An Asset Pricing Perspective on the Design of Cryptocurrencies

Zur Erlangung des akademischen Grades eines
Doktors der Wirtschaftswissenschaften

(Dr. rer. pol.)

von der KIT-Fakultät für Wirtschaftswissenschaften
des Karlsruher Instituts für Technologie (KIT)

genehmigte

DISSERTATION

von

M. Sc. Fabian Erich Eska

Tag der mündlichen Prüfung: 13. Juni 2024
Referentin: Prof. Dr. Marliese Uhrig-Homburg
Korreferent: Prof. Dr. Erik Theissen

Karlsruhe, 2024

Acknowledgements

This dissertation was written during my time at the Institute of Finance at the Karlsruhe Institute of Technology (KIT). The support I received from various sources was vital to the successful completion of this work, and I would like to express my heartfelt gratitude to all who contributed.

First and foremost, I am deeply gratefule to my supervisor, Prof. Dr. Marliese Uhrig-Homburg, for her excellent guidance and continuous support throughout my doctoral studies. Our numerous stimulating and inspiring discussions greatly enriched my research and this thesis. I extend my sincere thanks to my co-authors, Prof. Dr. Steffen Hitzemann, Dr. Marcel Müller, Yanghua Shi, and Prof. Dr. Erik Theissen for the numerous fruitful conversations and for the sound collaboration. I further thank Prof. Dr. Oliver Stein, Prof. Dr. Erik Theissen, and Prof. Dr. Christof Weinhardt for serving on the examination committee.

Additionally, my appreciation goes to my (former) colleagues at the Institute of Finance at KIT. In particular, I thank Julian Böll, Philipp Cölsch, Johannes Dinger, Dr. Jelena Eberbach, Dr. Stefan Fiesel, Caroline Grauer, Dr. Michael Hofmann, Annika Jung, Tobias Kargus, Viktoria Klaus, Fanchen Meng, Matthias Molnar, Dr. Marcel Müller, Dr. Michael Reichenbacher, Anian Roppel, and Jun.-Prof. Dr. Julian Thimme for their expert advice, engaging discussions, joint lunches, and friendly conversations, which made the past years truly enjoyable.

On a personal note, I am profoundly grateful for the unwavering support of my family and friends. Their encouragement, helpfulness, and the essential outside perspective they provided were invaluable. Lastly, I wish to thank everyone who has contributed, directly or indirectly, to this work, including those I may have inadvertently omitted. Every piece of criticism, praise, and every discussion has enriched this dissertation. Thank you all!

Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation and Thematic Overview

Bitcoin was introduced as a novel cash system eliminating the need for traditional financial intermediaries (Nakamoto, 2008) and marks the inception of the cryptocurrency market. Cryptocurrencies' peer-to-peer structures and novel mechanisms to achieve unified agreement on transaction records enable transfers directly from one party to another without reliance on trust. Also, the underlying blockchain technology is said to have disruptive character and promises transformative changes across various economic sectors, especially in financial applications such as securities settlement and collateralized loans, among others (see, e.g., Berentsen and Schär, 2017; Schuster et al., 2020). Despite Bitcoin and other cryptocurrencies not being widely accepted for payments, and many blockchain applications being still in their infancy, the cryptocurrency market has flourished since the launch of Bitcoin in January 2009. Various new cryptocurrencies have arisen, collectively forming a new financial asset class. According to coinmarketcap.com, the total market capitalization of this new asset class accounted for about 2.5 trillion U.S. dollars by the end of March 2024. In November 2021 the accumulated market capitalization even surged to a peak as high as 2.97 trillion U.S. dollars, surpassing the concurrent aggregated market capitalization of the Deutsche Aktienindex (DAX) by about 1.5 times.

Despite the consistent increase in the popularity of cryptocurrencies over time, many questions surrounding this asset class remained unanswered for a significant period and continue to challenge understanding. For example, what determines the value of these distributed databases representing units of virtual cash? Are we simply witnessing an enormous bubble or do cryptocurrencies rely on unique design features that justify at least part of the demand – for instance, the cryptographic techniques inducing a high degree of counterfeit safety or the protocols that set an upper bound on cryptocurrency supply acting as commitment device not to issue too much virtual money? Are such design features crucial value drivers and do they impact the price volatility of this emerging asset class? How is systematic risk, associated with specific design features, perceived within the markets? Do different consensus protocols have diverging effects on the price building mechanisms?

This dissertation addresses these open questions, focusing particularly on the unique features of the wide variety of cryptocurrencies. Most of the unique features, which specify the rules of the network, are directly encoded in the source codes and thus, they directly arise from the network design. Consequently, this dissertation refers to those features as design features. Examples include the consensus mechanisms applied to reach unified agreement on the decentralized ledger, the hash function employed to embed new information into the blockchain, or the supply curve with its direct implications for validator rewards. Each cryptocurrency is characterized by a unique set of design features, which may have diverse implications for prices, volatility, and risk, inter alia, compared to its competitors. Overall, the cryptocurrency landscape exhibits a wide variety of different design feature combinations, rendering the asset class of cryptocurrencies quite heterogeneous – a perspective on this asset class which is maintained throughout this dissertation.

Within literature that examines (cross-sectional) cryptocurrency returns, cryptocurrency valuation, and price volatility, a significant part predominantly focuses on financial markets-related determinants or macroeconomic and regulatory events. For instance, Liu et al. (2022) show that three factors adapted from traditional financial markets – cryptocurrency market, size, and momentum – explain the cross-section of cryptocurrencies' expected returns. Other studies introduce further financial market-related factors or concentrate on latent factors (see, e.g., Babiak and Bianchi, 2021; Liu et al., 2020). Albeit only being a small subset of this strand of literature, some papers drive this approach further and take into account the unique features and specific conditions of cryptocurrencies. These studies typically include cryptocurrency-specific factors such as the network adoption rate (see, e.g., Cong et al., 2021a; Liu and Tsyvinski, 2021) or the hash rate (see, e.g., Bhambhwani et al., 2023) and show that these factors indeed increase the explanatory power for cross-sectional returns. Yet, these factors are the outcome of the underlying cryptocurrency design features rather than unique features themselves. This dissertation addresses the gap in literature by analyzing the impact of cryptocurrency design features in the strict sense (i.e., as defined in the underlying source code) on various aspects of the cryptocurrency market, including valuation, volatility, and risk-return profiles.

The dissertation first develops a novel taxonomy that categorizes the broad spectrum of design features into six top-level groups, thereby providing a profound basis for analyzing design feature influence. Based on this taxonomy and utilizing hand-collected data, the dissertation investigates the impact of cryptocurrency design on valuation, measured through market capitalization, and on volatility in a second step. Since the design features generally have no time variation and the dependent variables are highly persistent, these analyses concentrate on a simple cross-section when studying the impact of various design features. The analyses' results are crucial for cryptocurrency investors, regulators, and developers, as they disclose the impact of design and the underlying technology on market outcomes, thereby aiding in informed decision-making and policy formulation.

A design feature that has drawn much attention is the consensus protocol. Consensus protocols define a network's rules by determining how unified agreement on transaction records is established within the network. Obviously, they are of upmost importance for cryptocurrency networks to maintain their integrity. Among the different types of consensus protocols, the Proof-of-Work (PoW) protocol has been the subject of much debate, particularly due to its perceived unsustainability. PoW networks rely on miners who update the ledger on a round-by-round basis by competitively solving cryptographic puzzles. This process demands vast computing power, resulting in immense energy consumption.[1] In response to this excessive energy consumption during times of high climate change concerns, alternative consensus protocols have emerged and gained in importance, with Proof-of-Stake (PoS) being the most notable. By the course of time, the number of PoS cryptocurrencies surpassed those using PoW (Irresberger et al., 2020). Most prominently, Ethereum, the second-largest cryptocurrency, completed a transition from PoW to PoS in September 2022 in an event known as *the Merge*. The basic procedure of PoS is fairly different to the one of PoW. Network members stake coins and get stake-proportional authorization to update the blockchain history. Following the network rules, updating users are granted a reward. Dishonest behavior, in contrast, can lead to sanctioning. Obviously, such systems do not only depend on their sound implementation, but are also critically determined by the financial economics of the network. Consequently, the economics and price building mechanisms of PoS systems are fairly different to PoW networks. By introducing a novel valuation model for PoS networks and analyzing its equilibrium outcome, this dissertation documents crucial differences between the two major consensus mechanisms with respect to network stability: Stemming from an opportunity cost problem, PoS is inherently more fragile than PoW. Juxtaposing to the PoW model of Pagnotta (2022), the dissertation shows that the stability of PoS networks is more sensitive to changes in certain design features.

In an ensuing chapter, the dissertation integrates established asset pricing methods with unique design feature data, thereby shedding light on the asset pricing significance of design-related characteristics of cryptocurrencies. Overall, this part relates design characteristics to expected returns and systematic risk. The focus on returns allows a combination of time-invariant design features with time-varying return predictors established in literature (e.g., Babiak and Bianchi, 2021; Liu et al., 2022), thereby employing a panel structure in the data. Using an Instrumented Principal Component Analysis (IPCA) as introduced by Kelly et al. (2019) and

[1] As of the end of 2023, the Cambridge Bitcoin Electricity Consumption Index estimates the annualised electricity consumption of Bitcoin, the most prominent PoW network, to be as high as the annual electricity consumption of countries like Poland or Malaysia (source: U.S. Energy Information Administration).

building upon the idea of Müller et al. (2023), this study elucidates systematic risk premiums associated with various design-related features of cryptocurrencies. The main focus centers around the risk premium of a long-short portfolio going long PoW-based cryptocurrencies and short PoS cryptocurrencies, albeit with the important feature that the long-short portfolio has zero exposure to all other characteristics. In the early parts of the sample, PoS is perceived systematically riskier than PoW. The systematic risk premium can be related to the health of the staking system, and thus to the inherent opportunity cost problem which induces a lower network stability, as documented in the preceding part of this dissertation. In more recent times, PoW carries a premium compensating for the energy consumption risk and climate risk concerns. Besides, the risk premiums associated with other design-related features are examined. Specifically, the analysis contrasts coins with tokens, privacy with non-privacy cryptocurrencies, as well as smart contract featuring networks with those that do not. This rounds off the dissertation, which discloses an asset pricing perspective on cryptocurrency design.

1.2 Structure of the Dissertation

This dissertation is structured as follows.

In Chapter 2, which bases on the working paper "Design and Valuation of Cryptocurrencies" (Eska et al., 2022b), we first propose the novel taxonomy of cryptocurrency design features and introduce hand-collected data on these features. This provides a valuable overview of which specific design characteristics are observed in the cryptocurrency market with what frequency. Further, the data builds the basis for the subsequent analysis that reveals the impact of cryptocurrencies' designs on cryptocurrency valuation. Using a two-stage regression approach and LASSO regressions, it is shown that forks and deviations from the design of Bitcoin are associated with lower market capitalization. Non-anonymous cryptocurrencies and cryptocurrencies that do not pass on any transaction fees and/or tips to agents who maintain the integrity of the network have, on average, higher market values. The results presented in this chapter are robust to variations in the way we measure market valuation.

Considering the design features introduced in Chapter 2, their impact on the cross-sectional volatility of cryptocurrencies is analyzed in Chapter 3. We estimate LASSO regressions using the design features as independent variables and volatility measures as the dependent variables. The results show that older cryptocurrencies tend to be less volatile. In contrast, the chapter provides evidence that networks passing transaction fees and/or tips on to verifiers are associated with higher volatility levels. Besides, cryptocurrencies with mandatory transaction fees, cryptocurrencies with non-public development teams, as well as the ones based on either

PoS or delegated Proof-of-Stake are more volatile. To assure robustness, the volatility measures are calculated on basis of Bitcoin and U.S. dollars denominated prices, respectively. Note that this chapter builds on the working paper "Do Design Features Explain the Volatility of Cryptocurrencies?" by Eska et al. (2024).

Chapter 4, which is based on the working paper "After *the Merge*: Network Fragility and Robust Design of PoS Cryptocurrencies" (Eska et al., 2022a), develops an economic model for cryptocurrencies that achieve consensus via PoS. The model links the demand-driving network structures with security-relevant components in PoS networks. The price interacts as the connecting component and can be determined in so-called stationary equilibria. The model reveals an opportunity cost problem in PoS systems. The usefulness of a PoS coin for transactions negatively affects the incentive for staking which can reduce network security and ultimately lead to a system breakdown. Consequently, PoS systems are inherently more fragile than cryptocurrencies utilizing a PoW-based consensus protocol. Several design parameters such as the inflation rate, the fork length, and others, critically determine the extent of the network fragility. In the second part of this chapter, the model is calibrated to the Ethereum network and thereby provides guidance on parameter choices ensuring the stability of the system.

In Chapter 5, which builds on the working paper "Climate Change, Energy Prices, and the Returns of Proof-of-Work vs. Proof-of-Stake Crypto Assets" by Eska and Müller (2024), systematic risk premiums of cryptocurrency design features are analyzed. Based on a latent factor asset pricing model, the returns of long-short portfolios managed by the design-related features are examined, thereby identifying systematic risk premiums linked to these design-related characteristics. This chapter particularly focuses on consensus-related risk premiums and thus on the question whether returns of PoW- and PoS-cryptocurrencies include different compensations for systematic risk. Specifically, we relate the systematic part of the returns from a portfolio that is long PoW and short PoS to proxies accounting for climate change concerns, energy consumption risk, and staking health. The analysis reveals a negative covariation with innovations in climate change concerns and energy consumption risk in recent times. Prior to 2021, PoS was systematically riskier than PoW. This can be attributed to the cyclicality of the opportunity cost associated with PoS, which dominates the energy-related risk premium of PoW in this period of the sample. Employing the same methodology, further design-related risk premiums are investigated. Except for coins versus tokens, we find similar structural breaks in the risk-return profiles during the time span of the consensus risk adjustment. For instance, privacy featuring cryptocurrencies earned a systematic risk premium of almost 20% p.a., which vanished to a level indistinguishable from zero during the break.

Chapter 6 recapitulates the main findings of this dissertation and gives a concise outlook on possible future research questions.

Chapter 2

Design and Valuation of Cryptocurrencies

2.1 Introduction

Cryptocurrency values are highly volatile. While the time-series variation of cryptocurrency values in general, and that of Bitcoin in particular, attracts a lot of public attention, the cross-sectional differences in cryptocurrency values receive much less attention and are not well understood. Some cryptocurrencies, the so-called stablecoins, are backed by a portfolio of assets and thus have valuations linked to those assets, but most are not. The question therefore arises of what determines the relative valuations of different cryptocurrencies. This question is of obvious importance to users of and investors in cryptocurrencies, to trading venue operators and regulators.

This chapter sheds light on a specific aspect of this issue. We analyze empirically whether design features of cryptocurrencies and the specific characteristics associated with them affect their relative valuation. To this end, we first develop a taxonomy of the wide range of cryptocurrency design features and sort them into six groups, namely, (i) features related to the development process of the cryptocurrency, (ii) technical design features, (iii) features related to cryptocurrency supply, (iv) features related to transactions and transaction processing, and (v) features related to the usability of the underlying network as well as (vi) general features. Additionally, we include the age of each cryptocurrency to take into account the fact that older cryptocurrencies may have more users and, because of the network externalities associated with the number of users, may be more valuable. We hand-collect a data set covering the design features and age of 79 cryptocurrencies with the highest market capitalization as of September 2020. Note that we only consider cryptocurrencies in the strict sense, i.e., coins, and exclude tokens because tokens do not operate on their own independent distributed ledger.[2]

We combine the data on design features with data on market capitalization, obtained by multiplying coin supply by coin prices. To take into account the overall market movements between the inception of a coin and our sample period, we additionally introduce and analyze a discounted version of market capitalization.

Our data set is characterized by a high number of potentially relevant independent variables relative to the number of cryptocurrencies in the sample. We use two methodological approaches to tackle this problem. First, we implement a two-stage cross-sectional regression approach inspired by Karnaukh et al. (2015). In step 1 we estimate six regressions in which we regress the market values of the cryptocurrencies in our sample on the design features contained in one of the six groups introduced above. In step 2 we estimate an encompassing regression in which we include those design features that have the highest explanatory power in the respective first-stage regression. Our second approach is the machine learning-based LASSO (least absolute shrinkage and selection operator) regression approach which combines variable selection and regularization. Our approach has two distinct characteristics which differentiate it from traditional asset pricing approaches. First, we explain the cross-section of market valuations, not the cross-section of returns. Second, we do not use a panel data set (or a repeated cross-section as in Fama and MacBeth, 1973) but rather a simple cross-section. This approach is warranted because our dependent variables (cryptocurrency market values) are highly persistent and most of our independent variables (the design features) have little or no time-series variation.

Our results indicate that cryptocurrencies with a Bitcoin-like combination of design features tend to have higher market capitalization than currencies that are distinctively different from Bitcoin. We also find that cryptocurrency networks that were spun off another network (so-called forks) and not built from scratch tend to have lower market capitalization, possibly because forks compete against their parent networks which are very similar and have a first-mover advantage. Cryptocurrencies that do not pass on any transaction fees and/or tips to agents who maintain the integrity of the network have, on average, a higher market capitalization. Such transaction fees can increase the fragility of the system: Some users drop out directly, waiting times increase as a result, and consequently, even more users drop out (Basu et al., 2023; Easley et al., 2019; Huberman et al., 2021). Adverse effects related to network security are also conceivable (Pagnotta, 2022). Our analysis also indicates that networks that require the disclosure of the real-world identities of their users have higher market capitalization. A possible reason for the higher valuation of non-anonymous currencies is that market participants price in the expectation of regulatory approval of non-anonymous currencies and/or regulatory

[2] Even though stablecoins have "coins" in their name, they are generally tokens operating on an existing distributed ledger and therefore are excluded from our analysis.

action against anonymous currencies. Finally, we find (weak) evidence that currencies which had for-profit companies as their main developers have lower market capitalization, possibly because of a lower degree of decentralization.

Related Literature

This chapter contributes to the literature on the valuation of cryptocurrencies. A first strand of this literature addresses the question why cryptocurrencies which are neither backed by a pool of assets nor by a trustworthy institution such as a central bank have a non-zero value (Abadi and Brunnermeier, 2018; Aoyagi and Adachi, 2018; Biais et al., 2023; Bolt and Oordt, 2020; Dwyer, 2015; Pagnotta, 2022; Schilling and Uhlig, 2019; Sockin and Xiong, 2023; Zimmerman, 2020). A second strand of the literature analyzes financial markets-related determinants of cryptocurrency values. Papers in this area analyze, for example, whether there are common factors driving cryptocurrency returns (Bianchi et al., 2022; Borri et al., 2022; Cai and Zhao, 2024; Hu et al., 2019; Leong and Kwok, 2023; Liu et al., 2020; Liu et al., 2022; Zhang et al., 2021), or whether macroeconomic or regulatory events affect cryptocurrency prices (Auer and Claessens, 2021; Corbet et al., 2020; Koenraadt and Leung, 2024; Li and Miu, 2023). Some papers in this strand of the literature also include cryptocurrency-specific factors driven by network effects or cryptocurrency production cost (Babiak and Bianchi, 2021; Bhambhwani et al., 2023; Cong et al., 2021a; Liebi, 2022; Liu and Tsyvinski, 2021). The third strand of the literature, and the one most closely related to our work, attempts to identify determinants of the cross-section of cryptocurrency values related to cryptocurrency design and blockchain functionality. Two early papers that relate cryptocurrency design to price levels and returns are Hayes (2017) and Wang and Vergne (2017). Hayes (2017) investigates the impact of cryptocurrency design features on prices. He considers prices on a single day in 2014 and examines four design features, two of which (the rate of coin creation and the use of the scrypt algorithm) are found to be significant for price formation.[3] Wang and Vergne (2017), in contrast, analyze the returns of five cryptocurrencies and find that they are positively related to a measure of innovation potential as well as to supply growth and liquidity. Furthermore, Shams (2020) demonstrates that the comovement structure of cryptocurrencies is too high to be explained by similarities in characteristics such as the consensus mechanism. He suggests that trading on cryptocurrency exchanges is the main driver of the comovement. We extend this line of research by analyzing a data set much broader both in terms of cryptocurrencies and in terms of design features, by implementing two distinctively different empirical methodologies and various model specifications, and by proposing a novel taxonomy of cryptocurrency design features.

[3] Hayes (2017) also finds that the hashrate affects prices. The hashrate, however, is not a design feature of a cryptocurrency but rather a market outcome.

The remainder of this chapter is structured as follows. In Section 2.2, we introduce our novel taxonomy of cryptocurrency design features, describe the data collection procedure, and present descriptive statistics on cryptocurrency design. In Section 2.3, we describe the methodology and in Section 2.4, we present and discuss the results of our empirical analysis. Section 2.5 concludes.

2.2 Cryptocurrency Design Features

In this section we introduce in Subsection 2.2.1 a novel taxonomy of cryptocurrency design features and hypothesize how the design features might affect the market value of a cryptocurrency. In Subsection 2.2.2 we describe how we collected data on the design features for a total of 79 cryptocurrencies and in Subsection 2.2.3 we present summary statistics.

2.2.1 Taxonomy

The different coins in the cryptocurrency universe can be characterized by combinations of various design features. While there exists a wide range of such features, these can be categorized into a small number of groups. The taxonomy we propose in this section differs from previous attempts which either do not allow a unique allocation of individual features to groups (Garriga et al., 2020), or which create abstract categories which are difficult to link to individual design features (Cousins et al., 2019). We propose six categories which are *Development*, *Technical*, *Supply*, *Transactions*, *Usability*, and *General*.

Development

During the development process of a cryptocurrency, a basic concept is transformed into implementable code. The identity of the developers and the organization of the process may affect the design and subsequent valuation of the cryptocurrency. With respect to the identity of the developers, we differentiate between: (i) a loose network of independent developers and development teams (*DeveloperPublic*), (ii) a non-profit organization (NPO) (*DeveloperNPO*), or (iii) a private, for-profit company (*DeveloperPrivate*). It is not a priori clear how the identity of the development team will affect valuation. On the one hand, users may prefer a public development team because everyone can contribute to the development process, resulting in a high degree of decentralization, a particularly appealing cryptocurrencies characteristic. On the other hand, private developers may have a stronger incentive to make design choices that result in high valuation while public development teams may maximize welfare, which is not necessarily the same thing.

A closely related aspect is the question who decides on code changes. In some networks, a privileged group decides on code changes. In other networks, the decision whether a suggested modification is integrated into the core code is made by the network members and thus by majority voting. We define the dummy variable *NoMajorityChanges* which is set to 1 for the cryptocurrencies without such majority voting.[4] For those cryptocurrencies enabling majority voting the variable *NoMajorityChanges* is set to 0. We expect that users value decentralized decision making and that, consequently, cryptocurrencies without majority voting will be less valuable.

We also record general code-related features such as the core code's primary implementation language and the accessibility of the core code. With respect to the implementation language we differentiate between C++ (dummy variable *CodeC++*), Go (*CodeGo*), and other languages (*CodeOther*). With respect to accessibility we record whether the core code is fully accessible on Github or a similar platform. If this is the case, we set the dummy variable *CodeNonPublic* to 0; otherwise, it takes a value of 1. We expect that the lower transparency associated with a non-accessible implementation lowers market capitalization.

The last design feature in the category development is *Fork*, a dummy variable that indicates whether the initial implementation of a cryptocurrency network was forked from another network ($Fork = 1$) or built from scratch ($Fork = 0$). Forks often involve improvements to certain aspects of the parent network, which may potentially lead to a higher valuation of the fork. On the other hand, though, a fork is essentially a (modified) imitation of the parent which lacks innovation and has to overcome the first mover advantage of the parent network. Our prior expectation is that the second effect dominates the first, resulting in lower valuations of forks.

Technical

The technical category comprises design features related to the consensus mechanism, the hash function, and the cryptographic methods used to authenticate signatures.

The consensus mechanism provides the rules for reaching agreement on the network status among its users and thus determines how transactions are validated. Validating a transaction is tantamount to authorizing a change to the distributed ledger that documents the change in ownership of the coins transacted. The first and most prominent consensus mechanism is "Proof-of-Work" (PoW), proposed by Nakamoto (2008).[5] The PoW mechanism results in extremely high energy consumption.[6] Currently, the most important alternative to PoW is

[4] To assign a value of zero to *NoMajorityChanges*, we do not require that *all* decisions on code changes are made by the network members. Instead, we only require that some decisions are made in this manner.

[5] In PoW, consensus is reached through the work of so-called miners who compete to solve cryptographic puzzles.

[6] For instance, in 2022 the total electricity consumption of Bitcoin, the most prominent cryptocurrency based on PoW, summed up to about 107.65 TWh according to the Cambridge Bitcoin Electricity Consumption Index

"Proof-of-Stake" (PoS). PoS is based on the idea that agents with higher coin holdings are generally more interested in a healthy network. In line with this incentive, the probability that a network member can authorize a transaction is positively related to the coin holdings of that member. Besides (i) PoW and (ii) PoS, Irresberger et al. (2020) identify three further main consensus mechanisms: (iii) hybrid PoW/PoS, (iv) delegated Proof-of-Stake (dPoS), and (v) non-standard consensus mechanisms. We condense these five consensus mechanisms into three dummy variables for PoW ($ConsensusPoW$), for PoS and dPoS ($ConsensusPoSdPoS$), and for nonstandard mechanisms ($ConsensusOther$). We combine PoS and dPoS into one variable because both are based on the aforementioned idea that "richer" network members are more interested in the success of the network and should therefore have more influence on the validation process.[7] We capture hybrids between PoW and PoS by assigning the value of one to both $ConsensusPoW$ and $ConsensusPoSdPoS$, for the respective cryptocurrencies. The lower energy consumption of PoS is a clear benefit and may result in higher valuation of cryptocurrencies adopting that mechanism. However, it is not clear that PoS and other alternative mechanisms are as resistant to attacks as PoW.[8] We therefore have no clear prediction on the sign of the coefficients for the three consensus mechanism dummy variables.

Transactions are combined into blocks, and hash functions are used to ensure that blocks cannot be altered discretely.[9] Within the cryptocurrency universe, many different hash functions are used for this purpose. For our data set on design features, we categorize them in to five different specifications: (i) SHA-256, the function which Bitcoin uses, (ii) Ethash or the closely related keccak256 function, (iii) blake, (iv) scrypt,[10] and (v) other hash functions. While we do collect the corresponding data for all cryptocurrencies in our sample, we do not want to inflate the number of independent variables in our empirical analysis. Therefore, we introduce the age of the hash function as a proxy for the quality of the hash function. More recently developed hash functions will typically offer a higher level of security.[11] Consequently, we anticipate that the age of the hash function will negatively affect market valuation.

Cryptocurrencies use Digital Signature Algorithms (DSA) which are based on elliptic curve

(see cbeci.org/) - a value roughly equal to the aggregated electricity consumption of the Netherlands (113 TWh in 2021) according to U.S. Energy Information Administration. Mora et al. (2018) argue that the carbon emissions caused by Bitcoin mining can push global warming above 2°C.

[7] The difference between PoS and dPoS is the fact that in dPoS the network member can outsource the task to third parties, so-called delegates.

[8] As a case in point, before the Ethereum network eventually adopted PoS in September 2022, it was stated on the Ethereum homepage that "[PoS] is still in its infancy, and less battle-tested, compared to [PoW]" (see ethereum.org/en/developers/docs/consensus-mechanisms/pos/ [Accessed: December+12, 2023]).

[9] Each block contains the hash value of the previous block. If a block is changed, its hash value will also change and will then deviate from the value written in the next block. This link between blocks makes ex-post changes to a block easily detectable.

[10] For PoW-based crpytocurrencies, Hayes (2017) finds a positive influence of scrypt on prices.

[11] See, e.g., Pfautsch et al. (2020) or https://www.streetdirectory.com/etoday/-ejcluw.html [Accessed: April 15, 2024].

cryptography in order to authenticate the signatures of the parties in a transaction. We differentiate between three types of elliptic curves, (i) ECDSA, the curve which is used, among others, by the Bitcoin network, (ii) Ed25519, a widely used alternative,[12] and (iii) other curves. While the DSAs are essential for secure coin transfer, not many network users are aware of the specific differences between the elliptic curves. We therefore do not expect a significant impact on market values.

Supply

The process of supplying cryptocurrencies is very different from the process of supplying fiat currency. While the supply of fiat currency depends on the monetary policy of the respective central bank and is therefore subject to discretionary decisions, the supply of cryptocurrencies is predetermined in most networks. Oftentimes, the growth in coin supply is linked to the process of verifying transactions – agents who successfully participate in the verification process are rewarded with newly created coins. In addition, many cryptocurrencies have a supply cap, implying that the maximum number of coins cannot exceed a predetermined threshold. We use the binary variable *NoMaxSupply*, set to 1 in case of no cap, indicating the existence of a predetermined maximum number of coins.

In general, cryptocurrencies can (i) have a fixed supply (a feature captured by the dummy variable *FixedSupply*), (ii) be deflationary (*Deflationary*), or (iii) be inflationary. If the supply is fixed, the number of coins in circulation does not vary over time. For deflationary currencies, the number of coins decreases over time as a result of certain "burn mechanisms". Inflationary currencies come in various forms, characterized by different supply growth schemes. Many cryptocurrencies with increasing supply have a reward reduction similar to that of Bitcoin in place. Consequently, the supply curve is increasing and concave over time, and possibly converges to a predetermined threshold. The dummy variable *InflationaryDecreasing* identifies currencies with that feature. Instead of a reward reduction, cryptocurrencies may have constant rewards, resulting in a linear supply function over time (*InflationaryFixed*). Finally, the supply curve may be convex. This can be achieved by fixing the supply growth rate (rather than the number of coins issued per unit of time). The growth rate is often referred to as the rate of inflation of the currency (*InflationaryFixedInflationRate*). Finally, some currencies have dynamic and thus time-varying supply growth rates, resulting in non-deterministic supply growth (*InflationaryDynamic*). We expect that cryptocurrencies with supply caps, fixed supply and deflationary currencies have lower value because the supply restrictions may limit the adoption of the currency by users.

[12] For instance, Lisk, Monero and Zcash use this elliptic curve for the authentification of signatures. Ed25519 offers a higher level of anonymity compared to ECDSA.

As noted, the reward to those agents verifying transactions in the network is linked to coin supply. The reward can be a coinbase reward (the creator of each new entry to the ledger earns a specific number of new coins) or an alternative reward distributions scheme based on inflationary schemes, e.g., one where rewards are distributed among a larger network user group (e.g., all verifiers) and are not necessarily attached to individual new ledger entries. We capture these two cases by the dummy variables *RewardCoinbase* and *RewardInflation*. In either case, those two reward distribution schemes incentivize agents to contribute to a healthy network and thus, we expect a positive influence on market capitalization.

Transactions

The category transactions contains design features related to transactions on the cryptocurrency network and the ways in which these transactions are processed.

The number of transactions a network can process per period of time is often referred to as the throughput. In theory it can be measured by transactions per second (TPS). However, TPS is controversial, primarily due to the inconstistency in its measurement across different networks. Therefore, we proxy TPS by the time between neighbouring blocks and the existence or non-existence of a blocksize limit. The time between blocks determines the frequency of changes of the distributed ledger. We differentiate between the theoretically intended minimum time between two blocks (*TheoreticalBlockTime*) and the actually observed time between blocks (*BlockTimeAverage*).[13] We note that shorter time between blocks does not only mean that more transactions can be processed per unit of time, but also means that the minimum time it takes to complete a transaction is lower. We therefore expect that shorter time between blocks is associated with higher valuation. A blocksize limit sets a limit to the number of transactions that can be processed per unit of time and thus limits the throughput of the network. The dummy variable *BlocksizeLimit* is set to 1 if such a limit exists.[14] We expect that the existence of a blocksize limit affects market value negatively.[15]

In many cryptocurrency networks users have to pay a fee for the processing of their transactions. We include three variables that intend to capture the existence and design of such fees, *TransactionFeeObligation*, *NoTipSpecialTreatment*, and *NoFeeTipForMinerForger*. *TransactionFeeObligation* records whether a cryptocurrency network has a mandatory fee for a transaction to be processed. Because the existence of a mandatory fee makes it more expensive to use the network, we expect a negative impact on market valuation. Some networks allow their users to prioritize a transaction by paying a special fee, often called tip. We define the dummy

[13] If there was a fork within a network that induced a change in at least one of these variables, we record the post-fork values of the variables. In the subsequent analysis, we restrict ourselves to the actually observed blocktime due to data availability and reliability.

[14] We were unable to verify whether a blocksize limit exists for some cryptocurrencies, implying that we have missing data for this variable.

[15] We note, though, that an unlimited block size may result in excessively large ledger entries.

variable *NoTipSpecialTreatment* which is set to 1 if such tips are not possible. We expect that investors value the possibility to prioritize their transactions and therefore expect a positive impact on market valuation. The third variable, *NoFeeTipForMinerForger*, is set to 1 for networks where the transaction fees and/or the tips are not – neither fully nor partly – passed on to the agents verifying transactions (e.g., miners in PoW and stakers in PoS). A scheme where fees and/or tips are passed on to those agents (miners or stakers) makes their activities more profitable and may thus attract more agents. This, in turn, increases the degree of network decentralization and the security (i.e., resistance against attacks) of the network. We therefore expect a negative effect of *NoFeeTipForMinerForger* on market values.

Usability

The first cryptocurrency, Bitcoin, was devised as a means of payment. However, there are use cases for cryptocurrencies beyond that. A cryptocurrency network can be a payment system, a platform for smart contracts (the Ethereum network is a case in point), or it can serve other purposes such as decentralized finance applications. We capture the intended use of a cryptocurrency by three dummy variables, *IntentionPayment*, *IntentionSmartContract*, and *IntentionOther*. We expect that cryptocurrencies that serve purposes beyond being a means of payment have higher market values.

In some networks the ownership of coins embodies rights (e.g., voting rights), or possibilities of usage beyond making payments. The variable *UsageBeyondPayment* takes on the value one for cryptocurrencies for which this is the case. We expect a positive coefficient. Some cryptocurrency networks offer implicit smart contract support (without requiring sidechains or similar arrangements).[16] For networks with this feature we set the dummy variable *SmartContractSupport* to one. We anticipate a positive value impact due to expanded functionalities, but the risk of hacking attacks on smart contracts resulting from implementation errors is likely to introduce a negative effect. The dominant effect remains undetermined.

General

The final category comprises three further design characteristics that may potentially affect valuation. Most cryptocurrencies bundle transactions into blocks and update the network status by appending blocks to a blockchain. Since Ripple's introduction in 2012, the cryptocurrency space has expanded to include networks that utilize alternative distributed open-source protocols instead of blockchain technology. The variable *LedgerOther* identifies such networks. Generally, these alternative designs aim at overcoming the scalability problem of blockchains, thereby potentially creating possibilities for new usages of cryptocurrencies. This aspect might

[16] There certainly are other features that extend the usability of a cryptocurrency. However, we are not aware of other features that are consistently documented in the public domain. We therefore restrict ourselves to the variable *SmartContractSupport*.

lead to a higher valuation of the respective cryptocurrencies. However, these no-blockchain designs may be less secure (or less battle-proof), limiting their adoption and lowering their valuation. As it is unclear which of these effects is stronger, we do not have a clear prediction for the sign of the coefficient on the *LedgerOther* variable.

There are two accounting schemes that are commonly applied in the cryptocurrency world. The first cryptocurrencies (including Bitcoin) rely on unspent transaction outputs (UTXOs) to balance the ledger. Under this accounting scheme the ledger does not store information on account balances. Consequently, to infer account balances one has to process the entire blockchain and sum up all UTXOs logged to the respective account. Given the enormous size of many blockchains this may not be the most efficient solution. Therefore, other cryptocurrency networks apply a traditional balance accounting scheme. Such networks store every account's balance on the blockchain (similar to banks that store customer account balances using electronic records). This accounting scheme does not require a network member to parse the whole ledger to infer account balances. Rather, a synchronization without accessing the whole history of the ledger becomes possible. We identify cryptocurrencies using such an accounting scheme by the variable *AccountingBalance*. We expect a positive coefficient because of the efficiency and intuitive appeal of these accounting schemes.

Another important feature is the degree of anonymity that a cryptocurrency network offers its users. In networks like Bitcoin, every transaction and wallet balance can be traced back to a pseudonymous public address. Other networks prioritize providing enhanced privacy and facilitate fully anonymous transactions through specific cryptographic methods.[17] We identify networks that allow anonymous transactions by the variable *Anonymous*. Enhanced privacy meets the demand for censorship resistance[18] and thus makes anonymous cryptocurrency networks more attractive. We therefore expect that networks supporting full anonymity have higher valuation than those which only allow pseudonymous transactions. On the other end of the anonymity spectrum are cryptocurrency networks that connect the addresses and transactions to real world identities (identified by the variable *NonAnonymous*). Such a non-anonymous

[17] Examples include zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge) of Zcash, a form of zero-knowledge cryptography. In this network, transactions can be fully encrypted but the validity can still be verified with specific zk-SNARK proofs. In detail, a "prover" can prove to a "verifier" that a statement is true without revealing any information beyond the validity itself. Via specific combinations, this procedure allows transaction processing without disclosing information about the transaction itself.

[18] Pagnotta and Buraschi (2018) state that censorship resistance "has multiple sources including financial repression through governmental capital controls; option-like hedging against government abuses such as arbitrary wealth confiscations or the targeting of political dissidents and/or religious groups; hedging against changes in inheritance laws; the risk of disruptions of the traditional banking system due to bank runs, fiat hyperinflation or forced maturity conversion of bank deposits; the ability to secure wealth transfers in the event of armed conflicts, territorial invasions, civil wars, refugee crises", as well as criminal activity.

design may offer advantages with respect to regulatory acceptance because KYC (Know-Your-Customer) is already fulfilled. Supervisory authorities might thus favor non-anonymous cryptocurrencies. In addition, note that these networks do not necessarily bear a higher risk to reveal their members' identity to the public. These currencies may have higher values than those with pseudonymous transactions due to the prospect for regulatory acceptance.

In Table 2.1, we list the introduced variables, specifying if they are binary and our expected coefficient signs ("+" or "-") based on the prior discussion. A "0" indicates that we either have no clear prediction for the respective variable, or that we consider its impact on valuation to be negligible.

2.2.2 Data Collection

Unlike price and quotation data for cryptocurrencies, data on design features cannot be obtained from data vendors. We therefore had to hand-collect data on the variables introduced in Section 2.2.1. We primarily used data sources directly related to the network founders, the development team, and the network community, such as whitepapers, official network websites, developers' documentation, and the code repository. When necessary information was not available from these sources, or when it was incomplete or inconsistent, we extended our search to expert forums like the respective subreddits and those on the developers' portals.[19] For the variables *IntentionPayment*, *IntentionSmartContract* and *IntentionOther*, we restricted our data collection procedure to the tags provided by Coinmarketcap and Messari. For well-known and highly capitalized cryptocurrencies we could collect the required data rather easily. However, the quality of documentation is often poor for less well known and less capitalized cryptocurrencies. For many of these currencies the data required for our analysis was unavailable, despite accessing a broad range of different data sources. Eventually we managed to collect data on the relevant design features for the 79 cryptocurrencies with the highest market capitalization as of September 2020. We admit that our data set is not free from survivorship bias. However, because data on design features of cryptocurrencies with low market valuations and of cryptocurrencies that were discontinued is unavailable, there is no obvious way to cure this problem. As explained below, we try to mitigate it by relating market valuation to *lagged* data on design features, i.e., the data on design features from September 2020, the month right before our sample period.

[19] Whenever relying on these data sources, we ensured that the information in our data set was backed by two independent sources.

Table 2.1: Design features variables, expected influence, and descriptive statistics

Maintaining the different design feature groups, this table lists the variables introduced in Section 2.2.1 and summarizes its expected influence on market capitalization. Additionally, the columns on the right provide descriptive statistics for each variable. We consider (i) all cryptocurrencies in our sample in their design configuration as of December 2020 and (ii) all cryptocurrencies in our sample including all of their historical design feature combinations. Since we do not include the specific hash functions into our empirical analysis, we do not attempt to predict their influences on market valuation.

