ	3.59	33.38	2014
Lisk	LSK	0.49	3.53	2016
Nonstandard				
Ripple	XRP	24.86	1749.45	2013
Stellar	XLM	11.28	943.16	2016
NEM	XEM	5.08	9.40	2014
NEO	NEO	3.63	54.75	2014

Thus, while Bitcoin remains the most studied blockchain in the economics literature and the one with the highest market capitalization, it is far from the most used blockchain in terms of on-chain transaction counts.

In summary, we find that there are only a few public blockchains of particular relevance, as measured by native asset market capitalization and transaction counts, and that these blockchains employ a variety of consensus protocols. None of the consensus protocol groups seem to dominate the others, but rather we observe a stark heterogeneity in relevance even within protocol groups. In the following, we put forward a framework that helps explain the heterogeneity in blockchain relevance by demonstrating that only a small set of blockchains are optimal for users to employ.

3 Theoretical Framework

Our model examines a setting in which users arrive randomly to a blockchain and seek to transact on that blockchain. We examine how the welfare of each user varies as a function of the blockchain's characteristics. We demonstrate that user utility depends upon three key blockchain attributes: adoption, scale, and security. Subsequently, we use these three attributes as the attributes of our empirical framework.

We model an infinite-horizon continuous time setting with time indexed by $t \geqslant 0$. Users with unit transaction demand arrive randomly according to a Poisson Process with rate $a > 0$. We assume that users are heterogeneous in terms of their economic purpose for using the blockchain, the value they place on the economic exchange and the disutility per unit time they incur from waiting for their transaction to be settled. With regard to heterogeneity of economic purpose, we assume that each User i possesses an economic type $\tau_i \in \mathcal{T}$. This economic type, τ_i, reflects that users have different purposes for using the blockchain in practice. For example, some users transact via the blockchain to engage in regular purchases (i.e., payments) whereas others transact via the blockchain to engage in more complex financial transactions that bypass traditional intermediaries (i.e., Decentralized Finance). Accordingly, two elements of $\mathcal{T}$ include payments and Decentralized Finance (DeFi), but there are other economic purposes for using a blockchain as we discuss in Section 4. With regard to how a user values the economic exchange, we follow Cong, Li, and Wang (2021b) and assume that each User i possesses a type $u_i \sim F[0, \overline{u}]$ which is proportional to her transaction surplus. With regard to heterogeneity of wait disutility, we assume that each User i incurs a disutility of waiting per unit time of $c_i \sim G[0, \overline{c}]$ with G being strictly increasing and twice continuously differentiable. We allow that a user may ameliorate her total disutility from waiting by paying a fee but users also dislike paying fees. This modelling choice reflects the fact that blockchain users are processed in descending fee order in practice so that higher fees induce lower wait times. Formally, User i selects fee $f_i \geqslant 0$ by solving:

$$f_i = \underset{f \geqslant 0}{\arg\max} \quad \underbrace{u_i \cdot \Psi(N_{\tau_i})}_{\text{Transaction Surplus}} - \underbrace{c_i \cdot W(f)}_{\text{Wait Disutility}} - \underbrace{f}_{\text{Fee}} \tag{1}$$

where N_{τ_i} denotes the number of active users on the blockchain with economic purpose τ_i and $W(f)$ denotes the expected wait of User i if she pays fee $f \geqslant 0$. Our specification of transaction surplus follows Cong et al. (2021b) in that we assume that $\Psi' > 0$ so that user transaction surplus depends positively upon the number of users on the blockchain with the same economic purpose. This assumption reflects the fact that it is easier to find a suitable counterparty in a larger community. We refer to N_{τ_i} as adoption hereafter and emphasize that user welfare increases in adoption.

A novelty of our analysis is that we expand the expected wait time, $W(f)$, to incorporate a novel feature relative to prior literature. In particular, our wait time term decomposes into two components with the latter term being novel relative to prior works:

$$W(f) = \underbrace{W_P(f)}_{Processing\ Time} + \underbrace{\kappa}_{Confirmation\ Time} \tag{2}$$

Prior papers consider exclusively that which we refer to here as processing time, $W_P(f)$. This term corresponds to the expected time from the point at which User i sends her transaction into the blockchain network for processing to the point at which the transaction appears on the blockchain's ledger. User i's processing time, $W_P(f)$, depends upon the fee that User i pays, f, and the fees from the set of transactions awaiting inclusion to the blockchain ledger. The set of transactions awaiting inclusion on the blockchain ledger is commonly referred to as the memory pool, which we assume follows its stationary distribution. Recall that the blockchain processes transactions in descending fee order so that User i's transaction is added to the blockchain only after all transactions in the memory pool with higher fees are processed. Moreover, a transaction with a higher fee arriving after User i's transaction would be prioritized ahead of User i's transaction if User i's transaction has not already been added to the blockchain at that time. Thus, User i may alleviate her waiting time by paying a higher fee, thereby reducing the number of transactions that are prioritized ahead of her transaction.

Following prior literature, we assume that blocks are created according to a Poisson Process with rate $\Lambda > a$. For exposition, we normalize block sizes to one transaction per block. Under these assumptions, we have the following result:

Proposition 3.1. *User i's fee, f_i, and her Processing Time, $W_P(f_i)$, both decrease in Scale, Λ*

In equilibrium, User i's fee choice is given by:

$$f_i = 2 \cdot a \cdot \Lambda \int_0^{c_i} \frac{g(x)}{(\Lambda - a \cdot \overline{G}(x))^3}\, dx$$

with $\overline{G}(x) := 1 - G(x)$. Moreover, the equilibrium processing time, $W_P(f_i)$, is given by:

$$W_P(f_i) = \frac{\Lambda}{(\Lambda - a \cdot \overline{G}(c_i))^2}$$

Both the equilibrium fee, f_i, and the equilibrium processing time, $W_P(f_i)$, decrease in the scale of the blockchain.

Proposition 3.1 establishes that fees depend negatively upon scale. The intuition behind this finding is that the value of priority to get on the blockchain decreases with scale so that the value of paying fees decreases as scale increases. Hence, as scale increases, fees endogenously fall.

To understand the aforementioned point, recall that users are processed in descending order of fees so that the number of users for which User i must wait depends upon the relative order of her fee among all fees. For concreteness, suppose that User i may pay $\varepsilon > 0$ extra to gain priority over one user in expectation. Then, the utility value for her to gain such priority equals $c_i \cdot \frac{1}{\Lambda}$ because c_i denotes her wait disutility per unit time and $\frac{1}{\Lambda}$ denotes the amount of time by which her expected wait falls if she gains priority over one user. Thus, since $c_i \cdot \frac{1}{\Lambda}$ decreases in scale, Λ, so too does User i's benefit from paying the additional $\varepsilon > 0$ in fees. Accordingly, as the scale increases, User i becomes less willing to pay higher fees and thus her fee choice also falls.

Proposition 3.1 also establishes that User i's processing time, $W_P(f_i)$, decreases with scale, Λ. This result follows for two reasons. First, holding fixed the number of users that receive service before User i, a higher scale directly reduces the expected time required to process those higher priority users. Second, the number of users that receive service before User i itself decreases as the scale increases. To see this last point, recall that User i must wait behind not only users already in the memory pool that pay higher fees but also later arriving users who pay a higher fee than User i if those users arrive before User i receives service. A higher scale reduces the probability that any new user arrives before any user already in the memory pool receives service; in turn, the number of users that receive service before User i receives service decreases in scale thereby also contributing to a reduced wait time for User i.

Our analysis of the processing time, $W_P(f_i)$, is standard (see, e.g., Huberman et al. 2019), but we expand on previous work by explicitly incorporating the confirmation time, κ, into the user wait time. The confirmation time refers to the time in between User i's transaction being entered on the blockchain and the time that User i receives delivery of the other leg of the exchange. For example, if User i is selling cryptocurrency units in return for fiat or some physical good then User i's transaction being posted to the blockchain does not imply that the receiver releases the fiat or goods to User i. Rather, when selling fiat or a physical good for cryptocurrency units, the seller employs a confirmation rule to reduce the risk that the transfer of the cryptocurrency units could be reversed. A confirmation rule requires that the seller of the fiat or physical good release the item to User i only after a set number of confirmations. A confirmation refers to an additional block being placed on top of the same chain that includes the transaction in which User i sends her cryptocurrency units to the other party. Accordingly, we refer to the expected time for a user to receive her goods starting from the time that her transaction is added to the blockchain as confirmation time, κ, which is given by:

$$\kappa = \frac{k}{\Lambda} \tag{3}$$

with k denoting the number of confirmations. The number of confirmations is a choice variable for the seller of the fiat or physical good, and we subsequently derive its relationship to a blockchain's security level.

To derive the relationship between the number of confirmations and a blockchain's security level, we require some minimal theoretical structure. As such, we let $p(s,k)$ denote the probability that a transaction entered on the blockchain is reversed with s denoting the security level of the blockchain, and k denoting the number of confirmations required by the counterparty receiving the cryptocurrency. We assume that $\frac{\partial p}{\partial s} < 0$ so that a more secure blockchain has a lower probability of a transaction being reversed, i.e., s is consistent with our conceptualization of security. Further, we assume $p(s,k)$ decreases in k, i.e., a higher confirmation number reduces the probability of a transaction being reversed. This relationship arises endogenously within Nakamoto (2008) and Saleh (2021) for PoW and PoS blockchains, respectively. We also assume that $\lim_{k\to\infty} p(s,k) = 0$ so that the probability a transaction is reversed vanishes as the number of confirmations diverges. Since arbitrarily large confirmation rules require arbitrarily large wait times and thus are undesirable, we assume that the counterparty receiving the cryptocurrency selects k to be as low as possible, subject to a risk constraint. Formally, we assume that the counterparty receiving the cryptocurrency requires that the probability a transaction is reversed is no more than some threshold, $\alpha > 0$, and determines the confirmation number by $k = k(s) := \min\{k \in \mathbb{N} : p(s,k) \leqslant \alpha\}$. Note that this technique resembles the widely-used Value-at-Risk (VaR) approach.

The following result gives the relationship between the endogenous confirmation number and the blockchain's security:

Proposition 3.2. *Confirmation number decreases in Security*
$k = k(s) := \min\{k \in \mathbb{N} : p(s,k) \leqslant \alpha\}$ *decreases in* s *for any* $\alpha > 0$.

Proposition 3.2 establishes that the endogenous confirmation number, k, decreases in a blockchain's security level, s. This result arises because the risk level for the transaction is targeted to be a fixed value, α. The transaction's risk level depends on both the underlying security of the blockchain, s, and the number of confirmations, k. When the blockchain is relatively secure (i.e., when s is high), then even a low confirmation number (i.e., low k) implies a low risk. However, when the blockchain is relatively insecure (i.e., when s is low), then a higher confirmation number (i.e., high k) is necessary to achieve the same level of risk. Thus, $k = k(s) := \min\{k \in \mathbb{N} : p(s,k) \leqslant \alpha\}$ decreases in s, and we have the following corollary:

Corollary 3.3. *Confirmation Time,* κ*, decreases in Security,* s*, and Scale,* Λ
User i*'s confirmation time,* κ*, equals* $\frac{k(s)}{\Lambda}$ *and thus decreases in both security,* s*, and scale,* Λ.