Panel A: Development

Variable	Binary	Predicted influence	As of December 2020			All-time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
DeveloperPublic	yes	+	79	0.2025	0.4045	114	0.2368	0.4270
DeveloperNPO	yes	+	79	0.2785	0.4511	114	0.2544	0.4374
DeveloperPrivate	yes	-	79	0.5190	0.5028	114	0.5088	0.5021
NoMajorityChanges	yes	+	79	0.3544	0.4814	114	0.3158	0.4669
CodeNonPublic	yes	-	79	0.0380	0.1924	114	0.0263	0.1608
CodeC++	yes	0	79	0.3924	0.4914	114	0.4386	0.4984
CodeGo	yes	0	79	0.3671	0.4851	114	0.3246	0.4703
CodeOther	yes	0	79	0.2532	0.4375	114	0.2456	0.4324
Fork	yes	-	79	0.5063	0.5032	114	0.5526	0.4994

Panel B: Technical

Variable	Binary	Predicted influence	As of December 2020			All-time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
ConsensusPoW	yes	0	79	0.3165	0.4681	114	0.4386	0.4984
ConsensusPoSdPoS	yes	0	79	0.4937	0.5032	114	0.4035	0.4928
ConsensusOther	yes	0	79	0.2278	0.4221	114	0.2018	0.4031
HashSHA256	yes	N/A	79	0.4304	0.4983	114	0.4035	0.4928
HashEthash	yes	N/A	79	0.1519	0.3612	114	0.1316	0.3395
HashScrypt	yes	N/A	79	0.0759	0.2666	114	0.0789	0.2708
HashBlake	yes	N/A	79	0.1392	0.3484	114	0.1140	0.3193
HashOther	yes	N/A	79	0.2785	0.4511	114	0.3421	0.4765
HashAge	no	–	79	4752.99	1993.83	114	4614.67	1994.05
CurveECDSA	yes	0	79	0.6329	0.4851	114	0.6316	0.4845
CurveED25519	yes	0	79	0.3418	0.4773	114	0.3158	0.4669
CurveOther	yes	0	79	0.0759	0.2666	114	0.0877	0.2841

Panel C: Supply

Variable	Binary	Predicted influence	As of December 2020			All time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
NoMaxSupply	yes	-	79	0.3418	0.4773	114	0.2895	0.4555
FixedSupply	yes	-	79	0.2278	0.4221	114	0.2105	0.4095
Deflationary	yes	-	79	0.1139	0.3197	114	0.0789	0.2708
InflationaryDecreasing	yes	0	79	0.4177	0.4963	114	0.4825	0.5019
InflationaryFixed	yes	0	79	0.1013	0.3036	114	0.1053	0.3082
InflationaryFixedInflationRate	yes	0	79	0.0506	0.2206	114	0.0439	0.2057
InflationaryDynamic	yes	0	79	0.1772	0.3843	114	0.1404	0.3488
Inflationary	yes	0	79	0.7468	0.4376	114	0.7719	0.4214
RewardCoinbase	yes	+	79	0.6582	0.4773	114	0.6930	0.4633
RewardInflation	yes	+	69	0.3165	0.4681	114	0.2632	0.4423

Table 2.1: Design features variables, expected influence, and descriptive statistics (cont.)

Panel D: Transactions

Variable	Binary	Predicted influence	As of December 2020			All-time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
TheoreticalBlockTime (seconds)	no	-	73	99.65	175.53	105	127.16	197.43
BlockTimeAverage (seconds)	no	-	76	97.83	170.27	106	127.55	196.0435
BlocksizeLimit	yes	-	60	0.7333	0.4459	91	0.7473	0.4370
TransactionFeeObligation	yes	-	77	0.7143	0.4547	111	0.6577	0.4766
NoTipSpecialTreatment	yes	+	73	0.4384	0.4996	105	0.4000	0.4922
NoFeeTipForMinerForger	yes	-	79	0.2025	0.4045	114	0.1667	0.3743

Panel E: Usability

Variable	Binary	Predicted influence	As of December 2020			All-time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
IntentionPayment	yes	0	79	0.3291	0.4729	114	0.4035	0.4928
IntentionSmartContract	yes	+	79	0.3671	0.4851	114	0.3070	0.4633
IntentionOther	yes	+	79	0.3038	0.4628	114	0.2895	0.4555
SmartContractSupport	yes	0	79	0.6835	0.4681	114	0.5789	0.4959
UsageBeyondPayment	yes	+	79	0.4430	0.4999	114	0.3947	0.4910

Panel F: General

Variable	Binary	Predicted influence	As of December 2020			All-time		
			Obs.	Mean	Std. Dev.	Obs.	Mean.	Std. Dev.
LedgerOther	yes	0	79	0.0633	0.2450	114	0.0702	0.2566
AccountingBalance	yes	+	79	0.5316	0.5022	114	0.4561	0.5003
Anonymous	yes	+	78	0.2692	0.4464	113	0.2832	0.4526
Pseudoanonymous	yes	-	78	0.7051	0.4589	113	0.6991	0.4607
NonAnonymous	yes	+	78	0.0641	0.2465	113	0.0442	0.2066

When we include in our data set soft forks that imply a change in at least one design features of our taxonomy,[20] our data set increases from 79 to 114 observations. Note, though, that this all-time data set includes those cryptocurrencies twice that experienced a design change that was not associated with a hard fork. These two versions of the same cryptocurrency existed in different periods; i.e., at each point in time only one of them existed. We retain the all-time data set because it allows to reconstruct the exact design configuration of all cryptocurrencies in the sample at any point in time during the sample period.

Despite our attempts to collect data on all design features introduced for all cryptocurrencies in our sample, there are some variables with missing observations. These include *RewardInflation* (10 missing entries), *TheoreticalBlockTime* (6 missing entries), *BlockTimeAverage* (3 missing entries), *BlocksizeLimit* (19 missing entries), *TransactionFeeObligation* (2 missing entries), *NoTipSpecialTreatment* (6 missing entries), and the degree of anonymity (1 missing entry). Only the observations with no missing entries among the variables are included in the analysis.

2.2.3 Summary Statistics

Table 2.1 shows summary statistics (number of observations, mean and standard deviation) for all design feature variables, both for the all-time data set (the one that contains soft-forked cryptocurrencies) and for our main data set containing 79 cryptocurrencies in their design configuration as of December 2020. We describe summary statistics for the latter data set. This description not only characterizes our sample but also offers an overview of the designs of the most important cryptocurrencies. We note that in some cases the categories we have created to capture alternative specifications of a design feature are not mutually exclusive. As a consequence, the fractions shown in Table 2.1 can add up to more than 100%.[21] During analysis, the dummy variables are handled conventionally, wherein the variables representing all categories except one are incorporated into the analysis as independent variables.

We find that approximately half of the cryptocurrencies were developed by private, for-profit entities, 27.9% by not-for-profit organizations, and 20.3% by networks of independent developers. In 64.6% of the cryptocurrency networks decisions on major code changes and/or decisions

[20] For instance, Monero, a cryptocurrency which allows completely anonymous transactions by obscuring transaction senders and recipients through cryptography, originally had a blocktime of one minute. In 2016, the blocktime was raised to two minutes (alongside with some other changes not relevant in the context of our design feature variables). Such a situation implies two entries in our all-time data set. The first one includes the initial blocktime of one minute while the blocktime variable is set to two minutes in the second entry. Such changes are not necessarily associated with hard forks that result in two cryptocurrencies existing simultaneously after the fork date.

[21] Consider, for example, the three dummy variables which capture the consensus mechanism (*ConsensusPoW, ConsensusPoSdPoS, and ConsensusOther*). Three cryptocurrencies use a combination of consensus mechanisms, for each of which we assign a value of one to two of the corresponding variables. Therefore, the means shown in the table add up to 1.038.

on governance issues are passed on to the network members. This figure implies that some networks developed by for-profit entities still involve the users in the development process. We further find that nearly all networks have publicly available core codes, and that most cryptocurrency networks are either using either C++ (∼39.2%) or Go (∼36.7%). About 50% of the cryptocurrencies were forked from another network, while the others were built from scratch.

31.7% of the cryptocurrencies in our sample use a consensus mechanism based on PoW. PoS or dPoS are more widely used (49.4%), and 22.8% of the cryptocurrencies use other consensus mechanisms. These figures are in line with the observation made by Irresberger et al. (2020), that proof of stake is becoming more popular. The most widely used hash function is Bitcoin's SHA-256 (43.0%), followed by HashEthash (15.2%). Although different elliptic curves can theoretically be used for signature generation, most coins use the two standard digital signing algorithms ECDSA (63.3%) and Ed25519 (34.2%).

Of the 79 cryptocurrencies in our sample, 27 (34.2%) have no supply cap. 22.8% of the coins have a fixed supply while 11.4% are deflationary. Of the cryptocurrencies with increasing supply (74.7%), most have adopted a scheme with decreasing growth rates (41.8% of the total, equivalent to 56% of the inflationary currencies). The alternative growth schemes are less popular. In about two thirds of the networks in our sample, the verifying agents are rewarded with coinbase rewards. An alternative reward scheme is used by 31.7% of the networks (note that there are some missing values for this variable).

The summary statistics of the design features in the category "transactions" indicate that the average theoretical blocktime amounts to 99.65 seconds with a standard deviation of 175.53. The blocktime that is actually observed in the market is slightly lower, at 97.83 seconds with a standard deviation of 170.27.[22] Of the 60 cryptocurrencies for which we could infer whether a blocksize limit exists, approximately three quarters (73.3%) have such a limit in place. 71.4% of the networks require their users to pay a mandatory transaction fee, and 56.2% allow a prioritization of transactions by paying a tip. In 20.3% of the cryptocurrency networks in our sample, transaction fees and/or tips are not included in the rewards for miners and stakers.

Turning to the variables in the "usability" group, we find that the original intention of the cryptocurrencies in our data set is roughly evenly distributed across the categories payment system, smart contract platform, and other. 68.4% of the cryptocurrency networks support smart contracts within their core code implementation, and in 44.3% of the networks coin holdings are associated with further rights, such as voting rights, or enable usages beyond pure transaction purposes.[23]

[22] Reducing the sample "as of December 2020" to the observations for which both, theoretical and actual, blocktimes are available, we have average blocktimes of 99.11 seconds and 99.43 seconds for the theoretical and the observed blocktimes, respectively.

[23] Binance coin is an example of a coin that provides such additional usage. The coins in this network can be used to pay for several fees when using the centralized exchange Binance, such as listing fees.

The overwhelming majority (93.7%) of the networks in our sample use a blockchain-based ledger. Only 6.3% use alternative ledgers. More than half (53.2%) of the cryptocurrencies use a balance accounting scheme, leaving 46.8% for UTXO accounting. With respect to the degree of anonymity, a strong majority (70.5%) of the networks allows pseudonymous transactions (as is also the case in the Bitcoin network). 26.9% are fully anonymous while only 6.4% of the networks require the disclosure of the real world identities of their users.

2.3 Empirical Methodology

2.3.1 Two-Stage Regressions and LASSO

We aim to empirically analyze which design features from our taxonomy have explanatory power for the cross-sectional valuation of cryptocurrencies. To identify those that significantly affect the value of cryptocurrencies, we regress two different measures of market valuation on the design feature variables introduced in Section 2.2. Our empirical design is characterized by a low number of observations (the 79 cryptocurrencies) and a large number of explanatory variables, making a standard regression analysis unlikely to yield reliable results. To tackle the issue of overfitting, we use two methodological approaches: a two-step regression approach inspired by Karnaukh et al. (2015) and LASSO (least absolute shrinkage and selection operator) regressions.

The two-step regression approach proceeds as follows. We first estimate six separate regressions with the respective market valuation measures as the dependent variable and the design features of one of our six categories as independent variables ("intra-group regressions"). Those variables with the highest explanatory power are then included as independent variables in the second-step regression ("encompassing regression"). We judge the explanatory power by the p-values in the intra-group regressions and use different cut-off values (0.3, 0.2 and 0.1). We further include the age of the cryptocurrencies in the encompassing regression.

The LASSO regressions integrate variable selection and regularization.[24] Specifically, we perform a 10-fold cross validation with random subsets selection to determine the tuning parameter λ that minimizes the mean squared error (MSE) for the LASSO regression with intercept. Based on the value of λ, the LASSO is then applied on the entire data set to determine the model's

[24] Compared to a standard linear regression (with intercept), a penalty term $\lambda \sum_{j=1}^{n} \mid \beta_j \mid$ is introduced and the algorithm's objective is to minimize $\sum_{i=1}^{n} \left(y_i - \alpha - \sum_j x_{ij}\beta_j \right)^2 + \lambda \sum_{j=1}^{n} \mid \beta_j \mid$, see e.g., Tibshirani (1996). The choice of λ is crucial. The higher λ, the more variables are eliminated, but the deviation of estimated values from observed data increases. If λ is low instead, more variables are selected and the variation in the predictions decreases.

parameter estimates and the intercept. We repeat this procedure $10,000$ times in order to base our inference on a broad range of different training and validation data subset compositions.[25]

The majority of our independent variables (i.e., the design characteristics) are time-invariant. We therefore use time-series averages of the dependent variables to eliminate effects that may be specific to individual days. As noted in Section 2.2.2, the 79 cryptocurrencies in our sample are those with the highest market capitalization as of September 2020. To alleviate endogeneity issues, we use market valuation data averaged over all days of the fourth quarter of 2020 in our main analysis. We show results for alternative specifications in Subsection 2.4.2.

2.3.2 Variables Definitions

Dependent Variables: Market Valuation Data

We measure market valuation by market capitalization and a discounted version of the market capitalization. The calculation of market capitalization requires data on cryptocurrency prices and circulating supply. We obtain the former from the APIs of the respective exchange and from cryptocurrency data provider Kaiko, while the latter is obtained from Messari.[26]

The price data that we use is a daily volume-weighted average of the prices of nine cryptocurrency exchanges.[27] Whenever a cryptocurrency is traded against USD on an exchange, our dataset which is combined from the exchange API and Kaiko provides daily volume-weighted average prices for the respective venue. We use these prices whenever available, and we refer to them as direct prices. Not every cryptocurrency is traded against USD on every exchange. Therefore, direct prices are not always available. However, these cryptocurrencies are usually traded against BTC, and BTC is traded against USD. We use these two prices to calculate an implicit USD price of the cryptocurrency under consideration and refer to these implicit prices as indirect prices.[28] In doing so we implicitly assume that USD and BTC quotes are consistent.

[25] When we use five folds instead of ten in the cross validation procedure, our results remain qualitatively similar.

[26] Pricing data from Kaiko is used only in case there are missing values in the API data. Messari provides cryptocurrency data and is recommended by Kaiko as a source for circulating supply. Circulating supply excludes coins/tokens from the outstanding supply that are (i) restricted by any contracts, e.g., on-chain-lockups, or (ii) are held by projects/foundations without selling intention (see https://messari.io/report/messari-proprietary-methods). This mitigates concerns that our market capitalization variable actually measures trading motives and/or investor sentiment rather than "equity value".

[27] We originally obtained data of the following ten exchanges from Kaiko: Binance, Bitfinex, Kraken, Bitstamp, Coinbase, bitFlyer, Gemini, itBit, Bittrex, and Poloniex. These exchanges are considered reliable, meaning that they do not report inflated volume (see Härdle et al. (2020); on the importance of reliable data in the context of cryptocurrency trading data, see Alexander and Dakos (2020)). We exclude Poloniex because the only fiat currency traded on this exchange is Malaysian ringgit (RM). Due to the low liquidity between RM and USD, we refrained from converting the RM quote to a USD quote via the RM-USD rate.

[28] For example, the price of ABBC Coin (ABBC) in USD is not available on Bittrex, but Bittrex trades ABBC against BTC and BTC against USD. With $\frac{USD}{ABBC} = \frac{BTC}{ABBC} \cdot \frac{USD}{BTC}$, we obtain the Bittrex USD price of ABBC coins.

One exchange, Binance, is an exception. It does not trade cryptocurrencies against USD, but it does trade them against EUR. We calculate indirect prices for those cryptocurrencies traded against EUR on Binance by combining the EUR price of the currency with the EUR-USD exchange rate (obtained from exchangerate.host).[29] To check the reliability of the indirect prices we calculate indirect prices for cryptocurrency-exchange combinations for which direct prices are also available. We observe average differences below 1% for almost all combinations.

There are different ways how we could construct our final data set. We could use direct prices where available and use indirect prices only when direct prices are unavailable, or we could generally use indirect prices. We opt for a combination of these procedures. We use indirect prices when only these are available, and we use a volume-weighted average of direct and indirect prices when both are available.[30] We end up with one price for each cryptocurrency-exchange pair that is either an indirect price or a weighted average of direct and indirect prices. These prices are then used to calculate the weighted average price across the nine exchanges. We then multiply this weighted average price by the circulating supply to obtain our measure of market capitalization (referred to as *plain* market capitalization in the sequel).

The cryptocurrencies in our sample are of very different age. For instance, the genesis block of Bitcoin was created in January 2009 while Avalanche was just introduced in mid-September 2020. On average, cryptocurrencies that are older and more established are associated with higher market capitalization, possibly because of network effects (Alabi, 2017; Metcalfe, 2013) and/or because older cryptocurrencies tend to be less volatile (Hafner, 2020; Kim, 2015; Nabilou and Prüm, 2019) and thus are better suited to act as a store of value. In addition, an older cryptocurrency may have established a "brand value" and customer loyalty and hence, are less impacted by adverse news.[31] These factors might result in higher market capitalization. Finally, these cryptocurrencies also benefit from the overall enhancement of the entire cryptocurrency market. Therefore, in addition to the "plain" market capitalization we also analyze discounted market valuation. Specifically, we adapt the fund size scaling procedure of Pástor et al. (2015) and calculate the discounted market capitalization of cryptocurrency i at time t according to

$$DiscountedMCap_{i,t} = MCap_{i,t} \cdot \frac{CRIX_{Genesis_i}}{CRIX_t} \tag{2.1}$$

[29] We are aware of the fact that there are arbitrage opportunities in the cryptocurrency market (see, e.g., Makarov and Schoar, 2020)). We note, though, that the exchanges in our sample are among the most liquid cryptocurrency exchanges, and higher liquidity is usually associated with higher market efficiency. Furthermore, the cryptocurrency market has generally become more efficient over time (Kristoufek and Vosvrda, 2019; Köchling et al., 2019; Noda, 2021).

[30] We do this to alleviate endogeneity concerns. Indirect prices may be systematically biased, and it is more likely that a cryptocurrency with low market capitalization is not directly traded against USD. Note that our results are qualitatively similar, when we use indirect prices throughout.

[31] Bianchi (2020), Finck (2018), Jo et al. (2020), and Polasik et al. (2015) argue that the cryptocurrency market is heavily sentiment-dependent and its users perceive blockchain as an immature technology that is still evolving, with uncertain practical implications. As a result, well-performing cryptocurrencies are likely to have been in existence for a longer time and are less impacted by adverse news.

with $CRIX_{Genesis_i}$ and $CRIX_t$ denoting the value of the CRIX (see, Trimborn and Härdle, 2018), a widely used cryptocurrency market index, at the genesis date of coin i and at time t, respectively. For the seven cryptocurrencies in our data set that were launched prior to the CRIX, i.e. before July 31, 2014, we set $CRIX_{Genesis_i}$ to the CRIX's initial value of 1000. Intuitively, the procedure described by Equation (2.1) deflates the value of cryptocurrency i at time t to its launch date.

For either methodological approach, we control for outliers by winsorizing the top three cryptocurrencies according to market capitalization (Bitcoin, Ethereum, and Ripple) and discounted market capitalization,[32] respectively. We rescale the market capitalization variables to the range $[0, 1]$ in order to obtain coefficient estimates of a convenient magnitude. As a robustness check we also estimate an alternative specification that avoids winsorizing. Specifically, we use the log of the plain and discounted market valuation as dependent variables and obtain results (not tabulated) that are qualitatively similar to those reported in this chapter.

Independent Variables: Design Feature Data

Irrespective of the methodology applied we furthermore reduce the number of independent variables by conflating some of them. Specifically, we do not include the variables *CodeGo* and *CodeOther* but rather the binary variable *CodeNonC++* which is set to 1 if at least one of the former variables is 1, and 0 otherwise. Similarly, we introduce the binary variable *CodeNonECDSA* to identify networks which do not use ECDSA for signature generation. Within the design feature group usability, we combine *IntentionSmartContract* and *IntentionOther* to the new variable *IntentionNonPayment.* Moreover, we do not include the variables that identify the different types of inflationary supply curves but restrict ourselves to the aggregated variable *Inflationary.* Finally, as already mentioned in Subsection 2.2.1, we do not include the specific hash function variables in our regression analysis but rather only include the age of the hash function.

Several of our independent variables are exhaustive sets of dummy variables (such as *CodeC++* and *CodeNonC++*). We therefore need to define a base case and exclude the corresponding dummy variable from the regression. We always dropped the variable that corresponds to the design of the Bitcoin network. As an implication of this specification, the constant in our regression captures the value of a network that has a Bitcoin-like combination of the design features captured by the dummy variables, with all other variables equal to zero. We then take this approach one step further and recalculate actual blocktimes as well as the age of the hash

[32] When considering different time horizons to calculate the time-series average of the discounted market capitalization, we notice that the top three cryptocurrencies are more than five interquartile ranges above the third quartile and therefore should be considered as outliers. Note that the top three cryptocurrencies are not always the same - for example, in the fourth quarter of 2020, the top three cryptocurrencies according to discounted market capitalization are Bitcoin, Polkadot and EOS.

function according to

$$
\begin{aligned}
BlockTime &= \frac{TheoreticalBlocktime_{Bitcoin} - BlockTimeAverage}{TheoreticalBlocktime_{Bitcoin}} \\
&= \frac{600 - BlockTimeAverage\,[s]}{600}
\end{aligned}
\tag{2.2}
$$

and

$$
HashAge = \frac{HashAge_{Bitcoin} - HashAge}{HashAge_{Bitcoin}}, \tag{2.3}
$$

respectively. These modified variables take on a value close to zero (equal to zero) for the Bitcoin network. Positive values indicate a blocktime lower than that the theoretical blocktime of Bitcoin (implying higher throughput of the network as compared to Bitcoin), and a hash function younger (and thus arguably more secure) than that used by the Bitcoin network, respectively. We note that Bitcoin has the highest theoretical blocktime (10 minutes) and the oldest hash function in our sample (SHA-256), implying that the two modified variables take on the value (close to) zero for Bitcoin and positive values for any cryptocurrency in our sample. We further rescale the two variables to the interval $[0, 1]$.

2.4 Results and Discussion

In this section, we present our empirical results. We present the main results, based on average market capitalization (both plain and discounted) in the fourth quarter of 2020 in Subsection 2.4.1. In Subection 2.4.2, we then show that we obtain qualitatively similar results when we vary the period over which we measure market capitalization.

2.4.1 Main Results

In Table 2.2 we show the results for the plain market capitalization. Panel A, i.e., columns (1) to (4), show the results of the two-stage regression analysis while Panel B, i.e., columns (5) to (8), shows the LASSO results. We start with the presentation of the two-stage regression results. The four columns of Panel A show the results of the encompassing regression. The corresponding intragroup regression results that determine the set of variables to be included in the encompassing regression are shown in Appendix A.1. Column (1) ((2), (3)) shows the results that we obtain when all variables with a p-value below 0.1 (0.2, 0.3) in the intragroup regression are included in the encompassing regression. Column (4) shows the results that we obtain when all independent variables are included in the encompassing regression.[33] Note that

[33] The number of observations is lower in columns (3) and (4) than in columns (1) and (2) because variables with missing values (such as *BlockTimeAverage*) are included in columns (3) and (4), but not in columns (1) and (2).

the F-statistics shown in the last line indicate that the independent variables have significant explanatory power for the market capitalization of the cryptocurrencies only in columns (1), (2), and (3), but not in column (4) where all independent variables are included. This finding supports our choice of the two-stage regression design.

The encompassing regressions of the two-step regression approach yield three main results. First, the age of a cryptocurrency network, as measured by the variable *DaysAge* (the number of days since the launch of the genesis block, rescaled to the range $[0, 1]$), is positively related to market capitalization.[34] Second, spin-offs from other cryptocurrencies (forks) have significantly lower market values. This result is in line with our argument that such networks are almost identical copies of already existing cryptocurrencies (i.e., their respective parent networks), and that this lack of innovation negatively affects valuation. Third, we find that a configuration of design features similar to that of Bitcoin is associated with higher valuation. Remember that we defined our dummy variables such that they essentially capture deviations from the Bitcoin design, and that the continuous variables *HashAge* and *BlockTimeAverage* take on the value zero for the Bitcoin network and positive values for other cryptocurrencies in the sample. The observation that most coefficient signs in Table 2.2 are negative thus implies that deviations from the Bitcoin design result in lower valuation. This result may be due to the first mover advantage of the Bitcoin network, to the higher attention that Bitcoin receives in comparison to other networks, and to the fact that cryptocurrency users and investors are better informed about the details of Bitcoin than about those of its contenders

We now turn to the discussion of the LASSO results which are independent of the design features classifications' following our taxonomy.[35] In Figure 2.1 we graphically illustrate for the first 200 (out of a total of 10,000) simulations the variables which were selected by the procedure and the magnitude of the coefficient estimates. The lines represent the independent variables and the columns the 200 simulation runs. Green (red) color indicates a positive (negative) coefficient estimate, and the intensity of the color represents the magnitude of the estimate. We show numerical results in columns (5) to (8) of Table 2.2. In column (5) we show the frequency with which a variable is selected. In columns (6) and (7), we show, conditional on a variable being selected, the frequency of positive and negative coefficient estimates, respectively. In column 8 we show the mean coefficient estimate.[36]

[34] The variable *DaysAge* potentially correlates with some other predictors. When we exclude *DaysAge* from the regression model we still observe the same significant effects, and no other variable shows up to be consistently significant.

[35] Since the LASSO procedure considers all design features without taking into account their allocation within our taxonomy, the results of the analysis show that our results are not driven by the taxonomy itself.

[36] The means are unconditional, i.e., they are calculated based on all 10,000 simulation runs. Whenever a variable is not selected, the coefficient estimate is set to 0. Conditional means (i.e., means that are calculated conditional on the respective variable being selected by the LASSO procedure) can be obtained by combining the unconditional means with the data on the selection frequency provided in column (5) of Table 2.2.

Table 2.2: Market capitalization regression analysis of Q4 2020

This table reports results of the cross-sectional regression of the average market capitalization in the fourth quarter of 2020 on the design feature variables and provides statistics for the variable selection process when applying LASSO with cross-validation. The encompassing models (1), (2), and (3) include the design feature variables with p-values below 0.1, 0.2 and 0.3 in the intra-group regressions, respectively. We control for multicollinearity and find that all variance inflation factors (VIF) in (1) - (3) are below 4.32. Column (4) shows the results for the case that all design feature variable are included (max. VIF of 8.65). Standard errors are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively. Column (5) reports the percentage of cases in which a variable is selected by LASSO while (6) and (7) indicate the related sign of the coefficient. Column (8) reports the average of the parameter estimates indicating the economic significance.

	Market capitalization							
	Panel A: Encompassing regression				**Panel B:** LASSO			
	(1) $p < 0.1$	(2) $p < 0.2$	(3) $p < 0.3$	(4) All	(5) Included	(6) Positive	(7) Negative	(8) ∅ coefficent
Constant	0.133	0.311*	0.367*	0.084	100%	100%	0%	0.024
	(0.112)	(0.159)	(0.216)	(0.384)				
DaysAge	0.583***	0.454**	0.486**	0.724*	80.86%	100%	0%	0.166
	(0.189)	(0.211)	(0.229)	(0.417)				
DeveloperNPO			-0.057	-0.151	0%	-	-	0
			(0.120)	(0.198)				
DeveloperPrivate	-0.066	-0.045	-0.110	-0.241	23.02%	0%	100%	-0.006
	(0.071)	(0.076)	(0.111)	(0.177)				
NoMajorityChanges				-0.021	0%	-	-	0
				(0.128)				
CodeNonC				0.235	2.75%	100%	0%	0.000
				(0.142)				
CodeNonPublic				0.002	2.75%	0%	100%	0.000
				(0.291)				
Fork	-0.132*	-0.164**	-0.193**	-0.226*	28.19%	0%	100%	-0.025
	(0.068)	(0.072)	(0.077)	(0.124)				
ConsensusPoSDPoS	-0.023	-0.138	-0.079	-0.105	2.03%	0%	100%	-0.000
	(0.083)	(0.123)	(0.139)	(0.200)				
ConsensusOther		-0.150	-0.109	0.051	0%	-	-	0
		(0.126)	(0.147)	(0.218)				
HashAge	-0.153	-0.232	-0.104	0.005	17.38%	0%	100%	-0.003
	(0.121)	(0.140)	(0.168)	(0.271)				
CurveNonECDSA				-0.013	0%	-	-	0
				(0.143)				
NoMaxSupply				0.079	0%	-	-	0
				(0.199)				
SupplyCirculation				0.105	0%	-	-	0
				(0.242)				
Deflationary				0.064	0%	-	-	0
				(0.182)				
FixedSupply		-0.051	-0.013	0.001	0%	-	-	0
		(0.086)	(0.095)	(0.170)				
RewardCoinbase			-0.019	0.085	0%	-	-	0
			(0.099)	(0.166)				
RewardInflation		-0.023	0.040	0.261	0%			0
		(0.084)	(0.116)	(0.213)				
BlockTimeAverage			-0.125	0.013	0.16%	0%	100%	-0.000
			(0.149)	(0.228)				
TransactionFeeObligation				-0.064	0%	-	-	0
				(0.139)				
NoTipSpecialTreatment				-0.040	0%	-	-	0
				(0.116)				
NoFeeTipForMinerForger	0.107	0.126	0.085	0.117	26.19%	100%	0%	0.012
	(0.080)	(0.090)	(0.113)	(0.171)				
IntentionNonPayment				0.284	0%	-	-	0
				(0.245)				
SmartContractSupport				-0.386**	24.24%	0%	100%	-0.014
				(0.187)				
UsageBeyondPayment				-0.061	0%	-	-	0
				(0.139)				
LedgerStyleOther			0.381	0.444	39.35%	100%	0%	0.049
			(0.270)	(0.439)				
AccountingBalance				0.026	0%	-	-	0
				(0.183)				
Anonymous		-0.031	-0.023	-0.048	24.24%	0%	100%	-0.005
		(0.086)	(0.094)	(0.119)				
NonAnonymous			0.373	0.561	25.50%	100%	0%	0.034
			(0.228)	(0.346)				
Observations	68	68	65	59	∅ Observations:			
R^2	0.256	0.294	0.386	0.525	59			
Adjusted R^2	0.182	0.170	0.198	0.082				
F Statistic	3.491***	2.375**	2.055**	1.185	∅ R^2:			
	(df=6;61)	(df=10;57)	(df=15;49)	(df=28;30)	0.108			

The variable that is most frequently selected (80.0% of the simulations) is the age of a cryptocurrency. Whenever selected, the coefficient estimates are consistent with the results of the two-stage regression approach, positive. All other variables are selected much less frequently. The variable *Fork* is selected in 28.2% of the simulations and the coefficient estimates are, again in line with the regression results presented above, always negative.

The LASSO procedure further selects the variables *DeveloperPrivate* (effect sign: $-$), *HashAge* ($-$), *NoFeeTipForMinerForger* (+), *SmartContractSupport* ($-$), *LedgerStyleOther* (+), *Anonymous* ($-$), and *NonAnonymous* (+) with reasonable frequency. In all cases the estimated direction of the effect is consistent with the sign of the coefficient estimates in the two-stage regressions.[37] The negative sign of *DeveloperPrivate* indicates that cryptocurrencies which were developed by for-profit entities have lower valuation. The negative impact of *HashAge* on valuation implies that, contrary to our prediction, younger hash functions, which arguably offer higher levels of security, do not increase market capitalization, ceteris paribus.[38] The positive coefficient sign of the variable *NoFeeTipForMinerForger* indicates that networks that do not pass on any transaction fees and/or tips to agents who maintain the integrity of the network have a higher market capitalization. In networks that directly reward contributions to transaction processing with fees and/or tips, transaction fees obviously play an important role. One drawback is that such transaction fees can lead to user non-participation: The fees directly cause some users to drop out, while longer waiting times cause other users who pay fees to drop out as well (Basu et al., 2023; Easley et al., 2019; Huberman et al., 2021). In addition, this can lead to adverse effects related to network security (Pagnotta, 2022). Overall, these fees can increase the vulnerability of the system, which may serve to explain the positive influence of the variable *NoFeeTipForMinerForger*.

The positive coefficient signs for the variable *LedgerStyleOther* indicate that non-blockchain-based cryptocurrencies have higher market valuation. This finding should be interpreted with care, though, because our sample only contains five cryptocurrencies with that feature. The effect signs of the variables *Anonymous* and *NonAnonymous* imply that cryptocurrencies that allow completely anonymous transactions have lower market values while those that require disclosure of real-world identities have higher market values. The former result may be due to concerns that fully anonymous networks might be misused for illegal transactions. The latter result may reflect the expectation of regulatory acceptance of non-anonymous cryptocurrencies.

The negative effect on market valuation ascribed to the variable *SmartContractSupport* runs counter to the intuition that a network that allows for smart contracts allows alternative uses beyond making payments and should thus be more valuable. However, smart contracts may

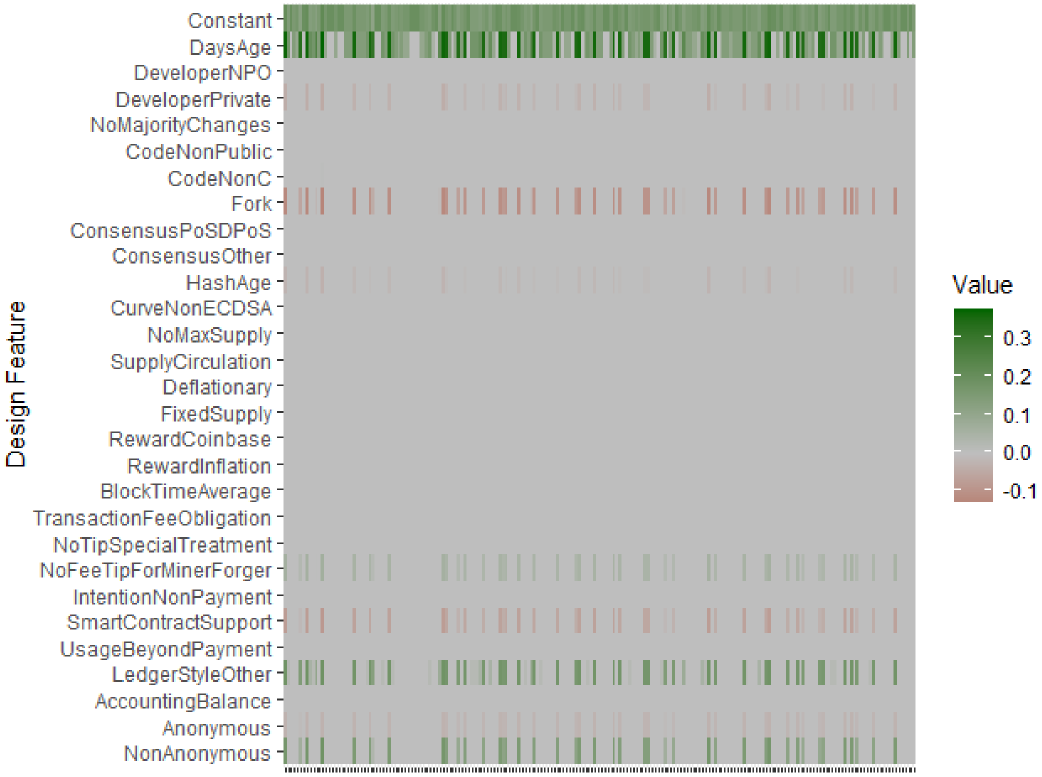
[37] Note that although the coefficient estimates were insignificant in the encompassing regression, the coefficients of the variables *DeveloperPrivate*, *HashAge*, and *NoFeeTipForMinerForger* were significant at the 10% level or better in the intra-group regressions.

[38] Remember that we defined the variable *HashAge* such that larger values mean younger hash functions.

also be gateways for fraudulent behavior and/or may be subject to coding errors which might result in security breaches.

Figure 2.1: LASSO variable selection and economic magnitudes (marketcap Q4 2020)

This figure shows the economic magnitude of the estimated coefficients for each design feature covering 200 randomly selected training and validation data subset compositions from our LASSO approach. Red (green) bars refer to a negative (positive) coefficient estimate, while grey bars refer to coefficient estimates equal to zero, i.e., to non-selected design features. More intense colors refer to stronger economic magnitudes.



We next turn to the results for the discounted market capitalization. The dependent variable is the time-series average of the discounted market capitalization (Equation (2.1)) during the last quarter of 2020. Otherwise the analysis is identical to the one presented above. We present in Table 2.3 results of the two-stage regressions (columns (1) to (4)) and the LASSO results (columns (5) to (8)). In addition, a graphical representation of the results for the first 200 runs of the LASSO procedure can be found in Figure 2.2.

The coefficient estimates for the age of the cryptocurrency (variable *DaysAge*) in the encompassing regressions are much smaller than before and are always insignificant. Furthermore, the variable is never selected by the LASSO approach. These results indicate that the discounting procedure successfully removed the effect of age on market valuation.

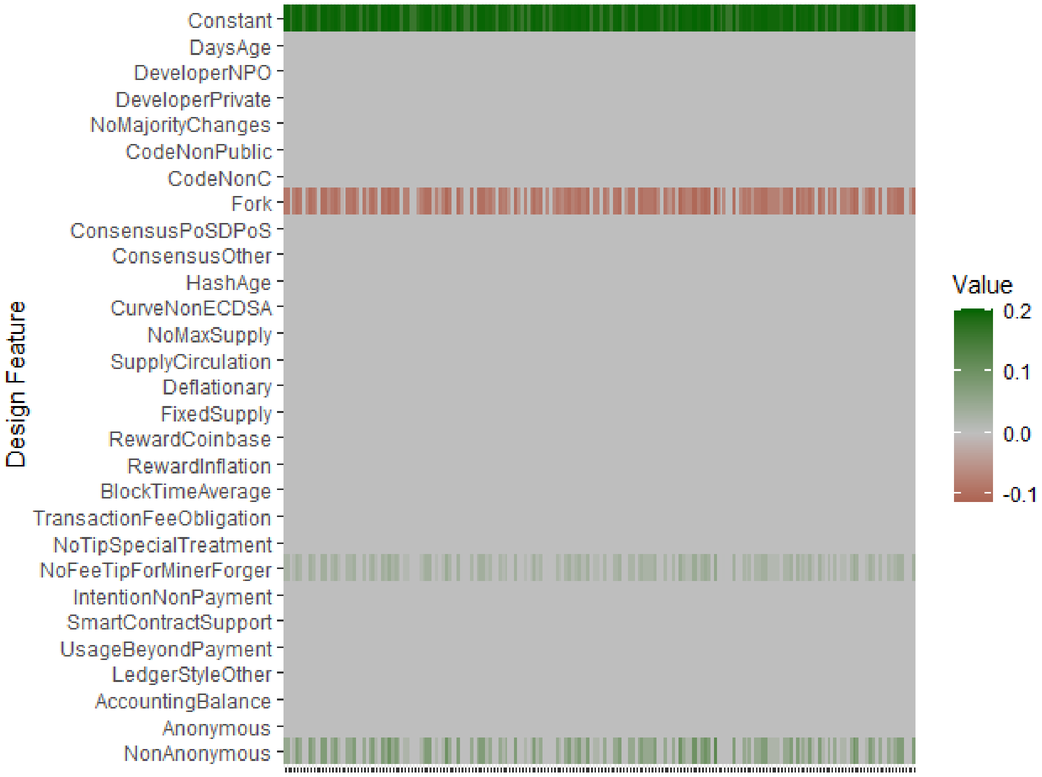
Table 2.3: Discounted market capitalization regression analysis of Q4 2020

This table reports results of the cross-sectional regression of the average discounted market capitalization in the fourth quarter of 2020 on the design feature variables and provides statistics for the variable selection process when applying LASSO with cross-validation. The encompassing models (1), (2), and (3) include the design feature variables with p-values below 0.1, 0.2, and 0.3 in the intra-group regressions, respectively. We control for multicollinearity and find that all variance inflation factors (VIF) in (1) - (3) are below 2.27. Column (4) shows the results for the case that all design feature variable are included (max. VIF of 8.65). Standard errors are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively. Column (5) reports the percentage of cases in which a variable is selected by LASSO while (6) and (7) indicate the related sign of the coefficient. Column (8) reports the average of the parameter estimate indicating the economic significance.

	Market capitalization							
	Panel A: Encompassing regression				**Panel B:** LASSO			
	(1) $p < 0.1$	(2) $p < 0.2$	(3) $p < 0.3$	(4) All	(5) Included	(6) Positive	(7) Negative	(8) ∅ coefficent
Constant	0.168**	0.186**	0.436***	0.049	100%	100%	0%	0.189
	(0.064)	(0.068)	(0.144)	(0.371)				
DaysAge	0.101	0.100	0.016	0.175	0%	-	-	0
	(0.158)	(0.158)	(0.169)	(0.402)				
DeveloperNPO		-0.059	-0.117	-0.232	0%	-	-	0
		(0.070)	(0.103)	(0.191)				
DeveloperPrivate			-0.150	-0.303*	0%	-	-	0
			(0.093)	(0.170)				
NoMajorityChanges				0.044	0%	-	-	0
				(0.123)				
CodeNonC				0.179	0%	-	-	0
				(0.137)				
CodeNonPublic				-0.094	0%	-	-	0
				(0.280)				
Fork	-0.170***	-0.175***	-0.221***	-0.315**	80.52%	0%	100%	-0.066
	(0.062)	(0.063)	(0.067)	(0.120)				
ConsensusPoSDPoS				-0.002	0%	-	-	0
				(0.193)				
ConsensusOther				0.116	0%	-	-	0
				(0.210)				
HashAge				0.043	0%	-	-	0
				(0.261)				
CurveNonECDSA				0.056	0%	-	-	0
				(0.138)				
NoMaxSupply				0.091	0%	-	-	0
				(0.192)				
SupplyCirculation				0.189	0%	-	-	0
				(0.234)				
Deflationary				0.032	0%	-	-	0
				(0.176)				
FixedSupply				-0.008	0%	-	-	0
				(0.164)				
RewardCoinbase				0.225	0%	-	-	0
				(0.160)				
RewardInflation				0.329	0%	-	-	0
				(0.205)				
BlockTimeAverage			-0.177	-0.010	0%	-	-	0
			(0.123)	(0.220)				
TransactionFeeObligation				-0.069	0%	-	-	0
				(0.134)				
NoTipSpecialTreatment				-0.091	0%	-	-	0
				(0.112)				
NoFeeTipForMinerForger	0.077	0.075	0.169**	0.199	73.74%	100%	0%	0.018
	(0.075)	(0.075)	(0.083)	(0.165)				
IntentionNonPayment				0.156	0%	-	-	0
				(0.236)				
SmartContractSupport				-0.261	0%	-	-	0
				(0.180)				
UsageBeyondPayment			0.062	0.002	0%	-	-	0
			(0.072)	(0.134)				
LedgerStyleOther				0.077	0%	-	-	0
				(0.423)				
AccountingBalance				-0.0001	0%	-	-	0
				(0.176)				
Anonymous				-0.041	0%	-	-	0
				(0.115)				
NonAnonymous	0.400**	0.415**	0.368*	0.611*	65.97%	100%	0%	0.036
	(0.184)	(0.186)	(0.186)	(0.333)				
Observations	68	68	65	59			∅ Observations:	
R^2	0.187	0.196	0.291	0.478			59	
Adjusted R^2	0.135	0.131	0.190	-0.009				
F Statistic	3.625**	3.028**	2.878***	0.982			∅ R^2:	
	(df=4;63)	(df=5;62)	(df=8;56)	(df=28;30)			0.087	

Figure 2.2: LASSO variable selection and economic magnitudes (discounted marketcap Q4 2020)

This figure shows the economic magnitude of the estimated coefficients for each design feature covering 200 randomly selected training and validation data subset compositions from our LASSO approach. Red (green) bars refer to a negative (positive) coefficient estimate, while grey bars refer to coefficient estimates equal to zero, i.e., to non-selected design features. More intense colors refer to stronger economic magnitudes.



Regarding the influence of the design features on the market valuation, the results for discounted market capitalization are similar to those for plain market capitalization. We note, though, that the LASSO procedure selects fewer variables when we use discounted market capitalization as the dependent variable. As before, we find that spin-offs from other cryptocurrencies (variable *Fork*) have lower valuation. The respective coefficient estimate is negative and highly significant in the encompassing regression, and it is very frequently (80.5%) selected by the LASSO procedure, always with a negative coefficient estimate. Finally, and again consistent with our previous results, we obtain a positive coefficient estimate for the variable *NonAnonymous*. It implies that cryptocurrency networks that require disclosure of real world identities tend to have higher valuation. Furthermore, our earlier result that networks in which agents who verify transactions are rewarded by a scheme independent of fees and/or tips have a higher market valuation is also confirmed. The respective coefficient estimate (variable *NoFeeTipForMinerForger*) in the encompassing regressions is always positive (significantly so in one case), and the variable is frequently selected (73.7%) by the LASSO procedure, always with a positive coefficient sign. Finally, there is still (albeit weak and only in the two-stage regression analysis) evidence that cryptocurrencies developed by private for-profit entities are less valuable. We no longer find evidence that younger hash functions are associated with lower valuation, nor is there evidence that fully anonymous networks are less valuable.

2.4.2 Robustness

So far we have analyzed whether design features can explain the average (both plain and discounted) market capitalization in the fourth quarter of 2020. While averaging over values for an entire quarter should make our results insensitive to day-to-day fluctuations in cryptocurrency prices, we still have to establish that our findings are not specific to the single quarter we have considered. To this end we repeat our entire analysis using the average (both plain and discounted) market capitalization over (i) the entire year 2020 and (ii) the first, second and third quarter of 2020. The results for the full year are shown in Tables A.3, A.4, A.5, and A.6 in Appendix A.1. The results for quarters 1 to 3 are qualitatively similar to those reported in this dissertation and are thus omitted.

The two-stage regression approach for the plain market capitalization averaged over the full year (Table A.3) fully confirms the three main results highlighted previously. Older cryptocurrencies have higher market valuation, forks have lower market capitalization, and deviations from the Bitcoin design are associated with lower market capitalization. The latter conclusion, as before, follows from the fact that the overwhelming majority of the coefficients of the encompassing regression are negative, and that we have defined all independent variables such that their values for the Bitcoin network are zero. The results in Table A.3 also confirm our previous finding that networks where the reward of agents who verify transactions are independent of fees and/or tips have higher valuation. The LASSO results in Table A.4 are fully consistent with those discussed previously. Furthermore, they are also consistent with the LASSO results in Table 2.2 in that the variables *DeveloperPrivate* (effect sign: −), *HashAge* (−), *SmartContractSupport* (−), *LedgerStyleOther* (+), *Anonymous* (−), and *NonAnonymous* (+) are again selected with reasonable frequencies, and have the same coefficient signs as in Table 2.2.

The results for the discounted market valuation, averaged over the entire year 2020 (Tables A.5 and A.6) again support all previous conclusions. The age of a cryptocurrency does not significantly affect its discounted market capitalization, forks have lower valuation, and most coefficient estimates in the encompassing regressions are negative, implying that deviations from the Bitcoin design are associated with lower valuation. Furthermore, the result that non-anonymous networks have higher value is confirmed, as is the previous result that networks in which transactions fees and/or tips are passed to agents maintaining the network's integrity at all have higher market capitalization. Even the (weak) evidence that cryptocurrencies developed by private for-profit entities are less valuable is confirmed.

2.5 Conclusion

In this chapter we analyze whether the value of cryptocurrencies as measured by their market capitalization can be related to specific cryptocurrency design features. To this end, we first propose a taxonomy of cryptocurrency design features and hand-collect a data set that contains these features for 79 cryptocurrencies. We then use two different methodological approaches, a two-stage regression analysis in the tradition of Karnaukh et al. (2015) and LASSO regressions, to analyze whether any of these design features are cross-sectionally related to cryptocurrency valuation. To control for the potential effect of the age of a cryptocurrency on its value more comprehensively we repeat the analysis using discounted instead of plain market capitalization as our dependent variable.

We find that cryptocurrencies that were spun off from other cryptocurrencies (i.e., forks) are less valuable. On the other hand, cryptocurrencies where agents who verify transactions are rewarded by a scheme independent of fees and/or tips tend to be more valuable. Interestingly, cryptocurrencies that require the disclosure of the real-world identities of its users have higher values, possibly in expectation of easier regulatory approval of these networks. Apart from that we find that deviations from the design of Bitcoin tend to be associated with lower valuation. Thus, even though Bitcoin may not be the most technologically advanced cryptocurrency, users and investors apparently value its design.

Overall, we provide evidence that design features partly affect the market valuation of cryptocurrencies. Due to the relatively new underlying technology of cryptocurrencies and its complexity, investors might not be aware of crucial design feature differences between the different cryptocurrency networks. Thus, they might not value the technology per se, but rather hope to invest in the “next Bitcoin”.

While we consider the impact of a large number of design features on cryptocurrency valuation, we do not take into account interactions between different design features. Such interactions may be relevant, though. For instance, the influence of shorter blocktime in a PoS network is expected to be positive due to higher throughput enabled by shorter blocktimes. In contrast, if the blocktime is too small in a PoW network, attacks on the network by fraudulent agents may become more likely which, in turn, may result in more reluctant network adoption and eventually in reduced market capitalization. Extending our research approach to incorporate such interaction effects is a promising avenue for future research.

Chapter 3

Do Design Features Explain the Volatility of Cryptocurrencies?

3.1 Introduction

High volatility appears to be a general characteristic of cryptocurrencies. However, not all cryptocurrencies are equally volatile. Rather, as documented below, there are large cross-sectional differences. Understanding the determinants of these differences in return volatility is crucial for cryptocurrency investors, regulators, and developers alike. In this chapter, we analyze whether differences in volatility can be traced back to differences in cryptocurrency design. If that were the case, investors could predict the volatility of a cryptocurrency based on its constellation of design features, and developers could deliberately design cryptocurrencies that can be expected to have low volatility. To conduct our analysis, we adopt the taxonomy proposed in Chapter 2. This chapter identifies a wide variety of cryptocurrency design features and sorts them into six categories, namely "development", "technical", "supply", "transactions", "usability", and "general". We collect a complete record of these design features for a broad sample of cryptocurrencies and then employ LASSO regressions to identify those design features that affect volatility.

This chapter contributes to the literature on cryptocurrency volatility. While numerous papers focus on the volatility of Bitcoin (e.g., Ardia et al., 2019; Baur and Dimpfl, 2021; Byström and Krygier, 2018; Conrad et al., 2018; Urquhart, 2017) or a limited number of other major cryptocurrencies, such as Ethereum or Ripple (e.g., Caporale and Zekokh, 2019; Cheikh et al., 2020; Chu et al., 2017; Gradojevic and Tsiakas, 2021), Panagiotidis et al. (2022) take a broader approach by analyzing a sample of 292 cryptocurrencies. They employ different GARCH-type models to examine regime changes in the volatility of these 292 cryptocurrencies. Other studies explore volatility dynamics across different cryptocurrencies and document spillover effects (e.g., Aslanidis et al., 2021; Ji et al., 2019; Katsiampa et al., 2019; Koutmos, 2018; Yi et al., 2018). Some further papers analyze factors and/or statistical models, as well as machine learning approaches, that can explain and predict cryptocurrency volatility (e.g., Amirshahi and Lahmiri, 2023; Baur and Dimpfl, 2018; Bouri et al., 2019a; Catania and Grassi, 2022; D'Amato et al., 2022; Katsiampa, 2019; Wang et al., 2023a; Yen and Cheng, 2021). Notably, Wang et al. (2023b) consider sentiment and blockchain data such as the average block size and the hash rate as determinants of cryptocurrency volatility. These cryptocurrency-specific factors are the outcomes of the design and the economics of a cryptocurrency network. We extend this literature by adopting a perspective which relates cryptocurrency volatility to cryptocurrency design in the strict sense. To the best of our knowledge, this work is the first to explore this relationship for a broad range of design features. The existence of a connection between design features and cryptocurrency valuation has been established by Hayes (2017) and within Chapter 2, both of which provide evidence that design features influence the market valuation of cryptocurrencies.

Our results are somewhat ambiguous because they partly depend on the volatility measure and the sample period. Nonetheless, several consistent findings emerge. In line with the theoretical model of Bolt and Oordt (2020), we observe that older cryptocurrencies tend to be less volatile. Additionally, starting from 2020, our results demonstrate that cryptocurrencies which do not pass on any transaction fees/tips to agents maintaining the network's integrity exhibit lower volatility levels. Also, the presence of mandatory transaction fees increases the volatility of the corresponding coin. Besides, we reveal that, from 2020 until 2022, cryptocurrencies developed by private, for-profit entities are associated with higher volatility levels. For the years 2019 to 2022, we demonstrate that cryptocurrencies based on Proof-of-Stake (PoS) or delegated Proof-of-Stake (dPoS) are more volatile. Thus, we do not find convincing support for the prediction made by Saleh (2018), that Proof-of-Work (PoW) cryptocurrencies are inherently more volatile than those employing alternative consensus mechanisms.

The remainder of this chapter is organized as follows. In Section 3.2 we describe our data and methodology, in Section 3.3 we present the results and Section 3.4 concludes.

3.2 Data and Methodology

Cryptocurrencies exhibit a range of design features, often reflecting choices made by their developers. For instance, the consensus mechanism (PoW, PoS, etc.) is a key aspect. Other features, such as whether the developer is a for-profit organization, relate to the development process. Efforts have been made to categorize these design features (see, e.g., Cousins et al., 2019; Eska et al., 2022b; Garriga et al., 2020). We adopt the taxonomy proposed in Chapter 2, which is designed to explore the relationship between cryptocurrency design features and market valuation – a research question related to ours. Table 3.1 presents the six categories of design features, and lists the variables within each category and their respective definitions. Our data set includes design feature information, sourced from official network websites, whitepapers and other reliable sources, for a total of 58 cryptocurrencies.[39]

Besides data on design features, we obtain daily price data on the cryptocurrencies in our sample from the exchange APIs of eight different cryptocurrency trading venues, covering the period from January 2019 to December 2023. The selected trading venues are Binance, Bitfinex, Kraken, Bitstamp, Coinbase, Gemini, Bittrex, and Poloniex. According to Härdle et al. (2020), they are all considered reliable since they do not report inflated trading volumes. Our primary data sources are the respective exchange APIs, and in case of missing data, we first consult CryptoDataDownload, then CoinGecko, and if data is still unavailable, we resort to Yahoo Finance.

For our analysis, we consider two different sets of cryptocurrency returns: (i) Bitcoin (BTC) denominated returns and (ii) U.S. dollar (USD) denominated returns. For the BTC sample, we use daily closing prices (price of last trade before midnight UTC against BTC), aggregate the time series from these trading venues, and construct the volume-weighted average price from which we calculate the daily returns. We obtain daily returns on BTC prices for all cryptocurrencies in our sample – except BTC itself, obviously.[40] Sample (ii) is based on daily closing prices in USD quotation. On Binance, cryptocurrencies are traded only against EUR, so we convert EUR prices into USD using the daily USD-EUR exchange rate. Poloniex is excluded from our USD sample because it solely trades in Malaysian ringgit (RM). Eventually, we are left with a set of cryptocurrency prices against USD which is referred to as *direct prices*. Unfortunately, not all cryptocurrencies have direct prices against USD on the trading venues used for data sourcing. For instance, Bitfinex, the exchange with the most direct USD quotes, only lists direct quotes for 42 of the cryptocurrencies in our sample. Therefore, we convert BTC prices into USD prices using the USD-BTC exchange rate from the respective trading venues. We refer to these converted USD prices as *indirect prices*. We then compile our final *USD sample* as follows: (i) For cryptocurrencies quoted only in BTC on each trading venue, we use the indirect prices to calculate daily returns. (ii) For cryptocurrencies with both BTC and USD prices available, we calculate volume-weighted direct and indirect prices separately. Using these two price series, we then compute the volume-weighted average price and, eventually, the daily returns for these cryptocurrencies.

Both the BTC sample and the USD sample offer distinct advantages and disadvantages. The

[39] We initially collected data on design features for 79 cryptocurrencies, but not all features are available for every cryptocurrency, resulting in a reduced number of cryptocurrencies considered in our analysis. Ultimately, the final sample comprises 58 cryptocurrencies that have a sufficiently long time series for volatility calculation.

[40] Note that, if a cryptocurrency is traded against BTC on none of the eight exchanges in certain sample years, we rely on data from CoinGecko or Yahoo Finance. Neither CoinGecko nor Yahoo Finance provide BTC-denoted prices. Thus, we construct their BTC price by dividing their USD price by the USD price of BTC from CoinGecko.

Table 3.1: Design features: variable description

This table describes the design feature variables, grouped according to the taxonomy developed in Eska et al. (2022b).

Panel A: Development

Variable(s)	Binary	Description
(i) DeveloperPublic (ii) DeveloperNPO (iii) DeveloperPrivate	yes (each)	Describes whether the development are conducted by (i) independent developers, (ii) a non-profit organization, (iii) a private, for-profit company
NoMajorityChanges	yes	Takes value of 1 if no part of the decision process about the networks' direction are passed on to the community
CodeNonPublic	yes	Describes whether the core code is fully accessible on Github or a similar platform
(i) CodeC++ (ii) CodeGo (iii) CodeOther	yes (each)	Primary language in which the core code is implemented is (i) C++, (ii) Go, or (iii) other
Fork	yes	Indicates whether a cryptocurrency network was forked from another one (take 1 as value) or built from scratch (take 0 as value)

Panel B: Technical

Variable(s)	Binary	Description
(i) ConsensusPoW (ii) ConsensusPoSdPoS (iii) ConsensusOther	yes (each)	Type of consensus mechanism used by the network: (i) Proof-of-Work, (ii) Proof-of-Stake or Delegated Proof-of-Stake, or (ii) other
(i) HashSHA256 (ii) HashEthash (iii) HashScrypt (iv) HashBlake (v) HashOther	yes (each)	Type of hash function used by the network to ensure transaction validity
HashAge	no	Age of the hash function used.
(i) CurveECDSA (ii) CurveED25519 (iii) CurveOther	yes (each)	Type of elliptic curve used in the respective network

Panel C: Supply

Variable(s)	Binary	Description
NoMaxSupply	yes	Takes value of 1 if there is no limitation regarding the maximum number of coins to be issued
(i) FixedSupply (ii) Deflationary (iii) Inflationary (InflationaryDecreasing, InflationaryFixed, InflationaryFixedRate, InflationaryDynamic)	yes (each)	The cryptocurrency (i) has a fixed supply, (ii) is deflationary, or (iii) is inflationary with different supply growth schemes
RewardCoinbase	yes	Takes a value of 1 if each new entry to the ledger entails a specific number of new coins.
RewardInflation	yes	Takes the value of 1 if the distribution of new coins is not directly linked with coinbase rewards. Note that also a no reward structure is possible.

Table 3.1: Design Features: variable Description (cont.)

Panel D: Transactions

Variable	Binary	Description
TheoreticalBlockTime (seconds)	no	Theoretically intended time between two ledger entries
BlockTimeAverage (seconds)	no	Average time between two ledger entries observed historically
BlocksizeLimit	yes	Takes the value of 1 when the network has a blocksize limit
TransactionFeeObligation	yes	Takes the value of 1 if the network has an obligatory fee for a transaction to be processed
NoTipSpecialTreatment	yes	Takes the value of 1 if the network does not allow their user to prioritize a transaction by paying a special fee (tip)
NoFeeTipForMinerForger	yes	Takes the value of 1 if the network does not (partly) pass transaction fees and/or tips to miners

Panel E: Usability

Variable(s)	Binary	Description
(i) IntentionPayment (ii) IntentionSmartContract (iii) IntentionOther	yes (each)	Take the value of 1 when the network is intended to be (i) a payment system, (ii) a smart contract platform, or (iii) neither of the aforementioned, by the developers
SmartContractSupport	yes	Network support smarts contracts, i.e., implicit smart contract possibility
TokenUsageBeyondPayment	yes	Services or rights beside the possibility to make financial transactions

Panel F: General

Variable(s)	Binary	Description
LedgerOther	yes	Take the value of 1 when the network does not apply the blockchain technology but an alternative distributed open source protocol
AccountingBalance	yes	Accounting system is balance based, i.e., the actual account balances are saved in blocks
(i) Anonymous (ii) Pseudoanonymous (iii) Non-anonymous	yes (each)	Describe the different privacy level of the network. Note that the Bitcoin network is identified as pseudoanonymous

BTC sample generally avoids currency conversions but relies on transactions of one cryptocurrency against another (BTC). On the other hand, the USD sample measures prices against a fiat currency but includes indirect prices, which may raise concerns about arbitrage opportunities in cryptocurrency markets.[41] To ensure robustness, we analyze both samples. The USD sample includes Bitcoin, whereas the BTC sample, with Bitcoin as the numeraire, does not. To validate consistency, we re-estimate all models for the USD sample excluding Bitcoin and find similar results.

We compute two volatility measures from the daily returns series: the interquartile range and the standard deviation. These are calculated for five sample periods (each year from 2019 to 2023), including cryptocurrencies with at least 90 daily returns per year. Our design feature data is from Eska et al. (2022b) and reflects the status as of September 2020. We are generally not capturing any time-series variation during the years 2021 to 2023. Even though certain networks undergo structural changes from time to time, these events are generally very rare.[42] Thus, the impact of those on the results of our analysis is negligible.

Table 3.2 shows the descriptive statistics for our ten subsamples, i.e., each combination of the BTC and USD sample with the five sample periods from 2019 to 2023. For each subsample, the table provides summary statistics for both volatility measures. The most important insight from the descriptive statistics is that the volatility of the cryptocurrencies in our sample varies considerably in the cross-section. It is this variation that we wish to explain in our empirical analysis. Additionally, the table highlights that volatility is generally higher in the BTC sample than in the USD sample.

In our empirical setup, we have a limited number of cross-sectional observations (cryptocurrencies) and numerous potentially relevant explanatory variables (design features). In a first step we reduce the number of explanatory variables by conflating some of the design feature variables.[43] Furthermore, instead of including the specific hash function employed by a cryptocurrency directly in our regression analysis, we capture its effect on volatility by considering its age. The majority of our independent variables are binary variables, with their default values corresponding to the design of the Bitcoin network. Furthermore, we redefine continuous

[41] Indirect prices are a possible cause for concern because it is known that there are arbitrage opportunities in the cryptocurrency market (see, e.g., Makarov and Schoar, 2020). We note, though, that the trading venues in our sample belong to the most liquid market places for cryptocurrencies, and higher liquidity tends to be associated with higher price efficiency (see, e.g., Wei, 2018). For cryptocurrency-exchange pairs for which both direct and indirect prices are available, we find only very small price deviations.

[42] Investigating the data originally collected, the aggregated lifetime of all cryptocurrencies in our sample equal 115,981 days. Furthermore, the sample had 33 events which caused a change in at least one of the design features. Consequently, within the whole sample, such an event occurs every 3,514.58 days which is about 9.6 years.

[43] We conflate the variables *CodeGo* and *CodeOther* to a single binary variable *CodeNonC++* which is set to one if at least one of the former variables is one, and zero otherwise. Similarly, we introduce the binary variables *CodeNonECDSA*, *IntentionNonPayment* and *Inflationary.* We refer the reader to Eska et al. (2022b) for further details.

Table 3.2: Return data: descriptive statistics

The table shows descriptive statistics (mean, quartiles, cross-sectional standard deviation) of the mean return, the standard deviation of daily returns and interquartile range of daily returns for each year of our investigation period.

	BTC sample					USD sample				
Measure	Mean	1st Quart.	Median	3rd Quart.	SD	Mean	1st Quart.	Median	3rd Quart.	SD
Panel A: 2019										
Mean Return	-0.0021	-0.0033	-0.0019	-0.0006	0.0028	-0.0	-0.0008	0.0003	0.002	0.0041
Standard Deviation	0.0489	0.0349	0.0419	0.0562	0.0204	0.0572	0.0458	0.0516	0.0602	0.0182
Interquartile Range	0.0429	0.0317	0.0379	0.0497	0.0158	0.0501	0.0417	0.0488	0.0547	0.0117
Panel B: 2020										
Mean Return	-0.0011	-0.0023	-0.001	0.0002	0.0036	0.0039	0.0024	0.0038	0.005	0.003
Standard Deviation	0.0556	0.041	0.0526	0.0625	0.0194	0.0656	0.0563	0.0634	0.0744	0.0138
Interquartile Range	0.0501	0.0361	0.0474	0.0575	0.0176	0.0592	0.0474	0.0564	0.0681	0.0162
Panel C: 2021										
Mean Return	0.0047	0.0024	0.0043	0.006	0.0038	0.007	0.0045	0.0064	0.0083	0.0039
Standard Deviation	0.0718	0.0603	0.0658	0.0782	0.0228	0.0849	0.0752	0.0804	0.0907	0.0233
Interquartile Range	0.0583	0.0495	0.061	0.0664	0.0124	0.0762	0.0676	0.0782	0.0841	0.0132
Panel D: 2022										
Mean Return	-0.0012	-0.0023	-0.0008	0.0002	0.003	-0.003	-0.0041	-0.0029	-0.002	0.0016
Standard Deviation	0.0425	0.0311	0.0382	0.0459	0.017	0.057	0.0478	0.0538	0.0618	0.0175
Interquartile Range	0.0344	0.0296	0.0331	0.0391	0.0073	0.053	0.048	0.0518	0.0584	0.0102
Panel E: 2023										
Mean Return	-0.0006	-0.0018	-0.0007	-0.0001	0.0017	0.0021	0.0009	0.002	0.0028	0.0018
Standard Deviation	0.0397	0.0271	0.0347	0.0437	0.0181	0.0454	0.0353	0.0415	0.0536	0.0158
Interquartile Range	0.0312	0.0254	0.0308	0.0336	0.0088	0.0398	0.0345	0.0389	0.0452	0.0099

variables such that the value for Bitcoin is zero. For example, we recalculate blocktimes as

$$BlockTime_{mod} = \frac{Blocktime_{Bitcoin} - Blocktime}{Blocktime_{Bitcoin}}.$$

We proceed in a similar way for the age of the hash function. Given this definition of our independent variables, all of them are zero for the Bitcoin network.

To assess the impact of cryptocurrency design on cryptocurrency volatility, we use LASSO (absolute shrinkage and selection operator) regressions, a widely-used technique in machine learning. This method is able to select those design variables that affect cryptocurrency volatility. Our LASSO regression approach connects variable selection and regularization by 10-fold cross validation, repeated $10,000$ times in our analysis.[44]

3.3 Results

Table 3.3 shows the LASSO results for the interquartile range as volatility measure for the BTC and the USD sample. If a variable is never selected by the LASSO procedure, the respective cell in the table has no entry. For all variables selected at least once, we provide an estimate of the sign and strength of their impact on volatility. To accomplish this, we calculate the average value of the corresponding coefficient, incorporating a value of zero for cases where the variable was not selected. Furthermore, we report how frequently a variable has been selected by the LASSO regressions. Specifically, *** [**, *, $^{\#}$] indicates that the respective variable has been selected in more than 80% [60%, 40%, 20%] of the cases. We will focus our discussion on the design feature variables selected by the LASSO in more than 50% of the ten subsamples, representing the years 2019 through 2023, each denominated in either BTC or USD.

Five design features stand out for being selected in more than half of all subsamples, with some subsamples even exceeding 80% of all LASSO regressions, and consistently exhibiting the same sign in all selected subsamples (light green in Table 3.3). First, among these features, age is the most noticeable, being selected in all subsamples: Older cryptocurrencies consistently exhibit lower volatility, aligning with studies by Bekaert and Harvey (1997) and Aggarwal et al. (1999) on traditional financial markets and Pessa et al. (2023) for the crypto universe.[45] Following this, cryptocurrencies that do not pass transaction fees or tips onto verifiers are associated with lower volatility, a trend observed since 2020 with a significant spike in 2022. Although not selected in either 2023 sample, cryptocurrencies with mandatory transaction fees exhibit higher volatility levels, reflecting similar patterns observed in traditional financial markets (see, e.g.,

[44] When we use five folds instead of ten in the cross-validation procedure our results remain qualitatively similar.

[45] Pessa et al. (2023) state that large price variations are less likely with increasing cryptocurrency age. Other design features – in contrast to this study – are not analyzed.

Table 3.3: LASSO results with interquartile range as dependent variable

This table reports the average of the parameter estimate, incorporating a value of zero for cases where the variable was not selected, indicating the economic significance from 10,000 LASSO regressions with the interquartile range of daily returns as the dependent variable and the design feature variables as the independent variables. Presented results in columns (1) to (5) base on the BTC sample whereas columns (6) to (10) consider the USD sample. $^{\#}$, *, **, and *** indicate that the respective variable is selected in at least 20%, 40%, 60% and 80%, respectively, of the 10,000 LASSO regression. Non-blank cells showing a figure without superscript belong to variables selected in less than 20% of the cases. Cells with "-" are associated with variables never selected.

	BTC sample					USD sample				
Variables	(1) 2019	(2) 2020	(3) 2021	(4) 2022	(5) 2023	(6) 2019	(7) 2020	(8) 2021	(9) 2022	(10) 2023
Constant	0.0423***	0.046***	0.0491***	0.0332***	0.0304***	0.0508***	0.0529***	0.0756***	0.052***	0.0412***
DaysAge	-0.0078***	-0.0004*	-0.0102***	-0.0009**	-0.0006$^{\#}$	-0.013***	-0.0059***	-0.0109***	-0.0123***	-0.0079***
DeveloperNPO	-	-	-	-0.0002	-	-	-	-	-0.0005***	-
DeveloperPrivate	-	0.0001$^{\#}$	0.0002*	0.0000	-	-	0.0012***	0.0008***	0.0022***	-
NoMajorityChanges	0.0013***	0.0000	-	-0.0000	-0.0000	-	0.0012*	-	-0.0008***	-
CodeNonPublic	-	0.0000	0.0000	-	-	-	-	-	-	-
CodeNonC	-	-	-0.0000	-0.0000	-0.0000	-	-	-	-	-
Fork	-	-	0.0013*	0.0001	0.0002$^{\#}$	-	-	0.0000	-	0.0001$^{\#}$
ConsensusPoSDPoS	0.005***	0.0013**	0.0037***	0.0008***	-	-	0.0000	-	0.0013***	-
ConsensusOther	-0.0000	-	-	-0.0001	-	-	-	0.0000	-	-
HashAge	-	-	0.0000	-	-	-	-	0.0000	-	-
CurveNonECDSA	-	0.0031***	-0.0000	0.0000	-	-	0.0069***	0.0000	-	-
NoMaxSupply	-	0.0000	0.004***	-	-0.0000	-	-	0.0003	-	-0.0000
Deflationary	-	-	0.0055***	-0.0000	-	-	-	0.0000	0.0000	-
FixedSupply	0.0000	-	0.0004*	-0.0000	0.0003$^{\#}$	0.0013***	-	0.0003	-	0.0019***
RewardCoinbase	-	-	-0.0011***	0.0000	-	-	-	-0.0003$^{\#}$	-0.0000	-
RewardInflation	0.0014***	-	0.0022***	-	0.0000	0.0059***	-	0.0016***	-	-
BlockTimeAverage	0.0000	-	0.0028***	0.0005	-	0.0001***	-	0.0003**	0.0053***	-
TransactionFeeObligation	0.0000	0.0000$^{\#}$	0.0019***	0.0001	-	0.0008***	0.0041***	0.0001$^{\#}$	-	-
NoTipSpecialTreatment	-	-	-0.0002*	-0.0002	-0.0000	-	-	-0.0000	-	-
NoFeeTipForMinerForger	-	-0.0000	-0.0021**	-0.0004	-0.0007***	-	-0.0003$^{\#}$	-0.0002	-0.0059***	-0.0011***
IntentionNonPayment	-	0.0025***	0.0034***	-	-	-	0.0017***	0.0023***	-	-
SmartContractSupport	-	-	0.0000	-	0.0000	-	-	-	-	-
TokenUsageBeyondPayment	-	-	-	-	0.0000	-	-0.0000	0.0000	-	-
LedgerStyleOther	-0.0000	-0.0000	-0.0012*	-0.0000	-	-	-0.0017$^{\#}$	-	-	-0.0000
AccountingBalance	-	-	-0.0000	-0.0001	-0.0000	-	-	-	-	-
Anonymous	-	-	0.0039***	0.0000	0.0000	0.0000	-	0.0011**	-	-
NonAnonymous	-	-	-0.0000	-0.0003	-0.0000	-	-0.0003$^{\#}$	-	-0.0003**	-
∅ Observations	48	57	57	57	57	49	58	58	58	58
∅ R^2	0.2012	0.1152	0.5061	0.0764	0.0318	0.3491	0.3078	0.2641	0.3940	0.1384

Jones and Seguin, 1997; Umlauf, 1993). Furthermore, from 2020 to 2022, private, profit-driven cryptocurrencies consistently demonstrate higher volatility. Lastly, cryptocurrencies employing PoS or dPoS consensus mechanisms show increased volatility, particularly evident in the BTC sample and during the early stages of the investigation period, contradicting Saleh (2018), who suggests Proof-of-Work cryptocurrencies are inherently more volatile.[46]

Two additional variables are selected in more than half of all cases, *FixedSupply* and *NoMajorityChanges* (light blue in Table 3.3). *FixedSupply* generally increases volatility, with an exception in the 2022 BTC sample where it has a negative value, but its economic impact and selection frequency are low. The impact of an absence of opportunities for network members to participate in the governance process on volatility shows a temporal structure. While it exacerbates volatility in the early subsamples (2019 and 2020), it has a volatility-reducing effect from 2022 onwards.

When we analyze volatility using the standard deviation instead of the interquartile range, we consistently observe the same sign for the selected variables across subsamples (provided that the variable is selected for both measures).[47] However, the results for the interquartile range show higher overall significance. This outcome is anticipated, as the interquartile range is a robust measure of volatility unaffected by outliers.

3.4 Conclusion

In this chaoter, we investigate whether the design features of cryptocurrencies affect their volatility. We utilize both BTC-denominated prices and USD-denominated prices to calculate daily returns. Conducted on a yearly basis, our analysis reveals that design features influence cryptocurrency volatility. While some design feature effects are limited to the volatility measure of choice and the time frame under consideration, others exhibit consistent patterns. We show that older cryptocurrencies tend to be less volatile, which corresponds with their increased maturities and their more established network structures. A transaction fees/tip structure with direct transfers from transaction senders to verifiers increases the volatility of the respective cryptocurrencies. Additionally, cryptocurrencies implementing mandatory transaction fees and those developed by private teams exhibit higher volatility. Moreover, details of the consensus mechanism also affect the volatility of the respective cryptocurrencies. While this chapter analyzes the impact of individual design features on volatility, it is conceivable that there are

[46] Another variable selected in more than half of the subsamples is *LedgerStyleOther*. The negative coefficient suggests that non-blockchain distributed ledger types decrease volatility. However, its economic impact and selection frequency are low, indicating minimal influence.

[47] In Appendix B, the LASSO results using the standard deviation as the dependent variable are presented and briefly discussed.

interdependencies between design features, and that specific combinations of design features drive volatility. Exploring such interdependencies is a promising avenue for future research.

Chapter 4

After *The Merge*: Network Fragility and Robust Design of PoS Cryptocurrencies

4.1 Introduction

Notwithstanding the fast-growing popularity of Bitcoin and other cryptocurrencies, one of the main points of criticism is the immense energy consumption of the underlying Proof-of-Work (PoW) technology. The electricity consumption of the Bitcoin network of about 121 TWh in the year 2023 exceeds that of whole countries such as the Netherlands or the Philippines.[48] As a result, many competing cryptocurrencies using the alternative Proof-of-Stake (PoS) mechanism have entered the market, and the pressure for established cryptocurrencies to adopt PoS is rising. Most prominently, the second-largest cryptocurrency Ethereum has completed a move from PoW to PoS in September 2022 in a transition event called *the Merge*.

While in PoW systems, so-called miners maintain the integrity of the network by using their computing power to solve difficult cryptographic puzzles, the consensus mechanism in PoS networks is based on *staking*: Network members post coin stakes, and those with large stakes are more likely to get selected for updating the blockchain history. While an update in line with the consensus is rewarded, dishonest behavior leads to a loss of the stake. The stability and security of such a system does obviously not only depend on its sound implementation, but is also critically driven by the financial economics of the network. In particular, the willingness of agents to stake their coins, the resulting security of the system against a potential

[48] The data on Bitcoin electricity consumption sources from Cambridge Bitcoin Electricity Consumption Index (https://cbeci.org/) and consumption data per country is published by the U.S. Energy Information Administration (https://www.eia.gov/international/data/world/electricity/electricity-consumption). Note that the comparative values is the 2021 electricity consumption for the Netherlands (113 TWh) and the Philippines (98TWh), respectively.

saboteur's attack, and the utility arising from using the PoS currency for goods transactions are all endogenous equilibrium outcomes that depend on the specific design of the network together with the agents' preferences.

In this chapter, we propose an economic model for PoS systems that allows us to analyze these aspects and their dependence on the design of the network in detail. We highlight that one of the central economic features of PoS systems compared to PoW networks is an opportunity cost problem: The incentive of agents to stake their coins does not only depend on the expected reward for staking, but is also critically influenced by the potential lost utility as coins cannot be used for transactions while they are staked. Therefore, a high utility derived from transactions with the coin compared to the staking reward can lead to a small amount of staked coins in equilibrium, negatively affecting the network security. If the staking reward falls far below the opportunity costs, the network completely breaks down. In PoW networks, this opportunity cost problem does not exist: Agents' mining activities do not affect their ability to use PoW coins for transactions; furthermore, miners only forego a potential one-time reward if the network breaks down and are not required to put large cryptocurrency stakes at risk.

In more detail, our model explicitly takes into account the security side as well as the demand side of PoS systems. On the security side, so-called forgers (i.e., network members staking coins) compete against a saboteur to maintain the network's transaction ability. Hence, their actions determine the security level of the network. On the demand side, there are agents who use the network for consumption goods transactions. In doing so, they are aware of the possibility that their transactions may fail as a result of a successful attack of the saboteur. Taking into account the cryptocurrencies' implicit coins function as a reward, as a means of exchange, and as a cost-related component to forgers, we are able to uniquely identify situations in which both model sides are jointly at equilibrium. We find that equilibria with strictly positive prices are unique and arise when the aggregated stake of the forgers exceeds the holdings of the saboteur. The staking decision is based on the expected reward, the initial endowment, and the foregone utility that forgers would generate from using coins for transactions. Therefore, both the current as well as the expected cryptocurrency price determine the aggregated stake and thus the security of the network. Our model points out that this influence provides an additional feedback loop for price changes and ultimately the stability of the network.

We point out several design features that are critical with respect to the network stability. Our analysis is based on a calibration to the Ethereum network as of August 2022, just before *the Merge*. The first critical parameter driving the stability of the PoS network is the money growth rate – one of the parameters that is explicitly set by the developers in the cryptocurrency's programming code. We find that generally, there is an optimal money growth rate in PoS systems that maximizes the welfare of the participating agents. When money growth is set higher than the optimal rate, excessive staking will occur at the expense of the utility that can be derived from goods transactions with cryptocurrency coins. On the other side, for a lower-than-optimal money growth rate, the amount of newly distributed coins as a reward for staking is too low to provide a good enough incentive for staking and to guarantee the system security. In fact, a money growth rate below a certain threshold leads to the breakdown of the system. The possibility of such breakdowns makes the PoS system fragile, especially when taking into account that the welfare-optimal level for the money growth rate is quantitatively very close to the breakdown threshold. As a remedy for this issue, we recommend PoS developers not to set the money growth rate exactly at the welfare-optimal level, but to leave a safety buffer that accounts for possible parameter and model uncertainty. Our recommendation is reminiscent of the inflation target in today's monetary systems, which is usually set close to zero to ensure price stability but still reasonably above zero to avoid the risk of deflation.