Corollary 3.3 highlights that a more secure blockchain generates a higher utility for a user. This result arises because a more secure blockchain has a low probability of having a transaction reversed even with a low confirmation number and thus the confirmation number is set low. Then, since the user wait time increases in the confirmation number and users dislike waiting, a more secure blockchain translates to a higher user utility.

Our preceding results collectively imply the following corollary:

Corollary 3.4. *User utility increases in Adoption,* N_{τ_i}*, Scale,* Λ*, and Security,* s

User i's utility depends upon the blockchain characteristics of adoption, scale, and security. Moreover, User i's utility increases in each such characteristic.

which establishes that the user utility from using a blockchain depends directly upon three blockchain characteristics: adoption, scale, and security. This result highlights that the welfare implications of blockchain stems from these three characteristics. Accordingly, we use these characteristics as the attributes for our empirical framework in Section 4.

While the utility of each user increases in the referenced three blockchain characteristics, it is important to recognize that users are not homogeneous so that different users may prefer different blockchains. In particular, there is no unique rank of all blockchains for arbitrary users, so we should expect several blockchains to co-exist simultaneously even when each user only transacts on the blockchain that is optimal for her. An important purpose of our analysis is to determine the subset of blockchains that are optimal for *some* user thereby enabling researchers to focus research efforts on this subset of blockchains. To enable straightforward determination of this subset of blockchains in our subsequent empirical analysis, we offer the following proposition:

Proposition 3.5. *Blockchain Dominance*
Let $N_{\tau,i}$ refer to the adoption level of Blockchain i for user type $\tau \in \mathcal{T}$, Λ_i refer to the scale of Blockchain i and s_i refer to the security level of Blockchain i. Then Blockchain 1 is preferred to Blockchain 2 for each user under all circumstances if and only if $N_{\tau,1} \geqslant N_{\tau,2}$ for all $\tau \in \mathcal{T}$, $\Lambda_1 \geqslant \Lambda_2$, and $\frac{\Lambda_1}{k(s_1)} \geqslant \frac{\Lambda_2}{k(s_2)}$.

Proposition 3.5 provides a set of conditions to determine the set of relevant blockchains. In particular, we establish that if Blockchain 1 dominates Blockchain 2 on the stated comparisons (i.e., $N_{\tau,1} \geqslant N_{\tau,2}$ for all $\tau \in \mathcal{T}$, $\Lambda_1 \geqslant \Lambda_2$, and $\frac{\Lambda_1}{k(s_1)} \geqslant \frac{\Lambda_2}{k(s_2)}$) then Blockchain 1 is always preferred to Blockchain 2. In turn, Blockchain 2 is then not optimal for any user and thus is also not part of the optimal blockchain ecosystem from the user perspective. In Section 5, we apply these comparisons empirically to eliminate blockchains that would not be optimal for any user, thereby highlighting the public blockchains most relevant for further study.

4 Empirical Framework

In this section, we implement our theoretical framework by establishing empirical metrics for each of our three attributes: adoption, scale, and security. We examine and discuss in detail how these attributes vary across a sample of major public blockchains. We find that the leading blockchains, highlighted within Section 2, perform well on at least one of these metrics, emphasizing the underlying economic basis for their relevance.

4.1 Adoption

Our theoretical model takes adoption as the number of users of the same type that can transact with each other on a particular blockchain. Intuitively, the probability of a given user finding a

suitable counterparty increases with the number of potential such counterparties. Consequently, the more users that transact on a particular blockchain and are active within the relevant user type community, the higher the transaction surplus generated. Accordingly, in our empirical analysis, we consider adoption metrics for multiple user types that each have their own economic purpose for transacting.

First, we use the number of users that have received or initiated a transaction with a blockchain's native cryptoasset on a given day (i.e., we define being active on a day as having been involved in a transaction on a day). We refer to this specific kind of user as a 'payment type' user. Second, we consider multiple types of users that seek to engage in more complex transactions than that of the payment type. Users of certain blockchains can make conditional transactions using self-executing programs, i.e., smart contracts, which are coded and run on the blockchain. This functionality allows developers to create decentralized applications (dApps) that mimic relevant economic interactions between users beyond simple payments without the need for a central intermediary. From the perspective of users, dApps represent access to unique networks of other users, bringing efficiency to the matching process. For example, if a user wants to exchange one cryptoasset for another, she searches for a matching set of other users that can provide the liquidity for this exchange. Blockchains with smart contract functionality facilitate the marketplace for such specific economic interactions.

Table 3: TOP 5 Blockchains by Number of Active Addresses

This table reports the average number of daily active addresses in the last 30 days for the five most adopted blockchains in the coinmetrics.io sample. Values are given as of February 21, 2021.

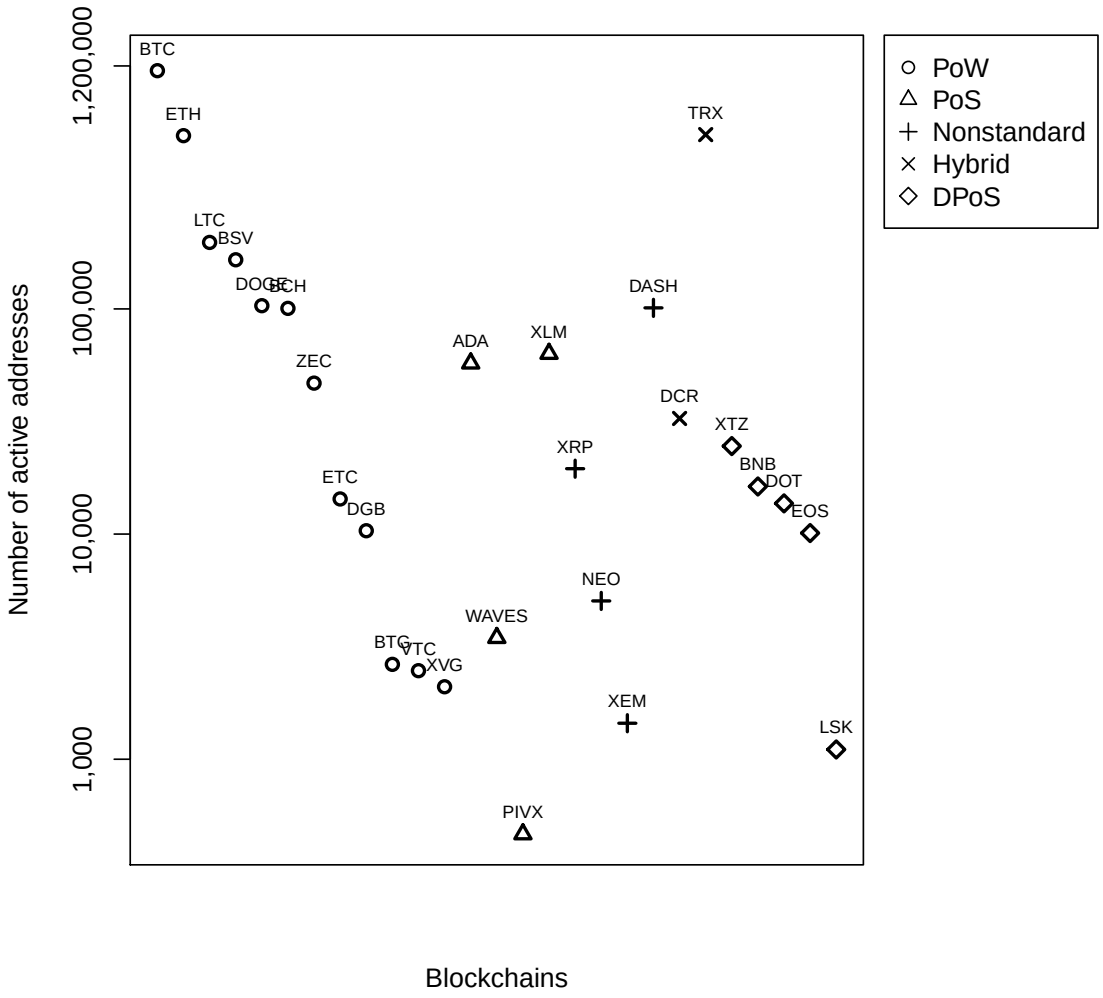
Blockchain	**Symbol**	**Consensus**	**# Active Addresses**	**Rank**
Bitcoin	BTC	PoW	1,143,343	1
TRON	TRX	DPoS	594,517	2
Ethereum	ETH	PoW	588,248	3
Litecoin	LTC	PoW	197,418	4
Bitcoin SV	BSV	PoW	165,334	5

Empirically, for payment type users, we employ as metrics the 30 day average of the number of active addresses up to the end of the sample period (February 21, 2021) and rank all blockchains from the coinmetrics.io sample accordingly. Results using the average number of active addresses are illustrated in Figure 5, while Table 3 reports this metric for the five blockchains that are most adopted by users of the payment type. Bitcoin (BTC) is the most adopted blockchain with a number of daily active addresses above one million. There are three other blockchains among the five most adopted blockchains that employ the PoW consensus protocol: Litecoin (LTC), Ethereum (ETH), and Bitcoin SV (BSV). However, the second most adopted blockchain, with almost 600,000 daily active users, is TRON (TRX), which employs DPoS as its consensus protocol.

Figure 5 highlights that there is stark heterogeneity in adoption not just across blockchains but

Figure 5: Adoption: Number of active addresses.

This figure displays the adoption metric for users of the payment type for each public blockchain in the coinmetrics.io sample. Blockchains are arranged along the x-axis (in no particular order) and are represented by the ticker symbol for their native cryptoassets. The shape of each data point indicates its consensus protocol: Proof-of-Work (PoW), Proof-of-Stake (PoS), Nonstandard, Hybrid PoW/PoS (Hybrid), and Delegated Proof-of-Stake (DPoS). The y-axis represents values of the 30 day average of the number of active addresses as of February 21, 2021 on a log scale. A higher number of active addresses corresponds to a more widely-adopted blockchain.



also within consensus protocol groups. For example, PoW protocols' strength in adoption, as is suggested by Table 3, is driven by the dominance of Bitcoin (BTC) and Ethereum (ETH), while older PoW blockchains such as ZCash (ZEC), Dogecoin (DOGE), or Ethereum Classic (ETC), are lagging behind by orders of magnitude. Nevertheless, some PoW blockchains such as Bitcoin Satoshi's Vision (BSV) or Bitcoin Cash (BCH), which are lagging far behind Bitcoin (BTC) in terms of user adoption, are ahead of many other non-PoW blockchains in our sample. Some of these blockchains have been in existence for many years and thus, may possess early-mover advantages, but the success of TRON (TRX) and Ethereum (ETH) on the adoption metric may stem from other factors such as their enhanced functionalities that enable an ecosystem with different types of blockchain users.

To empirically account for the added utility decentralized applications bring to users of different types, we retrieve information on the number of active users of dApps in economically relevant categories from stateofthedapps.com and dappradar.com. We deem a blockchain user address as active on a particular dApp when it has received or initiated a transaction within the last 30 days, i.e., the metric 'Monthly Active Users' (MAU) is the sum of unique monthly active users on each dApp across each blockchain.

Table 4: dApp statistics by blockchain

This table presents dApp statistics for ETH, EOS, TRON, NEO and WAVES blockchains. Data for ETH, EOS and TRON are collected from stateofthedapps.com, while data for NEO and WAVES are collected from dappradar.com. dApp count is the total number of dApps on each blockchain. dApp count (>100 MAU) is the total number of dApps with more than 100 unique monthly active users on each blockchain. MAU is the sum of the unique monthly active users on each dApp over a 30 day period for each blockchain. The 30 day period (considered in dApp txns and MAU) is from 22 January, 2021 to 20 February, 2021.

Blockchain	**ETH**	**EOS**	**TRON**	**NEO**	**WAVES**
dApp count	1,965	233	66	16	26
dApp count (>100 MAU)	163	31	16	4	2
MAU	1,766,762	79,532	109,566	4,887	7,166

Table 4 presents summary statistics for dApps across five blockchains with smart contract functionalities and available dApp user data (ETH, EOS, TRON, NEO and WAVES).[7] There are almost 2,000 dApps hosted on Ethereum, over 200 on EOS, and less than one hundred each on TRON, NEO, and WAVES, respectively. However, most of these dApps do not have significant user adoption. Less than ten percent of Ethereum dApps have over 100 MAU and the other four blockchains combined host only 53 dApps with a user base above 100 MAU. With respect to the overall MAU, Ethereum dApp adoption is an order of magnitude higher than all other blockchains, including TRON and EOS.

[7]Note that there are other blockchains that possess some form of smart contract functionality, such as Stellar (XLM) or Ripple (XRP), but none of these blockchains host widely-adopted, decentralized applications and are thus, not included in this subsample.

In terms of different user types, we consider a number of categories that are worth highlighting in terms of the size of their active user base and the distinct economic interactions that take place on respective platforms. *Decentralized Finance (DeFi)* applications bring together users that seek to engage in more complex financial interactions than payments. This includes matching of borrowers and investors as liquidity providers, trading cryptoassets on order books, and the creation of stablecoins and financial derivatives tied to other cryptoassets (see Harvey, Ramachandran, and Santoro, 2021, for an overview of DeFi applications). We combine all users of dApps in the 'Finance' and 'Exchange' categories from stateofthedapps.com to be of the *DeFi* user type. *Gambling* dApps attract types of users that wish to interact within lottery-type structures or tournaments (e.g., dices, sports betting, virtual casino slot machines). Users of the *Gambling* type are typically matched via smart contracts that collate and redistribute cryptoasset funds according the application-specific (quasi-)random payoff. *Games* dApps serve the purpose of user entertainment and do not necessarily have financial rewards. Users of the *Games* type interact directly with each other in online games, the rules of which are written in smart contracts and any within-game transaction and user interaction is recorded on the respective blockchain. *Storage* dApps provide blockchain-based data services by matching a unique set of consumers with producers of such services. Users of the *Storage* type interact with each other on dApps that facilitate, e.g., digital file sharing or provision of cloud storage, but in a decentralized setting where incentives to participate in respective peer-to-peer marketplaces are defined in smart contracts. We combine all remaining dApp categories under the umbrella category *Other*.

Figure 6: Overview of decentralized applications (dApp)

This figure displays the proportion of dApps and dApp Users in each relevant category. Data for ETH, EOS and TRON are collected from stateofthedapps.com, while data for NEO and WAVES are collected from dappradar.com. Dappradar.com categorization is hand-matched to stateofthedapps.com categorization. MAU is the sum of the unique monthly active users on each dApp over a 30 day period (from 22 January, 2021 to 20 February, 2021) for each category.

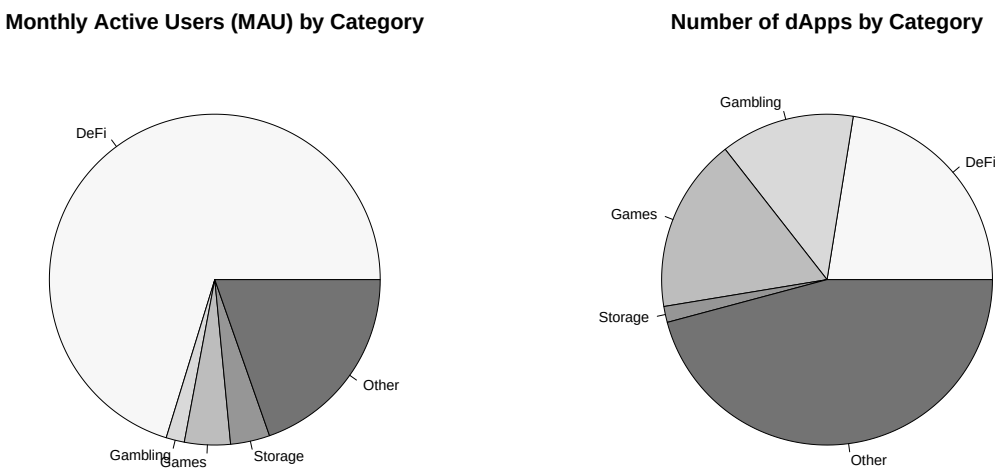


Figure 6 shows the distribution of the number of dApps and MAU across these categories (combined for all five blockchains) and reveals that the majority of dApp adoption stems from the growing relevance of DeFi within the blockchain ecosystem. Although *DeFi* dApps constitute only 22.4% of the total number of dApps in our sample, the user base of these represent 70.2% of all dApp users. The disparity between the proportion of total dApps and the proportion of total users for each category exists not only for *DeFi*, but also for other categories. *Storage* dApps account for only 1.6% of all dApps but the users of these make up 3.8% of total users. In contrast, *Games* and *Gambling* dApps account for 30.1% of total dApps but only 6.4% of all users have adopted them.

Table 5: Monthly Active Users (MAU) by dApp category and blockchain

This table shows the number (and percentage) of Monthly Active Users (MAU) within the dApp categories *Decentralized Finance* (*DeFi*), *Gambling*, *Games*, *Storage*, and *Other*, hosted across five blockchains: Ethereum (ETH), EOS (EOS), TRON (TRX), NEO (NEO) and WAVES (WAVES). Data for ETH, EOS and TRON are collected from stateofthedapps.com, while data for NEO and WAVES are collected from dappradar.com. Dappradar.com categorization is hand-matched to stateofthedapps.com categorization. MAU is the sum of the unique monthly active users on each dApp over a 30 day period (from 22 January, 2021 to 20 February, 2021) for each category.

dApp category	**ETH**	**EOS**	**TRX**	**NEO**	**WAVES**
DeFi	1,333,306	19,809	17,888	4,581	6,988
(MAU in %)	(96.44)	(1.43)	(1.29)	(0.33)	(0.51)
Gambling	8,012	8,658	18,546	0	35
(MAU in %)	(22.73)	(24.56)	(52.61)	(0.00)	(0.10)
Games	45,780	41,694	667	48	1
(MAU in %)	(51.91)	(47.28)	(0.76)	(0.05)	(0.00)
Storage	6,934	421	68,248	0	0
(MAU in %)	(9.17)	(0.56)	(90.27)	(0.00)	(0.00)
Other	372,730	8,950	4,217	258	142
(MAU in %)	(96.49)	(2.32)	(1.09)	(0.07)	(0.04)

Table 5 provides an overview of the distribution of MAUs within each of the five user types (dApp categories) across the five blockchains. While ETH dominates the *DeFi*, *Games*, and *Other* categories, it does not lead in all categories. TRON (TRX) leads in the *Gambling* and *Storage* categories, capturing more than 50% and 90% of the total user base within each of those categories, respectively. EOS falls slightly behind ETH in the *Games* category and is otherwise dominated by either ETH or TRX in terms of users in every other category. The user bases of NEO and WAVES dApps fall far behind that of the other three blockchains in all relevant categories.

4.2 Scale

Scale determines user welfare both through lowering the processing time as well as the costs users incur in the form of fees paid (see Proposition 3.1). Within our theoretical analysis, scale corresponds to the rate at which a blockchain can process users' submitted transactions. We

estimate a blockchain's transaction rate in terms of recorded transactions in a given time period (denominated in seconds). For that purpose, we employ historical daily transaction counts and take the maximum as our estimate of scale. Figure 7 displays the scale of each blockchain in the sample.

Figure 7: Scale: Transactions per Second (TPS).

This figure displays the scale metric for each public blockchain in the coinmetrics.io sample. Blockchains are arranged along the x-axis (in no particular order) and are represented by the ticker symbol for their native cryptoassets. The shape of each data point indicates its consensus protocol: Proof-of-Work (PoW), Proof-of-Stake (PoS), Nonstandard, Hybrid PoW/PoS (Hybrid), and Delegated Proof-of-Stake (DPoS). Scale is measured as the maximum of daily transaction counts denominated in transactions per second (TPS). The y-axis represents values of TPS on a log scale. A higher value of TPS corresponds to a higher scalability of a blockchain.