Second, the model highlights the critical importance of the required fork length – which is also defined in the cryptocurrency's code – for PoS network stability. A larger fork length positively affects the security of the system, as it becomes more difficult for the saboteur to attack the system. On the other hand, a large fork length negatively affects the adoption of a cryptocurrency, as shown by Easley et al. (2019). Our analysis reveals that for the fork length, there is also a minimum threshold below which the system collapses as the security is not guaranteed anymore. Interestingly, this minimum value is higher in PoS systems compared to PoW networks, leading to less favorable adoption prospects. The underlying economic reason is that forgers in PoS networks are exposed to the risk of a saboteur's attack, such that a higher security level is necessary to achieve a sufficient amount of staking. In PoW systems, a low security of the cryptocurrency network does, on the other hand, not directly affect the incentive to mine. We show that this disadvantage of PoS systems can be alleviated and the minimum fork length can be reduced when the network implements a transaction fee, which is paid by buyers and directly passed on to the forgers. These results support the design choice of the Ethereum network that forgers are rewarded through fees paid by buyers (called *Gas*) as well as through newly distributed coins.[49]

A third main feature of a PoS system that drives the fragility of the network is what is modeled as the meeting probability between buyers and sellers. This parameter corresponds to the extent of adoption of the network for buying and selling goods. We find that generally, the welfare of the participating agents increases with a greater meeting probability due to the greater utility derived from transactions. However, there is the critical caveat that if the meeting probability goes beyond a certain threshold, the network collapses and the welfare goes to zero. This network fragility again directly results from the opportunity cost problem: When the utility derived from transactions using the PoS coin becomes too large, agents are not willing to stake

[49] The creation of new coins which are distributed as the coinbase reward was stopped after the Merge. Nevertheless, our work provides evidence that the transaction fees incentivize forgers such that sufficiently high staking levels are achieved.

sufficient amounts of cryptocurrency anymore, such that the system becomes vulnerable to saboteurs' attacks. It directly follows that caution should be exercised regarding the idea that a pure PoS system could be used to facilitate a great multitude of day-to-day transactions. If the coin's utility for conducting transactions outruns the incentives for staking, the security of the system is not guaranteed anymore, and the network could become a victim of its own success. Our results imply that pure PoS networks are mainly feasible for markets with significant search frictions, while we recommend a hybrid PoS/PoW system for more general use cases.

Finally, the model allows us to analyze to what extent the developers' incentives when designing a network are aligned with the goal of maximizing welfare for the participating agents. Developers typically own a stake of the cryptocurrency that they are working on, and their economic incentive is to achieve a price increase of the coin through their innovative labor input. Our results show that for the highlighted parameters, the developers' incentives deviate from the welfare-optimal choices. On a positive note, however, the developers' profit-maximization typically leads to design choices that have a greater distance from the points at which the network breaks down, making the network less fragile. For instance, the welfare-optimal money growth rate is very close to the minimum threshold below which the network collapses, while the developers' profit-maximizing choice would yield a rate well above this point.

Related Literature

This chapter contributes to the growing literature on economic models of cryptocurrencies. One strand in this field of literature analyzes the conditions in which blockchain networks are expected to generate stable, decentralized consensus. Among them, Biais et al. (2019) identify equilibrium conditions under which the coordination among miners generates consensus. Leaded by the scalability trilemma, Abadi and Brunnermeier (2018) present a general model to analyze the situation in which a blockchain is preferable over a traditional centralized intermediary in record-keeping. While the former two are restricted to blockchains with PoW consensus mechanisms, Saleh (2021) formalizes consensus finding in PoS networks and establishes equilibrium conditions in which PoS generates consensus. Cong and He (2019) find that equilibria in blockchain networks have a wider economic range with their design affecting the consensus generation.

Besides models concentrating on consensus finding, this literature also covers pricing models. While Biais et al. (2023) concentrate on the interplay between price expectation and transactional benefits, Cong et al. (2021b) provide a fundamental-based dynamic valuation model with coin prices arising from the aggregated transactional demand and the platform adoption. Athey et al. (2016) focus on the dynamics of cryptocurrency adoption in the context of exchange rate uncertainty. In a similar vein, Sockin and Xiong (2023) formalize coins as a means of exchange and find that users' benefits as well as speculative demand drive prices which could lead to market breakdown. Bolt and Oordt (2020) state that the exchange rate of a virtual currency is determined by the current value of transactions, the expectation of forward-looking investors, and the future consumer adoption and merchant acceptance. Further, the more established the cryptocurrency, the less sensitive it is to shocks resulting from speculation. Within their endowment economy model with two competing currencies[50], Schilling and Uhlig (2019) even show that under certain conditions, speculation does not arise in equilibrium. These models all consider cryptocurrencies in general without particularly paying attention to different consensus mechanisms. They take the transaction ability of cryptocurrency networks and therefore also the security level as given. In contrast, Chiu and Koeppl (2022) explicitly model double-spending attacks in a PoW blockchain and show that mining competition and settlement delay tackle the issue of double spending. Next to double-spending attacks, Budish (2018) also models sabotage attacks and relates them to the cost for running a blockchain.

The model of Pagnotta (2022) picks up the possibilities for sabotage attacks and connects them to the valuation of the cryptocurrency. He uses a setting with mining competition in the sense of Nakamoto (2008) to jointly determine prices and security while particularly taking their interaction into account. Irresberger et al. (2020) also highlight the importance of the security within cryptocurrency networks. This chapter is closely related to Pagnotta (2022) whose results are restricted to PoW based cryptocurrencies. Consistency with his PoW model allows us to provide a direct comparison between price and security levels in networks with PoW and PoS consensus. Focusing on the effect of scaling, John et al. (2021a) compare PoW and PoS systems and find opposing effects of higher throughput on security and prices. The valuation framework for PoS payments systems introduced by Fanti et al. (2019) is also pertinent to our research. While their results are based on traditional quantity theory of money, they do not account for the feedback loop between security and prices. Jermann (2023) delves into the dynamics of the Ethereum network in its post-*the Merge* era, introducing a dynamic stochastic equilibrium model. His results show, inter alia, that the staking fraction is determined by the utility value of network coins, albeit overlooking potential meanchisms between transaction capability, network security, and prices. Staking equilibria are further studied by John et al. (2021b) and Cong et al. (2022).

The remainder of this chapter is structured as follows. In Section 4.2, we introduce our model for Proof-of-Stake cryptocurrency networks. Section 4.3 calibrates the model to the Ethereum network and provides a comparison between PoS and PoW networks with respect to the networks' fragility. In Section 4.4, we analyze the effects of specific design parameters on prices, welfare, and network fragility for PoS systems and compare our results to an analogous PoW

[50] The competition between cryptocurrencies and established fiat currencies is also assessed by Fernández-Villaverde and Sanches (2019) and Cong and Mayer (2021). Choi and Rocheteau (2021) shows that privately produced fiat currencies can reach a steady-state.

network. We further succinctly discuss the results and present design recommendations. Finally, Section 4.5 concludes.

4.2 Model

4.2.1 Setup

In our PoS model, time is discrete and goes from zero until infinity. Following the recent search-theoretic models of money,[51] we divide each period $t = 0, 1, 2, \dots$ into two subperiods, called day and night. During the day, the agents operate in a centralized competitive market in which they trade a general good. Any agent can produce and consume this general good which acts as the numeraire in our model. During the night, the agents operate in a decentralized market which is subject to frictions but opens beneficial exchange possibilities. We associate this market with a cryptocurrency network. Following the competitive equilibrium approach of Rocheteau and Wright (2005), we assume that all agents take prices as given in both subperiods.

We consider a saboteur who attempts to manipulate the cryptocurrency network so that it collapses and transactions are no longer feasible. We do not primarily think of within-network attacks here, but rather of an act of economic sabotage.[52] The attack of such a saboteur aggregates the various sources of risk affecting the cryptocurrency network and is primarily motivated from outside the network, e.g., to profit from short positions or to establish a competing currency. Within our model, an attack can basically take place every period between the day and the night market. In the event of a successful attack in period t, trust in the network is lost and the cryptocurrency network is destroyed. Transactions will then no longer be feasible in period t's night market, causing the value of the cryptocurrency network to fall to zero. As a result, the price of the network's inherent coin falls to zero, too, and we assume that it remains at this level thereafter. Formally, we consider the endogenous function Φ_t to capture the likelihood that the network resists a potential attack in period t. Thus, Φ_t proxies for the security of the network and we refer to it as the security function. Furthermore, we assume that all agents are aware of the fact that sabotage attacks can make the cryptocurrency network collapse. Hence, the time-t-expectation about the future coin price p_{t+1} in terms of

[51] The search-theoretic models of money following Lagos and Wright (2005) provide an appropriate framework which allows to study frictions that necessitate the usage of money while remaining analytically tractable and easily quantifiable. The approach has become a workhorse model in the monetary theory literature.

[52] There are natural economic limits for within-network attacks. If double spending is revealed, the cryptocurrency price drops which in return limits the profits for the fraudulent agents from double spending. Further, the possibility for successful double spending attacks, given that the fraudulent agent does not own the majority of hashrate (PoW) or stake (PoS), can efficiently be combated by setting-specific requirements on the number of confirming blocks to consider a transaction to be valid. For a detailed discussion of different sources of risk on cryptocurrency networks see e.g., Budish (2018).

the numeraire is given by $\mathbb{E}_t\left[p_{t+1}\right] = \Phi_t \mathbb{E}_t^{(1)}\left[p_{t+1}\right]$ with $\mathbb{E}_t^{(1)}$ representing the expectation given that the network resisted the attack.

The entirety of agents interacting in our model comprises two groups besides the saboteur. On the one hand, we have profit-maximizing agents whose actions facilitate transactions in the night market. These agents, called forgers, verify the correctness of the transactions within the cryptocurrency network. To be able to do so, they have to stake coins which they cannot use for transaction purposes. In return they are rewarded with newly created coins. Since the actions of this agent group determine whether the cryptocurrency network can withstand a sabotage attack, i.e., whether the transaction ability and thus the security of the network is maintained[53], we refer to this group as the security side.

On the other hand, there are cryptocurrency network users including all agents that are willing to make transfers in the night market. We further subdivide this group into two types according to their actions in the cryptocurrency network. Buyers want to consume during night but cannot produce while sellers are able to produce but do not want to consume. This setup with heterogeneous, anonymous[54] agents generates demand for a means of exchange, a function which the cryptocurrency network's inherit coins fulfill. In what follows, we refer to this group of buyers and sellers as the demand side.

We separate between forgers (security side) and users (demand side) in our model. In reality, one might argue that agents are willing to concurrently operate as a forger and as a buyer.[55] The competitive setting with Walrasian prices implies that such an agent would not need to consider inter-group interaction effects when choosing the optimal behavior. Hence, the optimal behavior of this agent would be subject to the same optimality conditions.

In the following, we discuss our PoS model in detail. We first concentrate on the security and the demand side before eventually combining the two groups.

4.2.2 Security Side

Network security in our setting is mainly determined by forgers' who compete against a saboteur. We characterize the forgers optimization problem, derive the aggregated total number of coins staked by all forgers for a given security level, and then deduct the security function.

[53] The likelihood for a successful sabotage attack depends on the ratio between the attacker's stake and the total stake provided by our second agent group.

[54] The anonymity excludes future trading promises and thereby credit arrangements between the two types of agents within this group. This causes the need for a means of exchange given the existence of a double-coincidence problem (Kocherlakota, 1998; Lagos and Wright, 2005; Temzelides and Yu, 2004).

[55] Other combinations than agents who partly stake and partly use coins for night market transactions, i.e., simultaneously selling in the night market while also staking coins, are irrelevant here as the optimal behavior overlaps solely in the optimal choice of the network coins bought in period t's day market.

Forgers and the Validation Process

The security side consists of N^F generation-t-forgers who can purchase coins in the day market and hold them in the night market of this period. Right after having bought coins and thereby having entered the night market, a forger stakes coins in order to get authorized for participation in the verification process in period t's night market.[56] Note that due to the investment in the network's inherit coins, the risk of sabotage attacks is also borne by the forgers. The likelihood that forger i gets selected for verification is equal to the ratio between her number of coins staked S_{it} and the total number of coins staked $S_t = \sum_{j=1}^{N^F} S_{jt}$. The verification itself does not come with any cost for the respective forger. Having correctly verified the transactions in the night market, the selected forger receives newly created network coins which she sells in the next period's day market and uses the proceedings for numeraire good consumption. We here assume a Bitcoin-like inflation and reward scheme. This means that the reward is the only source for changes of the total coin supply and that the reward per block is fixed within a specific time period. As the reward is only a very small fraction of the coins in circulation N_t^C, we introduce an inflation rate ρ with $N_{t+1}^C = N_t^C \rho$ which is approximately constant in such a situation.[57] In our model, the coin reward for the authorized forger is therefore $N_t^C (\rho - 1)$ coins. Thus, the present value of forger i's risk-adjusted expected reward is given by $\frac{S_{it}}{S_t} \cdot \delta \Phi_t \mathbb{E}_t^{(1)} [p_{t+1}] \cdot N_t^C (\rho - 1)$ in terms of the numeraire. $\frac{S_{it}}{S_t}$ captures the probability that forger i was authorized to verify the transactions and δ is the time preference.

While the verification itself is not associated with any cost, the forgers face opportunity cost in form of loosing transaction possibilities as coins staked cannot be used for transaction purposes in the night market. Within our model, we assume that the fewer coins a forger owns, the higher her marginal cost to stake one additional coin.[58]

More formally, given forger i's initial numeraire endowment e_{it} that could potentially be used in the night market, staking S_{it} coins reduces the maximum night market good quantity a forger could realize from $\frac{e_{it}}{z_t}$ to $\frac{e_{it}}{z_t} - S_{it} \frac{p_t}{z_t}$ with z_t denoting the night market good's numeraire price.[59]. To capture the foregone utility by staking, we define utility over consumption of the night market through the function $u_F(\cdot)$. We assume $u_F(\cdot)$ to be a continuous, strictly increasing and concave utility function fulfilling $u_F(0) = 0$, $u'_F(0) = \infty$, and $u_F(X) = X$ for some $X > 0$. In detail, we assume that the utility function has the same functional form and is based on the

[56] Carrying coins through the night market and not staking them is inefficient as the chance for the reward is reduced without cost saving.

[57] In the Bitcoin network, miners obtain a block reward of X_t coins. Approximately every four years, the block reward is reduced to $X_{t+4} = \frac{X_t}{2}$. The time period until the next reward halving can therefore be considered as an era in which the inflation is constant.

[58] For instance, if a forger owns 10 coins, staking 1 coin does not hurt him much since 9 coins are left for transaction purposes. If, in contrast, this forger already staked 9 coins, the marginal cost for staking her last remaining coin is higher than in the previous case.

[59] As we assume the initial endowment to be given in terms of the numeraire, $\frac{e_{it}}{z_t}$ and $\frac{e_{it}}{z_t} - S_{it}\frac{p_t}{z_t}$ refer to the number (quantity) of night market goods from which utility is generated.

same risk aversion parameter as the one on demand side (see Subsection 4.2.3). Furthermore, note that the quantity of night market goods traded between the two counterparties, denoted by Q_t, serves as the input variable for $u_F(\cdot)$.

However, it is uncertain whether a transaction counterpart is met and thus whether coins could actually be transferred. Therefore, we integrate search-model related night market frictions and assume that night market transactions are feasible with probability μ only. If no transaction counterpart is met, non-staked coins are simply carried through the night market.

Moreover, we also take into account that forgers might have specific preferences for staking over night market good transactions. To this end, we consider a staking preference parameter $\zeta \in [0,1]$ [60] that scales the foregone utility due to staking. In total, we thus capture the forgers' costs of staking as opportunity costs derived from the foregone utility in case of a meeting and the return of the coins in case of not having met a transaction counterpart. Formally, forger i ultimately faces the maximization problem

$$\begin{aligned}
\max_{S_{it}} \zeta\mu \max_{Q_{it}\le \frac{e_{it}}{z_t} - S_{it}\frac{p_t}{z_t}} & \left\{ u_F\left(Q_{it}\right) + \delta \mathbb{E}_t^{(1)}\left[\left(\frac{e_{it}}{p_t} - \frac{z_t Q_{it}}{p_t}\right) p_{t+1}\right]\right\} + \dots \\
& \dots + \zeta\left(1-\mu\right)\delta\mathbb{E}_t^{(1)}\left[\left(\frac{e_{it}}{p_t}\right)p_{t+1}\right] + \frac{S_{it}}{S_t}\cdot\delta\Phi_t\mathbb{E}_t^{(1)}\left[p_{t+1}\right]\cdot N_t^C\left(\rho-1\right) \qquad (4.1) \\
& \text{s.t. } S_{it}p_t \le e_{it}.
\end{aligned}$$

Note that parameters given in uppercase letters refer to quantities while lowercase letters are given in terms of the numeraire.

In what follows, we assume homogeneous forgers with the same initial endowments $e_{it} = e_t$ for all $i \in \left\{1, \dots, N^F\right\}$. The following lemma identifies a condition for the aggregated total number of coins staked by all forgers.

Lemma 4.1. *In a symmetric Nash equilibrium the total amount of coins staked S_t by N^F homogeneous forgers satisfies the condition*

$$S_t = \Phi_t\delta z_t N_t^C\left(\rho-1\right)\mathbb{E}_t^{(1)}\left[\frac{p_{t+1}}{p_t}\right]\frac{N^F-1}{N^F}\left(\zeta\cdot\mu\cdot u'\left(\frac{e_t}{z_t}-\frac{S_t}{N^F}\frac{p_t}{z_t}\right)\right)^{-1}. \tag{4.2}$$

Proof. See Appendix C.1. □

For given prices and security, (4.2) reveals that the total stake provided raises in the inflation rate ρ, in the time preference δ, and in the initial endowment e_t. The first two parameters

[60] Since the possibilities to use the network for transaction purposes and the coins as a means of payment is still limited, we introduce this scaling parameter and thereby account for the current situation in PoS-based networks.Furthermore, note that due to the homogeneity assumption, we do not consider individual staking preferences.

naturally increase the time-t-value of forgers' rewards leading to a higher number of coins staked. The initial endowment reduces the cost for forgers and in turn increases the aggregated stake. In contrast, increasing the total number of forgers while keeping their total initial endowment constant leads to a lower total stake. This is explained by the fact that with increasing N^F, each forger is able to only buy a smaller number of coins for staking. Thus, opportunity cost for providing an additional coin as stake is higher which in turn decreases the total stake.[61] Moreover, a higher probability for feasible night market transactions μ results in a lowered aggregated stake ceteris paribus. Intuitively, if μ rises, the expected utility from night market good consumption rises. As this situation is associated with higher opportunity cost, the amount staked decreases.

Note that in PoW systems like Bitcoin, the coins function as a means of exchange and as an incentive for maintaining the network integrity. In a PoS setting, coins serve additional roles: Along with their prices, they affect the cost of staking and thus also the cost for a saboteur to attack the network. The last term of equation (4.2) captures this dependency of staking costs on coin prices. This is a crucial difference to PoW networks, where, most notably, exogenous energy cost and the cost of leasing hardware drive the mining cost and the cost for a saboteur. Thus, the related formula determining the hashrate in PoW networks only depends on the expectation for p_{t+1} but not on the current value of p_t[62].

Security Function

So far, our derivations take the security level Φ_t as given. However, the aggregated stake actually determines the security level of the cryptocurrency network and thus, the likelihood that the network resists a sabotage attack. In our model, we focus on sabotage attacks as an aggregate source of risk rather than double-spending attacks. The saboteur's instrument to force a collapse of the cryptocurrency network is to establish an alternative blockchain history which makes the network members lose confidence in the network's integrity. We assume that this situation arises if a disruptive fork with $\kappa > 1$ blocks is realized. In a PoS network the authority to attach the next block to the blockchain is generally offered to a randomly selected stakeholder[63] according to the size of her deposit. Thus, the likelihood for such a disruptive fork and therefore a collapse is determined by the distribution of the total stake between honest forgers and the saboteur. To internalize this probability into our model, we introduce a gambler's ruin problem similar to Pagnotta (2022). Given the forgers' aggregated stake S_t and a saboteur's budget of $a_t = A_t \cdot p_t$ in terms of the numeraire, a κ block disruptive

[61] Conversely, a less intense competition would lead to higher stakes. As security is increasing in total stake provided by honest miners, fewer forgers (keeping total initial endowment fixed) in our model would imply a more secure network. In reality, however, decentralization would be partly given up which in return makes the network more vulnerable. This impact of centralization on security is not modelled.

[62] The model of Pagnotta (2022) reflects this intuition.

[63] In our model, the entity of stakeholders are the N^F forgers supplemented by the saboteur.

fork is established with probability $\left(\frac{A_t}{S_t}\right)^\kappa = \left(\frac{a_t}{p_t \cdot S_t}\right)^\kappa$ if $\frac{a_t}{p_t} < S_t$ and probability one if the saboteur's stake exceeds the honest forgers' aggregated stake.[64] Accordingly, we define the security function Φ_t as

$$\Phi_t\left(a_t, S_t\right) = \left(1 - \left(\frac{a_t}{p_t \cdot S_t}\right)^\kappa\right) \cdot \mathbb{1}_{\left\{\frac{a_t}{p_t} < S_t\right\}} \tag{4.3}$$

which can be interpreted as the likelihood that the cryptocurrency network resisted the saboteur's attack in period t. The security function is a key endogenous object within our model. It reflects the component which connects the security side to the demand side.

4.2.3 Demand Side

The demand side of our model comprises N^B buyers and an arbitrary number of sellers, all born in period t. In the day market of period t, any generation-t-buyer can produce the numeraire good at unitary production disutility and consume it at unitary marginal utility. In the following, we require the utility of consumption to be smaller or equal than the disutility from production and we let l_t denote the excess disutility. Furthermore, buyers can buy any non-negative amount of cryptocurrency coins C_{it}, $i = 1, \ldots, N_B$, at price p_t thereby gaining access to the cryptocurrency network, i.e., the night market. With probability μ, a buyer meets a seller in the night market. In case of a meeting, they exchange coins against the night market good which can be produced by the sellers at unitary marginal disutility in any number. The quantity of night market goods traded between the two counterparties will be denoted by Q_t and z_t again labels the price for one night market good in terms of the numeraire. From the consumption of the acquired night market good, buyers derive utility according to a utility function $u_B(\cdot)$ fulfilling the same properties as $u_F(\cdot)$ from Subsection 4.2.2. In the day market of period $t+1$, generation-t-buyers and generation-t-sellers sell their (remaining) coin holdings to the next generation, consume the numeraire good from the proceedings and then die. This microfounded demand-side setting to model the existence of cryptocurrency coins follows the PoW case of Pagnotta (2022).

In summary, the lifetime utilities of buyers and sellers are given by $-l_t + u_B(Q_t) + \delta c_{t+1}$ and $-Q_t + \delta c_{t+1}$, respectively, with time preference $\delta \in (0,1)$ and numeraire good consumption c_{t+1} in period $t+1$. Integrating risk-adjusted expected future prices and uncertain night market trading possibilities into the general model setting, we can rewrite the problems of the agents on the demand side as follows.

[64] See, e.g., Feller (1968).

A price-taking buyer i, $i \in \{1, \dots, N_B\}$, faces the maximization problem

$$\max_{l_{it}, C_{it}} - l_{it} + \Phi_t \mu \max_{Q_{it} \leq \frac{C_{it} p_t}{z_t}} \left\{ u_B \left(Q_{it}\right) + \delta \mathbb{E}_t^{(1)} \left[\left(C_{it} - \frac{z_t Q_{it}}{p_t} \right) p_{t+1} \right] \right\} + \Phi_t \left(1 - \mu\right) \delta \mathbb{E}_t^{(1)} \left[C_{it} p_{t+1}\right] \tag{4.4}$$

s.t. $C_{it} p_t \leq l_{it}$

Equation (4.4) represents a two-stage maximization problem. The first-stage problem requires buyers to choose the numeraire good surplus which they directly invest by buying C_{it} coins. The auxiliary condition imposes the budget constraint that no more than the numeraire good surplus can be spent on coins.[65] This first-stage problem also considers the proceeds from coins not traded in the night market provided that no meeting took place. The second-stage maximization problem determines the optimal amount of night market goods buyer i demands given that a meeting took place.

The program of a price-taking seller j is given by

$$\max_{Q_t} \left\{ -Q_t + \delta \mathbb{E}_t^{(1)} \left[\left(\frac{z_t Q_t}{p_t} \right) p_{t+1} \right], 0 \right\}. \tag{4.5}$$

For the case that the price of the night market good z_t and expected holding returns make the sellers break-even, maximization problem (4.5) requires $\delta \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] = \frac{1}{z_t}$ for sellers to be indifferent between any positive production level. In the case of inequality, sellers would seek unbounded production (would not produce at all) due to the circumstance that time- and risk-adjusted expected returns are strictly positive (negative).

In contrast to the PoW model of Pagnotta (2022), the demand for cryptocurrency coins does not just originate from the buyers but also from the saboteur and the forgers. Thus, market clearing requires that the total number of coins N_t^C in period t has to equal $\sum_{i=1}^{NB} C_{it} + S_t + A_t$. Stated differently, the number of coins in circulation for night market transactions $C_t = \sum_{i=1}^{NB} C_{it}$ is the total coin supply N_t^C reduced by $S_t + A_t$. Considering this market clearing condition and taking Φ_t as given, our model implies the following property for any partial equilibrium in which (4.4) and (4.5) are fulfilled:

Lemma 4.2. *In any equilibrium, $\delta \Phi_t \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] \leq 1 \ \forall t$. If the inequality is strict, the night markets clears at Q_t below the efficient exchange quantity Q_t^*, all buyers choose the same cryptocurrency holdings (in terms of the numeraire) below the level needed to meet Q_t^*, and there is*

[65] Due to the anonymity in our model framework, credit arrangements are infeasible and thus, short positions cannot be taken.

a unique market clearing price that satisfies

$$p_t = \delta \Phi_t \mathbb{E}_t^{(1)} \left[p_{t+1} \right] \left(1 + \mu \left(u_B' \left(\delta \frac{N_t^C - S_t - A_t}{N^B} \mathbb{E}_t^{(1)} \left[p_{t+1} \right] \right) - 1 \right) \right). \tag{4.6}$$

Proof. See Appendix C.1. □

The term $\delta \Phi_t \mathbb{E}_t^{(1)} \left[\frac{p_{t+1}}{p_t} \right] \leq 1$ states that net risk-adjusted expected holding returns are non-positive.[66] As a result, buyers try to avoid carrying coins through the night market and therefore choose Q_t below the efficient level Q_t^* with $u_B' \left(Q_t^* \right) = 1$, i.e., the situation in which buyers' marginal utilities and seller's marginal production costs balance out. Congruent to the PoW result from Pagnotta (2022), the resulting pricing equation (4.6) equals the present value of the risk-adjusted expected price plus a non-negative term designated as liquidity premium by Pagnotta (2022). The liquidity premium is mainly influenced by the meeting probability μ and the marginal utility from night market transactions. Since the number of coins circulating in the night market is lower in PoS than in the PoW case, exchange quantity per coin in the night market is higher ceteris paribus. Assuming equal meeting probabilities and an identical exchange quantity per coin, the liquidity premium is higher in PoW networks.

4.2.4 Stationary Equilibrium and Welfare

For our following analysis, we focus on non-negative price situations in which the optimality conditions of the different agent groups are met, the security function is given as in (4.3), the cryptocurrency market clears, and balances of the cryptocurrency holdings in numeraire terms are constant. More specifically, we require that forgers maximize their expected profit leading to (4.2), the buyers' actions satisfy (4.4), the sellers' production decisions satisfy (4.5), and market clearing according to $N_t^C = C_t + S_t + A_t$. Considering the inflation rate from Subsection 4.2.2, the stationary condition $N_t^C p_t = N_{t+1}^C p_{t+1}$ requires that the condition $\mathbb{E}_t^{(1)} \left[\frac{p_{t+1}}{p_t} \right] = \frac{1}{\rho}$ holds in a stationary equilibrium. By multiplying the pricing equation (4.6) with the number of outstanding coins N_t^C, we obtain the aggregated coin holdings $h_t := p_t \cdot N_t^c$ in terms of the numeraire. Integrating the stationary condition and defining constant numeraire holdings as $\bar{h} = h_t = h_{t+1}$, it has to hold that

$$\bar{h} = \frac{\delta}{\rho} \cdot \Phi_t \left(a_t, S_t \left(\bar{h} \right) \right) \cdot \bar{h} \cdot \left(1 + \mu \left(u_B' \left(Q \left(\bar{h} \right) \right) - 1 \right) \right) \tag{4.7}$$

with night market exchange quantity $Q \left(\bar{h} \right) = \frac{\delta}{\rho} \frac{\bar{h}}{N_t^c} \left(N_t^c - S_t \left(\bar{h} \right) - A_t \left(\bar{h} \right) \right)$ in any stationary equilibrium. Formula (4.7) presents a fix-point problem. In order to explicitly determine

[66] If this condition were not met, buyers would demand an unbounded amount of coins which they carry through the night market and thereby enlarge their lifetime utility.

stationary equilibria, we use numerical methods for root determination of nonlinear functions to solve for $\bar{h}$ and consequently prices. This setup follows the stationary equilibrium analysis of Pagnotta (2022) and allows for a direct comparison between his PoW setting and our PoS model.

Furthermore, we analyze welfare implications in our forthcoming analysis. We do not consider the saboteur's benefits from a successful attack to be part of the welfare since these benefits arise outside the cryptocurrency network, if at all. Thus, the social welfare of a cryptocurrency network is given by the buyers' trade surplus in the night market less cost associated with staking. Forgers' rewards as well as sellers' proceeds do not positively contribute to welfare since they only represent a reallocation of the same real coin holdings, i.e., coin holdings in terms of the numeraire, between the different agents groups. For our PoS model, welfare is thus defined as:

$$W = N^B \mathbb{E}\left[u_B\left(Q\right) - Q\right] - N^F \mathbb{E}\left[u_F\left(\frac{e_t}{z_t}\right) - u_F\left(\frac{e_t}{z_t} - S_{jt}\frac{p_t}{z_t}\right)\right]. \tag{4.8}$$

4.3 PoS Network Fragility in a Calibrated Setting

We explore the equilibria of our model as defined in Subsection 4.2.4 and point out that for certain parameter constellations, the only existing equilibrium is one where prices, security, and welfare are zero. Such situation – which we call a network breakdown – is the worst possible scenario for a cryptocurrency that should be avoided by all means. After calibrating our model to the Ethereum network in Subsection 4.3.1, we characterize the equilibria in Subsection 4.3.2. We show that moving to PoS makes the system more vulnerable to network breakdowns compared to the PoW case due to an opportunity cost problem that arises from the PoS mechanism.

4.3.1 Calibration to the Ethereum Network

Our empirical analysis is based on the parameters of the Ethereum network as in August 2022, just prior to *the Merge*. During this time, the Ethereum mainnet generated consensus using a PoW implementation, albeit running a PoS implementation on a testnet. Due to the timely proximity to the transition event, a very similar network structure could be observed after the mainnet's subsequent move from PoW to PoS. Thus, calibrating our model to the August 2022 data provides an ideal setting for understanding the implications of the PoS mechanism on the one hand and for further comparing these implications to the PoW case.[67]

For our calibrated model version, we assume that each period represents one month. In August 2022, there were about 15,610,000 active addresses using the Ethereum network for transaction purposes according to theblock.co. In order to estimate the night market's meeting probability, which is not directly observable to us, we assume that each buyer was willing to transact on the network every third day. With the number of buyers $N^B = 15{,}610{,}000$ this results in a demand for 161,303,333 transactions in August 2022. During that time, there were only 34,900,623 transactions recorded on the Ethereum blockchain. Accordingly, we set our model's meeting probability μ to match these numbers, i.e., $\mu = \frac{34{,}900{,}623}{163{,}303{,}333} = 0.2164$. Within our calibration, buyers value consumption of the night market goods according to a Constant Relative Risk Aversion (CRRA) utility function $u_B(X) = \frac{X^{1-\sigma}}{1-\sigma}$. Following Lagos and Wright (2005) and Pagnotta (2022), we set the risk aversion parameter σ to 0.5, which also reflects the intuition that cryptocurrency users are not highly risk-averse.

Since agents in a PoS based cryptocurrency network decide between staking their coins and using them for transaction purposes, each buyer is also a potential forger. Thus, we assume that the number of buyers and forgers are both equal to the number of active addresses.[68] Further, we set the parameter to $\zeta = 0.15$ indicating a strong preference for staking which is explained by the actual number of transactions in the Ethereum network, the average size per transaction, and the fact that block proposers and block validators in the Ethereum network also receive transaction fees which upgrades the expected reward compared to the cost. For a forger's endowment $e_{it} = e_t$, we assume that the aggregated endowment $N^F e_t$ equals the total market capitalization. Due to the homogeneity assumption, each of the N^F forgers is thus endowed with $\frac{N_t^C p_t}{N^F}$ coins.

On the supply side, there was a circulating supply of $N_t^C = 119{,}922{,}554$ Ether[69] on August 1, 2022. This number increased by 422,169 Ether until September 1, 2021 which corresponds to a monthly inflation rate of 0.3520%. Consequently, we set $\rho = 1 + 0.3520\%$. Similar to the Bitcoin network, we assume that the only source of inflation is the coinbase reward[70] for agents verifying transactions.

[67] Using more recent data from the Ethereum network to work out the PoS implications would indeed be possible, the comparison with PoW would require to forward fill certain parameters like the hashrate, leading to less reliable results.

[68] We here ignore a potential minimum staking amount as implemented in Ethereum (32 Ether minimum amount), for instance. Due to the possibility of pooling in so-called stacking pools, this threshold barrier is rather theoretical and no real constraint in reality. Furthermore, remember that we do not need to consider interaction effects between staking and using coins for transactions due to our model's competitive setting.

[69] The coins in the Ethereum network are named Ether.

[70] While most part of the newly generated Ether are "common" coinbase rewards, an insignificant number of new coins arise from uncle block rewards. Uncle blocks are blocks that are valid and verified but have not been included into the chain due to the simultaneous propagation of a two blocks at the same time in the network. In contrast to the orphan blocks in the Bitcoin network, the miners of the uncle blocks are also rewarded with newly created Ether.

On the security side, we need to calibrate the security function (4.3). We require that a disruptive fork with $\kappa = 20$ blocks needs to be established to force a network collapse in our model. This number is based on the confirmation requirements of Kraken, one of the leading cryptocurrency exchanges. They prescribe that an Ethereum transaction has to be confirmed by 20 subsequent blocks in order for funds to be credited to a customer's deposit. Furthermore, the saboteur in our model is endowed with 2% of the average market capitalization of the network in August 2022, i.e., $a_t = N_t^C \cdot p_t \cdot 0.02 = 119{,}922{,}554 \cdot 1{,}698.93 \cdot 0.02 = 4{,}074{,}800{,}493$, which is approximately twice the amount that the richest Ethereum address which could not be linked to an exchange owned during that time.[71]

Besides, we fix the time discount factor δ to 0.9957 what equals an annual rate of 0.95. Table 4.1 summarizes the values of the model parameters which constitute the basis for our quantitative analyses.

Table 4.1: Calibrated model parameters

Description	Variable	Value
Number of buyers	N^B	15,610,000
Meeting probability	μ	0.2164
Number of forgers	N^F	15,610,000
Number of coins in network	N_t^C	119,922,554
Inflation rate	ρ	$1 + 0.3520\%$
Staking preference	ζ	0.15
Length of fork to force collapse	κ	20
Attacker stake (in terms of numeraire)	a_t	4,074,800,493
Risk aversion	σ	0.5
Time preference	δ	0.9957

Given this parameterization, coin prices and corresponding security levels can be computed by solving (4.7). Our PoS model specification results in an equilibrium price of 1,330.38 with a security level of $\Phi = 99.99\%$. Security levels in this range are a direct result of our rather high choice of the necessary length of the saboteur's fork to cause a collapse of the network. The aggregated stake of the forgers adds to 6,325,277.67 or, stated differently, 5.274% of the circulating supply.

In addition to the calibration of our PoS model, we aim at providing a comparison with the PoW model of Pagnotta (2022). On the PoW model's security side, we assume 17 miners consistent with the 17 pools who each mined at least 1% of all blocks mined in August 2022. These

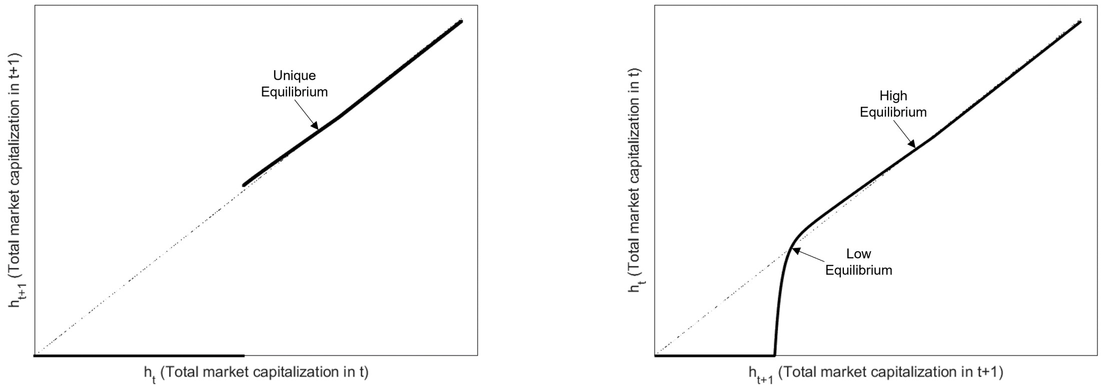
[71] The average daily closing price in August 2022 was 1,698.93 U.S. dollars.

numbers capture the notion that staking in a PoS cryptocurrency network is more competitive compared to PoW mining due to the lack of cooperation via pools and lower entry barriers. Furthermore, we follow Pagnotta (2022) and calibrate the cost component within the PoW setting such that the average hashrate of 928,256 GH/s observed during August 2022 is met by honest miners. In our quantitative setting, the saboteur's hashrate amounts to one third of the honest miners' hashpower. All other parameters are kept as in the PoS model calibration. In this PoW setting, two different stationary equilibria[72] exist, one associated with low prices and security and the other with higher prices and security. For our quantitative example, the two prices levels are 643.54 and 1221.94 with security levels of 92.24% and 99.99%.

4.3.2 Network Fragility: PoS vs. PoW

Figure 4.1a graphically illustrates the identification of stationary equilibria in the PoS network based on equation (4.7). In Figure 4.1b, we show the corresponding plot for an otherwise analogous PoW network in line with Pagnotta (2022) as discussed in Subsection 4.2.3. The plot for PoS networks reveals that there is a unique non-negative equilibrium in the PoS case. In this equilibrium, coin prices exceed a certain threshold level, such that forgers provide $S_t > A_t$ (a higher hashrate than the attacker) due to the high expected rewards. On the other hand, there are cases where the non-negative equilibrium does not exist. In that case, coin prices are low and honest forgers do not exceed the saboteur's stake. In this case, the network fails its mission to facilitating transfers which results in a network value of zero.

Figure 4.1: Determination of stationary equilibria



(a) PoS

(b) PoW

[72] The equilibrium conditions follow the Decentralized Monetary Equilibrium of Pagnotta (2022) and reflects a PoW network's equivalent situation to our PoS equilibrium discussed in Subsection 4.2.4.

Network breakdowns can also happen in PoW systems – however, there is a broader range of parameters for which non-negative equilibria exist and in fact, two equilibria emerge (consistent with Pagnotta, 2022): one with high cryptocurrency prices and high security levels, and one with low prices and low security. A low equilibrium is not viable in a PoS system. This can be attributed to the fact that forgers are exposed to the risk of sabotage attacks due to their coin investment. They are aware that their stake might become worthless and thus consider the network's security level when determining the optimal stake. This interplay generates a downward feedback loop for low prices which ultimately makes the network worthless.

As a result, the initial requirement on the price threshold for an equilibrium to exist is higher in PoS than in PoW. This finding indicates that PoW systems are more robust to sabotage attacks than PoS systems when coin prices are low. If, in contrast, prices are high, the feedback loop increases security which leads to slightly higher equilibrium prices and security levels in a PoS system compared to the high equilibrium of a PoW network.

4.4 Designing Breakdown-Resistent PoS Cryptocurrencies

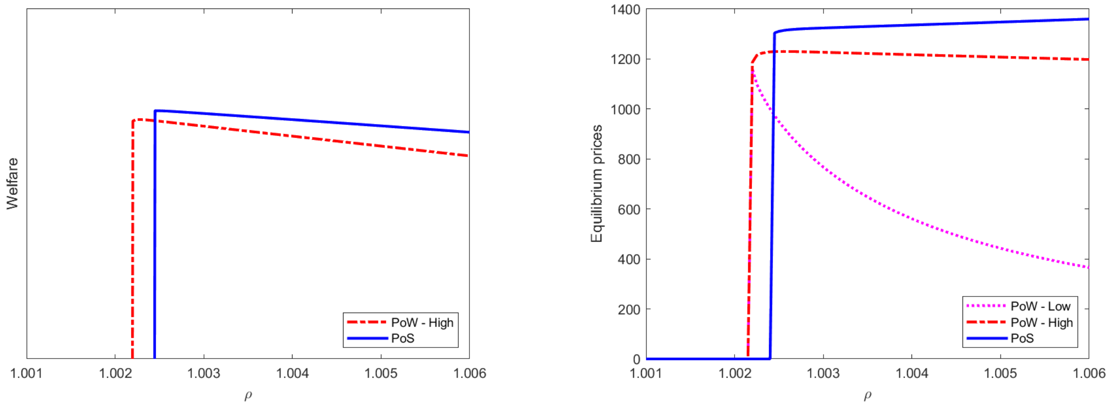
Based on the quantitative setting introduced in Subsection 4.3.1, we analyze the fragility of PoS cryptocurrency networks dependent on different design parameters. In particular, Subsection 4.4.1 presents our results on the impact of these parameters on prices and welfare and characterizes scenarios in which a positive equilibrium does not exist. As an important reference point, we conduct the same analysis in an analogous PoW-based network. In Subsection 4.4.2, we provide specific design recommendation for PoS cryptocurrencies with the goal of maximizing the welfare provided by the system while ensuring at the same time that the scenario of a network breakdown is avoided.

4.4.1 Critical Network Features

Money Growth Rate
At first, we turn our focus to the money growth rate in the PoS system, which is defined by the parameter ρ. This parameter is defined by the implementation of the respective network's core code. Hence, it is subject to the developer team's choice, and our model framework can provide insights on the parameter value's impact on welfare, price development, and network fragility.

Figure 4.2 shows the effect of the money growth rate parameter on welfare and equilibrium cryptocurrency prices. We directly observe that for a broad range of values for ρ, welfare increases with a declining money growth rate. In this range of values, $\rho > \bar{\rho}_W$, the marginal effect of buyers' trade surplus is lower than the marginal cost associated with staking. In this case, one would observe socially excessive staking. The welfare level provided by the system reaches a maximum at $\bar{\rho}_W$. Below that point, welfare decreases again since the amount of newly distributed coins as a reward for staking is too low to provide a good enough incentive for staking and to guarantee the system security. In such scenario, a beneficial planner would need to raise the inflation rate to incentivize forgers. In fact, a money growth rate below a certain threshold leads to the breakdown of the system. The possibility of such breakdowns makes the PoS system fragile, especially when taking into account that the welfare-optimal level for the money growth rate is quantitatively very close to the breakdown threshold.

Figure 4.2: Effect of changes in inflation rate ρ



(a) On welfare

(b) On prices

The relation of equilibrium cryptocurrency prices to the underlying money growth rate of the system is qualitatively different. Understanding the price outcomes of the model is important for design choices as well, as developers holding a significant stake of coins have an incentive to make choice that lead to price increases. We find a consistent price increase with the inflation rate ρ in a PoS-based cryptocurrency network, which is in clear contrast to classical monetary systems in which higher central bank money supply translates to a lower value of money.

The reason is that in PoS systems, there are two value-enhancing effects that dominate the classical negative money growth channel. These effects are on the one hand the security channel, under which a higher ρ leads to more staking and thus an increased security of the system, and on the other hand the scarcity channel, as the number of coins used for transaction purposes is effectively reduced by the additional stake. Formally, the three different effects can be illustrated by integrating the stationary condition into the equilibrium price (4.6) for a given security level, such that we obtain:

$$p_t = \left(\frac{\mu \Phi_t(\rho)\, \delta^{1-\sigma} \rho^{\sigma}}{\rho - \delta \Phi_t(\rho)(1-\mu)} \right)^{\frac{1}{\sigma}} \cdot \frac{N^B}{N_t^C - A_t - S_t(\rho)} \tag{4.9}$$

pos. security channel, neg. money growth channel, pos. scarcity channel

As the formula reveals, ρ enters negatively through the money growth channel, but positively through the security and scarcity channels.

Fork Length

The fork length parameter κ is an important ingredient in blockchain-based systems that has to be specified by the developers. In particular, it implies that a saboteur needs to generate a fork of length κ in order to provoke a collapse of the system, in accordance with our security function in equation (4.3). A larger fork length therefore increases the security of the network, but also leads to longer waiting times for transactions (Easley et al., 2019). Figure 4.3 reveals the influence of κ on welfare and price levels in PoS systems, again compared to the PoW case. Our model reflects the intuition that the smaller κ is, the more likely it is for a saboteur's attack to be successful.[73] Thus, welfare and prices rise in the necessary fork length. If κ is high, the effect of further increasing this parameter vanishes as the security is already very high and hardly increases when κ rises further. For lower κ values that are still higher than a certain threshold $\bar{\kappa}$, prices are more sensitive to κ changes. If the necessary fork length is below $\bar{\kappa}$, there is no viable, strictly positive equilibrium. This behavior is observed for both PoS and PoW networks. However, all else equal, the threshold level in a PoW network is lower than in a PoS system which can be traced back to the circumstance that forgers participate at the risk of sabotage attacks. Regarding welfare, the price level transmits to the trade surplus as well as to the cost of forging in PoS and of mining in PoW, respectively.[74]

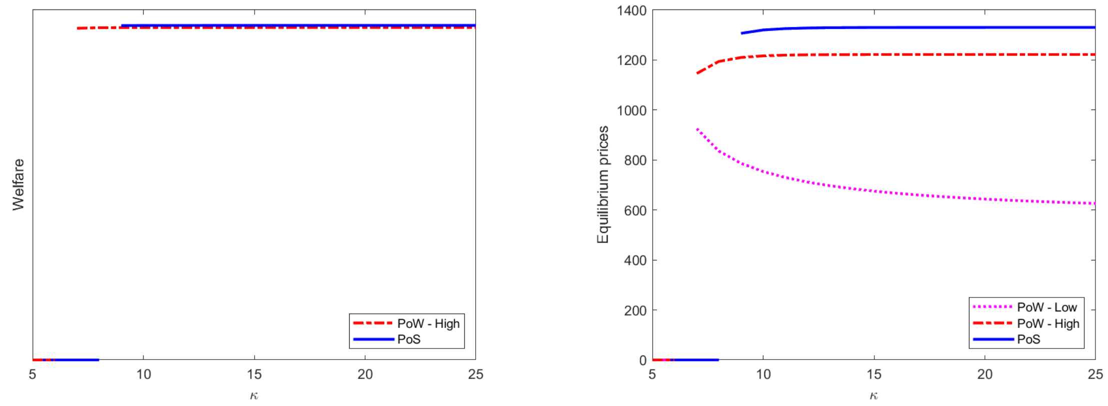
Our model parameter κ also captures the number of blocks that should be required for a transaction to be considered valid and thus the waiting time until the transaction is finally processed. Easley et al. (2019) state that the longer this waiting time becomes, the more users exit the network.[75] Hence, the network parameter κ captures two opposing effects. While

[73] Additionally, the required fork length also proxies for the waiting time until a reward can be paid out to a miner or forger, respectively. A faster payout of the rewards increases the present value of the risk-adjusted expected return, the investment in maintaining the network integrity, and consequently prices. Our model setting, however, does not reflect this intuition. Nevertheless, we argue that the likelihood of a successful attack offsets this effect, particularly because forgers take potential attacks into consideration when determining their optimal stake.

[74] Scaling the y-axis of Figure 4.3a reveals that the graphs' shapes are similar to the one of the influence on prices.

[75] Their analysis, however, is restricted to the Bitcoin network. Further, they find that mining fees that are able to prioritize transactions can partly help in offsetting this effect. The impact of fees is also discussed within Huberman et al. (2021) and Basu et al. (2023), inter alia.

Figure 4.3: Effect of changes in necessary fork length κ for collapse



(a) On welfare

(b) On prices

a higher value in this variable is obligatory for a positive price equilibrium to exist, network effects might be mitigated if the waiting time for transactions to be considered valid is too long. Regarding this concern, transaction fees could help in balancing out those opposing effects.

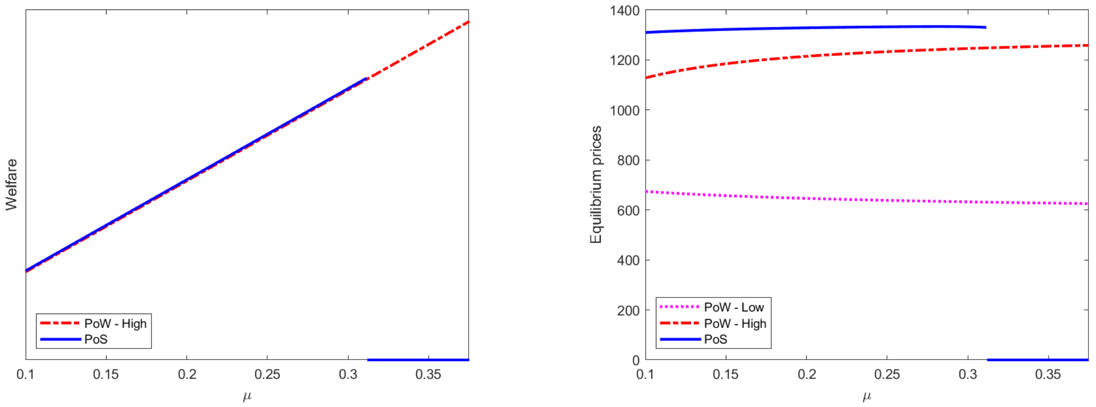
Meeting Probability

The third network primitive that is critically related to the network's fragility is the meeting probability μ. If the probability that buyers and sellers meet in the night market increases, the demand side within our PoS model generates an upward price pressure due to a higher expected value of night market utility per coin. This makes it more costly for forgers to give up transaction possibilities, directly affecting the security side.

Figure 4.4 shows that for a broad range of values for μ, the welfare provided by the system increases in the meeting probability in the night market. Despite the fact that the cost of staking for forgers increases, the utility for the buyers increases as well, such that the overall welfare goes up. However, there is a threshold beyond which the opportunity cost for the forgers becomes so high that their stake is reduced to the level at which the security of the system is not guaranteed anymore. As a result, the network breaks down. In other words, widespread adoption of a PoS cryptocurrency and the resulting increased meeting probability in the night market can make the network a victim of its own success.

Comparing these results with PoW systems highlights a critical economic difference between PoS and PoW networks: The analogous PoW network does not break down due to a substantial increase in μ. In contrast to a PoS system, the miners' decision is independent from the actual meeting probability. As the upward pressure on the demand side applies to PoW system as

Figure 4.4: Effect of changes in meeting probability μ



(a) On welfare

(b) On prices

well, strictly increasing welfare and price curves arise.

In summary, our analysis shows that a PoS system is not viable for a market that has only very minor search-type frictions, in contrast to PoW networks where less restrictive search-type frictions lead to larger welfare and higher prices. The presence of frictions motivates agents to stake their coins, while in a frictionless situation they would prefer to use their coins for transaction purposes instead, and the reduced incentive for staking leads to the risk of a network collapse. Our results complement the findings of Budish (2018) and Hinzen et al. (2022), who point out breakdown scenarios in other cryptocurrency-related settings.

4.4.2 Design Recommendations

Based on our analysis of the critical network parameters in Subsection 4.4.1, we provide informed guidance on the design of PoS systems. Our recommendations are made with the goal to increase the welfare provided by the system while also ensuring that a network breakdown is avoided.

Set Robust Money Growth Rate

As shown in Subsection 4.4.1, the welfare-optimal money growth rate of a PoS system is quantitatively close to the lower threshold below which the system breaks down. While it is therefore important to set the money growth reasonably close to its welfare-optimal level, it should also be ensured that the presence of parameter and model uncertainty does not lead to a scenario below the critical threshold. This situation is reminiscent of the inflation targeting problem in today's monetary system. While an inflation close to zero is desired to ensure price stability, policy-makers typically define an inflation target reasonably above zero – such as 2% p.a. – to avoid a deflation scenario. In a similar vein, we recommend PoS developers to leave a safety buffer that accounts for possible parameter and model uncertainty. Quantitatively, Figure 4.2 reveals that the welfare-optimal money growth rate is around 0.3% per month, and a network breakdown occurs at 0.27% per month. We therefore recommend a money growth rate of around 0.4% per month to establish a certain distance to the breakdown scenario, but still not lose too much welfare in case the parameter values turn out to be exactly as assumed.

Use Network Transaction Fees

In Subsection 4.4.1, we further have shown that the fork length in PoS networks needs to be set to a level that is significantly larger than for PoW systems, at the expense of longer waiting times for transactions. In the subsequence, we show that transaction fees that are paid by buyers and passed along to the forgers, can help mitigate the risk of a collapse for lower fork lengths. For that, we extend our model as follows: If a buyer and seller meet in the night market and agree on a transaction with a value of X, the buyer pays X to the sellers and a fractional transaction fee $\tau \cdot X$ with $\tau \in [0, 1]$ to the network, which is directly passed to the forger validating the respective transaction. Since sellers are unaffected by this kind of transaction fees, forgers are cross-financed by buyers. Integrating the transaction fee in the forgers' and the buyers' maximization problems (4.1) and (4.4), the problems transform to

$$\begin{aligned}
\max_{S_{it}} \; & - S_{it}p_t + \zeta\mu u_F \left(\frac{e_{it}}{z_t} - S_{it}\frac{p_t}{z_t}\right) + \dots \\
& \dots + \frac{S_{it}}{S_t} \cdot \delta\Phi_t \mathbb{E}_t^{(1)}\left[p_{t+1}\right] \cdot \left[N_t^C\left(\rho - 1\right) + \mu \frac{N_t^C - S_t - A_t}{(1+\tau)} \cdot \tau\right] + \delta S_{it}\mathbb{E}_t^{(1)}\left[p_{t+1}\right] \qquad (4.10) \\
& \text{s.t. } S_{it}p_t \leq e_{it}.
\end{aligned}$$

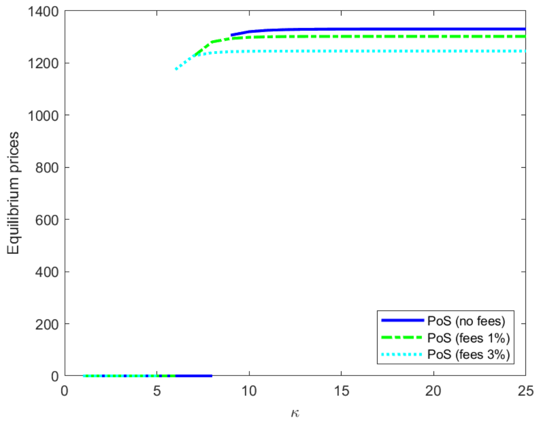
and

$$\begin{aligned}
\max_{l_{it}, C_{it}} & - l_{it} + \Phi_t \mu \max_{Q_{it} \leq \frac{C_{it}p_t}{z_t(1+\tau)}} \left\{u_B\left(Q_{it}\right) + \delta\mathbb{E}_t^{(1)}\left[\left(C_{it} - \frac{z_t Q_{it}}{p_t}\right)p_{t+1}\right] - z_t Q_{it}\tau\right\} + \dots \\
& \dots + \Phi_t\left(1-\mu\right)\delta\mathbb{E}_t^{(1)}\left[C_{it}p_{t+1}\right] \qquad (4.11) \\
& \text{s.t. } C_{it}p_t \leq l_{it},
\end{aligned}$$

respectively.

Figure 4.5 shows the equilibrium prices in the model, dependent on the fork length, for different transaction fee scenarios. The plots directly reveal that transaction fees of 1% and 3% mitigate the risk of a network breakdown for a range of smaller fork lengths. The underlying economic intuition is that when transaction fees are introduced, the expected reward of the forgers increase ceteris paribus. Therefore, more stake is provided which increases security and thus prices for a constant fork length (κ) and constant demand. On the demand side, transaction fees imply that the exchange quantity q and thus demand is reduced which reduces prices. Regarding the network fragility the increased security level resulting from higher staking incentives dominates the demand-caused loss in expected rewards (result of the reduced expected future price from demand side). The security level itself also depends on the interplay with the saboteur and a reduced model fork length decreases security. Since the higher staking incentives increase security, a designer could reduce κ and thereby, the network will effectively have the security level as in the case when no transaction fee is present. Even though this comes along with a slightly reduced price, we observe a more robust network. Stated differently, we have a “shift of price to security level” similar to the cross-financing of the security side from the demand side. We could state that the lower network fragility comes at the cost of reduced prices.

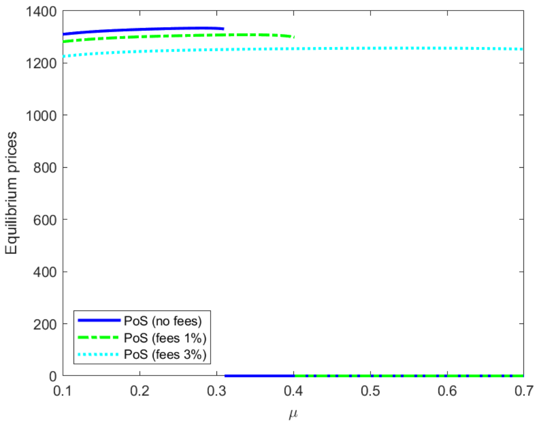
Figure 4.5: Effect of changes in necessary fork length κ for collapse with transaction fees



Implement Pure PoS Only for Markets with Significant Frictions

We finally discuss the implications of our result related to the meeting probability from Subsection 4.4.1, i.e., that a very high meeting probability in the night market leads to a network breakdown. This result provides a somewhat pessimistic view on the prospects of pure PoS systems to be used for applications with high transactions throughput. In particular, a network solely based on PoS does not appear to provide a suitable platform for providing high-frequency financial transactions. As the utility from conducting transactions would be very high, this utility competes with the incentive to stake the coins, and in equilibrium a reasonable amount of stakes coins cannot be guaranteed. For such use cases, we recommend a hybrid system that combines PoS with the PoW algorithm. On the other hand, one could very well imagine a PoS system that is specialized for personal real estate transactions. In this market, there are significant search frictions and liquid coins are not frequently needed, such that they can very well be staked, leading to a sufficient security level of the system. Finally, Figure 4.6 shows that transaction fees also mitigate the issue with the meeting probability rate to some extent. In summary, a network design in which the forgers' reward is not only generated from newly created coins, but also from buyers' transaction fees, is strongly supported by our analysis.

Figure 4.6: Effect of changes in meeting probability μ with transaction fees



4.5 Concluding Remarks

Since PoW systems are considered unsustainable, particularly due to their huge energy consumption, and since there are concerns regarding their economic viability,[76] other consensus protocols like PoS have gained in importance and continue to further do so. These concerns highlight the importance for a deeper economic understanding of these alternative consensus protocols. Against this background, this chapter presents a first valuation model for PoS cryptocurrencies that connects prices and security. We argue that the findings from Pagnotta (2022) who analyzes a similar setting within PoW based cryptocurrencies do not transfer to other cryptocurrency systems per se due to different network structures arising from the particular consensus protocol. The quantitative analysis which is built on our PoS model discloses several interesting findings with crucial influence on the design of PoS networks. Jointly determining prices and security, we find that any stationary equilibrium with strictly positive prices and security levels is unique. Such an equilibrium exists if prices and thus expected rewards for staking reach a level in which the aggregated stake of honest forgers exceed the coin holdings of

[76] See, e.g., Budish (2018) and Hinzen et al. (2022).

the saboteur.[77] The costs of honest forgers and the saboteur arise within the network, as both have to buy coins. This way they are exposed to price changes. Hence, the forgers participate at the risk of sabotage attacks and, furthermore, the higher prices are the less coins a saboteur can purchase for her attack given a fixed initial endowment. As a result, an equilibrium with low prices and low security, as it is found in a PoW system, is not viable in PoS.

Considering specific network design components and network primitives we further find major differences between the two network types. A first crucial difference arises with respect to the influence of inflation rates. In a PoS system, changes in this parameter affect prices by three different channels: (i) the positive security channel, (ii) the positive scarcity channel, and (iii) the negative money growth channel leading to prices that monotonically increase in inflation rate. Determining the optimal welfare level, there exists an inflation rate level for which welfare is maximized which requires developers to carefully balance out the two opposing objectives of price and welfare optimality. Furthermore, our model indicates that the waiting time for a transaction to be considered valid should be chosen higher in a PoS system compared to a PoW one as the threshold level for a necessary fork length leading to a collapse in demand is higher in PoS. Regarding meeting frictions, we also find that a crucial difference between the two network types. While a PoW network rises when search-type frictions vanish, their existence is necessary in a PoS network for a positive price equilibrium to exist limiting the possible adoption and economic importance.

In addition, our work contributes to transformation process from PoW to a PoS cryptocurrency, exemplified by the Ethereum network on the verge of *the Merge*. The effects of design feature changes indicate that the network structures may need to be transformed in order to maintain a network's viability after such a transition. If a developer who holds a considerable amount of coins aims at maximizing her profit, she would need to set the inflation rate infinitely large according to our model. Such an inflation rate would result in a substantial shift of coin holdings from network users to forgers. In a more generalized model whose security function penalizes wealth centralization, that redistribution would lead to declining demand from users and thus lower prices. Consequently, the developer's profit from large inflation rates would be limited and the long-term viability of the network could be questioned. Hence, an orientation of the inflation rate at the welfare optimal level seems favorable, particularly to maintain the long-term viability without major wealth redistribution. Moreover, the motivation beyond the pure coinbase reward for network members to stake needs to be strengthened, particularly when the coinbase reward is reduced or even a suppression of coin generation is intended. Otherwise, increased adoption and higher economic importance might result in a collapse. Nevertheless, one needs to consider that transaction fees might help mitigating this issue. While this approach

[77] In any stationary equilibrium with strictly positive prices, the security level of a PoS is rather high. In our quantitative setting we choose a necessary fork length of $\kappa = 20$ to observe a collapse of the network. Alleviating κ to levels which are still higher than 10, security levels would only marginaly decrease.

is partly addressed for Bitcoin-like networks,[78] their usefulness within PoS networks still needs to be evaluated.[79]

[78] See, e.g., Basu et al. (2023) and Huberman et al. (2021).

[79] The Ethereum network reduced and eventually even removed coinbase rewards. Instead, the validators are rewarded solely with transaction fees. In unreported result, we investigate the influence of transaction fees as in Subsection 4.4.2 with respect to the non-existence of coinbase rewards. In our calibrated setting, it is required that a 3% (10%) transaction fee still requires $\rho - 1$ to be as high 0.1395% (0.0312%) for a positive price equilibrium to exist.

Chapter 5

Climate Change, Energy Prices, and the Returns of Proof-of-Work vs. Proof-of-Stake Crypto Assets

5.1 Introduction

Since the introduction of Bitcoin in 2009, a huge number of crypto assets has emerged. As of the end of 2023, coinmarketcap.com reports more than 23,000 cryto assets with a total market capitalization of 1.5 trillion U.S. dollars. During this period of crypto-emergence, the severe threats associated with global warming grew obvious (NASA, 2024), which triggered a steady rise in climate change concerns among individuals and institutions (Ardia et al., 2023). This particularly fostered the discussion about the immense energy consumption of crypto assets (Kolbert, 2024; EIA, 2024). In September 2022, the Office of Science and Technology Policy consulting the White House published a report estimating that crypto assets consume an amount of electricity that falls within the range of 0.4% to 0.9% of total global electricity usage (OSTP, 2022).

Although often grouped together, it is important to note that different crypto assets consume different amounts of energy. The most significant differentiator with respect to energy intensiveness is the consensus mechanism, which is the crypto assets' fundamental building block, as it facilitates participants to have a homogeneous view of the ownership records. While many crypto assets employ Proof-of-Work (PoW) mechanisms, others rely on Proof-of-Stake (PoS). Within PoW, the miners, as the ones that update the ledger on a round-by-round basis, have to competitively solve a numerical problem where the winner in each round is permitted to append new transactions to the ledger. There is no analytical solution to this problem, requiring solutions to be found through trial and error, necessitating considerable computational power and leading to substantial energy consumption. The winning miner is compensated for their efforts with a mining reward, paid in the respective network's native cryptocurrency. On the other hand, in PoS, the minter chosen to update the ledger is selected randomly, with the selection probability generally proportional to a specific staking amount. Staked coins are locked from other uses, incurring opportunity costs for PoS (Eska et al., 2022a; Jermann, 2023). However, there is no severe energy cost associated with minting in PoS. As compensation, the minter receives a staking reward, also in the ledger's native cryptocurrency.

Since energy price dynamics are related to the business cycle (see, e.g., Kilian and Park, 2009; Ready, 2018), PoW-based crypto assets as assets with high energy consumption, could carry a risk premium over their PoS peers without such energy dependence (see, e.g., Dittmar et al., 2020). On the contrary, if the opportunity cost of staking co-move with the business cycle, PoS crypto assets could sustain a risk premium over their PoW peers without the opportunity cost problem. Within this chapter, we elaborate on the systematic relevance of the consensus mechanism from an empirical asset-pricing perspective by contrasting these two hypotheses. Carefully isolating the risk premium of PoW vs. PoS, we show that in the early part of our sample, i.e., prior to November 2020, the opportunity cost effect of PoS is dominant, whereas, for the most recent period, starting from December 2021, the energy reliance of PoW makes crypto assets using PoW for consensus finding the riskier assets. Our findings indicate that growing concerns about climate change accompanied by an increasing impact of energy prices on the marginal investor's decisions are major factors driving the shift towards assessing PoW crypto assets as riskier compared to PoS assets in the later part of our sample.

As a basis for our empirical analyses we compile a data set that integrates design-related as well as price- and trading-related characteristics of a broad cross-section of crypto assets. For the design-related characteristics, we extract tags and detailed descriptions of each crypto asset from coinmarketcap.com. Example tags are `Proof-of-Work` and `Proof-of-Stake` but also non-consensus related tags such as `Smart Contracts` or `Coin`. Coinmarketcap.com's maintenance of these tags is partially incomplete. In particular, it often occurs that tags are forgotten. Utilizing the descriptions and the subset of crypto assets with available tags, we train machine learning models to label the data with missing tags. For the resulting enriched set of tagged crypto assets, we subsequently develop design-related characteristics with respect to consensus, coin/token, privacy, and smart contracts. On top of these design-related characteristics, we also gather a variety of price- and trading-related characteristics such as the return, the market cap, and the trading volume of a crypto asset, thereby following the footsteps of Babiak and Bianchi (2021), Liu and Tsyvinski (2021), and Liu et al. (2022), who all show the price relevance of several price- and trading-related characteristics on the crypto market. Our analyses are conducted based on weekly returns for all crypto assets with a market capitalization above one million U.S. dollars from February 2016 until January 2023. Leveraging all collected characteristics, we estimate an asset pricing model for the crypto market employing an Instrumented Principal

Component Analysis (IPCA) as introduced by Kelly et al. (2019). Proceeding further based on the estimated asset pricing model, we follow the methodological idea of Müller et al. (2023) and analyze the systematic returns of a portfolio that is exposed only to consensus-related risk while maintaining zero exposure to all other design-, price- and trading-related characteristics. This approach is akin to constructing long-short portfolios going long PoW crypto assets and short PoS crypto assets, albeit with the important additional feature that the long-short portfolio has zero exposure to all other characteristics. The analysis is conducted in a rolling-window manner, leaving us with a time series of systematic risk premiums associated with PoW vs. PoS crypto assets.

Our results show that compensation for consensus risk in the crypto market is not constant, but varies over time. We identify periods of exuberant information arrival (PEIAs) in the crypto market during 2020-21 using the method proposed by Phillips et al. (2015). These PEIAs, which can be interpreted as the time when mainstream investors became aware of and entered the crypto market, appear to have caused a structural break that led to a shift in the risk preferences of the marginal investor. Prior to the PEIAs, PoS crypto assets were systematically riskier compared to PoW crypto assets, with a significantly negative consensus risk premium of approximately -9.1% per annum (p.a.). However, following the PEIAs, from December 2021 onwards, the sign of this premium reversed, with PoW crypto assets earning a premium of 20.1% p.a. over PoS crypto assets.

Examining the time series relationship between the consensus risk premium and variables linked to either the opportunity cost of PoS, the energy cost of PoW, or climate change concerns, we identify a significant negative relationship between changes in the Google Trends score for the term *Staking Crypto* during the pre-PEIAs period. The score serves as a proxy for the popularity of staking and, thereby, an indirect proxy for the opportunity cost associated with PoS. A high score indicates that staking is very popular, and hence, opportunity costs for staking are relatively low. This negative relationship between the score and the consensus premium is sensible, as PoS is the short leg in the consensus portfolio. Theory suggests that higher staking popularity, i.e., lower opportunity cost, should contemporaneously be positively associated with the systematic part of PoS returns, which is exactly what we observed during the pre-PEIAs period of our sample. In terms of economic significance, a positive one-standard-deviation shock to changes in the Google Trends score is associated with a decrease of the consensus risk premium by 5% of its standard deviation. During this pre-PEIAs period, there is no significant relationship between the consensus risk premium and variables linked to either the energy cost of PoW or climate change concerns.

In the post-PEIAs period, during which PoW carries a positive risk premium over PoS, we observe a significantly negative relationship between the consensus premium and changes in the Media Climate Change Concerns Index (MCCC) by Ardia et al. (2023), as well as between the premium and the returns of the U.S. oil price. No significant relationships are found with the other variables (returns of the Chinese coal price, the U.S. gas price, and the Google Trends score for *Staking Crypto*). This suggests that if climate change concerns are rising, the prices of the energy-intensive PoW crypto assets, the long leg of the consensus portfolio, systematically decrease over the post-PEIAs period, and a similar relationship holds for the oil price. The economic significance between a positive climate change concerns shock and the systematic consensus premium is -25%. In other words, when climate change concerns rise by one standard deviation, returns of PoW crypto assets fall by 25% of their standard deviation. For the relationship between the U.S. oil price and the systematic consensus premium, the economic significance is -11%.

To summarize, in the pre-PEIAs period, the opportunity cost of PoS crypto assets appears to be the primary driver of the consensus premium, with higher opportunity costs leading to less attractive staking and, consequently, lower systematic PoS returns. However, in the post-PEIAs period, the relationship between the opportunity cost of staking and the consensus premium is no longer observable, and instead, the premium is strongly related to climate change concerns and oil prices, with an increase in either one being associated with lower PoW returns. The shift from opportunity cost dominance to climate change dominance between the pre- and post-PEIAs periods suggests that a change in the marginal investor's preferences occurred during the PEIAs, which is the period where crypto broadly became mainstream. Prior to the PEIAs, the fragility of PoS networks might have been a relevant systematic concern, but this concern diminished as the asset class grew during the PEIAs. Simultaneously, during the PEIAs, a different group of investors with more sustainable preferences compared to the early crypto investors entered the market, resulting in a shift towards more environmentally conscious preferences of the marginal investor.

We further examine the risk premiums associated with other design-related characteristics. Specifically, we analyze coins vs. tokens, privacy featuring vs. non-privacy featuring crypto assets, as well as smart contract featuring vs. non-smart contract featuring crypto assets. With the exception of the coins vs. tokens characteristic, the systematic risk premiums of all the other characteristics also suffered a structural break during the PEIAs. Over our entire observation period, coins earn a significantly positive systematic risk premium over tokens at the magnitude of around 21.5% p.a. (PEIAs excluded). This premium is relatively stable across the pre- and post-PEIAs periods. However, privacy featuring crypto assets earn a systematic risk premium of 18.7% p.a. in the post-PEIAs period and no risk premium pre-PEIAs. This increase in the risk premium from pre to post-PEIAs could be related to increasing regulatory concerns of the marginal investor regarding privacy featuring crypto assets. Smart contract featuring crypto assets earn risk premiums of 19.0% p.a. over their respective peers during the pre-PEIAs period. Post-PEIAs, the premium drops to zero. The drop could be in line with an increased resilience of the crypto space in general during the PEIAs, which led to less vulnerability of smart contracts enabling various services and applications, particularly in the field of Decentralized Finance (DeFi).

Our findings demonstrate robustness across various specifications of the underlying asset pricing model. In detail, the number of principal components considered in the IPCA model does not change the consensus premium notably, albeit economic magnitudes slightly differ. This consistency underscores the resilience and reliability of our findings independent of the specific asset pricing model assumed.

Related Literature

This chapter first contributes to the literature that examines the influence of design features on the price behavior of crypto assets. In this strand, Eska et al. (2022b) and Hayes (2017) highlight that the network design of crypto assets impacts market capitalization and prices, respectively. In a similar vein, Chapter 3 of this dissertation relates network design to volatility. Wang and Vergne (2017) explores cross-sectional returns, demonstrating that innovation potential and supply growth drive returns. Meanwhile, Shams (2020) examines returns' co-movements and states that its structure cannot be solely explained by similarities in design-based characteristics. We extend this strand of literature by connecting design-related risks to investors' perceptions via expected returns. Thereby, we established an understanding of systematic risk associated with specific design-related crypto asset characteristics.

A design feature that has drawn significant attention is the consensus mechanism, which is of upmost importance for crypto asset networks to maintain their integrity. Particularly, PoW and PoS as the most prominent protocols stand out. In a general equilibrium model, Chapter 4 of this dissertation investigates the effects of certain design features within a PoS network and reveal distinctive impacts on network stability compared to the PoW model of Pagnotta (2022). The disparity between PoW and PoS stems from an inherent opportunity cost problem in PoS networks, as also addressed by Jermann (2023). Additional studies exploring differences between PoW- and PoS-based crypto assets include Chiu and Koeppl (2022), Vashchuk and Shuwar (2018), and John et al. (2021a), among others. We contribute to this literature by empirically determining the risk premium of a long-short portfolio going long in PoW-based crypto assets and short in PoS, thereby unveiling systematic risk perception of these two consensus protocol types.[80]

In a risk-neutral simulation study, Zhang and Chan (2020) demonstrate that PoW crypto assets, unlike PoS networks, are strongly related to energy prices due to higher energy consumption.

[80] Employing portfolio analysis, Sapkota and Grobys (2021b) do not find return differences between PoW- and PoS-based crypto assets.

The energy consumption and resulting environmental cost associated with mining in PoW-based crypto assets like Bitcoin is quantified within several papers (see, e.g., Gallersdörfer et al., 2020; Krause and Tolaymat, 2018; Mora et al., 2018). Hayes (2017) and Kristoufek (2020) outline a connection between production cost, measured through the energy consumption, and PoW-based crypto asset prices. Similarly, Wang et al. (2022) show a co-movement between the production cost and public environmental attention of crypto assets.[81] Clark et al. (2023) reverse the assumption that crypto assets create environmental cost and investigate the causal effect of several environmental variables on Bitcoin returns. Similarly, Corbet et al. (2021) investigate mining dynamics and price volatility of Bitcoin, demonstrating an effect on large electricity and utilities markets. We contribute to this literature by showing that energy intensive crypto assets carry a risk premium in recent times, which correlates with energy prices and environmental awareness. We such establish the view that crypto assets, which require high amounts of energy, are compensated for their higher energy consumption risk. Thus, this chapter contributes to the literature connecting crypto assets with energy prices and environmental cost.

Besides, this chapter aligns with another strand of literature, which focuses on cross-sectional asset pricing within the crypto market, reflecting its growing prominence. Numerous studies investigate return determinants from traditional financial markets and relate them to crypto assets (see, e.g., Borri, 2019; Cai and Zhao, 2024; Dunbar and Owusu-Amoako, 2022; Leong and Kwok, 2023; Liu et al., 2020; Liu et al., 2022; Zhang et al., 2021). Further papers contributing to this strand of literature analyze the influence of macroeconomic and regulatory events as well as geopolitical risk (Ciner et al., 2022; Koenraadt and Leung, 2024; Li and Miu, 2023; Long et al., 2022). Other studies further delve into crypto asset-specific network and production factors as potential determinants of cross-sectional returns (Bhambhwani et al., 2023; Borri et al., 2022; Liebi, 2022; Liu and Tsyvinski, 2021). Notably, Babiak and Bianchi (2021) apply an IPCA framework on the crypto market, building on the work of Kelly et al. (2019) in the equity market and Kelly et al. (2023) in the bond market. Albeit relying on a similar methodological approach to ours, the focus differs significantly. While Babiak and Bianchi (2021) aim at constructing a well performing factor model based on relevant characteristic from traditional financial markets, our work establishes connections between cross-sectional return differences, systematic risk, and, most importantly, design-related features. Thereby, this chapter adds a valuable dimension to the existing literature on cross-sectional asset pricing in the crypto market.

[81] Based on the equity market, various studies show that increased awareness for environmental issues among investors causes a demand for sustainable assets (see, e.g., Carpentier and Suret, 2015; El Ouadghiri et al., 2021; Gutsche and Ziegler, 2019). Combing the two markets, Naeem and Karim (2021) show that a combination of green financial assets and Bitcoin can provide hedging characteristics.

The remainder of this chapter is structured as follows. In Section 5.2, we introduce and describe our data set. In Section 5.3, we first establish our methodology by showing how to derive the consensus-related risk premium (Subsections 5.3.1 and 5.3.2). We then proceed to discuss the trajectory of the consensus premium in the time series and investigate its relation with proxies for the opportunity cost of PoS, climate change concerns, and energy prices (Subsection 5.3.3), followed by our examination of potential risk premiums of other design-related features (Subsection 5.3.4). In Section 5.4, we conclude.

5.2 Data

We require a rich set of variables to be able to estimate an asset pricing model for the crypto-market using an IPCA analyis (see Subsection 5.3.1) as a basis for our further analyses. To this end, we collect trading data as well as data concerning design-related features of crypto assets from coinmarketcap.com, a leading provider of crypto asset data. Our data set encompasses all crypto assets available during the period from February 12, 2016, to January 18, 2023. Albeit coinmarketcap.com provides data starting on April 29, 2013, we restrict our data set to this time horizon in order to include a sufficiently large cross-section. Note that our sample includes both listed and delisted crypto assets, thus alleviating any concerns regarding survivorship bias. Coinmarketcap.com aggregates trading data (e.g., closing price, trading volume, circulating supply) from a wide variety of exchanges, resulting in a comprehensive data set comprising 22,796 individual crypto assets over the analyzed time span. Additionally, coinmarketcap.com features a unique tagging system that facilitates the classification of crypto assets into various categories, such as stablecoins (e.g., Tether and USDC), crypto assets using PoW for consensus finding (e.g., Bitcoin and Dogecoin), or crypto assets featuring smart contracts (e.g., Ethereum and Cardano). Alongside the trading data outlined in Subsection 5.2.1, we incorporate variables derived from these tags into our study to proxy for the design-related features of the crypto assets as described in Subsection 5.2.2.

5.2.1 Trading Data and Common Characteristics

Coinmarketcap.com aggregates information on prices and trading volumes from 227 centralized exchanges (CEXs) and 430 decentralized exchanges (DEXs). The platform provides daily data on open, high, low, and close prices, market capitalization, and the 24-hour aggregated trading volume. We use these metrics and characteristics derived from this information for our subsequent risk-return analysis. Specifically, we calculate returns using close prices and subtract the respective risk-free rate derived from the one-month Treasury bill rate, to determine excess returns. To ensure the robustness of our study and the validity of our results, various filters are implemented. These filters aim to eliminate data errors, crypto assets tethered to other assets such as gold, highly illiquid crypto assets, and data points indicative of fake or suspicious trading activity. In detail, we apply the following filters on each crypto asset-day pair:

- We filter out all stablecoins and wrapped coins/tokens.
- We exclude crypto assets that exhibit a closing price of zero.
- As in Liu and Tsyvinski (2021) and Liu et al. (2022), we eliminate crypto assets with a market capitalization below 1,000,000 U.S. dollars. To tackle errors in the data, we furthermore ensure that the market capitalization does not exceed the one of Bitcoin, the network with the largest capitalization at any point in time.
- We calculate the daily market capitalization return and retain only those observations with a return below 500%. Pairs failing to meet this criterion are likely to exhibit erroneous changes in the coin supply.
- We introduce a dollar volume filter to remove trading days with negligible trading activity, as those are frequently associated with anomalously high or low returns. Specifically, any crypto asset-day pair with a volume below 10 U.S. dollars is eliminated.
- We calculate the ratio of traded volume to market capitalization (turnover) and exclude the observations with a ratio greater than 2.[82] Thereby, we filter out pairs of potentially artificial trading volume.