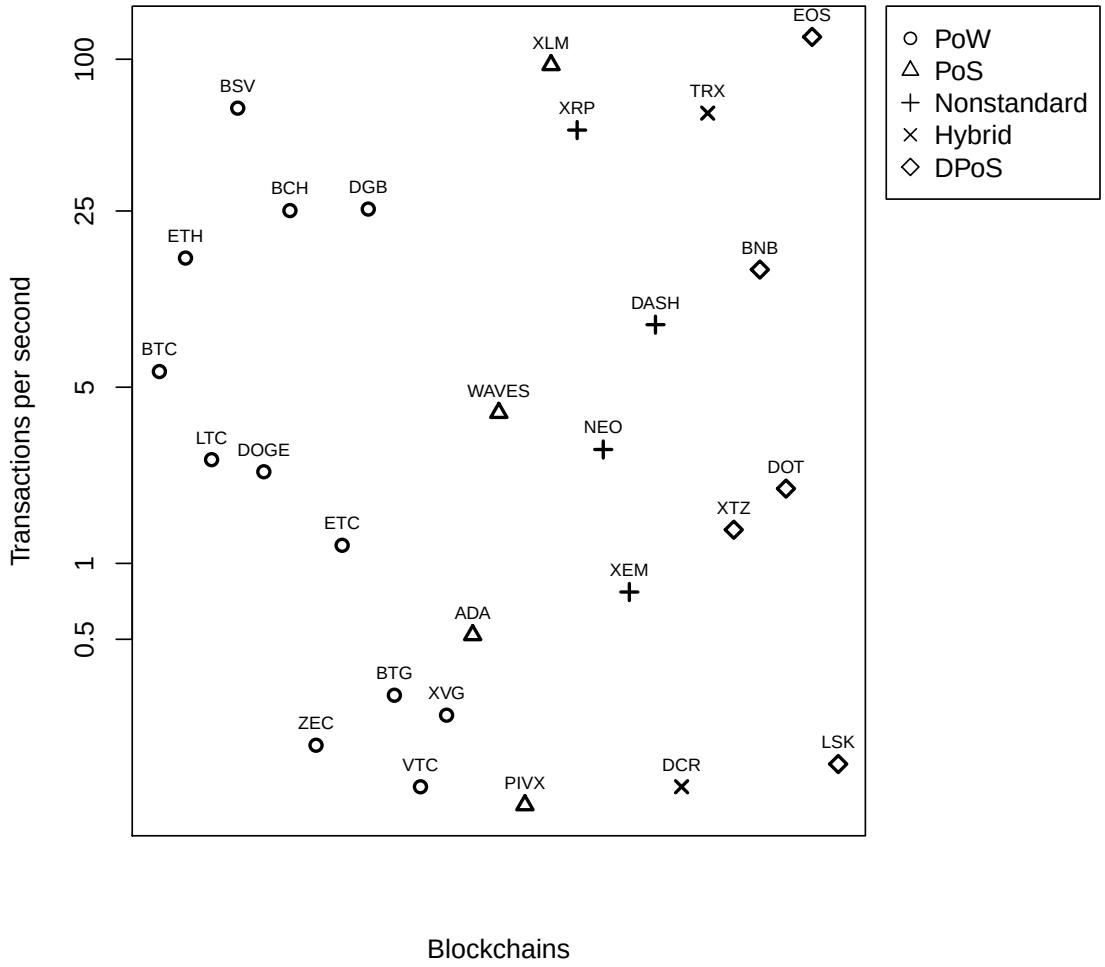


Figure 7 highlights that, although Bitcoin (BTC) leads on adoption by *Payment* type users, it does not perform well on scale as it records fewer than 10 TPS. Consequently, users that require

higher scale for fast processing times or the ability to send micro-transactions at low transaction costs would opt for alternatives to Bitcoin, such as the ones listed in Table 6.

Table 6: TOP 5 blockchains by transactions per second (TPS)

This table shows the top five blockchains in the coinmetrics.io sample as ranked by scale. Scale is measured as the maximum of daily transaction counts denominated in transactions per second (TPS).

Blockchain	Symbol	Consensus	TPS	Rank
EOS	EOS	DPoS	122.6	1
Stellar	XLM	Nonstandard	94.9	2
Bitcoin SV	BSV	PoW	64.0	3
TRON	TRX	DPoS	61.1	4
Ripple	XRP	Nonstandard	52.4	5

The DPoS blockchain EOS (EOS) performs substantially better than all other blockchains, even other DPoS blockchains, and can process an estimated 122.6 TPS. Stellar (XLM), a nonstandard blockchain, is second on scale with almost 95 TPS, while the blockchains ranked third to fifth on scale can process only at approximately half of the rate of EOS. These findings highlight that public blockchains have made significant progress since the birth of Bitcoin when it comes to scale, but remain inferior to traditional alternatives (e.g., payment systems like VISA can process over 1,000 TPS).

4.3 Security and Confirmation Time

Security For our security metric, we rely upon Proposition 3.2, which implies that the blockchain ranking by security is the reverse of the blockchain ranking by confirmation numbers (i.e., if $k \leqslant k'$, then $s \geqslant s'$). While we cannot directly observe the security of a blockchain, we can infer its level by considering the confirmation rules imposed by major users of blockchains. In particular, we collect information on confirmation numbers disclosed by the largest institutions that trade via blockchains: cryptoasset exchanges. We collate a list of major cryptoasset exchanges from cryptocompare.com. We consider all exchanges with daily trading volume above $1 million (n=122; as of March 25, 2021). For each exchange, we search for and browse through its FAQ and support web pages and are able to extract the required number of block confirmations for each particular cryptoasset from a total of 32 cryptoasset exchanges.[8] Different exchanges may view the security levels of the same blockchain differently and thus, could impose different confirmation rules. For example, every exchange has a confirmation rule for Bitcoin (BTC) transactions, but some exchanges require up to six confirmations for BTC transactions while others require only one or two. To infer an order of security levels s for each blockchain in our sample, we take the median confirmation number $k(s)$ for a given blockchain to aggregate across exchanges.

[8]For transparency, Appendix A lists all confirmation rules used in constructing our security metric as well as web links to data sources.

Figure 8: Security: Number of block confirmations.

This figure displays the security metric for each public blockchain in the coinmetrics.io sample. Blockchains are arranged along the x-axis (in no particular order) and are represented by the ticker symbol for their native cryptoassets. Security is measured as the median number of block confirmations required by major cryptoasset exchanges to settle a transaction. Appendix A reports data sources and confirmation numbers of individual cryptoassets for all 32 exchanges. The y-axis represents values of block confirmation rules on a reversed log scale. Lower values indicate better security for a blockchain.

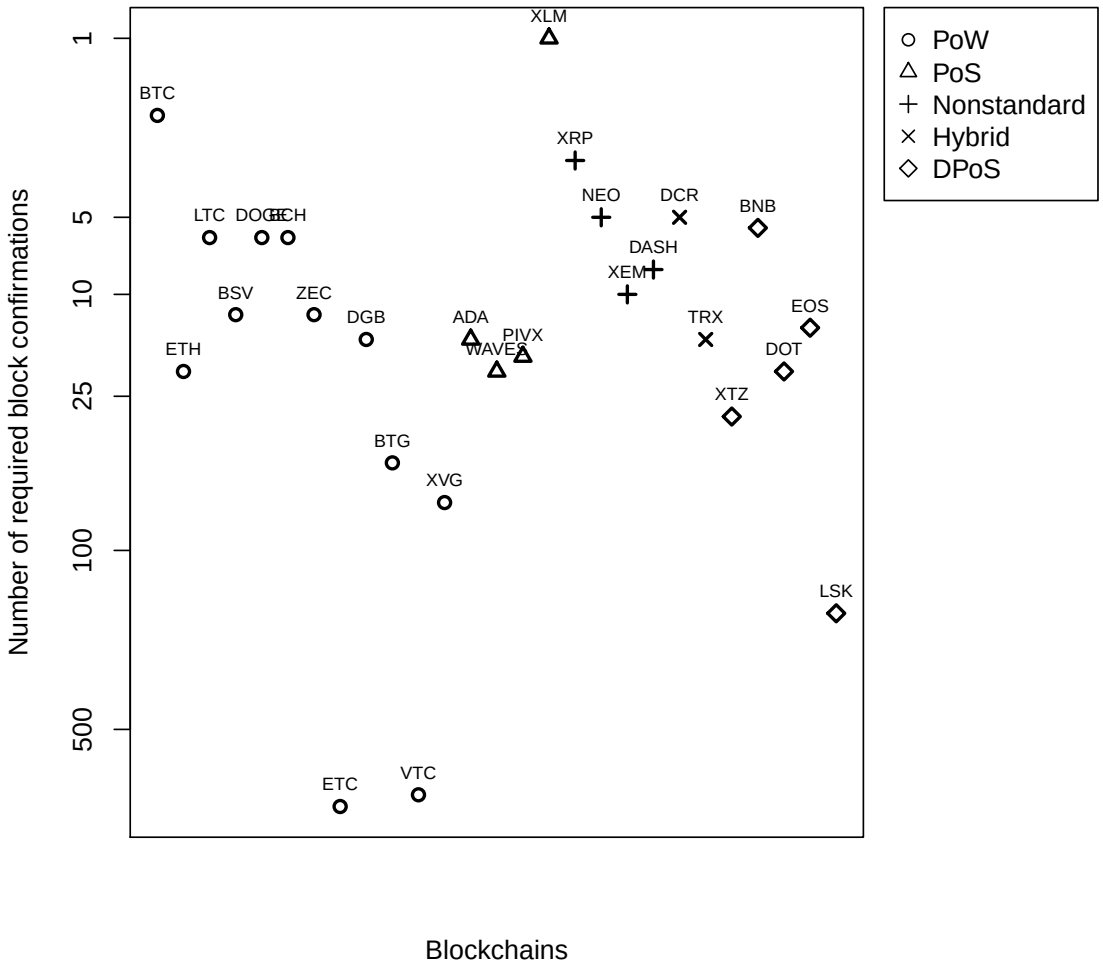


Figure 8 reveals that Stellar (XLM) is the most secure blockchain, as it has a median required confirmation number of $k(s) = 1$, followed by Bitcoin (BTC) with $k(s) = 2$. Blockchains with Nonstandard consensus protocols, such as Ripple (XRP) or NEO (NEO), as well as the Hybrid PoW/PoS protocols employed in Decred (DCR) and Dash (DASH) perform comparatively well on security with confirmation numbers below $k(s) = 10$. While this is also true for older PoW blockchains such as Litecoin (LTC), Bitcoin Cash (BCH) or Dogecoin (DOGE), there is much more heterogeneity among the group of PoW protocols, with exchanges requiring far beyond 500 required confirmations for the least secure blockchains in order for transactions to be considered final. With the exception of Binance Coin (BNB), which has a median confirmation number of $k(s) = 5.5$, all PoS and DPoS blockchain transactions require over twelve confirmations and thus place in the lower half of the blockchain sample in terms of security.

Confirmation time Corollary 3.3 directly states that user welfare increases with lower confirmation times, κ, which in turn depend upon confirmation numbers (security), $k(s)$, and the rate at which blocks arrive. We estimate block arrival rates using historical data on block arrivals. For each blockchain, we take the average of daily block counts to estimate its block arrival rates as the time in seconds for one additional block to be added to the blockchain.[9] Table 7 shows block arrival rates as well as confirmation numbers that are used to calculate user confirmation times κ.[10]

The best performing blockchains on this metric employ either Nonstandard protocols or consensus protocols based on delegated Proof-of-Stake. Binance Coin (BNB) blockchain transactions take an estimated $\kappa = 2.2$ seconds to be considered final by cryptoasset exchanges, making it the blockchain with the shortest confirmation wait time. The two blockchains ranked second and third with respect to this metric are Stellar (XLM) and EOS (EOS), with confirmation times $\kappa = 5.2$ and $\kappa = 6.8$ seconds, respectively, which is more than twice as long as is required for Binance Coin. All of the top five blockchains with respect to confirmation times have short block arrival rates and low confirmation numbers, resulting in overall wait times until final confirmation below one minute, whereas the majority of other blockchains require more than five minutes to complete the confirmation process in an exchange.[11] The set of blockchains performing worst on this metric includes known PoW blockchains such as Bitcoin Satoshi's Vision (BSV) and Ethereum Classic (ETC), which exhibit estimated transaction confirmation times required by cryptoasset exchanges of two hours or more. It is worth highlighting that Ethereum (ETH), which captures a considerable amount of the activity in the ecosystem in terms of active users of decentralized applications and payments, is more desirable than Bitcoin (BTC) in terms of confirmation times, as exchanges involving ETH are settled in a quarter of the time it takes to settle those using BTC (5 versus almost 20 minutes). Thus, although Bitcoin is viewed as relatively secure by exchanges in terms of required confirmation numbers, user utility, ceteris paribus, is higher for other blockchains that

[9] Block counts are missing in coinmetrics.io for Polkadot (DOT), but we obtain an estimate of its block time (6 seconds) from the Polkascan blockchain explorer.