For an in-depth description of the data processing with filtering we refer the reader to Appendix D.1.1. After applying all filters, we are left with a panel of 3,910 crypto assets and a total of 2,123,600 daily observations.

Based on this sample, we derive a set of 25 trading data related characteristics, which we refer to as common characteristics, from information on price, volume, and market capitalization, solely. These characteristics encompass price- and size-related characteristics, volume-based characteristics, CAPM estimates, liquidity measures, past returns to capture momentum and reversal effects, as well as the age of the crypto assets to control for time-driven network effects. For a detailed list and definitions of the characteristics, see Table D.1 in Appendix D.1.1. All characteristics are calculated on a daily basis, first. As we run our analyses on a weekly grid, we then aggregate the daily data to weekly data similar to Liu and Tsyvinski (2021) and Liu et al. (2022). This means that we divide each year into 52 weeks, with the first seven days of a year constituting the first week of the year. Weeks 1 through 51 each consist of seven days, and the last week of each year includes the last 8 or 9 days of the year. We consider the characteristics as of the last day of each week. If this day is filtered out, no observation is recorded for this

[82] This filter was also incorporated by Bianchi et al. (2022) and Babiak and Bianchi (2021) who opted for a threshold level of 1 instead of 2 as we do here. Applying the stronger and less conservative threshold of Bianchi et al. (2022) yields qualitatively similar results.

crypto asset-week pair. Eventually, our filtered sample has 248,757 total observations (crypto asset-week pairs) and a cross-section of 3,126 crypto assets.

Panel A of Table 5.1 presents the summary statistics of the 25 common characteristics. The crypto assets in our sample have an average market capitalization of 628.23 million U.S. dollars. The market capitalization demonstrates a highly positive skewness, primarily driven by a few big networks like Bitcoin and Ethereum. Similarly, the weekly trading volumes comprises 385.43 million U.S. dollars, with 95% of the observations having a weekly volume below 361.78 million U.S. dollars. The weekly returns show a mean of 2.63% and a standard deviation of 24.64%. The average bid-ask spread is 4.28%.

5.2.2 Design-Related Characteristics

To classify crypto assets based on their specific designs, we employ the tagging system of coinmarketcap.com. We download the tags as of January 2023 from coinmarketcap.com.[83] While the tags are predominantly assigned and populated by coinmarketcap.com, network developers are also permitted to provide tags and information on predefined tags for their respective projects. For our classification, we consider tags from both sources. Specifically, we select the set of tags that are related to the design of the crypto assets. We allocate them into different groups related to the specific design-related feature they connect to and construct comprehensive labels out of these groups. In total, coinmarketcap.com includes a set of 512 different tags. The tagging system is well-maintained for larger, well-known crypto assets but is often incomplete for smaller, lesser-known ones. Alongside the tags, coinmarketcap.com provides textual descriptions for all crypto assets, enabling us to enhance the tagging system using machine learning-based classification algorithms applied to these descriptions. Typically, tagged crypto assets represent an incomplete set of positive examples (attribute is present), while untagged examples could be either positive or negative (attribute is not present). We use the descriptions of all crypto assets, along with the tagged part of the unfiltered data, and apply adequate machine-learning techniques to assign missing proxies to the untagged part of the data. The following paragraphs describe in detail how we obtain design-related labels forming the basis for our analysis.

[83] This means that we are not capturing any time-series variation of the tags. Occasionally, certain networks undergo structural changes with respect to design-related components. Generally, such events are very rare. Nevertheless, we correct for changes in design characteristics, e.g., for the transition of Ethereum from PoW to PoS, as far as we are aware of them. Even though we might not be aware of all relevant changes of the design-related characteristics in our data set, the impact of those on the results of our analysis should be negligible due to their rarity (see, e.g., data set of Eska et al., 2022b) and the equal-weighting of our long-short portfolios.

Table 5.1: Summary statistics

This table reports summary statistics of the characteristics used in our analysis. Panel A presents time-series averages of the cross-sectional mean, standard deviation, and various quantiles for the 25 common characteristics that can be calculated from data on price, volume, and market capitalization only. Descriptions of these characteristics can be found in Table D.1 in Appendix D.1.1. The statistics are derived from the final filtered data set on a weekly basis. Panel B displays the cross-sectional mean and standard deviation of the design-related characteristics, alongside their definitions and value sets.

Panel A: Common characteristics, 248,757 crypto asset-week pairs

Variable	Mean	Std.	Percentiles						
			1%	5%	25%	50%	75%	95%	99%
Price	77.34	1,016.28	0.00	0.00	0.02	0.13	0.80	23.47	587.33
MaxPrice (week)	91.04	1,241.03	0.00	0.00	0.03	0.16	0.99	28.77	678.58
MaxPrice (month)	114.96	1,676.39	0.00	0.00	0.04	0.21	1.28	36.19	817.75
ClosenessToHigh (3-month, %)	0.52	0.19	0.08	0.19	0.40	0.52	0.64	0.82	0.92
Mcap (10^6)	628.23	9,933.63	1.15	1.45	3.48	10.41	42.25	590.70	5,763.18
TradeVol (10^6)	385.43	5,220.97	0.00	0.02	0.33	2.25	17.22	361.78	4,966.41
AvgTradeVol (10^6)	53.87	729.72	0.00	0.00	0.06	0.39	2.87	51.50	692.07
TradeVolShock	-0.01	0.05	-0.19	-0.10	-0.03	−0.01	0.01	0.06	0.09
WeeklyTurnover	0.08	0.13	0.00	0.00	0.01	0.03	0.09	0.32	0.64
CAPM-β	0.87	0.81	-1.08	-0.19	0.50	0.86	1.22	1.96	3.08
CAPM-α	0.01	0.02	-0.03	-0.02	-0.01	0.00	0.01	0.04	0.09
Ivol (%)	8.34	7.88	1.52	2.56	4.36	6.34	9.63	20.56	40.15
AvgBidAskSpread (month, %)	4.28	4.32	0.87	1.32	2.18	3.13	4.77	10.92	21.23
WeeklyReturn (%)	2.63	24.64	-36.39	-22.27	-8.51	-0.99	8.38	37.56	85.81
MonthlyReturn (%)	15.48	66.01	-57.98	-39.25	-15.36	1.82	26.22	109.13	260.48
3-MonthReturn (%)	87.00	240.93	-75.82	-53.64	-13.50	27.93	98.37	401.90	970.84
LaggedWeeklyReturn (%)	2.81	25.80	-36.57	-22.45	-8.62	-1.05	8.45	38.34	89.90
Lagged2-WeekReturn (%)	7.24	42.70	-45.55	-29.24	-11.62	-0.42	14.48	63.81	157.54
MaxDailyReturn (month, %)	28.85	29.19	5.01	7.63	13.05	19.85	32.74	80.18	155.19
MaxWeeklyReturn (month, %)	55.91	73.09	4.82	10.46	21.95	35.73	61.48	158.87	360.33
MaxWeeklyReturn (3-month, %)	106.51	120.91	16.88	25.41	43.76	68.62	117.28	318.75	634.08
StdDailyReturn (month)	255.93	9,180.73	0.03	0.04	0.06	0.08	0.11	0.22	0.48
SkewnessDailyReturn (month)	0.57	1.03	-1.48	-0.79	-0.08	0.42	1.07	2.49	3.64
KurtosisDailyReturn (month)	5.25	3.41	2.11	2.41	3.17	4.11	5.98	12.29	18.67
Age (Days)	756.01	504.79	113.51	165.13	375.00	660.00	1,025.09	1,793.15	2,173.78

Panel B: Design-related characteristics, 3,126 crypto assets

Label variable	Mean	Std.	Value set	Definition
Consensus	-0.0096	0.4366	$[1, -1]$	$PoW - PoS$ (hybrids are included)
Coin	0.2710	0.4445	$\{0, 1\}$	$\mathbb{1}_{\text{Coin}}$
Privacy	0.0502	0.2184	$\{0, 1\}$	$\mathbb{1}_{\text{Privacy}}$
Smart Contract	0.3631	0.4810	$\{0, 1\}$	$\mathbb{1}_{\text{Smart Contract}}$

Consensus

To be able to explore the impact of consensus-related risk premiums, we introduce the *Consensus* characteristic, which characterizes crypto assets based on their consensus mechanisms on a unified scale between 0 and 1. PoS crypto assets like Cardano obtain a value of 0 in the consensus characteristic, PoW assets, e.g., Bitcoin, have a value of 1, and assets using hybrid consensus mechanisms receive a value between 0 and 1, depending on the closeness of the mechanism to either PoS or PoW. For details on the consensus classification of crypto assets and the construction of this characteristic we refer the reader to Appendix D.1.2.

As noted above, the tagging system providing the consensus identifiers is partially incomplete. Thus, we employ a neural network to enrich our data set with respect to the *Consensus* characteristic. In detail, we utilize our labeled subsample, i.e., the crypto assets for which respective tags are provided, alongside the descriptions of the crypto assets from coinmarketcap.com, to train a neural network in a first step. The neural network is then employed to estimate the variable *Consensus* for the unlabeled portion of our data set, in the second step. It is important to note that we only assign values to the unlabeled coins while unlabeled tokens are disregarded. This is due to the circumstance that tokens, in contrast to coins, inherit the values of their parent network. The details of this machine learning classification procedure are explained in detail in Appendix D.1.2.

Other Design-Related Characteristics

On top of the consensus mechanism, we also incorporate further design-related features of crypto assets in our analysis by, again, relying on the tagging system of coinmarketcap.com. First, we distinguish between coins and tokens and define the characteristic variable *Coin* to take a value of one if the crypto asset operates on its own blockchain (coin) or zero in the case of a token (operates on its parent network's ledger). Second, we construct a *Privacy* characteristic via aggregating the assets tagged with `Bulletproofs`, `Privacy`, or `Zero Knowledge Proofs`. Examples of privacy-focused crypto assets are *Monero*, *Zcash*, and *Firo*. Third, we incorporate a *Smart Contract* characteristic indicating whether or not a crypto asset features smart contracts. Such crypto assets provide an essential platform feature allowing for a wide variety of different applications, most notably in the field of Decentralized Finance (DeFi). For each of these three characteristics, we also enrich the data set using a machine learning methodology similar to the one we use for the consensus characteristic. Details on the characteristics and the specific machine learning procedures can be found in Appendix D.1.2.

As depicted in Panel B of Table 5.1, the mean consensus characteristic value is -0.01. This means that, on average, our final sample maintains a relative balance between PoW and PoS crypto assets. 27.1% of the crypto assets operate on their own blockchain, qualifying them as coins. About 5% of the networks in our sample prioritize anonymity, resembling privacy crypto assets. 36.3% of the crypto assets feature smart contracts.

5.3 Empirical Analysis of the Consensus Premium

Based on an Instrumented Principal Component Analysis (IPCA), this chapter identifies risk premiums associated with design-related characteristics of crypto assets, such as the consensus mechanism. This section first provides the basis for the empirical methodology. Having introduced the IPCA model and motivated the specifications for our main analysis in Subsection 5.3.1, Subsection 5.3.2 shows how to derive the consensus-related risk premiums. Further it motivates the consideration of so-called periods of exuberant information arrival (PEIAs). This provides a profound basis for the subsequent discussion of consensus risk and its relation with climate change concerns, energy prices, and staking health (Subsection 5.3.3). Eventually, Subsection 5.3.4 discloses risk premiums associated with further design-related characteristics.

5.3.1 Estimation of an Asset Pricing Model

We estimate an asset pricing model for the crypto market using an IPCA, as introduced by Kelly et al. (2019) (henceforth, KPS) for the equity market and also applied by Kelly et al. (2023) to the corporate bond market. IPCA identifies a set of latent asset pricing factors by applying a restricted principal component analysis. Formally, the core concept of IPCA is pinned down by the following two equations[84]:

$$r_{i,t+1} = \beta'_{i,t} f_{t+1} + \varepsilon_{i,t+1}, \tag{5.1}$$

with

$$\beta_{i,t} = z'_{i,t} \Gamma_\beta, \tag{5.2}$$

where $r_{i,t+1}$ represents the excess return of crypto asset i over week $t+1$. The loadings $\beta_{i,t}$ of asset i with respect to the risk factors f_{t+1} are calculated through the product of the characteristics vector $z'_{i,t}$ and the mapping matrix Γ_β. The characteristics vector $z'_{i,t}$ is an $(L \times 1)$ vector, stacking all of the crypto asset i's characteristics at the end of week t, including a constant (thus, $L = \#\text{characteristics} + 1$). All common characteristics are cross-sectionally ranked, demeaned, and scaled to range within $[-0.5, 0.5]$. The design-related characteristics are only scaled to the interval of $[-0.5, 0.5]$. Demeaning and ranking the design-related characteristics is renounced

[84] The version of IPCA characterized by Equations (5.1) and (5.2) is the restricted version where the intercept is set to zero. In Panel C of Table D.4 in Appendix D.2, we present results following the bootstrapping procedure proposed by KPS, demonstrating that for $K \geq 3$ the intercept in our setting is statistically indistinguishable from zero.

due to their discrete character. Γ_β is an $(L \times K)$ matrix, where K represents the number of estimated latent risk factors. Both Γ_β and the factors f_{t+1} are estimated concurrently using alternating least squares.

We use weekly excess returns and the 29 characteristics introduced in Section 5.2 (plus a constant) to apply the out-of-sample setting of KPS for models with $K = 4$ principal components. We utilize a rolling window of 3 years (156 weeks) of backward-looking data to finally obtain a time series of estimates for Γ_β and f_{t+1}. Our first out-of-sample test week is week 7, 2019, and our last one is week 2, 2023.[85] Note that each estimated factor in the vector f_{t+1} constitutes a portfolio of the assets used in the estimation. To prevent a look-ahead bias, the weights of these portfolios are fixed based on the in-sample estimation results, utilizing data up until t. To derive the $t + 1$ values of the factors, these weights are subsequently multiplied by the $t + 1$ returns of the assets.

To the best of our knowledge, we are the first to incorporate design-related features in an IPCA model for the crypto market. In Appendix D.2, we offer a detailed performance analysis of the IPCA models. By comparing IPCA models using only the common characteristics with those incorporating the full set of characteristics, we demonstrate that design-related features improve the model performance notably when judged by the out-of-sample relative pricing error, although this comes at the cost of slightly lower R^2s. Furthermore, increasing the number of principal components beyond $K = 4$ improves the model performance only very modestly, which is the reason we opt for $K = 4$ as our main specification.[86]

5.3.2 Derivation of the Consensus Premium

Based on the estimated asset pricing factors and the mappings for the crypto assets' risk exposures with respect to these factors, we now want to examine to which extent crypto asset returns are systematically driven by the consensus mechanism. To this end, we analyze the returns of a portfolio of crypto assets whose characteristic vector $z_{ls}^{Consensus}$ is uniformly zero, except for having a value of one at the position of the consensus characteristic. Such a portfolio has a maximum exposure in the consensus dimension and can be interpreted as a long-short portfolio going long PoW crypto assets and short PoS crypto assets. In contrast to a classical long-short portfolio, this portfolio has zero exposure to all other characteristics. Formally, we define the systematic part of this long-short portfolio return as our estimator for the systematic

[85] Even though the data of coinmarketcap.com starts in April 2013, the cross-section of our final, filtered data set of crypto assets is smaller than the number of characteristics considered in the IPCA until week 7, 2016. Estimation technique requires that the number of crypto assets is sufficiently large for the whole estimation window. Consequently, the initial estimation period is from week 7, 2016, to week 6, 2019, leading to the first out-of-sample test week in week 7, 2019.

[86] We show in Appendix D.5.1 the robustness of our results when using various different numbers of principal components instead.

consensus premium

$$sp_t^{Consensus} = z_{ls}^{Consensus'} \widehat{\Gamma}_{\beta,t-1} \widehat{f}_t, \tag{5.3}$$

where t corresponds to the out-of-sample test week. Since we estimate the IPCA model in a rolling window manner, we can examine the evolution of these systematic risk premiums over time.

It is important to emphasize that Equation (5.3) represents a realized return. Our intention is to use this realized return as an estimator for expected returns, i.e., as an estimator for the systematic consensus premium. As Elton (1999) points out, using realized returns as an unbiased estimator for expected returns relies on the assumption that information surprises cancel out over the estimation period. A prominent and recent example that demonstrates violations of this assumption leading to biased results is the examination of the Greenium, the expected return of green versus brown assets, during the 2010s, highlighted by Pástor et al. (2022). The authors demonstrate that naively assuming information surprises for green offset those for brown stocks between 2010 and 2020 leads to the conclusion that green stocks are riskier compared to brown ones. However, accurately correcting for unexpected information arrival, the results indicate the opposite. Brown stocks are riskier than green stocks, and consequently, brown stocks have higher expected returns.

Therefore, particularly given our case of a short sample for the crypto market, drawing conclusions about the systematic consensus premium based on Equation (5.3) must be handled with great care. By simply adopting the naive approach of estimating expected returns via realized returns, we would implicitly assume that unexpected news for PoW and PoS crypto assets cancels out during our examination period. This assumption might be problematic as the literature documents that the crypto market exhibited periods of exuberant information arrival within our sample period (Bouri et al., 2019b; Corbet et al., 2018; Geuder et al., 2019; Hafner, 2020). Following this literature, we apply the methodology of Phillips et al. (2015) to the time series of the value-weighted crypto market index constructed from our final data set and identify two periods of exuberant information arrival (PEIAs):

(i) from October 13, 2020 (week 41) to May 20, 2021 (week 20) and

(ii) from October 7, 2021 (week 40) to December 2, 2021 (week 48).

The procedure is explained in detail in Appendix D.3.

The two identified PEIAs are close to each other, with only a gap of 19 weeks in between them. Notice that the timeframe from the beginning of the first PEIA in October 2020 to the end of the second PEIA in December 2021 can be viewed as a period when crypto assetsy became mainstream and attracted many new investors. In addition to the asymmetric arrival of new information, the fact that the ecosystem potentially underwent structural changes during our sample period raises a second concern regarding the link between realized returns and expected returns. Such structural changes could have an impact on (i) the systematic risk exposure of PoW vs. PoS assets as well as (ii) the properties of the stochastic discount factor. To understand this more clearly, keep in mind that before this period, the crypto asset market was primarily dominated by tech-savvy enthusiasts. However, during the PEIAs, many new types of investors entered the crypto asset space. This surge in popularity, along with the expanding user base, might have altered the properties of the underlying decentralized networks as well as the preferences of the marginal investor simultaneously.

To rule out any potential biasing effects stemming from the PEIAs period and to potentially allow for variation in the underlying properties of the ecosystem, when examining the results of our risk premium analysis in the following, we focus on the subsamples of the pre-PEIAs period (before the first PEIA) as well as on the post-PEIAs period (after the second PEIA) separately.

5.3.3 Consensus Risk Premium over Time

Before examining the results, we want to explain in detail the economic arguments behind the two competing hypotheses regarding the sign of the consensus premium outlined in the introduction. The opportunity cost hypothesis originates from a PoS network's dependence on stakeholders staking the network's native coins, to enable secure transaction processing. Staked coins are refrained from other usage, which introduces an opportunity cost. The impact of the opportunity cost is examined in the theoretical model of Chapter 4, where it is shown that the loss of transaction opportunities due to staked PoS coins negatively impacts the staking incentive, diminishing network security and affecting the overall vulnerability of the network.[87] This opportunity cost problem is only restricted to PoS but not to PoW and thus, if the opportunity cost of staking co-moves with the business cycle, PoS crypto assets should sustain a risk premium over their PoW peers. On the contrary, the energy dependence hypothesis is derived from the fact that PoW networks consume significantly more energy compared to PoS, as the PoW mechanism requires miners to numerically solve a mathematical problem in order to process transactions. Given that energy price dynamics are linked to the business cycle (see, e.g., Kilian and Park, 2009; Ready, 2018), PoW assets should carry a systematic risk premium over PoS peers without such energy dependence (see, e.g., Dittmar et al., 2020).

Against this background, Figure 5.1 illustrates the evolution of the consensus risk premium over time. While we observe a negative premium prior to the shaded PEIA periods, the premium reverses its sign after the PEIAs. Based on the trajectory of the premium, it becomes obvious

[87] This opportunity cost problem is also addressed in Jermann (2023). In his model, however, prices are not directly linked with security and their interplay is disregarded.

that the PEIAs introduce a notable structural break in the time-series. The first row of Table 5.2 shows that pre-PEIAs the consensus risk premium has an average value of -9.13% p.a. with a t-statistic of -4.54. This is in line with the opportunity cost hypothesis, as PoS is short in the consensus portfolio. In recent times, for the period starting after the second PEIA, the associated risk premium turns positive to 20.14% p.a. with a t-statistic of 9.54. As PoW is long in the consensus portfolio, the latter is in line with the energy dependence hypothesis. Additionally, the downward correction of PoW prices relative to PoS during the PEIAs is directionally in line with the dynamics of the risk premium changing its sign from negative pre-PEIAs to positive post-PEIAs. As a whole, the results can be interpreted as if pre-PEIAs energy intensiveness of PoW is irrelevant for the consensus premium, and the opportunity cost hypothesis is dominating, which is in line with the negative consensus premium. Then, during the PEIAs, the preferences of the marginal investor adjust towards a higher relevance of energy intensiveness, which is in line with the negative returns of the consensus portfolio during that time. Finally, in the post-PEIAs period the energy intensiveness hypothesis dominates, which aligns with the positive consensus premium during this time. Note that this pattern is observable regardless of the number of principal components we use in the IPCA. We provide, for robustness, the results of this analysis and of all analyses following in the remainder of this chapter in Appendix D.5.1.

Figure 5.1: Risk premium of *Consensus*

This figure shows the annualized weekly *Consensus* risk premium over time. Intuitively, this is the systematic part of a portfolio that is long in PoW and short in PoS while having zero exposure to all other characteristics. The results are based on the restricted IPCA model with $K = 4$ latent factors. EWMA is the exponentially weighted moving average using the observations of the current week and the preceding 51 weeks. Gray-shaded areas belong to PEIA periods.

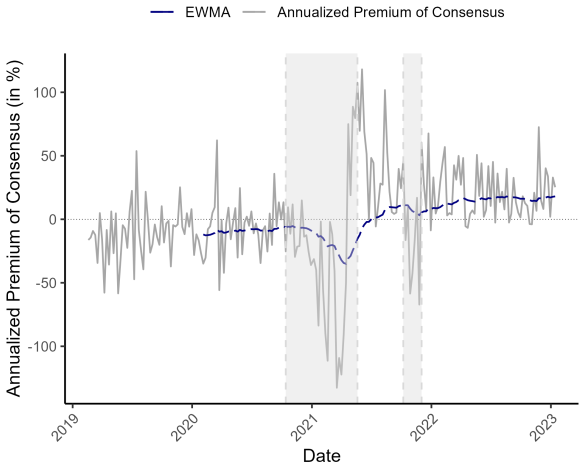


Table 5.2: Risk premiums of design-related characteristics

This table shows the average risk premiums of the design-related characteristics resulting from the restricted IPCA model with $K = 4$ latent factors. The values in columns (1) to (3) are obtained by taking the time series average from the risk premiums of the portfolios that are long in the respective characteristic and short in the inverse of the characteristic. All values are reported in % on an annualized basis. For (1), we consider the time prior to the first PEIA period, i.e., from week 7, 2019 until week 41, 2020. (2) refers to the sample after the second PEIA period, i.e., from week 48, 2021, until week 2, 2023. (3) includes the whole time horizon, i.e., from week 7, 2019 until week 2, 2023. Newey and West (1987) adjusted t-statistics for the null hypothesis that the given value is equal to zero are given in parentheses. Column (4) reports the test statistics t of Welch's t-tests under the null hypothesis that the sample means of (1) and (2) are equal. * and ** indicate statistical significance at the 5% and 1% level, respectively.

Characteristic	Annualized systematic risk premium in %			(4) Welch's t-test
	(1) Pre-PEIAs	(2) Post-PEIAs	(3) Whole sample	
Consensus	-9.13 (-4.54)**	20.14 (9.54)**	1.38 (0.26)	-8.43**
Coin	15.56 (6.83)**	27.31 (7.36)**	13.33 (2.60)*	-2.63**
Privacy	-3.56 (-0.46)	18.73 (5.32)**	21.39 (2.46)*	-2.66**
Smart Contract	18.95 (7.87)**	-3.62 (-1.16)	18.12 (3.14)**	5.42**

Dissecting the consensus premium

In the previous section, we have demonstrated that the consensus premium shifts from negative in the pre-PEIAs period to positive in the post-PEIAs period, indicating that PoS is riskier before the PEIAs and PoW is riskier afterwards. Generally, this is in line with the narrative that the energy intensiveness of PoW crypto assets became a more dominating part of investors' preferences post-PEIAs, whereas the opportunity cost associated with PoS might have been the more relevant factor pre-PEIAs. In this section, we explore the factors driving the trajectory of the consensus premium in the pre- and post-PEIAs periods to elaborate on whether or not this narrative makes sense. Our analysis asses the contemporaneous relationship between the systematic returns of the consensus portfolio and proxies for climate change concerns, energy prices, and the opportunity cost of staking. The intuition behind this approach is that changes in expected returns affect today's prices. If expected returns increase, today's prices decrease, and vice versa.

If staking becomes less attractive due to higher opportunity costs, PoS networks become more vulnerable and, therefore, riskier. Hence, contemporaneously, a rise in opportunity costs should be associated with declining PoS prices during this period. Recalling that PoS is in the short leg of the consensus portfolio, we expect a positive relationship between the return of the consensus portfolio and opportunity cost for staking in the pre-PEIAs period. For the post-PEIAs period, we particularly expect to observe correlations between changes in climate change concerns and changes in energy prices with the returns of the consensus portfolio. According to our hypothesis, rising climate change concerns and energy prices alike decrease the utility of PoW crypto assets for the marginal investor in the post-PEIAs period. As PoW is in the long leg of the systematic consensus portfolio, we expect a negative relationship between these two variables and the systematic consensus premium contemporaneously.

Before we can check for these correlations in the two subperiods, we first need to introduce proxies for the different measures of interest, including some potentially confounding variables. As our proxy for climate change concerns, we utilize the Media Climate Change Concerns Index (MCCC) by Ardia et al. (2023). This index assesses climate change concerns based on newspaper articles from major U.S. newspapers and newswires, measured daily. We use the seven-day moving average of this index for our weekly analysis. Note that the MCCC index is available only up to August 2022. To extend it up to January 2023, we consider the Google Trends scores for `climate risk` and employ a regression model. For a detailed explanation of the extension procedure, we refer the reader to Appendix D.4.

The incorporation of energy costs associated with PoW crypto assets requires us to consider the global distribution of miners. Although detailed information about the locations of miners is generally scarce, the Bitcoin mining map by the Cambridge Centre for Alternative Finance provides a time series of each country's share in the Bitcoin hash rate serving us as an indicator for the general hash rate distribution of all PoW crypto assets. This data indicates a significant concentration of mining power in a few countries. Prior to the mining ban in May 2021, China was the primary domicile of Bitcoin miners, with a hash rate share well above 50%. Following the ban, there has been a significant shift towards the U.S. As China's electricity generation is heavily reliant on coal, we use the generic 1st Zhengzhou thermal coal (ZCE) future converted to U.S. dollars (denoted as *Coal*) as our first proxy for energy costs. In the U.S., natural gas is the main energy source for electricity generation, prompting our second proxy, the generic 1st futures of natural gas (Henry Hub) in the U.S. (denoted as *Gas*). Given that miners in the U.S. frequently utilize flare gas from oil drilling for mining (see, e.g., Sigalos, 2022), we introduce a third energy cost proxy, the generic 1st futures of crude oil (WTI) in the U.S. (denoted as *Oil*).[88]

To investigate the opportunity cost hypothesis, we incorporate a proxy for the opportunity cost of staking in our analysis. Specifically, we utilize the Google Trends score for the term `Staking Crypto` (denoted as *GT Staking Crypto*), which measures the popularity of staking. Since high popularity of staking suggests lower opportunity costs and vice versa, it is important to have

[88] The time series of the generic 1st Zhengzhou thermal coal future (ticker: TRC1 Comdty), the CNY/USD rate (ticker: CNY Curncy), the generic 1st futures of natural gas (ticker: NG1 Comdty), and the generic 1st futures of oil (ticker: CL1 Comdty) source from Bloomberg. The ZCE coal, Henry Hub natural gas, and WTI crude oil are the most quoted products in these commodity classes. Furthermore, the futures used to proxy for energy cost on the Chinese, i.e., thermal coal (ZCE), and the U.S. market, i.e., natural gas (Henry Hub) and crude oil (WTI), are the most liquid futures on the respective products.

in mind that this is an inverse proxy for the opportunity cost of staking.

In addition to the aforementioned variables of interest, we integrate a set of control variables into our analysis. First, it is crucial to understand that the expenses associated with mining in PoW networks are influenced not only by energy costs but also by the amount of energy consumed during the mining process. In a PoW network, the total hash rate is a proxy for the total computational power allocated to mining activities and thus mirrors the actual electricity consumption of the respective network. Due to the lack of precise energy consumption data for each of the 282 PoW crypto assets included in our data set, we employ the hash rate of Bitcoin (*Hashrate*) as a proxy. Second, while miners and minters are compensated in the crypto assets they mine or mint, their energy expenditures or opportunity costs are settled or measured in fiat currencies. Therefore, the price of these crypto assets in U.S. dollars is also considered to capture their cost/reward relationship accurately.[89] For this purpose, we utilize both an equal-weighted PoW U.S. dollar basket price (*PoW Basket*) and an equal-weighted PoS U.S. dollar basket price (*PoS Basket*) as control variables. These basket prices represent a one-dollar investment distributed equally across all PoW or PoS crypto assets in our sample, respectively. It is noteworthy that these two baskets differ from the long and short legs of $sp^{Consensus}$, as the long and the short leg of $sp^{Consensus}$ both maintain nonzero exposure to all characteristics beyond consensus.

Equipped with the above-introduced proxies, we can now analyze whether it makes sense to argue that the consensus premium was driven by opportunity cost pre-PEIAs and climate change concerns post-PEIAs. To this end, we estimate the following regression model:

$$\begin{aligned} sp_t^{Consensus} = {} & \alpha + \beta_{MCCC} \cdot r_t^{MCCC} + \beta_{Coal} \cdot r_t^{Coal} + \beta_{Gas} \cdot r_t^{Gas} + \beta_{Oil} \cdot r_t^{Oil} + \\ & \beta_{GT\ Staking\ Crypto} \cdot r_t^{GT\ Staking\ Crypto} + \beta_{Hashrate} \cdot r_t^{Hashrate} + \\ & \beta_{PoW\ Basket} \cdot r_t^{PoW\ Basket} + \beta_{PoS\ Basket} \cdot r_t^{PoS\ Basket} + \epsilon_t \end{aligned} \tag{5.4}$$

with standardized relative weekly net returns r^{Coal}, r^{Gas}, r^{Oil}, $r^{PoW\ Basket}$, $r^{PoS\ Basket}$, and standardized percentage changes r^{MCCC}, $r^{GT\ Staking\ Crypto}$, $r^{Hashrate}$. We standardize by dividing the respective values through their in-sample standard deviation. The dependent variable $sp^{Consensus}$ is standardized as well. Hence, beta estimates indicate by which fraction of a standard deviation the consensus premium changes if a right-hand side variable is upward shocked by one standard deviation.

Before examining the results, let us briefly summarize the expected signs for the betas that align with our narrative of a dominating opportunity cost pre-PEIAs and a dominating energy intensiveness post-PEIAs. Pre-PEIAs, we expect to observe a relationship between staking

[89] One might debate the importance of accounting for the height of mining and minting rewards in terms of crypto assets. However, a negative trend in the rewards becomes negligible when focusing on first differences, which is why we can overlook this aspect.

popularity and the returns of the consensus portfolio. Specifically, we expect a negative beta for staking popularity for the pre-PEIAs period. Rising staking popularity implies lower opportunity costs, and lower opportunity costs contemporaneously align with higher returns of PoS assets, which are included in the short leg of the consensus portfolio. Post-PEIAs, we expect to observe a relationship between climate change concerns and energy prices with the returns of the consensus portfolio. A negative sign is expected for all of these betas during this period. Higher climate change concerns, as well as higher energy prices, align with lower prices of PoW assets, which are in the long leg of the consensus portfolio.

The results for the pre- and post-PEIAs periods separately are documented in columns (1) and (2) of Table 5.3. Beginning with the pre-PEIAs period in column (1), we find that among our variables of interest, only staking popularity exhibits a significant relationship with the consensus premium. The coefficient is significantly negative at -0.05 (t = -3.35). This suggests that during the pre-PEIAs period, reduced staking popularity is contemporaneously associated with lower PoS prices, which is in line with our expectations. The size of the coefficient yields an economic significance of -5%, i.e., a one standard deviation upward shock to relative changes in staking popularity relates to lower consensus premium by 5% of a standard deviation. Climate change concerns and energy prices do not seem to be related to the consensus premium during the pre-PEIAs period. This supports the hypothesis that in the pre-PEIAs era, the opportunity cost of PoS was the primary driver of the consensus premium.

Examining the results for the post-PEIAs period in column (2), the picture shifts significantly. We now identify a significant negative relationship between the consensus premium and both climate change concerns and oil prices, with coefficients of -0.25 (t = -3.17) and -0.11 (t = -2.32), respectively. This is in line with our expectations that, post-PEIAs, higher climate change concerns, as well as higher energy prices are contemporaneously associated with lower prices for energy-intensive PoW assets. The economic significance of the relationship between climate change concerns and the premium is particularly striking. A one standard deviation shock to relative changes in the MCCC index is associated with a 25% standard deviation decrease in consensus portfolio returns. For oil price changes the economic significance is lower, yet still notable at -11%. Interestingly, we observe that staking popularity does not exhibit a significant relationship with the premium during this period.

To complete the picture, column (3) documents the results for the entire sample period. Among the variables of interest, we only observe a significant relationship between staking popularity and the consensus premium at -0.09 (t = -4.22). However, given our assumption of structural changes in the ecosystem during the PEIAs, we hold no definitive expectations regarding the behavior of any of our variables of interest over the entire sample, and thus we refrain from drawing conclusions based on the whole sample results.

In summary, the results of this analysis support the narrative that there is a negative consensus premium pre-PEIAs due to the opportunity cost effect, which transitions to a positive consensus premium post-PEIAs that is driven by the hypothesis of energy intensiveness. The results indicate that pre-PEIAs, changes in the opportunity cost proxy are indeed related to the consensus premium in the hypothesized direction, whereas post-PEIAs, this relationship disappears. Conversely, post-PEIAs, changes in climate change concerns and changes in oil price are connected with the premium in the hypothesized direction, but these relationships are not observable in the pre-PEIAs period.

Table 5.3: Risk premium of *Consensus*, sustainability awareness, energy prices, and staking popularity

This table reports the results of multivariate regressions as in Equation (5.4). For (1), we consider the time prior to the first PEIA period, i.e., from week 7, 2019 until week 41, 2020. (2) refers to the sample after the second PEIA period, i.e., from week 48, 2021, until week 2, 2023. (3) includes the whole time horizon, i.e., from week 7, 2019 until week 2, 2023. Newey and West (1987) adjusted t-statistics are given in parentheses. * and ** indicate statistical significance at the 5% and 1% level, respectively.

	(1) Pre-PEIAs	(2) Post-PEIAs	(3) Whole sample
r^{MCCC}	-0.01	-0.25**	-0.09
	(-0.44)	(-3.17)	(-1.84)
r^{Coal}	0.12	0.005	0.04
	(1.73)	(0.09)	(0.76)
r^{Gas}	0.004	-0.02	-0.01
	(0.16)	(-0.50)	(-0.11)
r^{Oil}	0.02	-0.11*	0.00
	(1.22)	(-2.32)	(0.06)
$r^{GT\ Staking\ Crypto}$	-0.05**	0.43	-0.09**
	(-3.35)	(2.01)	(-4.44)
$r^{Hashrate}$	-0.02	-0.04	0.07
	(-0.70)	(-0.84)	(1.09)
$r^{PoW\ Basket}$	-0.27**	-0.08	-0.17*
	(-3.05)	(-0.67)	(-2.02)
$r^{PoS\ Basket}$	0.23**	-0.18	0.26**
	(2.78)	(-1.40)	(2.61)
Constant	-0.14*	0.62**	0.15
	(-2.52)	(8.99)	(1.03)
Obs.	85	58	203
Adj. R^2	0.56	0.10	0.17

5.3.4 Other Design-Related Risk Premiums

While Subsection 5.3.3 concentrates on the systematic risk premium of the consensus mechanism, our methodology, in principle, allows us to examine the systematic premium associated with each characteristic. Within this section, we want to have a brief look at the time series of the remaining three design-related characteristics in our analyses. Specifically, these are the risk premiums of the coin vs. token characteristic, the privacy vs. non-privacy characteristic as well as the smart contract vs. non-smart contract characteristic.

Coin vs. Token

Starting with the coin vs. token characteristic, the literature provides arguments that coins and tokens have different systematic risk profiles. Tokens are usually built on established platforms like Ethereum and, therefore, benefit from the security and reliability of these platforms. Often, as in the case of security tokens, they are even regulated. Therefore they should be less exposed to systemic risks compared to coins, which may be more exposed to speculative demand and less regulated environments. This inherent difference suggests that tokens could exhibit lower systematic risk than coins, due to both the stability of their parent networks and regulatory oversight (Alabi, 2017; Charfeddine et al., 2022; Gandal and Halaburda, 2016; Gandal et al., 2021; Nadler and Guo, 2020; Wu et al., 2018).

Figure 5.2a shows the trajectory of the coin vs. token premium over time, line two in Table 5.2 has the corresponding average values. Indeed we observe an overall significant positive premium of coins vs. tokens by a magnitude of 13.33% p.a. In the course of time, the coin over token systematic risk premium increased from 15.56% p.a. in the pre-PEIAs period to 27.31% p.a. in the post-PEIAs era, both at statistically significant levels. This is accompanied by a sharp decline in coin prices relative to tokens during the PEIAs, as shown in Figure 5.2a, which supports the notion that during the PEIAs, token-favorable information was released, which is in line with the increased systematic riskiness of coins compared to tokens from pre- to post-PEIAs.

Privacy vs. non-privacy

Public blockchains with the possibility to link real-world identities to public addresses bear the risk of completely revoking anonymity. In this view, some privacy-enhancing networks, such as Zcash, offer complete anonymity by making it technologically infeasible to track transaction information and the members themselves.[90] Narayanan et al. (2016), Pagnotta and Buraschi (2018), and Harvey and Branco-Illodo (2020) identify several channels motivating

[90] Sapkota and Grobys (2021a) state that privacy networks and non-privacy crypto assets are associated with two distinct asset market equilibria. Somewhat contrary, Ahmed et al. (2020) demonstrate that simple technical trading rules do not generate positive returns for privacy crypto assets, albeit ignoring systematic risk.

privacy crypto assets that can insure users against bad states of the world, which provides arguments for a negative systematic privacy premium. On the other hand, full anonymity opens doors for maleficent behavior and illegal activities like terrorist financing or money laundering (Europol, 2017), thereby drawing the attention of regulators. These concerns put pressure on widespread adoption and regulatory acceptance (Dupuis and Gleason, 2020; Houben and Snyers, 2018; Li et al., 2019), which might give a reason for a positive systematic privacy premium.[91]

Figure 5.2b shows the trajectory of the privacy premium over time, the corresponding average values are presented in the third line of Table 5.2. Overall the privacy premium is significantly positive at a value of 21.39% p.a. It is statistically indistinguishable from zero in the pre-PEIAs time span. Post-PEIAs, it rises to a statistically significant level of 18.73% p.a. By examining the trajectory of the premium, it seems as if during the first PEIA, information in favor of privacy-featuring crypto assets arrived, which is indicated by the positive peak in the time series during that time. Overall, the positive privacy risk premium rather supports the notion that regularity concerns dominate the actual privacy-protecting effects, especially for the post-PEIAs period. This finding aligns with the shift of the crypto asset user base towards mainstream investors which induces a change in the preference of the marginal investor towards regulatory certainty.