[10] We also consider the mean of confirmation numbers across exchanges as an alternative measure to calculate confirmation times, but the ranking is quantitatively and qualitatively similar to taking the median values.

[11] This statement is robust to taking the mean instead of median values of confirmation numbers.

Table 7: Block arrival rates and confirmation wait times.

This table shows block arrival times, confirmation numbers $k(s)$, and confirmation times κ for all blockchains in the coinmetrics.io sample. Block arrival times are denominated in seconds and are estimated as 14,400 seconds (one day) divided by the average daily block count. Confirmation numbers are given as median values of block confirmations required by 32 major cryptoasset exchanges for a given blockchain (cf. Appendix A for details and data sources). Confirmation time is the product of block arrival time and confirmation number. Blockchains are displayed according to their rank on confirmation time, where 1 corresponds to lowest (best) and 27 to highest (worst) confirmation times.

Blockchain	**Symbol**	**Consensus**	**Block arrival rate** (in seconds)	$k(s)$	**Confirmation time** κ (in seconds)	**Rank**
Binance Coin	BNB	DPoS	0.4	5.5	2.2	1
Stellar	XLM	Nonstandard	5.0	1	5.0	2
EOS	EOS	DPoS	0.5	13.5	6.8	3
Ripple	XRP	Nonstandard	4.2	3	12.5	4
TRON	TRX	DPoS	3.0	15	45.3	5
NEO	NEO	Nonstandard	20.9	5	104.6	6
Polkadot	DOT	DPoS	6.0	20	120.0	7
Digibyte	DGB	PoW	18.0	15	270.3	8
Ethereum	ETH	PoW	14.8	20	295.3	9
Cardano	ADA	PoS	20.1	15	301.0	10
Dogecoin	DOGE	PoW	62.9	6	377.3	11
NEM	XEM	Nonstandard	60.5	10	604.8	12
Litecoin	LTC	PoW	147.6	6	885.8	13
PIVX	PIVX	PoS	58.5	17.5	1023.1	14
Bitcoin	BTC	PoW	570.3	2	1140.5	15
WAVES	WAVES	PoS	60.2	20	1203.0	16
Dash	DASH	Hybrid	157.0	8	1255.8	17
Zcash	ZEC	PoW	118.0	12	1416.1	18
Decred	DCR	Hybrid	299.6	5	1498.1	19
Lisk	LSK	DPoS	10.2	176	1792.4	20
Tezos	XTZ	DPoS	61.7	30	1851.7	21
Verge	XVG	PoW	42.2	65	2745.5	22
Bitcoin Cash	BCH	PoW	569.6	6	3417.4	23
Bitcoin SV	BSV	PoW	603.6	12	7243.1	24
Ethereum Classic	ETC	PoW	14.0	1000	14049.7	25
Bitcoin Gold	BTG	PoW	574.8	45.5	26153.1	26
Vertcoin	VTC	PoW	148.4	900	133579.2	27

have much shorter confirmation times.

5 The Blockchain Frontier

Given Proposition 3.5 and our empirical implementation, we turn to identifying which blockchains are worthy of study as those that are not dominated by any other blockchain with respect to the three attributes. The underlying reasoning for the focus on these blockchains is that, by definition, only such blockchains could provide the maximum utility among all blockchains for some user. To empirically identify whether a blockchain is dominated by another blockchain, we perform pairwise comparisons of confirmation time, scale and adoption metrics to check whether the conditions for dominance in Proposition 3.5 hold. For that purpose, we rank all sample blockchains from 1 (best) to 27 (worst) with respect to each of the empirical metrics and summarize the results in Table 8.

We extract a subset of seven blockchains that are not dominated by any other blockchain, which we refer to as the "blockchain frontier." The blockchain frontier consists of not only those blockchains that tend to have their relative strength only in adoption, confirmation time (security), or scale, but also blockchains that exhibit a unique combination of attributes, which results in them not being dominated overall.

The financial economics literature has largely focused on the specifics of the Bitcoin blockchain, but our findings suggest that other, less-known blockchains dominate on economically relevant dimensions, such as scale, confirmation time, or adoption within specific user type groups (e.g., *DeFi*). Notably, this frontier does not necessarily list the blockchains with highest market capitalization of its native cryptoasset, but rather the blockchains which bring some unique utility to users. Thus, the frontier translates to the list of blockchains that are optimal for at least *some* users even if that quantity of users is small. We provide an overview of blockchain frontier members below, along with specific examples of users who may prefer the economic attributes of each blockchain.

Bitcoin (BTC) Bitcoin is by far the most adopted blockchain in terms of active users of the *Payment* type. Because it ranks first in this category, Bitcoin cannot be dominated by any other blockchain. Bitcoin benefits from the largest network of other users, facilitating the matching process between these users of the payment type. For example, a user seeking to purchase any goods or services using a cryptocurrency would find it easier to match with a merchant willing to accept BTC, relative to other native cryptoassets. Moreover, BTC's widespread usage renders it as relatively liquid compared to other cryptoassets, and thereby makes it the preferred choice for agents taking a trading position in cryptoasset markets in general. This point can be seen most clearly by the fact that BTC has the highest overall trading volume on cryptoasset exchanges (see, e.g., cryptocompare.com).

Despite its dominance on the adoption by user of the *Payment* type, Bitcoin falls behind on other dimensions such as scale and confirmation time, where it ranks only 11th and 15th, respectively, and it does not support adoption of other user types (e.g., DeFi). Because of these shortcomings,

Table 8: Blockchain Ranking by Attributes

This table shows rankings of blockchains with respect to our attributes: adoption by different user types, scale and the wait time it takes to confirm transactions entered on a particular blockchain. The 27 blockchains in the coinmetrics.io sample are ranked from 1 (best) up to 27 (worst) to indicate their performance on each individual attribute. Blockchains highlighted in the final column are members of the blockchain frontier, i.e., there exists no other than the given blockchain that performs better in each of the categories.

		Adoption								
Blockchain	**Consensus**	**Payment**	**DeFi**	**Gambling**	**Games**	**Storage**	**Other**	**Scale**	**Confirmation**	**Frontier?**
BCH	PoW	8	-	-	-	-	-	7	23	
BSV	PoW	5	-	-	-	-	-	3	24	x
BTC	PoW	1	-	-	-	-	-	11	15	x
BTG	PoW	22	-	-	-	-	-	21	26	
DGB	PoW	18	-	-	-	-	-	6	8	
DOGE	PoW	6	-	-	-	-	-	15	11	
ETC	PoW	16	-	-	-	-	-	18	25	
ETH	PoW	3	1	3	1	2	1	8	9	x
LTC	PoW	4	-	-	-	-	-	14	13	
VTC	PoW	23	-	-	-	-	-	26	27	
XVG	PoW	24	-	-	-	-	-	22	22	
ZEC	PoW	11	-	-	-	-	-	23	18	
ADA	PoS	10	-	-	-	-	-	20	10	
PIVX	PoS	27	-	-	-	-	-	27	14	
WAVES	PoS	21	4	4	5	-	4	12	16	
NEO	Nonstandard	20	5	-	4	-	-	13	6	
XEM	Nonstandard	25	-	-	-	-	-	19	12	
XLM	Nonstandard	9	-	-	-	-	-	2	2	x
XRP	Nonstandard	14	-	-	-	-	-	5	4	
DASH	Hybrid	7	-	-	-	-	-	10	17	
DCR	Hybrid	12	-	-	-	-	-	25	19	
BNB	DPoS	15	-	-	-	-	-	9	1	x
DOT	DPoS	17	-	-	-	-	-	16	7	
EOS	DPoS	19	3	2	2	3	2	1	3	x
LSK	DPoS	26	-	-	-	-	-	24	20	
TRX	DPoS	2	2	1	3	1	3	4	5	x
XTZ	DPoS	13	-	-	-	-	-	17	21	

there are multiple blockchains that are not dominated by Bitcoin.

Ethereum (ETH) Ethereum enters the frontier as it leads on *DeFi* user adoption, which exhibits the highest relative importance within the current dApp ecosystem, but it also wins in several other categories such as *Games*. This dominance in terms of *DeFi* user adoption means that users with a preference for more complex but decentralized financial services will find a more suitable counterparty for their needs by using Ethereum over all other blockchains.

An example of such a *DeFi* dApp is Uniswap, which is a decentralized exchange, allowing users to exchange one cryptoasset (e.g., any 'ERC-20' token) for another without an intermediary. For the exchange to function without a centralized market maker, liquidity is provided by the users that are willing to offer specific cryptoassets in exchange for a representative share of a pool of assets. Other users that want to exchange pairs of cryptoassets can do so at a price, which is set by a preset algorithm on the basis of the size and structure of cryptoassets in the liquidity pool. Each trade requires users to pay a flat transaction fee that in turn is distributed among the liquidity providers.

Nevertheless, Ethereum falls behind Bitcoin and TRON in adoption by users of the *Payment* type and it even falls behind TRON in adoption with respect to users interested in gambling and data storage services. The Ethereum blockchain also does not scale well and requires a longer confirmation time for ETH transactions, making it inferior compared to other blockchains when it comes to speed and finality of transactions.

TRON (TRX) The TRON blockchain performs well on all attributes: it is widely adopted by many user types, it has high scale and requires short confirmation times. It does, however, not dominate all other blockchains as there are only a few metrics on which TRON ranks first. The two metrics in which TRON ranks first are adoption by users of the *Gambling* and *Storage* types, i.e., there are more active users of dApps in these categories than on any other blockchain.

An example of a successful dApp for *Storage* type users is the BitTorrent Speed TRON dApp which enables users to obtain from or send files to other users. The BitTorrent Speed TRON dApp facilitates a peer-to-peer marketplace for digital media downloads. Users that offer media files for other users to download are rewarded in the form of platform-specific BitTorrent (BTT) tokens, which in turn can be sold in markets or redeemed within the dApp to download files at higher speeds. This dApp is successful only because it is sufficiently widely adopted by *Storage* type users to generate a large media library for downloads.

In addition to its relative strength in scale, confirmation time, and specific user type adoption, TRON ranks second behind Bitcoin in terms of *Payment* user adoption. However, TRON falls behind Ethereum in the important *DeFi* category.