Smart contract vs. non-smart contract

With the rise of blockchains, many have appraised their groundbreaking potential for various applications and use cases. Among the most prominent use cases that have persisted beyond the initial hype are so-called decentralized finance (DeFi) applications and services. These aim to create financial systems in a decentralized and open manner, obviating the need for centralized intermediaries.[92] DeFi can deliver financial services in situations where centralized intermediaries face restrictions. A typical example of such a service is liquidity provision on exchanges. In traditional centralized financial markets, it is well-documented that liquidity tends to diminish during crisis periods (Hu et al., 2013; Næs et al., 2011; Schestag et al., 2016). According to intermediary asset pricing literature, in a market mediated by intermediaries, asset prices are heavily influenced by the health of these intermediaries (see, e.g., Haddad and Muir,

[91] Privacy crypto assets even face the risk of being banned by central authorities. Some authorities (Japanese Financial Security Agency, United States Secret Service) already banned the use of privacy crypto assets (see, e.g., Novy, 2018; Viglione, 2018; Wilmoth, 2018).

[92] According to Harvey et al. (2021), DeFi has the potential to address some inherent "flaws" in traditional finance by eliminating the need for centralized intermediation. Such flaws include inefficiency, centralized control, limited access, lack of interoperability, and opacity. Similarly, Schär (2021) suggests that DeFi could reinvent the financial industry, offering a more robust, open, and transparent infrastructure, provided challenges related to smart contract execution, operational security, dependencies on other networks, external data, and illicit activities are resolved. However, Makarov and Schoar (2022) adopt a more skeptical stance, noting that DeFi may introduce additional problems in areas such as tax enforcement, regulation, and financial malfeasance, potentially impacting the broader economy negatively.

2021; He et al., 2017), which is typically pro-cyclical. Thus, crypto assets in the field of DeFi exhibit resilience in adverse economic conditions and should display a negative systematic risk premium compared to crypto assets that are not related to DeFi services. An essential building block for DeFi applications are smart contracts. Thus, following the argumentation from above, smart contract featuring crypto assets should exhibit negative systematic risk premiums over non-smart contract featuring networks.[93]

Figure 5.2c and the averages in line four of Table 5.2 show that, generally, the results cannot support this hypothesis. The risk premium for crypto assets featuring smart contracts over those that are not is significantly positive at 18.12% p.a. for the whole sample. Although, this is mainly due to the pre-PEIAs period where the premium is at 18.95% p.a. Post-PEIAs, the privacy premium becomes indistinguishable from zero. Examining the trajectory of the premium reveals positive peaks during both PEIAs, which yields the arrival of smart contract-favoring information in that time. This is in line with the negative shift in the level of the smart contract premium from pre-PEIAs to post PEIAs.

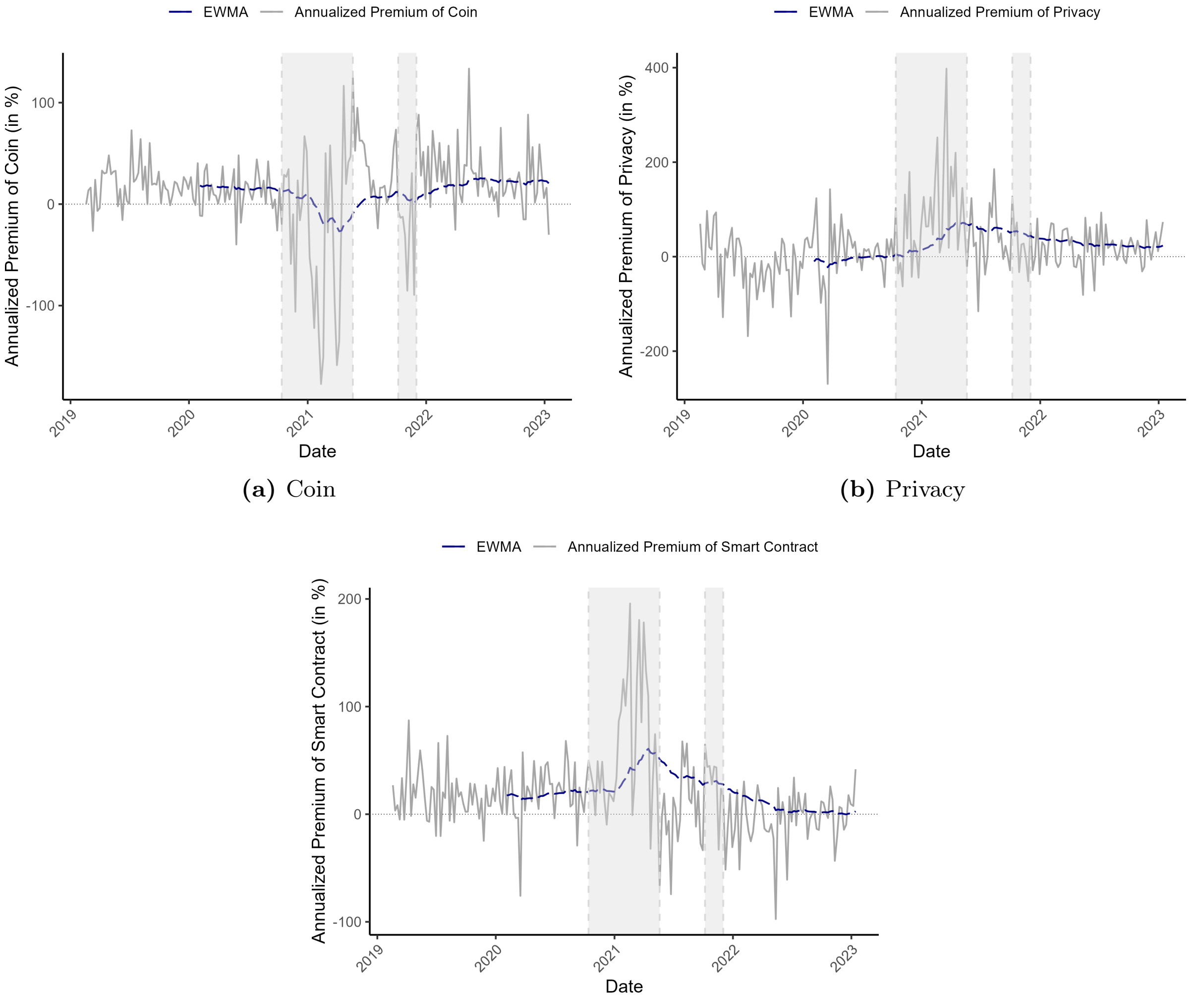
5.4 Conclusion

Using the IPCA framework by Kelly et al. (2019) and following the methodological idea of Müller et al. (2023), we are able to analyze the systematic returns associated with PoW over PoS. While in the early part of our sample, between the beginning of 2019 and October 2020, PoS earns a premium over PoW, our results show that the more energy-intensive PoW carries a risk premium over PoS for the period from December 2021 onwards. This finding for the latter part of our sample aligns with asset pricing theory, suggesting that energy-intensive assets such as PoW-based crypto assets are systematically riskier due to the cyclicality of energy prices (Dittmar et al., 2020; Kilian and Park, 2009; Ready, 2018). Using a multivariate regression approach, we relate the systematic part of the returns from a portfolio that is long PoW and short PoS with various proxies for energy prices, climate change concerns, and staking popularity. We find a significant negative covariation of this premium with climate change concerns as well as with the oil price for this latter period. Both of these covariations are unobservable in the early part of our sample during which PoS carries a positive risk premium over PoW. Interestingly, during this early period of our sample prior to the PEIAs, the risk premium co-moves with a proxy for staking popularity. Overall, our results align well with the narrative that at the beginning of our sample, PoS was systematically more risky compared to PoW, which seems to be linked to the opportunity cost problem associated with PoS. After

[93] Atzei et al. (2017), Schuster et al. (2020), and Milkau (2023) investigate smart contract risks and point towards several risk channels like coding errors and single points of failure. These sources of risk, however, are rather idiosyncratic and non-systematic.

Figure 5.2: Risk premiums of other design-related characteristics

This figure shows the annualized weekly risk premiums of the long-short portfolios managed by the design-related characteristics *Coin*, *Privacy*, and *Smart Contract*. These portfolios are long in the crypto assets with the specific characteristic and short the respective peers while the exposure to all other characteristics is zero. Baseline model is the restricted IPCA model with $K = 4$ latent factors. EWMA is the exponentially weighted moving average using the observations of the current week and the preceding 51 weeks. Gray-shaded areas belong to PEIA periods.



(a) Coin

(b) Privacy

(c) Smart Contract

the PEIAs, this shifted to PoW being systematically riskier than PoS, and the premium then is mostly linked to changes in climate change concerns as well as to oil-price returns. Taken together, this fits well with an alternation of the marginal investor's preferences during the PEIAs towards a higher concern regarding sustainability.

It is not unlikely that the preferences of the marginal investor at current times are closer to the ones from the period starting in December 2021, the post-PEIAs period of our analyses. Hence, the results for this period are particularly relevant for current market participants. Focusing on this period, the two most important results are (i) that PoW assets earn a systematic premium over PoS assets of roughly 20% per year, which by our interpretation is a compensation for the additional risk of PoW assets due to their energy intensiveness, and (ii) shocks in climate change concerns and energy prices are related to drops of PoW vs. PoS prices by economic significance of 25% and 11%, respectively.

To leverage our approach for the consensus mechanism, we also examine the systematic risk premiums for three other design-related features of crypto assets. Distinguishing between coins and tokens, we document that tokens are less risky compared to the average coin. Further, privacy-featuring networks earn a risk premium over non-privacy networks. This finding points towards a compensation for intervention risk posed by regulating authorities. Concerning smart contract-featuring crypto assets, our results show market participants initially perceived smart contract-featuring assets as systematically more risky. However, the premium vanished over the course of time.

Overall, we observe that an adjustment of the systematic risk premiums took place during periods of exuberant information arrival to the crypto market during the years 2020 and 2021. The adjustment in systematic risk perception of the marginal investor during the PEIAs indicates a shift in preferences, likely due to a change of crypto asset investors from tech-savvy enthusiasts to mainstream and institutional investors.

Chapter 6

Summary and Outlook

This dissertation discloses an asset pricing perspective on the design of cryptocurrencies. In its first part (Chapters 2 and 3), it relates the broad range of different design characteristics to market capitalization and volatility, thereby providing a more profound understanding of how the design affects the market outcome. Overall, it is shown that differences in the network designs are associated with diverging market outcomes.

Chapter 2 first introduces a novel taxonomy which allocates 47 design feature variables, predominantly binary, into six categories. Based on this taxonomy and a hand-collected sample of 79 cryptocurrencies, we analyze whether the design of cryptocurrencies helps to explain the huge cross-sectional variation in the market values of cryptocurrencies. While we find that forked network are less valuable, cryptocurrencies with an fee-independent reward scheme have higher market capitalizations. Further, non-anonymous cryptocurrencies have higher market capitalizations, possibly in expectation of regulatory approval of these networks. Apart from that, we find that deviations from the design of Bitcoin tend to be associated with lower valuation. Thus, even though Bitcoin may not be the most technologically advanced cryptocurrency, users and investors apparently value its design. Albeit our results reveal that certain design features affect the market valuation of cryptocurrencies, one needs to be aware of the circumstance that a large part of investors might not be aware of cross-sectional differences in the cryptocurrency design. Consequently, valuation might be partly driven by sole speculative demand as investors seek for the “new Bitcoin”. Due to the large cross-section of different cryptocurrencies and speculative demand being at random, this chapter nevertheless provides an indication of which cryptocurrencies design feature might predominate the cryptocurrency universe in the future. Our analysis, however, does not consider interaction effects between the single features. Thus, we encourage future research to incorporate interactions between different design features. Also, revisiting the results taking into account timely changes in investor structures, as described in Chapter 5, might open new perspectives on the influence of cryptocurrency design on market valuation.

In a similar vein, Chapter 3 introduces volatility measures on daily returns calculated from two distinct samples. They are then related to the design features introduced in Chapter 2. The results of the corresponding analysis indicate, inter alia, that older cryptocurrencies and networks that do not pass transactions fees and/or tips on to transaction verifiers are less volatile. In contrast, cryptocurrencies with mandatory transaction fees, the ones developed by private teams and those using (delegated) Proof-of-Stake as consensus mechanisms tend to be more volatile. The findings presented in this chapter help predicting the volatility of a cryptocurrency based on its design feature constellation, thereby providing assistance for developers deliberately aiming to design cryptocurrencies with low expected volatility. While this chapter analyzes the impact of individual design features, exploring interdependencies between design features could be a promising avenue for future research.

In the following parts, the focus of the dissertation shifts to one of the most essential design features of cryptocurrencies, the consensus protocols. While Proof-of-Work (PoW) algorithms like the one of Bitcoin are accompanied by excessive energy consumption, other protocols gained in importance over time. Most prominently, Proof-of-Stake (PoS) protocols have drawn more and more attention. Albeit the underlying economics of PoS networks are fairly different, many studies focus on solely PoW-like cryptocurrencies. Chapter 4 addresses this gap by introducing a valuation model for PoS cryptocurrencies. It reveals that PoS network have an inherent opportunity cost problem which introduces a higher degree of network instability to these networks. In particular, some design features such as the inflation rate are crucial determinants for extent network fragility. We show that transaction fees can help mitigating the collapse risk. While this approach is partly addressed for Bitcoin-like networks, the precise impact and its usefulness within PoS networks is an avenue for future research.

Building on the theoretical considerations of Chapter 4, Chapter 5 investigates how the opportunity cost problem transfers to the risk-return structure of PoS cryptocurrencies compared to their PoW counterparts. For the early sample, the consensus-related systematic risk premium reveals that PoS networks are systematically riskier than PoW cryptocurrencies supporting the theoretical model's outcome. From December 2021 onwards, the sign of the risk premium reverses and PoW earns a premium over PoS. This shift indicates that the perception of risk changed by the course of time towards a dominance of energy consumption risk and climate change concerns. This finding aligns with with asset pricing theory, suggesting that energy-intensive assets, such as PoW-based crypto assets, are systematically riskier due to the cyclicality of energy prices. In addition, Chapter 5 analyzes further design-related systematic risk premiums. Overall, adjustments of these systematic risk premiums took place during periods of exuberant information arrival to the crypto market – similar to the consensus premium. This points towards a change in investor structure and a potential increase in market efficiency, which can be revisited by future research in light of our results. Furthermore, by employing the methodology that isolates specific characteristic-related systematic risk premiums, theoretical assumptions, models, and abstract considerations about the cryptocurrency market can be evaluated – such as the impact of centralized (CEXs) vs. decentralized trading (DEXs).

Appendix A

Design and Valuation of Cryptocurrencies

This appendix includes complementary results to Chapter 2. Section A.1 includes the intra-group regressions' results and Section A.2 shows the results of the robustness analysis presented and discussed in Subsection 2.4.2.

A.1 Intra-Group Regressions Results from Main Analysis

Table A.1: Intra-group market capitalization regressions of Q4 2020

This table reports results of the cross-sectional intra-group regression of the average market capitalization in the fourth quarter of the year 2020 on the design feature variables.We control for multicollinearity and find that all variance inflation factors (VIF) are below 2.6. p-Values are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively.

	Market capitalization					
	(1)	(2)	(3)	(4)	(5)	(6)
Constant	0.406***	0.397***	0.323***	0.325**	0.270***	0.204***
	(0.000)	(0.000)	(0.003)	(0.011)	(0.000)	(0.001)
DeveloperNPO	-0.145					
	(0.224)					
DeveloperPrivate	-0.190*					
	(0.074)					
NoMajorityChanges	0.024					
	(0.772)					
CodeNonC	-0.025					
	(0.769)					
CodeNonPublic	-0.185					
	(0.397)					
Fork	-0.183**					
	(0.024)					
ConsensusPoSDPoS		-0.208**				
		(0.039)				
ConsensusOther		-0.150				
		(0.179)				
HashAge		-0.280*				
		(0.056)				
CurveNonECDSA		-0.022				
		(0.766)				
NoMaxSupply			-0.011			
			(0.899)			
SupplyCirculation			-0.0003			
			(0.917)			
Deflationary			0.058			
			(0.634)			
FixedSupply			-0.136			
			(0.166)			
RewardCoinbase			-0.118			
			(0.231)			
RewardInflation			-0.126			
			(0.184)			
BlockTimeAverage				-0.199		
				(0.206)		
TransactionFeeObligation				-0.015		
				(0.873)		
NoTipSpecialTreatment				0.030		
				(0.745)		
NoFeeTipForMinerForger				0.191*		
				(0.089)		
IntentionNonPayment					-0.032	
					(0.801)	
SmartContractSupport					-0.113	
					(0.341)	
UsageBeyondPayment					0.007	
					(0.931)	
LedgerStyleOther						0.161
						(0.248)
AccountingBalance						-0.037
						(0.622)
Anonymous						-0.111
						(0.179)
NonAnonymous						0.270
						(0.214)
Observations	68	68	68	59	68	68
R^{2}	0.109	0.089	0.077	0.078	0.047	0.073
Adjusted R^{2}	0.022	0.031	-0.014	0.009	0.003	0.014
F Statistic	1.248	1.533	0.845	1.138	1.060	1.245
	(df=6;61)	(df=4;63)	(df=6;61)	(df=4;54)	(df=3;64)	(df=4;63)

Table A.2: Intra-group discounted market capitalization regressions of Q4 2020

This table reports results of the cross-sectional intra-group regression of the average discounted market capitalization in the fourth quarter of the year 2020 on the design feature variables.We control for multicollinearity and find that all variance inflation factors (VIF) are below 2.6. p-values are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively.

	Discounted market capitalization					
	(1)	(2)	(3)	(4)	(5)	(6)
Constant	0.320***	0.202**	0.158	0.241**	0.116*	0.125**
	(0.001)	(0.033)	(0.116)	(0.038)	(0.066)	(0.026)
DeveloperNPO	-0.149					
	(0.163)					
DeveloperPrivate	-0.119					
	(0.209)					
NoMajorityChanges	0.015					
	(0.837)					
CodeNonC	0.037					
	(0.621)					
CodeNonPublic	-0.139					
	(0.476)					
Fork	-0.210***					
	(0.004)					
ConsensusPoSDPoS		0.018				
		(0.846)				
ConsensusOther		-0.066				
		(0.525)				
HashAge		-0.111				
		(0.415)				
CurveNonECDSA		-0.046				
		(0.510)				
NoMaxSupply			-0.001			
			(0.993)			
SupplyCirculation			0.0002			
			(0.927)			
Deflationary			0.007			
			(0.950)			
FixedSupply			-0.094			
			(0.306)			
RewardCoinbase			-0.014			
			(0.882)			
RewardInflation			0.054			
			(0.543)			
BlockTimeAverage				-0.150		
				(0.297)		
TransactionFeeObligation				-0.006		
				(0.948)		
NoTipSpecialTreatment				0.028		
				(0.740)		
NoFeeTipForMinerForger				0.210**		
				(0.042)		
IntentionNonPayment					0.089	
					(0.442)	
SmartContractSupport					-0.102	
					(0.349)	
UsageBeyondPayment					0.085	
					(0.245)	
LedgerStyleOther						-0.096
						(0.446)
AccountingBalance						0.057
						(0.396)
Anonymous						-0.056
						(0.456)
NonAnonymous						0.349*
						(0.078)
Observations	68	68	68	59	68	68
R^2	0.144	0.041	0.032	0.091	0.041	0.089
Adjusted R^2	0.060	-0.020	-0.064	0.024	-0.004	0.031
F Statistic	1.710	0.669	0.333	1.349	0.905	1.540
	(df=6;61)	(df=4;63)	(df=6;61)	(df=4;54)	(df=3;64)	(df=4;63)

A.2 Results of the Robustness Analysis

Table A.3: Market capitalization regression analysis of year 2020

This table reports results of the cross-sectional regression of the average market capitalization in the whole year 2020 on the design feature variables. Columns (1) - (6) shows the coefficients for the intra-group regressions. Models (7), (8), and (9) include the design feature variables with intra-group regression p-values below 0.1, 0.2, and 0.3, respectively. We control for multicollinearity and find that all variance inflation factors (VIF) in (1) - (7) are below 2.4 and below 4.43 in (8) and (9). Column (10) shows the results for the case that all design feature variable are included (max. VIF of 8.78). Standard errors are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively.

	Market capitalization									
	(1)	(2)	(3)	(4)	(5)	(6)	(7) $p < 0.1$	(8) $p < 0.2$	(9) $p < 0.3$	(10)
Constant	0.366***	0.373***	0.270**	0.321**	0.234***	0.172***	0.119	0.382**	0.497***	0.108
	(0.091)	(0.089)	(0.094)	(0.113)	(0.060)	(0.054)	(0.101)	(0.168)	(0.180)	(0.325)
DaysAge							0.516***	0.419**	0.282	0.655*
							(0.171)	(0.183)	(0.201)	(0.355)
DeveloperNPO	-0.150							-0.022	-0.029	-0.159
	(0.106)							(0.102)	(0.104)	(0.170)
DeveloperPrivate	-0.172*						-0.043	-0.080	-0.089	-0.235
	(0.094)						(0.064)	(0.097)	(0.099)	(0.152)
NoMajorityChanges	0.008									-0.037
	(0.074)									(0.108)
CodeNonC	-0.014									0.249*
	(0.076)									(0.123)
CodeNonPublic	-0.158									0.072
	(0.197)									(0.253)
Fork	-0.170**						-0.115*	-0.175**	-0.201***	-0.191*
	(0.071)						(0.061)	(0.067)	(0.068)	(0.101)
ConsensusPoSDPoS		-0.198**					-0.030	-0.103	-0.081	-0.133
		(0.088)					(0.076)	(0.125)	(0.126)	(0.173)
ConsensusOther		-0.142						-0.109	-0.134	0.009
		(0.098)						(0.128)	(0.132)	(0.187)
HashAge		-0.280**					-0.155	-0.205	-0.215	-0.041
		(0.130)					(0.110)	(0.138)	(0.147)	(0.233)
CurveNonECDSA		-0.031								-0.046
		(0.066)								(0.120)
NoMaxSupply			0.002							0.026
			(0.079)							(0.169)
SupplyCirculation			-0.0002							0.043
			(0.003)							(0.207)
Deflationary			0.047							0.034
			(0.111)							(0.158)
FixedSupply			-0.129					-0.021	-0.008	-0.033
			(0.088)					(0.083)	(0.087)	(0.148)
RewardCoinbase			-0.090							0.082
			(0.086)							(0.131)
RewardInflation			-0.103						0.008	0.233
			(0.084)						(0.081)	(0.171)
BlockTimeAverage				-0.202				-0.130	-0.113	-0.024
				(0.141)				(0.128)	(0.133)	(0.192)
TransactionFeeObligation				-0.029						-0.084
				(0.087)						(0.120)
NoTipSpecialTreatment				0.007						-0.056
				(0.081)						(0.101)
NoFeeTipForMinerForger				0.199*			0.090	0.177**	0.119	0.125
				(0.100)			(0.072)	(0.083)	(0.097)	(0.143)
IntentionNonPayment					-0.011					0.355
					(0.107)					(0.210)
SmartContractSupport					-0.121				-0.115	-0.433**
					(0.101)				(0.085)	(0.162)
UsageBeyondPayment					0.011					-0.039
					(0.070)					(0.117)
LedgerStyleOther						0.124			0.319	0.496
						(0.118)			(0.226)	(0.375)
AccountingBalance						-0.021				0.070
						(0.067)				(0.157)
Anonymous						-0.094			-0.003	-0.026
						(0.075)			(0.082)	(0.098)
NonAnonymous						0.187				0.405
						(0.198)				(0.285)
Observations	71	71	71	61	71	71	71	67	67	61
R^2	0.107	0.103	0.067	0.099	0.049	0.054	0.245	0.331	0.383	0.564
Adjusted R^2	0.023	0.048	-0.021	0.035	0.006	-0.003	0.174	0.212	0.218	0.183
F Statistic	1.279	1.887	0.763	1.542	1.146	0.948	3.452***	2.776***	2.310**	1.479
	(df=6;64)	(df=4;66)	(df=6;64)	(df=4;56)	(df=3;67)	(df=4;66)	(df=6;64)	(df=10;56)	(df=14;52)	(df=28;32)

Table A.4: LASSO variable selection for market capitalization regression of year 2020

This table provides statistics for the variable selection process when applying LASSO with cross-validation using the average market capitalization in the whole year 2020 as the dependent variable. Column (1) reports the percentage of cases in which a variable is selected by LASSO while (2) and (3) indicate the related sign of the coefficient. Column (4) reports the average of the parameter estimate indicating the economic significance. Deviance is defined as $2\,(loglike_{sat} - loglike)$, where $loglike_{sat}$ is the log-likelihood for the saturated model. Null deviance is defined to be $2\,(loglike_{sat} - NULL)$ with $NULL$ referring to the intercept model.

	Market capitalization			
	(1) Included	(2) Positive	(3) Negative	(4) ∅ coefficent
Constant	100%	100%	0%	0.162
DaysAge	51.16%	100%	0%	0.082
DeveloperNPO	0%	-	-	0
DeveloperPrivate	13.27%	0%	100%	-0.002
NoMajorityChanges	0%	-	-	0
CodeNonC	1.78%	100%	0%	0.000
CodeNonPublic	0%	-	-	0
Fork	16.93%	0%	100%	-0.015
ConsensusPoSDPoS	0.27%	0%	100%	-0.000
ConsensusOther	0%	-	-	0
HashAge	14.95%	0%	100%	-0.007
CurveNonECDSA	0%	-	-	0
NoMaxSupply	0%	-	-	0
SupplyCirculation	0%	-	-	0
Deflationary	0%	-	-	0
FixedSupply	1.78%	0%	100%	-0.000
RewardCoinbase	0%	-	-	0
RewardInflation	0%			0
BlockTimeAverage	10.82%	0%	100%	-0.002
TransactionFeeObligation	0.01%	0%	100%	-0.000
NoTipSpecialTreatment	0%	-	-	0
NoFeeTipForMinerForger	16.93%	100%	0%	0.009
IntentionNonPayment	0%	-	-	0
SmartContractSupport	16.03%	0%	100%	-0.010
UsageBeyondPayment	0%	-	-	0
LedgerStyleOther	19.80%	100%	0%	0.024
AccountingBalance	0.015%	100%	0%	0.000
Anonymous	14.95%	0%	100%	-0.002
NonAnonymous	14.31%	100%	0%	0.009
∅ Observations			61	
∅ Fraction of (null) deviance explained			0.062	

Table A.5: Discounted market capitalization regression analysis of year 2020

This table reports results of the cross-sectional regression of the average market capitalization in the whole year 2020 on the design feature variables. Columns (1) - (6) shows the coefficients for the intra-group regressions. Models (7), (8), and (9) include the design feature variables with intra-group regression p-values below 0.1, 0.2, and 0.3, respectively. We control for multicollinearity and find that all variance inflation factors (VIF) in (1) - (9) are below 2.4. Column (10) shows the results for the case that all design feature variable are included (max. VIF of 8.78). Standard errors are given in parentheses. *, **, and *** indicate statistical significance at the 10%, 5% and 1% level, respectively.

	Discounted market capitalization									
	(1)	(2)	(3)	(4)	(5)	(6)	(7) $p < 0.1$	(8) $p < 0.2$	(9) $p < 0.3$	(10)
Constant	0.324***	0.218**	0.155	0.283*	0.127**	0.129**	0.203***	0.361***	0.527***	0.205
	(0.095)	(0.096)	(0.101)	(0.120)	(0.063)	(0.056)	(0.067)	(0.110)	(0.153)	(0.383)
DaysAge							0.028	-0.053	-0.078	0.050
							(0.167)	(0.173)	(0.179)	(0.419)
DeveloperNPO	-0.164							-0.170*	-0.116	-0.214
	(0.111)							(0.098)	(0.109)	(0.200)
DeveloperPrivate	-0.133							-0.149	-0.165*	-0.329*
	(0.098)							(0.091)	(0.097)	(0.180)
NoMajorityChanges	0.010									0.039
	(0.077)									(0.128)
CodeNonC	0.058									0.194
	(0.079)									(0.144)
CodeNonPublic	-0.109									-0.053
	(0.205)									(0.298)
Fork	-0.198***						-0.159**	-0.206***	-0.225***	-0.296**
	(0.074)						(0.066)	(0.070)	(0.072)	(0.119)
ConsensusPoSDPoS		0.018								-0.012
		(0.096)								(0.204)
ConsensusOther		-0.063								0.108
		(0.106)								(0.221)
HashAge		-0.111								-0.010
		(0.141)								(0.275)
CurveNonECDSA		-0.052								0.039
		(0.072)								(0.141)
NoMaxSupply			-0.004							0.061
			(0.085)							(0.199)
SupplyCirculation			0.0001							0.178
			(0.003)							(0.244)
Deflationary			-0.0001							0.004
			(0.119)							(0.187)
FixedSupply			-0.089							-0.021
			(0.094)							(0.175)
RewardCoinbase			0.010							0.209
			(0.093)							(0.154)
RewardInflation			0.060							0.276
			(0.089)							(0.201)
BlockTimeAverage				-0.160					-0.219*	-0.069
				(0.150)					(0.131)	(0.226)
TransactionFeeObligation				-0.019						-0.083
				(0.092)						(0.142)
NoTipSpecialTreatment				0.014						-0.115
				(0.086)						(0.118)
NoFeeTipForMinerForger				0.201*			0.045	0.068	0.160*	0.240
				(0.106)			(0.078)	(0.079)	(0.088)	(0.168)
IntentionNonPayment					0.067					0.137
					(0.113)					(0.247)
SmartContractSupport					-0.078					-0.269
					(0.107)					(0.191)
UsageBeyondPayment					0.090				0.060	0.031
					(0.074)				(0.076)	(0.138)
LedgerStyleOther						-0.125				0.036
						(0.122)				(0.442)
AccountingBalance						0.067				0.046
						(0.069)				(0.185)
Anonymous						-0.030				0.012
						(0.077)				(0.116)
NonAnonymous						0.355*	0.402**	0.423**	0.363*	0.521
						(0.204)	(0.198)	(0.196)	(0.199)	(0.336)
Observations	71	71	71	61	71	71	71	71	67	61
R^2	0.123	0.038	0.028	0.078	0.033	0.083	0.146	0.189	0.263	0.452
Adjusted R^2	0.041	-0.020	-0.063	0.012	-0.010	0.027	0.094	0.113	0.161	-0.027
F Statistic	1.493	0.651	0.306	1.188	0.764	1.485	2.810**	2.482**	2.587**	0.943
	(df=6;64)	(df=4;66)	(df=6;64)	(d =4;56)	(df=3;67)	(df=4;66)	(df=4;66)	(df=6;64)	(df=8;58)	(df=28;32)

Table A.6: LASSO variable selection for discounted market capitalization regression of year 2020

This table provides statistics for the variable selection process when applying LASSO with cross-validation using the average discounted market capitalization in the whole year 2020 as the dependent variable. Column (1) reports the percentage of cases in which a variable is selected by LASSO while (2) and (3) indicate the related sign of the coefficient. Column (4) reports the average of the parameter estimate indicating the economic significance. Deviance is defined as $2\,(loglike_{sat} - loglike)$, where $loglike_{sat}$ is the log-likelihood for the saturated model. Null deviance is defined to be $2\,(loglike_{sat} - NULL)$ with $NULL$ referring to the intercept model.

	Discounted market capitalization			
	(1) Included	(2) Positive	(3) Negative	(4) ∅ coefficent
Constant	100%	100%	0%	0.194
DaysAge	0%	-	-	0
DeveloperNPO	0%	-	-	0
DeveloperPrivate	0%	-	-	0
MajorityChanges	0%	-	-	0
CodeNonC	0%	-	-	0
CodePublic	0%	-	-	0
Fork	65.01%	0%	100%	-0.035
ConsensusPoSDPoS	0%	-	-	0
ConsensusOther	0%	-	-	0
HashAge	0%	-	-	0
CurveNonECDSA	0%	-	-	0
MaxSupply	0%	-	-	0
SupplyCirculation	0%	-	-	0
Deflationary	0%	-	-	0
FixedSupply	0%	-	-	0
RewardCoinbase	0%	-	-	0
RewardAlternative	0%			0
BlockTimeAverage	0%	-	-	0
TransactionFeeObligation	0%	-	-	0
TipSpecialTreatment	0%	-	-	0
NoFeeTipForMinerForger	14.55%	100%	0%	0.001
IntentionNonPayment	0%	-	-	0
SmartContractSupport	0%	-	-	0
UsageBeyondPayment	0%	-	-	0
LedgerStyleOther	0%	-	-	0
AccountingBalance	0%	-	-	0
Anonymous	0%	-	-	0
NonAnonymous	30.03%	100%	0%	0.007
∅ Observations			61	
∅ Fraction of (null) deviance explained			0.035	

Appendix B

Do Design Features Explain the Volatility of Cryptocurrencies?

This appendix includes additional results for the volatility analysis in Chapter 3.

B.1 Standard Deviation as Volatility Measure

Table B.1 presents the results from the LASSO regression approach introduced in Chapter 3 with the second volatility measure, the standard deviation of daily returns, as the dependent variable. In line with Table 3.3, variables highlighted in light green or light blue indicate selection in at least 50% of the ten subsamples, with consistent or inconsistent signs, respectively. The results again show that cryptocurrency age reduces volatility levels, while cryptocurrencies with mandatory transaction fess tend to be more volatile. Also, cryptocurrencies with private, for-profit developement teams demonstrate higher volatilities, albeit a negative outlier with negligible economic magnitude is observed in the 2019 USD sample. Although no other variables are selected across more than half of the subsamples, the results confirm the findings presented in Chapter 3, as we observe sign consistency for the variables discussed and selected for either volatility measure.

Table B.1: LASSO results with standard deviation as dependent variable

This table reports the average of the parameter estimate, incorporating a value of zero for cases where the variable was not selected, indicating the economic significance from 10,000 LASSO regressions with the standard deviation of daily returns as the dependent variable and the design feature variables as the independent variables. Presented results in columns (1) to (5) base on the BTC sample whereas columns (6) to (10) consider the USD sample. $^{\#}$, *, **, and *** indicate that the respective variable is selected in at least 20%, 40%, 60% and 80%, respectively, of the 10,000 LASSO regression. Non-blank cells showing a figure without superscript belong to variables selected in less than 20% of the cases. Cells with "-" are associated with variables never selected.

	BTC sample					USD sample				
Variables	(1) 2019	(2) 2020	(3) 2021	(4) 2022	(5) 2023	(6) 2019	(7) 2020	(8) 2021	(9) 2022	(10) 2023
Constant	0.0477***	0.0522***	0.0703***	0.0411***	0.0391***	0.0557***	0.0629***	0.0838***	0.0531***	0.0451***
DaysAge	-0.0006***	-0.0001	-	-	-	-0.0009***	-0.0008*	-	-0.0066***	-0.0000
DeveloperNPO	-	-	-	-	-	0.0000	-	-	-0.0000	-
DeveloperPrivate	-	0.0000	-	0.0011$^{\#}$	-	-0.0000	0.0002*	0.0000	0.005***	-
NoMajorityChanges	0.0000	-	-	-0.0006$^{\#}$	-	0.0000	0.0000	-	-0.0042***	-
CodeNonPublic	0.0004	-	-	-	-	0.0000	-	-	-	-
CodeNonC	-	-	-	-	-	-	-	-	-	-
Fork	-	-	-	0.0000	0.0000***	-	-	0.0000***	-	0.0000
ConsensusPoSDPoS	-	0.0052***	-	0.0005$^{\#}$	-	-	0.0007*	-	-	-
ConsensusOther	-0.0000	-	-	-	-	-0.0000	-	-	-	-
HashAge	-	-	-	-	-	-	-	-	-	-
CurveNonECDSA	-	-	-	-	0.0000	-	0.0000	-	-	0.0000
NoMaxSupply	-	-	-	-	-0.0000	-	-	0.0000	0.0015***	-
Deflationary	-	-	-	0.0000	-	-0.0000	-	-	0.0044***	-
FixedSupply	-	-	-	-	-	-	-	-	-	0.0000
RewardCoinbase	-	-	-	-	-	-	-	-	-	-
RewardInflation	0.0000	-	-	0.0002$^{\#}$	-	0.0000	-	-	0.0019***	-
BlockTimeAverage	-	-	-	-	-	-	-	-	0.004***	-
TransactionFeeObligation	-	0.0000	-	0.0000	-	-	0.0016***	-	0.0009***	0.0000
NoTipSpecialTreatment	-	-0.0000	-	-	-	-0.0000	-	-	-	-
NoFeeTipForMinerForger	0.0000	-	-	-0.0013$^{\#}$	-	0.0000	-	-	-0.0082***	-
IntentionNonPayment	-	0.0001	-	-	-	-	0.001*	-	-0.0000	-
SmartContractSupport	-	-	-	-	-	-	-	-	-	-
TokenUsageBeyondPayment	-	-	-	-	-	-0.0000	-	-	-	-
LedgerStyleOther	-	-	-	-	-	-	-	-	-	-
AccountingBalance	-	-	-	-	-	-	-	-	-	-
Anonymous	-	-	-	-	-	-0.0000	-	-	-	-
NonAnonymous	-	0.0000	-	-	-	-0.0000	-	-	-	-
∅ Observations	48	57	57	57	57	49	58	58	58	58
∅ R^2	0.0067	0.0927	0.0000	0.0389	0.0001	0.0079	0.0699	0.0003	0.2660	0.0008

Appendix C

After *The Merge*: Network Fragility and Robust Design of PoS Cryptocurrencies

This appendix includes additional information on and complementary results to Chapter 4. It includes the proofs of Lemmas 4.1 and 4.2 from Subsections 4.2.2 and 4.2.3.

C.1 Proofs

C.1.1 Proof of Lemma 4.1

We can transform the maximization problem (4.1) into:

$$\max_{S_{it}} \zeta \underbrace{\left(\mu M + (1-\mu)\,\delta \mathbb{E}_t^1 \left[e_{it} \frac{p_{t+1}}{p_t}\right]\right)}_{V(S_{it})} + \frac{S_{it}}{S_t} \cdot \delta \Phi_t \mathbb{E}_t^{(1)}\left[p_{t+1}\right] \cdot N_t^C \left(\rho - 1\right)$$

This equation implies

$$\zeta V'\left(S_{it}\right) + \Phi_t \delta N_t^C \left(\rho - 1\right) \mathbb{E}_t^{(1)}\left[p_{t+1}\right] \frac{S_t - S_{it}}{S_t^2} = 0 \tag{C.1}$$

for $S_{it} > 0$. The inner maximization problem denoted by M is given by the term

$$M = \max_{Q_{it} \leq \left(\frac{e_{it}}{z_t} - S_{it}\frac{p_t}{z_t}\right)} \left\{ u_B\left(Q_{it}\right) + \delta \mathbb{E}_t^{(1)}\left[\left(\frac{e_{it}}{p_t} - \frac{z_t Q_{it}}{p_t}\right) p_{t+1}\right]\right\}$$

and requires the unconstrained solution Q_t^* with $u_B'\left(Q_t^*\right) - \delta \mathbb{E}_t^1 \left[z_t \frac{p_{t+1}}{p_t}\right] = 0$. The sellers' program (4.5) implies $u_B'\left(Q_t^*\right) = \delta z_t \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t}\right] = 1$.

Let $q_t^* = Q_t^* z_t$, i.e., the unconstrained inner solution in numeraire terms. Then if

(i) $q_{it} \geq q_t^*$, forger i demands all night market goods that the sellers provide, e.g., Q_t^* with the remaining coins. Due to uncertainty about the possibility of trading the night good, they do not intentionally want to bring more coins than they actually want to exchange for night market goods and staking is the preferred option.

Then $V\left(S_{it}\right) = \mu \left(u_B\left(Q_t^*\right) + \delta \mathbb{E}_t^1 \left[\left(e_{it} - q_t^*\right) \frac{p_{t+1}}{p_t}\right]\right) + (1-\mu)\, \delta \mathbb{E}_t^1 \left[e_{it} \frac{p_{t+1}}{p_t}\right]$. It follows that $V'\left(S_{it}\right) = 0$. With the original condition of the forgers' problem (C.1), we have that for positive expected rewards and $S_{it} > 0$ the demand for staking and thus the demand for coins would be unbounded.