EOS (EOS) EOS is the blockchain with the highest scale and is therefore included in the frontier. Users who wish to have their transactions quickly recorded on a blockchain at a low fee cost prefer a higher scaling blockchain. For instance, this may include users who wish to use a decentralized

application that involves frequent micro-transactions. Apart from scale, EOS has the third shortest confirmation time, which adds to the utility of users that prefer not only fast processing times, but also finality of transactions after only few seconds. Related to this point is the fact that EOS ranks second on adoption by users of the *Games* type, i.e., there are many active users employing the EOS blockchain to interact via gaming dApps for entertainment.

A prime example of a dApp that involves many micro-transactions is Upland, which is a *Games* dApp on the EOS blockchain. In the Upland dApp, users buy, sell, and collect virtual properties that resemble real estate in specific cities such as San Francisco and Manhattan. User actions extend beyond purchase and sale of properties; in fact, users must travel nearby in the virtual world to purchase properties so that the game involves frequent small transactions associated with traveling. Any such interaction within the game requires a transaction to be recorded on the blockchain and thus Upland players require low fees to make playing the game feasible. As shown by Proposition 3.1, transaction costs decline in scale so that the high scale of EOS makes its particularly appropriate for such dApps.

Note that despite its success on scale and confirmation time, EOS is not a blockchain widely adopted by *Payment* type users and thus, it does not dominate the majority of the blockchains in our sample on all of the metrics considered.

Binance Coin (BNB) Transactions on the Binance Coin (BNB) blockchain have the shortest confirmation times of all blockchains in our sample and thus, the BNB blockchain is part of the frontier. However, it neither ranks highly on *Payment* user adoption nor is particularly fast in terms of scale. This means that BNB user utility is highest for those types of users that require fast confirmation of transactions above all, but do not require the same scale as blockchains like EOS.

A primary application for BNB is in trading on the Binance cryptoasset exchange. In particular, the exchange offers discounts when BNB is used to pay for fees incurred on their platform. Thus, trading possession of BNB itself is important for any trader seeking to trade on the Binance cryptoasset exchange. As BNB possesses the shortest confirmation time, it is particularly well-suited for this purpose.

Stellar (XLM) Stellar is ranked second on confirmation time and scale, respectively. It is not dominated by the most scalable blockchain, EOS, as it performs better on confirmation time, and it is not dominated by the blockchain with the shortest confirmation time, BNB, as it scales better.

The Stellar blockchain is primarily used by financial technology companies, such as digital wallet, trading and payment providers, which transact using the Stellar blockchain on behalf of their customers. For example, TEMPO, a European electronic payment company, offers its customers global remittances denominated in EUR. To do so, they issue a stablecoin, EURT, upon the Stellar blockchain, which is backed by actual EUR fiat currency stored in the company's audited bank accounts. As soon as the digital EUR representation exists, it can be transferred to the counterparty as a transaction upon the Stellar blockchain, accompanied by small a transaction fee paid in XLM.

Given the type of network participants, it is not surprising that Stellar is not among the top five blockchains in terms of *Payment* type user adoption, but rather, it relies on secure and fast transactions between fewer entities (e.g., financial technology companies on behalf of their customers). In typical applications, including the one referenced above above, Stellar benefits from shorter overall processing and confirmation times than both traditional and other blockchain-based alternative payment systems.

Bitcoin Satoshi's Vision (BSV) Bitcoin SV enters the blockchain frontier not because it leads on any particular attribute, but it exhibits a combination of high scale and wide adoption by *Payment* type users. It ranks only third on scale, but the two blockchains that perform better on scale do not dominate Bitcoin SV as they perform comparatively poorly on *Payment* user adoption, where Bitcoin SV ranks high. Given this combination of attribute strengths, Bitcoin SV users prefer a higher scale than Bitcoin, i.e., more transactions can be processed at lower fee costs in the same time period, but also require a certain level of adoption for payment services, which blockchains with even higher scale do not offer. That is, some users value the Bitcoin SV blockchain because of this trade-off between *Payment* user adoption and scale.

6 Conclusion

We provide the first extensive overview of the public blockchain ecosystem and find that although there exist hundreds of blockchains, only a few are of economic relevance. We offer a simple theoretical framework that helps explain and deepen that finding. Our framework suggests that three blockchain characteristics drive user utility - scale, security, and adoption - and that only a few blockchains are not dominated by some other blockchain in terms of utility for some user. We empirically identify an exclusive set of seven such blockchains, and we refer to those blockchains as the blockchain frontier.

An important takeaway from our analysis is that there are several blockchains other than Bitcoin that are of economic relevance. Accordingly, our work highlights the need for more research in financial economics that is focused on alternatives to Bitcoin.

References

Alsabah, H., and A. Capponi. 2020. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. *Working Paper* .

Arnosti, N., and S. M. Weinberg. 2018. Bitcoin: A Natural Oligopoly. *CoRR* abs/1811.08572. URL http://arxiv.org/abs/1811.08572.

Basu, S., D. Easley, M. O'Hara, and E. Sirer. 2018. Towards a Functional Fee Market for Cryptocurrencies. *Working Paper* .

Benetton, M., G. Compiani, and A. Morse. 2019. CryptoMining: Local Evidence from China and the US. *Working Paper* .

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The Blockchain Folk Theorem. *Review of Financial Studies* 32(5):1662–1715.

Budish, E. 2018. The Economic Limits of Bitcoin and the Blockchain. *NBER Working Paper* .

Chen, L., L. W. Cong, and Y. Xiao. 2019. A Brief Introduction to Blockchain Economics. *Working Paper* .

Chiu, J., and T. V. Koeppl. 2018. The Economics of Cryptocurrencies - Bitcoin and Beyond. *Working Paper* .

Chiu, J., and T. V. Koeppl. 2019. Blockchain-based Settlement for Asset Trading. *Review of Financial Studies* 32(5):1716–1753.

Chod, J., and E. Lyandres. 2019. A Theory of ICOs: Diversification, Agency, and Information Asymmetry. *Management Science* Forthcoming.

Cong, L. W., Z. He, and J. Li. 2021a. Decentralized Mining in Centralized Pools. *Review of Financial Studies* 34(3):1191–1235.

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

Davydiuk, T., D. Gupta, and S. Rosen. 2019. De-crypto-ing Signals in Initial Coin Offerings: Evidence of Rational Token Retention. *Working Paper* .

Dwork, C., and M. Naor. 1992. Pricing via processing or combatting junk mail. *In 12th Annual International Cryptology Conference* pp. 139–147.

Easley, D., M. O'Hara, and S. Basu. 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics* 134(1):91–109.

Gan, R. J., G. Tsoukalas, and S. Netessine. 2020. Initial Coin Offerings, Speculators, and Asset Tokenization. *Management Science* Forthcoming.

Griffin, J. M., and A. Shams. 2020. Is Bitcoin Really Un-Tethered? *Journal of Finance* 75:1913–1964.

Härdle, W., C. R. Harvey, and R. C. Reule. 2020. Understanding Cryptocurrencies. *Journal of Financial Econometrics* 18(2):181–208.

Harvey, C. 2016. Cryptofinance. *Working Paper* .

Harvey, C. R., A. Ramachandran, and J. Santoro. 2021. DeFi and the Future of Finance. *http://dx.doi.org/10.2139/ssrn.3711777* .

Hinzen, F., K. John, and F. Saleh. 2020. Bitcoin's Fatal Flaw: The Limited Adoption Problem. *NYU Stern Working Paper* .

Howell, S. T., M. Niessner, and D. Yermack. 2020. Initial Coin Offerings: Financing Growth with Cryptocurrency Token Sales. *Review of Financial Studies* 33(9):3925–3974.

Huberman, G., J. D. Leshno, and C. Moallemi. 2019. An Economic Analysis of the Bitcoin Payment System. *Working Paper* .

Irresberger, F. 2019. Coin Concentration of Proof-of-Stake Blockchains. *Working Paper* .

King, S., and S. Nadal. 2012. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. White paper: https://peercoin.net/assets/paper/peercoin-paper.pdf.

Lee, J., T. Li, and D. Shin. 2019. The Wisdom of Crowds in FinTech: Evidence from Initial Coin Offerings. *Working Paper* .

Li, J., and W. Mann. 2020. Digital Tokens and Platform Building. *Working Paper* .

Li, T., D. Shin, and B. Wang. 2019. Cryptocurrency Pump-and-Dump Schemes. *Working Paper* .

Liu, Y., J. Sheng, and W. Wang. 2020. Do Cryptocurrencies Have Fundamental Values? *Working Paper* .

Liu, Y., and A. Tsyvinski. 2020. Risks and Returns of Cryptocurrencies. *Review of Financial Studies* Forthcoming.

Liu, Y., A. Tsyvinski, and X. Wu. 2019. Common Risk Factors in Cryptocurrency. *NBER Working Paper* .

Lyandres, E., B. Palazzo, and D. Rabetti. 2019. Do Tokens Behave like Securities? An Anatomy of Initial Coin Offerings. *Working Paper* .

Makarov, I., and A. Schoar. 2019. Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics* 135(2):293–319.

Malinova, K., and A. Park. 2018. Tokenomics: When Tokens Beat Equity. *Working Paper* .

Mora, C., R. L. Rollins, K. Taladay, M. B. Kantar, M. K. Chock, M. Shimada, and E. C. Franklin. 2018. Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change* 8:931–933.

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf* .

Pagnotta, E. 2020. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Working Paper* .

Rosu, I., and F. Saleh. 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science* 67:661–672.

Saleh, F. 2019. Volatility and Welfare in a Crypto Economy. *Working Paper* .

Saleh, F. 2021. Blockchain Without Waste: Proof-of-Stake. *Review of Financial Studies* 34:1156–1190.

Shams, A. 2020. The Structure of Cryptocurrency Returns. *Working paper* .

Yermack, D. 2015. Is Bitcoin a Real Currency? An economic appraisal. *Handbook of Digital Currency* pp. 31–43.

Yermack, D. 2017. Corporate Governance and Blockchains. *Review of Finance* 21(1):7–31.

Appendices

A Data

Table A.1: Required block confirmations by cryptoasset exchanges

This table reports the number of block confirmations required by 32 cryptoasset exchanges for a deposit/transaction to be considered as settled. The list of exchanges is obtained from cryptocompare.com on March 25, 2021 and consists of all exchanges with a daily trading volume above $1 million (n=122). We search the FAQ and support web pages of each cryptoasset exchange for disclosed number of block confirmations for each blockchain from the coinmetrics.io sample.

Exchange/Blockchain	ADA	BCH	BNB	BSV	BTC	BTG	DASH	DCR	DGB	DOGE	DOT	EOS	ETC
Bilaxy					3								
Binance					1								
Bitbank		20			2								
Bitbay		10		50	3	120	50						
Bitbuy		6			3							1	
Bitcoin.com	20	2			1		10					25	60000
Bitmax		3			3							15	3
Bitso		6			4								
Bittrex	20	12		12	2		6	6	20	6	20	1	400
BTCBOX		18			2								
CEX.IO	21	10			3	41	6						
Coinbase	10	12			3		2					1	10000
Coineal					1								
CoinEx	12	1	10	12	1		12	1	10	3	5	12	1000
CoinField		2			2		10						
Coinfloor					3								
Coins Pro		12			3								
Currency.com		6			2								
EXMO	15	6			6	50	6	12		4		30	500
FTX		2	1		2							1	
Gemini		15			3								
GOPAX		2			2							45	
Independent Reserve		5		5	2						11	300	300
itBit		15			3								
Korbit	20	3	12	12	2						30	360	1000
Kraken	15	15			4		6			40	25	1	80640
Liquid		4			2		1				60		
Nominex					3								
OKEX	12	2			1	2	10		10			1	100
Polionex		11	1		1		50	4	40	6	1	350	200000
PrimeXBT					3								
VALR					2								
Median	15	6	5.5	12	2	45.5	8	5	15	6	20	13.5	1000

Exchange/Blockchain	ETH	LSK	LTC	NEO	PIVX	TRX	VTC	WAVES	XEM	XLM	XRP	XTZ	XVG	ZEC
Bilaxy	32			3							3			
Binance	12													
Bitbank	24		6							1	6			
Bitbay	12	150	6			10				10	6			20
Bitbuy	12		6							1	1			
Bitcoin.com	20		5			5		50		10	20			6
Bitmax	12		3								1			
Bitso	30		6								1			
Bittrex	36	202	6	10	30	20	600	20	10	2	10	20	100	30
BTCBOX	12		3											
CEX.IO	25		3	5		21				1	1	30		
Coinbase	35		12							1		30		24
Coineal	30													
CoinEx	12	12	3	1	5	3		10	1	1	3	1	30	1
CoinField	30		4								5			12
Coinfloor														
Coins Pro	20										6			
Currency.com	12		4											
EXMO	6	15	4	5		20		20	15	1	1			
FTX	10		2								1			
Gemini	12		12											24
GOPAX	45		6							1				12
Independent Reserve	20		10							6	6			
itBit	12		12											
Korbit	24		6			20				3	1			
Kraken	20	303	12			20		10		1	1	20		24
Liquid	21		6							10	20	30		
Nominex	12													
OKEX	12		1	1		1			1	1	1			6
Polionex	12	303	4	18		1	1200		18	2	2	30		8
PrimeXBT	10													
VALR	30										10			
Median	20	176	6	5	18	15	900	20	10	1	3	30	65	12

Table A.2: Sources of block confirmation rules.

Name	Country	URL
Bilaxy	Republic of Seychelles	https://bilaxy.zendesk.com/hc/en-us/articles/360020196932-Deposit-Instructions
Binance	Malta	https://www.binance.com/en/support/articles/360030775291
Bitbank	Japan	https://bitbank.cc/docs/deposit
BitBay	Estonia	https://bitbay.net/en/helpdesk/payments-and-withdrawals/when-funds-will-be-added-to-my-account
Bitbuy	Canada	https://support.bitbuy.ca/hc/en-us/articles/360032483832-Cryptocurrency-deposit-processing-times
Bitcoin.com	Saint Kitts and Nevis	https://support.bitcoin.com/en/articles/3851763-cryptocurrency-deposit-processing-times
BitMax	Singapore	https://bitmaxhelp.zendesk.com/hc/en-us/articles/360012169694-Why-Haven-t-I-Received-My-Deposits
Bitso	Mexico	https://bitso.com/fees/transactions
Bittrex	U.S.A	https://bittrex.com/api/v1.1/public/getcurrencies
BTCBOX	Japan	https://blog.btcbox.jp/en/fees-introduction-2
Cex.io	United Kingdom	https://support.cex.io/en/articles/4383405-processing-your-crypto-deposits-and-withdrawals
Coinbase	U.S.A	https://help.coinbase.com/en/coinbase/trading-and-funding/sending-or-receiving-cryptocurrency/why-is-my-transaction-pending
Coineal	Republic of Seychelles	https://support.coineal.com/hc/en-001/articles/360022989414-Deposit-Missing
CoinEx	Unknown	https://support.coinex.com/hc/en-us/articles/900004316823-FAQ-about-Deposit-
CoinField	Estonia	https://coinfield.freshdesk.com/support/solutions/articles/36000104043-how-many-blockchain-confirmations-are-needed-in-order-to-see-my-cryptocurrency-deposits-
Coinfloor	United Kingdom	https://coinfloor.zendesk.com/hc/en-us?mobile_site=false
Coins Pro	Philippines	https://support.coins.ph/hc/en-us/articles/203165130-When-will-my-balance-update-after-making-a-blockchain-transfer-to-from-my-wallet-
Currency.com	Belarus	https://currency.com/cryptocurrency-faq
Exmo	United Kingdom	https://info.exmo.com/en/wallet/how-quickly-will-my-cryptocurrency-deposit-be-added-to-my-balance/
FTX	Antigua and Barbuda	https://help.ftx.com/hc/en-us/articles/360034865571-Blockchain-Deposits-and-Withdrawals
Gemini	U.S.A	https://support.gemini.com/hc/en-us/articles/205424836-How-long-until-my-digital-asset-deposit-reaches-my-account-
GOPAX	South Korea	https://help.gopax.com/support/solutions/articles/42000020261-how-to-check-the-transaction-status-of-funds-deposited-to-gopax-com
Independent Reserve	Australia	https://www.independentreserve.com/help/faq
itBit	U.S.A	https://help.paxos.com/hc/en-us/articles/360042320931-Daily-Deposits-Withdrawal-Schedule
Korbit	South Korea	https://www.korbit.co.kr/faq/articles/?id=5fFcnrIQ6ILjsSelbxYqjr
Kraken	U.S.A	https://support.kraken.com/hc/en-us/articles/203325283-Cryptocurrency-deposit-processing-times
Liquid	Japan	https://help.liquid.com/en/articles/4713100-crypto-deposit-processing-time
Nominex	Seychelles	https://support.nominex.io/article/7-deposit-withdrawal-does-not-arrive
OKEX	Malta	https://www.okex.com/support/hc/en-us/articles/360000205532-Token-Confirmation-Requirements-Blockchain-Explorers
Poloniex	U.S.A	https://poloniex.com/public?command=returnCurrencies
PrimeXBT	Republic of Seychelles	https://help.primexbt.com/deposits-withdrawals/how-to-deposit#direct-crypto-deposits
VALR	South Africa	https://support.valr.com/hc/en-us/articles/360029561452-How-do-I-deposit-cryptocurrencies-on-VALR-

B Proofs

Lemma B.1. *Stationary Distribution of Memory Pool*
Let $a_f > 0$ denote the arrival rate of transactions with fees at least as large as $f \geqslant 0$ and assume that arrivals follow a Poisson process and that $a_f < \Lambda$. Let M_f denote the stationary distribution for number of transactions in the memory pool with a fee of at least f. Then, the distribution of M_f is given as follows:

For any $m \in \{0, 1, ...\} : \mathbb{P}(M_f = m) = (\frac{a_f}{\Lambda})^m \cdot (1 - \frac{a_f}{\Lambda})$

Proof.
Note that the number of transactions in the memory with fees at least as large as f can only change in unit increments. In particular, either a new transaction with fee greater than or equal to f arrives and the transaction number increases by one or a block is mined and the transaction number reduces by one. Since both arrivals and departures follow a Poisson process, the described process is the classical birth-death process. The steady state distribution of such a process, $\{\pi_f(m)\}_{m\in\mathbb{N}}$, is restricted by the following balance equations:

$$\pi_f(0) \cdot a_f = \pi_f(1) \cdot \Lambda \tag{4}$$

and

$$\pi_f(m) \cdot (a_f + \Lambda) = \pi_f(m-1) \cdot a_f + \pi_f(m+1) \cdot \Lambda \quad \text{for} \quad m \in \{1, 2, ...\} \tag{5}$$

which imply $\pi_f(m) = (\frac{a_f}{\Lambda})^m \cdot \pi_f(0)$ for all $m \in \{0, 1, ...\}$. Then, since $\{a_f(m)\}_{m\in\mathbb{N}}$ must be a valid probability distribution, we must have that $1 = \sum_{m=0}^{\infty} \pi_f(m) = \sum_{m=0}^{\infty} \pi_f(0) \cdot (\frac{a_f}{\Lambda})^m$, which yields $\pi_f(0) = 1 - \frac{a_f}{\Lambda}$. Then, $P\{M_f = m\} =: \pi_f(m) = (\frac{a_f}{\Lambda})^m \cdot (1 - \frac{a_f}{\Lambda})$ for all $m \in \{1, 2, ...\}$ which completes the proof. □

Lemma B.2. *Processing Time*
Let $a_f \geqslant 0$ denote the arrival rate of transactions with fees at least as large as $f \geqslant 0$. Assume also that arrivals follow a Poisson process, that $a_f < \Lambda$ and that the arrival rate for transactions with fee exactly f is zero. Then, the expected time for a transaction with fee f to be included in a block (i.e., processing time), $W_P(f)$, is given by:

$W_P(f) = \frac{\Lambda}{(\Lambda - a_f)^2}$

Proof.
Let X_t denote the number of transactions in the memory pool of equal or higher priority than a transaction with fee f at a time t units after the transaction with fee f is first entered in the memory pool. We define X_0 to include the transaction with fee f itself so that the first occurrence of $X_t = 0$ corresponds to the transaction with fee f being processed. Thus:

$$W_P(f) = \mathbb{E}[T_f] \tag{6}$$

with

$$T_f := \min\{t > 0 : X_t = 0\} \tag{7}$$

Let $\{Y_t\}_{t\in\mathbb{N}}$ denote the embedded Discrete Time Markov Chain in the Continuous Time Markov Chain, $\{X_t\}_{t\geqslant 0}$. Then, the following equation holds by definition:

$$T_f := \sum_{n=1}^{N_f} A_n \tag{8}$$

with

$$N_f := \min\{t > 0 : Y_t = 0\} \tag{9}$$

and $A_n \sim exp(\Lambda + a_f)$ denoting the inter-arrival times for transitions in the $\{X_t\}_{t\geqslant 0}$ process. Then, plugging Equation 8 into Equation 6 and applying the Law of Iterated Expectation yields:

$$W_P(f) = \mathbb{E}[\ \mathbb{E}[\sum_{n=1}^{N_f} A_n \mid Y_0]\ ]\ ] \tag{10}$$

Since A_n is independent of N_f and X_0, Equation 10 becomes:

$$W_P(f) = \frac{1}{\Lambda + a_f}\mathbb{E}[\ \mathbb{E}[N_f \mid Y_0]\ ] \tag{11}$$

Optional Stopping Theorem then implies:

$$\mathbb{E}[N_f \mid Y_0] = \frac{Y_0}{\frac{\Lambda - a_f}{\Lambda + a_f}} = Y_0\frac{\Lambda + a_f}{\Lambda - a_f} \tag{12}$$

Plugging Equation 12 into Equation 11 then yields:

$$W_P(f) = \frac{\mathbb{E}[Y_0]}{\Lambda - a_f} \tag{13}$$

Note that $Y_0 \sim M_f + 1$ with M_f defined in Lemma B.1. Thus:

$$\mathbb{E}[Y_0] = \sum_{m=0}^{\infty} (m+1) \cdot (\frac{a_f}{\Lambda})^m \cdot (1 - \frac{a_f}{\Lambda}) = \frac{\Lambda}{\Lambda - a_f} \tag{14}$$

Plugging Equation 14 into Equation 13 then completes the proof.

□

Lemma B.3. *Endogenous Fee Function*

There exists an equilibrium such that each User i selects a fee $\phi(c_i)$, with $\phi(c_i)$ being given by:

$$\phi(c_i) = 2 \cdot a \cdot \Lambda \int_0^{c_i} \frac{g(x)}{(\Lambda - a \cdot \overline{G}(x))^3} \, dx$$

Proof.

Recall that each User i selects a fee, f_i, to solve Equation 1. Following the convention in the literature (see, e.g., Huberman et al. 2019 and Hinzen et al. 2020), we solve for a pure strategy equilibrium characterized by a strictly increasing fee function, ϕ, that maps user disutility to optimal fee choices. In particular, we derive a function, ϕ, such that:

$$\phi(c_i) = \arg\max_{f \geqslant 0} \; u_i \cdot \Psi(N_{\tau_i}) - c_i \cdot W(f) - f \tag{15}$$

for all c_i so that $\phi(c_i)$ is the optimal fee choice for each User i and thus $f_i = \phi(c_i)$ for each User i.

Applying Equation 2 to Equation 15 yields:

$$\phi(c_i) = \arg\max_{f \geqslant 0} \; u_i \cdot \Psi(N_{\tau_i}) - c_i \cdot (W_P(f) + \kappa) - f \tag{16}$$

In turn, the first order condition implies:

$$- c_i \frac{d}{df}[W_P(f)]|_{f=\phi(c_i)} = 1 \tag{17}$$

Note that, since each User i selects a fee given by $f_i = \phi(c_i)$ then the arrival rate of transactions with fees at least as large as $f \geqslant 0$ is given by $a_f = a \cdot \overline{G}(\phi^{-1}(f))$ with $\overline{G}(x) := 1 - G(x)$. Moreover, in such a case, the transaction arrivals with fees at least f follow a Poisson process and the arrival rate of transactions with exactly fee f is zero because total transaction arrivals follow a Poisson process and G is strictly increasing. Therefore, the hypothesis of Lemma B.2 is satisfied so that we can apply the result from Lemma B.2 with $a_f = a \cdot \overline{G}(\phi^{-1}(f))$:

$$W_P(f) = \frac{\Lambda}{(\Lambda - a \cdot \overline{G}(\phi^{-1}(f)))^2} \tag{18}$$

Then, applying Equation 18 to Equation 17 yields:

$$\frac{2 \cdot c_i \cdot \Lambda}{(\Lambda - a \cdot \overline{G}(c_i))^3} \times (a \cdot g(c_i)) \times \frac{1}{\phi'(c_i)} = 1 \tag{19}$$

with $g(x) := \frac{dG}{dx}$. Solving the differential equation in Equation 19 and imposing $\phi(0) = 0$ (which is implied trivially by Equation 1) then completes the proof:

$$\phi(c_i) = 2 \cdot a \cdot \Lambda \int_0^{c_i} \frac{x \cdot g(x)}{(\Lambda - a \cdot \overline{G}(x))^3} \, dx \tag{20}$$

□

Proof of Proposition 3.1.
Lemma B.3 implies that:

$$f_i = 2 \cdot a \cdot \Lambda \int_0^{c_i} \frac{x \cdot g(x)}{(\Lambda - a \cdot \overline{G}(x))^3} \, dx$$

Then, direct verification yields $\frac{df_i}{d\Lambda} < 0$ thereby establishing that User i's fee decreases in Scale, Λ.

Lemma B.3 also establishes that User i pays $\phi(c_i)$ in equilibrium with $\phi(c_i)$ being a strictly increasing function. Accordingly, the set of users paying a higher fee than User i in equilibrium is given by $\{j : \phi(c_j) > \phi(c_i)\} = \{j : c_j > c_i\}$ and each user is drawn to be of such type with probability $\overline{G}(c_i)$ so that transactions with fees exceeding that of User i's fee arrive according to a Poisson process with rate $a \cdot \overline{G}(c_i)$. Note that the hypothesis of Lemma B.2 are all satisfied so that Lemma B.2 then implies that User i's expected time for her transaction to be included on a block (i.e., processing time) is given by:

$$W_P(f_i) = \frac{\Lambda}{(\Lambda - a \cdot \overline{G}(c_i))^2}$$

Direct verification yields $\frac{d}{d\Lambda}[W_P(f_i)] < 0$, establishing that User i's processing time decreases in Scale, Λ and thereby completing the proof.

□

Proof of Proposition 3.2.
We first establish that $k(s, \alpha) := \min\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$ is well-defined for any $\alpha > 0$ and then prove that $k(s, \alpha)$ decreases in s for any $\alpha > 0$. To establish that $k(s, \alpha)$ is well-defined, we only need to show that $\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$ possesses a well-defined minimum for any $\alpha > 0$. Recall that for any s, we have $\lim_{k \to \infty} p(s, k) = 0$ and $p(s, k)$ decreases in k so that $\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$ is a nonempty set. Let $\tilde{k} \in \mathbb{N}$ be such that $\tilde{k} \in \{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$. Then $\inf\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\} = \inf\{k \in \mathbb{N}, k \leqslant \tilde{k} : p(s, k) \leqslant \alpha\} = \min\{k \in \mathbb{N}, k \leqslant \tilde{k} : p(s, k) \leqslant \alpha\} = \min\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$, with the second equality following from $\{k \in \mathbb{N}, k \leqslant \tilde{k} : p(s, k) \leqslant \alpha\}$ being nonempty and compact. Thus, $k(s, \alpha) := \min\{k \in \mathbb{N} : p(s, k) \leqslant \alpha\}$ is well-defined for any $\alpha > 0$ as desired. To establish $k(s, \alpha)$ decreases in s for any $\alpha > 0$, we need to show that $k(s + \delta, \alpha) \leqslant k(s, \alpha)$ for $\delta \geqslant 0$. Note that $\alpha \geqslant p(s, k(s)) \geqslant p(s + \delta, k(s))$ with the first inequality following from the definition of $k(s)$ and the second inequality following from $p(s, k)$ decreasing in s. Then $k(s, \alpha) \in \{k \in \mathbb{N} : p(s + \delta, k) \leqslant \alpha\}$ so that $k(s + \delta, \alpha) := \min\{k \in \mathbb{N} : p(s + \delta, k) \leqslant \alpha\} \leqslant k(s, \alpha)$, which completes the proof. □

Proof of Corollary 3.3.
$\kappa = \frac{k(s)}{\Lambda}$ decreases in security, s, as an implication of Proposition 3.2 and decreases in Λ via direct verification (i.e., $\frac{d}{d\Lambda}[\frac{k(s)}{\Lambda}] = -\frac{k(s)}{\Lambda^2} < 0$). □

Proof of Corollary 3.4.
Proposition 3.1, Equation 1 and Equation 2 imply that user utility is given by:

$$u_i \cdot \Psi(N_{\tau_i}) - c_i \cdot \left(\frac{\Lambda}{(\Lambda - a \cdot \overline{G}(c_i))^2} + \frac{k(s)}{\Lambda}\right) - 2 \cdot a \cdot \Lambda \int_0^{c_i} \frac{x \cdot g(x)}{(\Lambda - a \cdot \overline{G}(x))^3}\, dx \tag{21}$$

Then, direct verification reveals that user utility increases in adoption, N_{τ_i}, and scale,Λ. Moreover, Proposition 3.2 implies that $k(s)$ decreases in security, s, so that user utility also necessarily decreases in security, s. This last implication follows because Equation 21 decreases in $k(s)$. □

Proof of Proposition 3.5.
$N_{\tau,1} \geqslant N_{\tau,2}$ for all $\tau \in \mathcal{T}$, $\Lambda_1 \geqslant \Lambda_2$, and $\frac{\Lambda_1}{k(s_1)} \geqslant \frac{\Lambda_2}{k(s_2)}$ implies that Blockchain 1 is preferred to Blockhain 2 for all users by Proposition 3.1, Corollary 3.3 and the preference structure given by Equation 1 (see the proof of Corollary 3.4 for additional detail).

To establish the converse, we proceed by contradiction. Formally, we wish to show that Blockchain 2 being preferred to Blockchain 1 by some user under some model parameters is inconsistent with the disjunction of the following four propositions:

(i) $N_{\tau,1} < N_{\tau,2}$ for all $\tau \in \mathcal{T}$

(ii) $\Lambda_1 < \Lambda_2$

(iii) $\frac{\Lambda_1}{k(s_1)} < \frac{\Lambda_2}{k(s_2)}$

Blockchain 1 being preferred to Blockchain 2 for each user under all circumstances means that users of any type (i.e., for any values of u_i, c_i and τ_i) receive higher utility from Blockchain 1 than Blockchain 2 for any transaction arrival rate (i.e, for any a).

More explicitly, letting the equilibrium user utility of User i when using blockchain j be denoted by $\mathcal{U}_{i,j}$, then Proposition 3.1, Equation 1 and Equation 2 imply:

$$\mathcal{U}_{i,j} = u_i \cdot \Psi(N_{\tau_i,j}) - c_i \cdot \left(\frac{\Lambda_j}{(\Lambda_j - a \cdot \overline{G}(c_i))^2} + \frac{k(s_j)}{\Lambda_j}\right) - 2 \cdot a \cdot \Lambda_j \int_0^{c_i} \frac{x \cdot g(x)}{(\Lambda_j - a \cdot \overline{G}(x))^3}\, dx$$

so that we must prove that $U_{i,1} \geqslant U_{i,2}$ for all u_i, c_i, τ_i and a is inconsistent with the disjunction of (i) - (iii). As discussed, we proceed by contradiction, imposing $U_{i,1} \geqslant U_{i,2}$ for all u_i, c_i, τ_i and a throughout the following argument and establishing a contradiction with the disjunction of (i) - (iii).

Letting $c_i = 0$ precludes $N_{\tau_i,1} < N_{\tau_i,2}$ so that at least one of (ii) or (iii) must hold. Then, holding c_i fixed but taking $a \to \infty$ and setting $u_i = 0$ precludes $\Lambda_1 < \Lambda_2$ so that (iii) must hold. However, holding c_i fixed but taking $a \to 0^+$ and setting $u_i = 0$ precludes $\frac{\Lambda_1}{k(s_1)} < \frac{\Lambda_2}{k(s_2)}$, thereby delivering the desired contradiction and completing the proof. □