(ii) $q_{it} < q_t^*$, the budget constraint within M is binding, e.g., $Q_{it} = \frac{e_{it}}{z_t} - S_{it} \frac{p_t}{z_t}$ as giving up beneficial transaction possibilities is costly. In this case

$$V'\left(S_{it}\right) = -\frac{p_t \mu}{z_t} u_B' \left(\frac{e_{it}}{z_t} - S_{it} \frac{p_t}{z_t}\right).$$

It is required that $-\zeta V'\left(S_{it}\right) = \frac{p_t \mu}{z_t} u_B' \left(\frac{e_{it}}{z_t} - S_{it} \frac{p_t}{z_t}\right) \overset{!}{=} \delta N_t^C (\rho - 1)\, \mathbb{E}_t^{(1)} \left[p_{t+1}\right] \frac{S_t - S_{it}}{S_t^2}$. Using homogeneity among forgers, i.e., $S_{it} = S_{jt}$ and $S_t = N^F \cdot S_{it}$, we obtain $S_t = \Phi_t \delta z_t N_t^C (\rho - 1)\, \mathbb{E}_t^{(1)} \left[\frac{p_{t+1}}{p_t}\right] \frac{N^F - 1}{N^F} \left(\zeta \cdot \mu \cdot u' \left(\frac{e_t}{z_t} - \frac{S_t}{N^F} \frac{p_t}{z_t}\right)\right)^{-1}$ in any equilibrium. □

C.1.2 Proof of Lemma 4.2

Our proof of this lemma follows the one of Pagnotta (2022) who extended the analysis of Lagos and Wright (2005) and Rocheteau and Wright (2005) to the PoW equivalent of our model setting.

With cryptocurrency balances in terms of the numeraire $c_{it} = C_{it} p_t$, the budget constraint of equation (4.4) can be written $-l_{it} \leq -c_{it}$ and we have the transformed maximization problem

$$\max_{c_{it}} -c_{it} + \Phi_t \underbrace{\left(\mu M + (1-\mu)\, \delta \mathbb{E}_t^1 \left[c_{it} \frac{p_{t+1}}{p_t}\right]\right)}_{V(c_{it})}. \tag{C.2}$$

Equation (C.2) implies $-1 + \Phi_t V'\left(c_{it}\right) \leq 0$ and $\Phi_t V'\left(c_{it}\right) = 1$ if $c_{it} > 0$. The inner maximization denoted by $M = \max_{Q_{it} \leq \frac{c_{it}}{z_t}} \left\{u\left(Q_{it}\right) + \delta \mathbb{E}_t^1 \left[\left(c_{it} - z_t Q_{it}\right) \frac{p_{t+1}}{p_t}\right]\right\}$ requires the unconstrained solution Q_t^* with $u_B'(Q_t^*) - \delta \mathbb{E}_t^1 \left[z_t \frac{p_{t+1}}{p_t} \right] = 0$. The sellers' program (4.5) implies $u_B'(Q_t^*) = \delta z_t \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] = 1$ [94].

Let $c_t^* = Q_t^* z_t$. Then if

(i) $c_{it} \geq c_t^*$, a buyer demands all night market goods that the sellers provide, e.g., Q_t^*. Due to uncertainty about the night good amount traded and as buyers do not intentionally buy more coins than they want to exchange for night market goods, buyers do not stake the additional coins and interaction effects are neglible. Then $V(c_{it}) = \mu \left(u_B(Q_t^*) + \delta \mathbb{E}_t^1 \left[(c_{it} - c_t^*) \frac{p_{t+1}}{p_t} \right] \right) + (1-\mu) \delta \mathbb{E}_t^1 \left[c_{it} \frac{p_{t+1}}{p_t} \right]$ and therefore, $V'(c_{it}) = \delta \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right]$. Eventually, the first order condition requires $\delta \Phi_t \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] \leq 1$. Otherwise, demand for coins would be unbounded.

(ii) $c_{it} < c_t^*$, the budget constraint within M is binding, e.g., $Q_{it} = \frac{c_{it}}{z_t}$, since otherwise buyers would just carry coins through the night market. This is costly as beneficial transaction possibilities are given up at no cost reduction. In this case

$$V'(c_{it}) = \frac{\mu}{z_t} u_B' \left(\frac{c_{it}}{z_t} \right) + (1-\mu) \delta \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right]. \tag{C.3}$$

Given the properties of the utility function, i.e., strictly increasing and convex as well as $u_B(0) = 0$, $-1 + \Phi_t V'(c_{it})$ is strictly decreasing in $c_{it} \in [0, c_t^*]$. Thus, for $\delta \Phi_t \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] < 1$ with $\Phi_t > 0$, there is an unique $\tilde{c} < c_t^*$ satisfying $\Phi_t V'(\tilde{c}) = 1$.

Considering (C.3), it holds $\Phi_t \left(\frac{\mu}{z_t} u_B' \left(\frac{c_{it}}{z_t} \right) + (1-\mu) \delta \mathbb{E}_t^1 \left[\frac{p_{t+1}}{p_t} \right] \right) = 1$ and with the condition from the sellers problem and the market clear, i.e., $N^B C_{it} + S_t + A_t = N_t^C$, (4.6) is obtained. □

[94] In this situation, the buyer's marginal utility and the seller's marginal production cost are balanced.

Appendix D

Climate Change, Energy Prices, and the Returns of Proof-of-Work vs. Proof-of-Stake Crypto Assets

This appendix includes additional information on and complementary results to Chapter 5. Section D.1 provides a detailed description of the data processing with filtering, characteristic descriptions and calculations as well as the application of the machine learning-based classification techniques to enrich the data sample with respect to the design-related characteristics. The asset pricing performance of the IPCA models is shown and discussed in Section D.2. Section D.3 contains the identification of the periods of exuberant behavior (PEIAs). In Section D.4, we show how we extended the Media Climate Change Concerns Index (MCCC) by Ardia et al. (2023). Further, Section D.5 includes robustness considerations regarding the design-related risk premiums and the relation between climate change concerns, energy prices, and consensus risk.

D.1 Data Procession

D.1.1 Trading Data Procession, Filters, and Common Characteristics

As illustrated in Subsection 5.2.1, we implement several filters to eliminate errors in the data and observations with fake or suspicious trading activity. However, calculating the characteristics after having applied all filters significantly reduces the number of observations. By combining these two steps meaningfully, we not only derive more reasonable characteristics but also minimize the number of crypto asset-week pairs that are excluded unnecessarily. For instance, applying our market capitalization filter of 1,000,000 U.S. dollars before calculating the average trading volumes over the last n days could significantly bias the true average trading volume. Therefore, we will provide a chronological overview of our data processing and calculation of the common characteristics in the following.

1. We initially filter out all stablecoins and wrapped coins/tokens, i.e., the crypto assets that are tagged as *Algorithmic Stablecoin*, *Asset Backed Stablecoin*, *Asset Backed Token*, *EUR Stablecoin*, *Stablecoin*, *Tokenized Gold*, *Tokenized Stock*, *USD Stablecoin*, or *Wrapped Tokens* by coinmarketcap.com.
2. We delete crypto assets on those days on which their market capitalization exceeds the one of Bitcoin.
3. We exclude crypto asset-day pairs with a closing price equal to zero.
4. We eliminate all daily low (high) prices that are lower (higher) than 1% (10,000%) of the opening and/or closing price. Thereby, we filter out those crypto asset-day pairs on which the daily low and/or high price is unreasonable.
5. We determine the price-related characteristics. In detail, we establish maximum (minimum) prices over the last n days and the closeness to those. Further, we use the remaining open, high, low, and close prices to estimate bid-ask spreads as in Abdi and Ranaldo (2017).[95]
6. We calculate the crypto assets' returns for different time horizons. Further, we subtract the respective risk-free rate, computed using the one-month Treasury bill rate, from the calculated returns to determine excess returns.
7. We filter out unreasonable returns. In detail, we set daily (weekly, 2-week, 1-month, 2-month, 3-month, 6-month) returns to NA if they are above 300% (1000%, 1500%, 2000%, 3000%, 6000%, 10000%)
8. We determine maximum returns over the last n days and compute the skewness and kurtosis of daily returns.
9. We filter out crypto asset-day pairs associated with erroneous changes in the coin supply. We do so by calculating the daily return of the market capitalization and filter out observations with returns above 500%.
10. We only maintain observations with a volume to market capitalization ratio smaller or equal than 2. Thereby, we filter out pairs of potentially artificial trading volume

[95] We solely use the bid-ask spread to measure illiquidity. This is particularly due to the circumstance that that the illiquidity measure of Amihud (2002) performs purely on the crypto market due to a reversed relation between volume and liquidity (Brauneis et al., 2021). Investigating calculations of the Amihud (2002) measure based on our data, we also find unreliable illiquidity levels. Extending our set of characteristics within the IPCA analysis by the Amihud (2002) measure, we further investigate a poor model performance with respect to this variable. Therefore, estimated bid-ask spreads remain the only liquidity characteristic in our IPCA analysis.

11. We calculate the volume-based characteristics, i.e., average trading volumes, volume shocks, and turnovers
12. We only maintain crypto asset-day pairs with associated trading volumes in excess of 10 U.S. dollars. We thereby ensure that small, isolated trades triggering unreasonable prices changes remain unconsidered.
13. We filter out crypto assets on those days on which their market capitalization is below 1,000,000 U.S. dollars as in Liu and Tsyvinski (2021) and Liu et al. (2022).
14. We estimate the CAPM alpha and beta based on a 30-day rolling window. The market return is calculated as the value-weighted average of all single crypto asset returns available at each day. Further, we calculate the resulting idiosyncratic volatility as the standard deviation of the residuals from the CAPM.

Table D.1 provides an comprehensive overview and detailed descriptions of the 25 common characteristics used in our study. These characteristics can all be calculated solely from information on open, high, low, and close prices, trading volumes, and market capitalizations. Within our IPCA analysis, they serve as the common characteristics next to the design-related characteristics introduced in Subsection 5.2.2.

D.1.2 Design-Related Characteristics and Machine Learning-Based Classification

In Subsection 5.2.2, we introduce four design-related characteristics, namely *Consensus*, *Coin*, *Privacy*, and *Smart Contract*. In the following paragraphs, we further delve into the construction of the characteristic variables relying on the tagging system of coinmarketcap.com. Furthermore, recall that this tagging system is well-maintained for larger, well-known crypto assets but lacks completeness for smaller, lesser-known crypto assets. As outlined in Subsection 5.2.2, we address this data gap by using textual crypto asset descriptions. We apply suitable machine learning-based classification algorithms to these descriptions alongside the tagged data, thereby classifying untagged observations. In the following paragraphs, we further describe the approach to enrich the design-related characteristic data.

Consensus

To explore the impact of consensus-related risk premiums, it is essential to categorize crypto assets based on their consensus mechanisms. To this end, we introduce the three label variables *PoW*, *PoS*, and *Other*. Each crypto asset in our dataset is assigned a value for these variables, allowing for a range between zero and one to account for the presence of hybrid consensus mechanisms. The assignment process begins by grouping the tags from coinmarketcap.com into seven tag groups, as detailed in Panel A of Table D.2. A crypto asset tagged with an

Table D.1: Common asset characteristics

This table lists and describes the 25 common characteristics used in our analysis. They are all calculated from only the information on open, high, low, and close prices, trading volumes, and market capitalizations as provided by coinmarketcap.com.

Characteristic	Description
Price	Daily close price denoted in U.S. dollars
MaxPrice (week)	Maximum daily close price over the last week (7 days)
MaxPrice (month)	Maximum daily close price over the last month (30 days)
ClosenessToHigh (3-month)	Ratio of daily close price to the maximum daily close price over the last 3 months (90 days)
Mcap	Market capitalization in U.S. dollars
TradeVol	Weekly trading volume in U.S. dollars
AvgTradeVol	Average daily U.S. dollars volume over the last 2 months (60 days)
TradeVolShock	Log average volume over the last week minus log average volume over the past month (30 days) scaled by the log standard deviation as in Bianchi et al. (2022)
WeeklyTurnover	Ratio of average weekly U.S. dollars volume to U.S. dollars market capitalization. This ratio is equal to trading volume (in coins/tokens) over the coin/token supply
CAPM-β	CAPM beta calculated on a 30-day rolling window. Market portfolio is value-weighted portfolio of filtered data
CAPM-α	CAPM alpha calculated on a 30-day rolling window. Market portfolio is value-weighted portfolio of filtered data
Ivol	Idiosyncratic volatility based on the standard deviation of the residuals from CAPM calculation on a 30-day rolling window
AvgBidAskSpread (month)	Monthly average of the “two-day” corrected bid-ask estimator of Abdi and Ranaldo (2017)
WeeklyReturn	Weekly return calculated from U.S. dollars close prices
MonthlyReturn	Monthly return calculated from U.S. dollars close prices
3-MonthReturn	Three-month return calculated from U.S. dollars close prices
LaggedWeeklyReturn	Weekly return lagged by one week
Lagged2-WeekReturn	2-week return lagged by two weeks
MaxDailyReturn (month)	Maximum daily return within the past month
MaxWeeklyReturn (month)	Maximum weekly return within the past month
MaxWeeklyReturn (3-month)	Maximum weekly return within the last 3 months
StdDailyReturn (month)	Standard deviation of the last month’s daily returns
SkewnessDailyReturn (month)	Skewness of the last month’s daily returns
KurtosisDailyReturn (month)	Kurtosis of the last month’s daily returns
Age	Number of days listed on coinmarketcap.com

identifier from the first three tag groups will see its corresponding variable set to one, while the other two variables are assigned zero values. For assets associated with hybrid tag groups, the relevant variables are assigned fractional values of $\frac{1}{2}$ (for hybrids between two categories) or $\frac{1}{3}$ (for hybrids among all categories), respectively. In situations where a crypto asset is tagged with identifiers from multiple tag groups, we consider it as a hybrid version between the consensus types for which at a least one tag is provided. In a final step, we ensure that the sum of the three label variables for one crypto asset always equals one. This procedure leaves us with a labeled subsample of 813 crypto assets with a value greater than zero in at least one of the three label variables. Since the three variables are mutually exclusive, our approach also generates negative observations (feature is not present). This enables the application of neural networks to categorize the remaining coins out of the 22,460 crypto assets unlabeled regarding consensus.[96] To do so, we initially convert the crypto assets' descriptions into numerical vectors utilizing the embedding model `text-embedding-ada-002` of OpenAI. Subsequently, we use the resulting embedding vectors alongside the consensus label variables of the labeled subsample, reformulated to the vector structure [*PoW*, *PoS*, *Other Consensus*], as input data for training a neural network featuring two hidden layers. The first hidden layer incorporates 500 neurons, the second one 300. Activation functions employed are ReLU (rectified linear unit) for the first and the second layer and softmax for the final layer. We then apply the trained neural network to classify untagged observations with respect to consensus, i.e., to ultimately determine the value of the consensus label variables *PoW*, *PoS*, and *Other* for all unlabeled coins.

To evaluate the performance of our neural network, we randomly divide the tagged data into training (90% of observations) and validation (10% of observations) subsamples. Applying the neural network, as described, 100 times, the average percentage of correctly classified observations into the vector structure [*PoW*, *PoS*, *Other Consensus*] is 64.7%. Investigating the misspecified examples, we observe that hybrid version are more error-prone. For instance, a PoW-PoS hybrid network $[0.5, 0.5, 0]$ is classified as PoW ($[1, 0, 0]$) or PoS ($[0, 1, 0]$) at times and not always as its actual hybrid version. In this view, we contend that the performance of our neural network is appropriate. Investigating our final, classified sample, the label variables *PoW*, *PoS*, and *Other* have averages of 0.46, 0.48, and 0.06, respectively.

Finally, as we are interested in the distinctions between PoW and PoS crypto assets, for each asset, we aggregate the three label variables into the *Consensus* characteristic. *Consensus* is defined as the differences between the *PoW* and *PoS* label variables, scaled to range within 0 and 1. Consequently, a value of 0 in this characteristic variable indicates that the respective crypto asset is PoS-based, while a value equal to 1 belongs to PoW crypto asset. Hybrid versions are assigned with a value in between 0 and 1, dependent on the closeness of the mechanism to

[96] Note that we solely classify coins and exclude tokens. Tokens inherit the consensus mechanism from their parent network's crypto asset and consequently, we intentionally omit them from our analysis of consensus-related risk premiums.

either PoS or PoW.

Table D.2: Overview on tags from coinmarketcap.com

This table lists the tags which we retrieve from the tagging system of coinmarketcap.com and indicates the mapping procedure. Panel A includes the tags associated with consensus-related characteristics. Panel B refers to the other design-related characteristics.

Panel A: Consensus-related characteristics

Tag groups	Tags from coinmarketcap.com
PoW	`CryptoNight`, `CryptoNight-Lite`, `Hybrid-dPoW&PoW`, `M7 POW`, `PoW`, `PoWT`
PoS	`Hybrid-PoS&LPoS`, `LPoS`, `PoS`, `PoS 2.0`, `PoS 3.0`, `PoS+`, `PoST`, `rPOS`
Other	`PoA`, `PoC`, `PoI`, `PoP`, `PoSign`, `Proof-of-Authority`
Hybrid PoW-PoS	`Hybrid-PoW&DPoS`, `Hybrid-PoW&nPoS`, `Hybrid-PoW&PoS`
Hybrid PoW-Other	-
Hybrid PoS-Other	`Hybrid-PoW&PoD`, `Hybrid-PoS&PoP`
Hybrid PoW-PoS-Other	`Hybrid-PoS&PoW&PoT`, `Hybrid-PoW&PoM&PoSII`

Panel B: Other design-related characteristics

Tag groups	Tags from coinmarketcap.com
Coin	`Coin`
Token	`Token`
Privacy	`Bulletproofs`, `Privacy`, `Zero Knowledge Proofs`
Smart Contract	`Smart Contracts`

Other Design-Related Characteristics

Besides *Consensus*, we consider three additional design-related characteristics. First, we distinguish between coins and tokens. Every crypto asset in our sample is explicitly tagged as either `Coin` or `Token`. The tags are mutually exclusive, enabling us to directly introduce the design-related characteristic variable *Coin* which takes a value of either 1 (Coin) or 0 (Token). Note that the tagging system of coinmarketcap.com is complete with respect to these two tags which eliminates the need for additional post-processing. Second, we identify crypto assets that particularly protect privacy by obscuring transaction details such as senders, recipients, and amounts, thereby rendering it nearly impossible to trace users and their transaction histories. We label a crypto asset with the value *Privacy* as 1 if any of the associated tags `Bulletproofs`, `Privacy`, or `Zero Knowledge Proofs` is assessed. The third design-related characteristics identifies crypto assets with implicit smart contract support by employing the tag `Smart Contracts`. These networks provide an essential platform characteristic enabling services and applications in the field of DeFi, among others. A crypto asset is labeled with the value *Smart Contract* as 1 if it fulfills this platform characteristic.

Recall the incompleteness issue of the tagging system maintained by coinmarketcap.com. In contrast to the consensus-based variables, the design-related characteristics *Privacy* and *Smart Contract* are not mutually exclusive, making the application of neural networks impractical due to missing negative examples. Note that at this stage, the two design-related characteristic variables have a value of 1 if the corresponding feature is present. A value equal to 0, indeed, is equal to unlabeled data. In this view, we adopt the approach proposed by Elkan and Noto (2008), which is specifically designed for scenarios in which labeled data is an incomplete set of positive examples (feature is present) and unlabeled examples either being positive or negative (feature is not present). Initially, we again generate embedding vectors from the crypto asset descriptions utilizing the embedding model `text-embedding-ada-002` of OpenAI. We then train a support vector machine (SVM) classifier on the embedding vectors and the labels of the crypto assets, treating the tagged data as positive examples and the unlabeled observations as negative examples. We employ the SVM with a radial basis function kernel. Subsequently, the trained SVM classifier is used to determine the probability of a data point being labeled and the probability of a positive data point being labeled. Assuming that labeled examples are randomly selected from positive examples, the probability that a sample is positive is obtained by dividing the probability that an unlabeled sample is labeled by the probability that a positive sample is labeled. This procedure, as proposed by Elkan and Noto (2008), such enables to finally predict that an unlabeled sample is positive. Specifically, we consider a probability threshold level of 0.5 for untagged crypto assets to be assumed to feature the respective design-related characteristic. We use this approach to categorize the part of the data unlabeled with respect to the characteristic variables *Privacy* and *Smart Contract* which proxy for the presence of the corresponding design-related features.

To evaluate the performance of this classification technique, we apply the trained model to the observations that are known to be positive, i.e., crypto assets with tags for the respective design-related label variables. We find high hit ratios, attesting the resilience and reliability of the approach. Specifically, for *Privacy* (*Smart Contract*), 79.67% (84.80%) of the positive observations are correctly specified.

D.2 Asset Pricing Performance of IPCA Models

Similar to Kelly et al. (2019) (henceforth, KPS) and Kelly et al. (2023), we evaluate the asset pricing performance for models with different numbers of principal components using the following metrics:

$$
\begin{aligned}
R^2_{Total} &= 1 - \frac{\sum_{i,t}(r_{i,t+1} - \widehat{\beta}'_{i,t}\widehat{f}_{t+1})^2}{\sum_{i,t} r^2_{i,t+1}}, \\
R^2_{TS} &= \frac{1}{T^i}\sum_i T^i R^2_i \quad \text{with} \quad R^2_i = 1 - \frac{\sum_t(r_{i,t+1} - \widehat{\beta}'_{i,t}\widehat{f}_{t+1})^2}{\sum_t r^2_{i,t+1}}, \\
R^2_{CS} &= \frac{1}{T}\sum_t R^2_t \quad \text{with} \quad R^2_t = 1 - \frac{\sum_i(r_{i,t+1} - \widehat{\beta}'_{i,t}\widehat{f}_{t+1})^2}{\sum_i r^2_{i,t+1}}, \text{ and} \\
RPE &= \frac{\sum_i(\frac{1}{T^i}\sum_t(r_{i,t+1} - \widehat{\beta}'_{i,t}\widehat{f}_{t+1}))^2}{\sum_i(\frac{1}{T^i}\sum_t r_{i,t+1})^2},
\end{aligned}
$$

where T^i equals the respective number of non-missing observations for crypto asset i in our test sample, and T is the total number of test months. R^2_{Total}, R^2_{TS}, and R^2_{CS} measure the total, time-series, and cross-sectional variation of the returns explained by a model. The relative pricing error (RPE) measures how well the differences in crypto assets' average returns are explained by a model. Table D.3 shows these metrics for models with different numbers of principal components. Panel A presents the results based on our full set of characteristics using individual crypto assets as test assets. The measures R^2_{Total}, R^2_{TS}, and R^2_{CS} increase with the number of latent factors K. The RPE fluctuates for different Ks. We observe the lowest values of 39.1% and 47.3% for $K = 1$ and $K = 2$, respectively, followed by 51.1% for $K = 4$. Particularly, the RPE of the model with $K = 4$ appears as a low outlier compared to the models that have a high explanatory power of individual crypto asset returns in terms of the different R^2-measures, i.e., among all models with $K \geq 3$. The pattern of increasing R^2s with the number of principal components is consistent when using managed portfolios as test assets, as shown in Panel B. For the managed portfolios, we observe a monotonically declining RPE, the more principal components we allow the model to have, contrasting the bumpy pattern of RPE for the single assets. We observe high R^2s combined with a relatively low RPE for $K = 4$ principal components among the results of both Panel A, with individual crypto assets as test assets, and Panel B, with managed portfolios as test assets. Inclusion of more than $K = 4$ principal components only marginally improves the performance and thus, we select the IPCA model with $K = 4$ principal components as our main specification for the analyses that results are presented and discussed in Subsections 5.3.3 and 5.3.4. However, we demonstrate in a set of robustness tests in Appendix D.5.1 that our results are qualitatively similar regardless of the number of principal components considered.

We also estimate asset pricing models without the four design-related features to evaluate whether these characteristics are already spanned by the common characteristics. Comparing the metrics for the model fits using only the common characteristics in Panels C (individual

Table D.3: Out-of-sample performance of the restricted IPCA models

This table reports the out-of-sample asset pricing performance of the restricted IPCA models with $K = 1, \dots, 7$ latent factors. Specifically, we report total, time series, and cross-section R^2, as well as the relative pricing error. Panel A (C) show the results with individual crypto assets when (no) design-based characteristics are considered. Panel B (D) present the results with managed portfolios as test assets when (no) design-based characteristics are used. We estimated the models on a 3-year rolling-window basis starting week 7, 2016 until week 2, 2023.

	K						
	1	2	3	4	5	6	7
Panel A: Individual crypto assets, with design-based characteristics							
R^2_{Total} (%)	20.6	21.3	22.0	22.5	22.9	23.1	23.3
R^2_{TS} (%)	30.1	30.9	31.6	32.1	32.6	32.8	33.0
R^2_{CS} (%)	16.0	16.7	17.4	17.9	18.2	18.5	18.7
RPE (%)	39.1	47.3	53.1	51.2	55.6	53.3	51.7
Panel B: Managed portfolios, with design-based characteristics							
R^2_{Total} (%)	96.1	97.0	97.7	98.3	98.5	98.6	98.8
R^2_{TS} (%)	18.6	37.0	51.2	64.2	68.3	70.8	73.7
R^2_{CS} (%)	83.6	86.4	89.0	91.8	92.6	93.1	93.5
RPE (%)	13.0	6.7	3.1	1.9	1.8	1.3	0.8
Panel C: Individual crypto assets, no design-based characteristics							
R^2_{Total} (%)	21.2	21.9	22.6	23.2	23.5	23.7	23.9
R^2_{TS} (%)	31.0	31.9	32.5	33.1	33.4	33.5	33.8
R^2_{CS} (%)	16.3	17.0	17.7	18.2	18.5	18.7	19.0
RPE (%)	50.1	60.0	67.1	65.4	71.5	67.4	66.7
Panel D: Managed portfolios, no design-based characteristics							
R^2_{Total} (%)	95.9	97.1	97.8	98.5	98.7	98.9	99.0
R^2_{TS} (%)	6.1	30.2	46.8	62.1	66.9	69.7	72.6
R^2_{CS} (%)	83.1	86.2	89.2	92.5	93.2	93.9	94.4
RPE (%)	28.2	14.4	4.7	2.8	2.1	1.4	1.4

crypto assets) and D (managed portfolios) with their respective counterparts in Panels A and B reveals that although the R^2_{Total}s and the R^2_{CS}s are consistently slightly larger for the reduced set of characteristics, the designed-based features add significant information with respect to explaining crypto asset returns, over and above the common characteristics, as evidenced by the higher R^2_{TS}s and most notably the much lower RPEs.

The IPCA version we consider in Chapter 5 is restricted by setting the intercept to zero. In order to test the validity of this assumption, we show the in-sample asset pricing performance of the restricted IPCA models with $K = 1, \dots, 7$ principal components and thereof, bootstrapped p-values for the null hypothesis that the IPCA model intercept is equal to zero. In doing so, we follow the procedure of KPS. The results are illustrated in Table D.4. For $K \geq 3$, the null hypothesis cannot be rejected at any conventional significance level. Note that again, the performance measures show a reasonable explanatory power with R^2_{Total} in ranges around 25% and 95% for the cases with individual crypto assets and characteristic managed portfolios as test assets, respectively. Also the RPE is reasonable small, particularly for the managed portfolios.

Additionally, Table D.5 shows the out-of-sample performance of unrestricted IPCA models with $K = 1, \ldots, 7$ principal components. These models allow for intercepts in the central IPCA Equation (5.1), i.e.,

$$r_{i,t+1} = \alpha_{i,t} + \beta'_{i,t} f_{t+1} + \varepsilon_{i,t+1}, \tag{D.1}$$

while $\alpha_{i,t}$ is calculated as the product of the characteristics vector $z'_{i,t}$ and a mapping matrix Γ_α. Γ_α is estimated simultaneously to the factors f_{t+1} and the matrix Γ_β determining the factor loadings $\beta_{i,t}$ with the characteristics vector $z'_{i,t}$ (see Equation (5.2)). We find that the asset-pricing performance of the restricted models are superior compared to their unrestricted counterparts, particularly with respect to the RPE. From these results, we conclude that the intercept-to-zero restriction in our main specification is reasonable.

Table D.4: In-sample performance of the restricted IPCA model

This table reports the in-sample asset pricing performance of the restricted IPCA models with $K = 1, \ldots, 7$ latent factors. Specifically, we report total, time series and cross-section R^2, as well as the relative pricing error. Panels A and B show the results with individual crypto assets and for the case that managed portfolios are used as test assets, respectively. Panel C reports the bootstrapped p-values (200 simulations) for the test of $H_0 : \Gamma_\alpha = 0$ as in Kelly et al. (2019). The data covers the period from week 7, 2016 until week 2, 2023.

	K						
	1	2	3	4	5	6	7
Panel A: Individual crypto assets							
R^2_{Total}	24.2	25.7	26.6	27.2	27.7	28.2	28.5
R^2_{TS}	31.7	33.0	33.7	34.4	34.8	35.1	35.3
R^2_{CS}	17.8	18.6	19.5	20.1	20.5	20.8	21.1
RPE	37.3	48.3	53.3	53.1	51.3	48.6	48.6
Panel B: Managed portfolios							
R^2_{Total}	92.4	94.6	95.8	96.7	97.0	97.4	97.7
R^2_{TS}	20.9	43.5	56.6	65.1	69.6	72.9	76.4
R^2_{CS}	76.6	80.4	83.8	86.9	88.5	90.0	90.7
RPE	6.5	2.9	0.8	0.6	0.7	0.5	0.6
Panel C: Testing $H_0 : \Gamma_\alpha = 0$							
p-value	0.00	0.00	50.50	50.50	50.50	15.00	96.50

Table D.5: Out-of-sample performance of unrestricted IPCA models

This table reports the out-of-sample asset pricing performance of the unrestricted IPCA models with $K = 1, \dots, 7$ latent factors. Specifically, we report total, time series and cross-section R^2, as well as the relative pricing error. Panels A and B show the results with individual crypto assets when (no) design-based characteristics are considered. Panels C and D present the results for the case that managed portfolios are used as test assets when (no) design-based characteristics are used. We estimated the models on a 3-year rolling-window basis starting week 7, 2016 until week 2, 2023.

	K						
	1	2	3	4	5	6	7
Panel A: Individual crypto assets, with design-based characteristics							
R^2_{Total} (%)	1.7	11.3	19.1	20.1	20.8	21.4	22.3
R^2_{TS} (%)	5.8	16.7	27.4	28.5	29.7	30.4	31.6
R^2_{CS} (%)	-14.9	-2.8	12.3	14.3	15.0	16.0	17.2
RPE (%)	863.2	824.2	288.2	220.5	220.2	187.1	129.3
Panel B: Managed portfolios, with design-based characteristics							
R^2_{Total} (%)	19.3	56.4	84.9	87.0	89.3	90.6	93.3
R^2_{TS} (%)	-0.5	-0.8	8.4	10.2	34.6	41.1	52.4
R^2_{CS} (%)	-368.0	-249.9	11.1	31.9	43.7	55.3	68.0
RPE (%)	1268.3	1087.0	452.9	360.6	377.5	256.7	116.9
Panel C: Individual crypto assets, no design-based characteristics							
R^2_{Total} (%)	-39.9	-23.6	16.0	16.5	19.2	20.3	22.1
R^2_{TS} (%)	-47.4	-29.8	21.1	21.5	27.4	28.5	30.9
R^2_{CS} (%)	-85.8	-66.5	8.2	8.4	11.4	13.3	16.0
RPE (%)	1804.8	3607.0	776.3	713.8	621.3	549.3	311.2
Panel D: Managed portfolios, no design-based characteristics							
R^2_{Total} (%)	-134.9	-74.8	71.8	73.2	83.4	86.6	92.5
R^2_{TS} (%)	-39.4	-26.4	-1.6	-12.2	24.9	36.2	51.4
R^2_{CS} (%)	-2276.2	-1994.8	-108.3	-116.3	-62.2	-24.8	31.2
RPE (%)	3001.4	8071.5	1934.2	1809.1	1665.4	1327.7	536.1

D.3 Identification of Periods of Exuberant Information Arrival

Literature documented that the crypto market exhibited periods of exuberant information arrival (PEIAs). Phillips et al. (2015) (henceforth, PSY) propose a method that enables to identify multiple periods of exuberance within a time series of prices. This method is applied by several other studies within the overall crypto market or subsets of it (Bouri et al., 2019a; Corbet et al., 2018; Geuder et al., 2019; Hafner, 2020).[97] It first tests for the presence of exuberance behavior and then uses a recursive backward regression technique to identify the start and the end date of these periods. The method generalizes the supremum Augmented Dickey–Fuller (SADF) test statistic of Phillips et al. (2011). It considers the regression

$$y_t = \mu + \beta y_{t-1} + \sum_{i=1}^{k} \delta_{r_w} \beta \Delta y_{t-i} + \varepsilon_t \text{ }^{98} \tag{D.2}$$

and tests the null hypothesis $H_0 : \beta = 1$ against the alternative hypothesis $H_1 : \beta > 1$ which indicates that the underlying time series contains an explosive root. PSY propose to use the test statistic

$$GSADF\,(r_0) = \sup_{\substack{r_2 \in [r_0,1] \\ r_1 \in [0, r_2 - r_0]}} \left\{ ADF_{r_1}^{r_2} \right\}$$

to detect exuberance behavior. $ADF_{r_1}^{r_2}$ denotes the ADF statistic obtained from regression (D.2). After that the starting and end dates of the periods with exuberance behavior are stamped using the backward $GSADF$ ($BSADF$)

$$BSADF_{r_2}\,(r_0) = \sup_{r_1 \in [0, r_2 - r_0]} \left\{ ADF_{r_1}^{r_2} \right\}.$$

In detail, exuberance periods are defined by start date(s) $\hat{r}_b$ and end date(s) $\hat{r}_e$ according to

$$\hat{r}_b = \inf_{r_2 \in [r_0,1]} \left\{ r_2 : BSADF_{r_2}\,(r_0) > scv_{r_2}^{\alpha} \right\}$$

and

$$\hat{r}_e = \inf_{r_2 \in [\hat{r}_b,1]} \left\{ r_2 : BSADF_{r_2}\,(r_0) < scv_{r_2}^{\alpha} \right\},$$

[97] For an overview about periods of exuberance in the crypto market, we refer to Kyriazis et al. (2020).

[98] The variables are defined and determined as follows. y_t is the value of the price time series at time t. k refers to the maximum number of lags; the number of lags is set according to the BIC. The rolling window regression sample bases on the (fractional) window size $r_w = r_2 - r_1$ starting with a fraction r_1 and ending with a fraction r_2 of the total sample. OLS is used to estimate the model parameters μ, β, and δ.

respectively. $scv_{r_2}^{\alpha}$ defines the $1-\alpha$ critical value of the test statics based on the subsample r_2.

We use this methodology to identify PEIAs in a value-weighted crypto market index calculated from the final data (on a weekly basis and after application of the implemented filters described in Appendix D.1.1). We use 500 simulations to determine the critical value sequence. As in PSY, the initial window size is calculated by $0.01 + \frac{1.8}{\sqrt{T}}$ with T equal to the total number of observations. Further, we define a PEIA to last more than one month, i.e., at least 5 weeks in our sample. Figure D.1 presents the results of the $GSADF$ test. In Subfigure D.1a, one can observe that the $BSADF$ sequence (black line) exceeds the 95% critical value sequence (red line) twice for a time horizon for more than a month. The two PEIAs are gray-shaded and cover the periods

(i) from October 13, 2020 (week 41) to May 20, 2021 (week 20) and

(ii) from October 7, 2021 (week 40) to December 2, 2021 (week 48).

As can be seen in Subfigure D.1b, the crypto market sharply increased to new all-time peaks during these periods.

When extending the time horizon considered for the systematic premium discussion in our main analysis, i.e., prior to week 7, 2019, we identify further PEIAs from February 2017 until June 2017 and from late July 2017 until February 2018. These findings are consistent with the aforementioned literature.

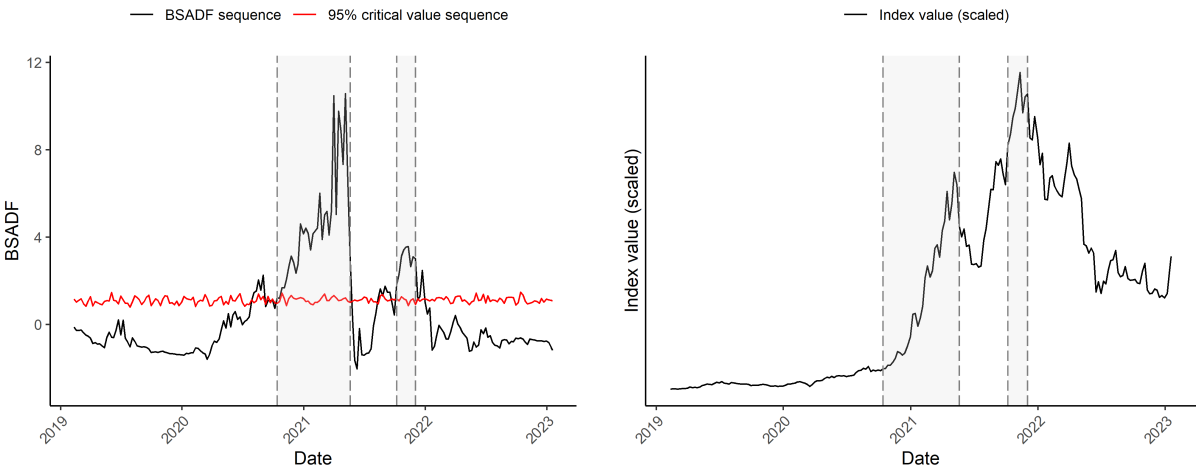
D.4 Extension of Media Climate Change Concerns Index

As our proxy for climate change concerns, we use the Media Climate Change Concerns Index (MCCC) by Ardia et al. (2023) which is available up to the end of August 2022 only. To investigate the relation between the consensus-related risk premium and the MCCC, we are required to the extent the MCCC time series until the end of our investigation period, i.e., until January 18, 2023. In doing so, we first regress the 7-day moving average of the MCCC on the weekly Google Trends score for the term `Climate Risk` considering all observations up to August 31, 2022. The results of this in-sample regression are presented in Table D.6. In a second step, we then predict the missing observations from September 2022 until the end of our investigation period. Using the linear regression model from the first step and the Google Trends scores for `Climate Risk` over this time span, we extend the MCCC time series for our investigation period.

Figure D.2 graphically illustrates the 7-day moving average of the MCCC alongside the predicted time series from our regression approach. Albeit we observe lower total magnitudes for the predicted time series, relative changes are little affected by these discrepancies.

Figure D.1: Identification of periods with exuberant information arrival

This figure shows the BSADF sequence and the corresponding 95% critical value sequence of the index values in Subfigure D.1a. We obtain the critical value sequence by Monte Carlo simulations and define exuberance periods as those periods in which the BSADF exceeds the critical value more than a month (4 weeks). Subfigure D.1b connects the identified periods of exuberant information arrival to the value of the value-weighted crypto market index.



(a) BSADF test

(b) Crypto market index

Figure D.2: MCCC vs. predictions

This figure shows the 7-day moving average of the MCCC alongside the predicted time series from our regression approach.

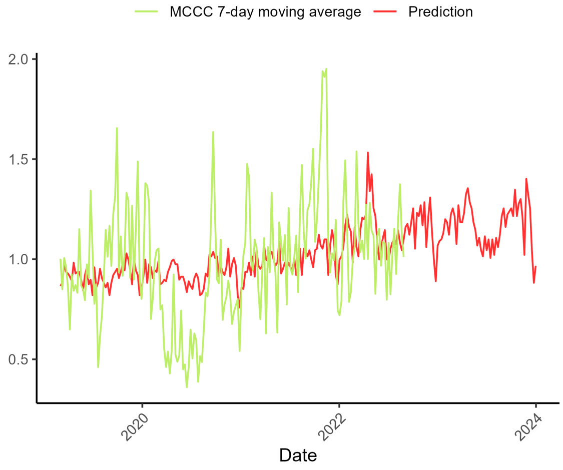


Table D.6: MCCC extension

This table reports the results of a linear regression, where the 7-day moving average of the MCCC is regressed on the weekly Google Trends score for the term `Climate Risk`. Newey and West (1987) adjusted t-statistics are given in parentheses. * and ** indicate statistical significance at the 5% and 1% level, respectively.

	MCCC
GT `climate risk`	0.01^{**}
	(2.84)
Constant	0.76^{**}
	(8.28)
Obs.	183
Adj. R^2	0.13

D.5 Robustness

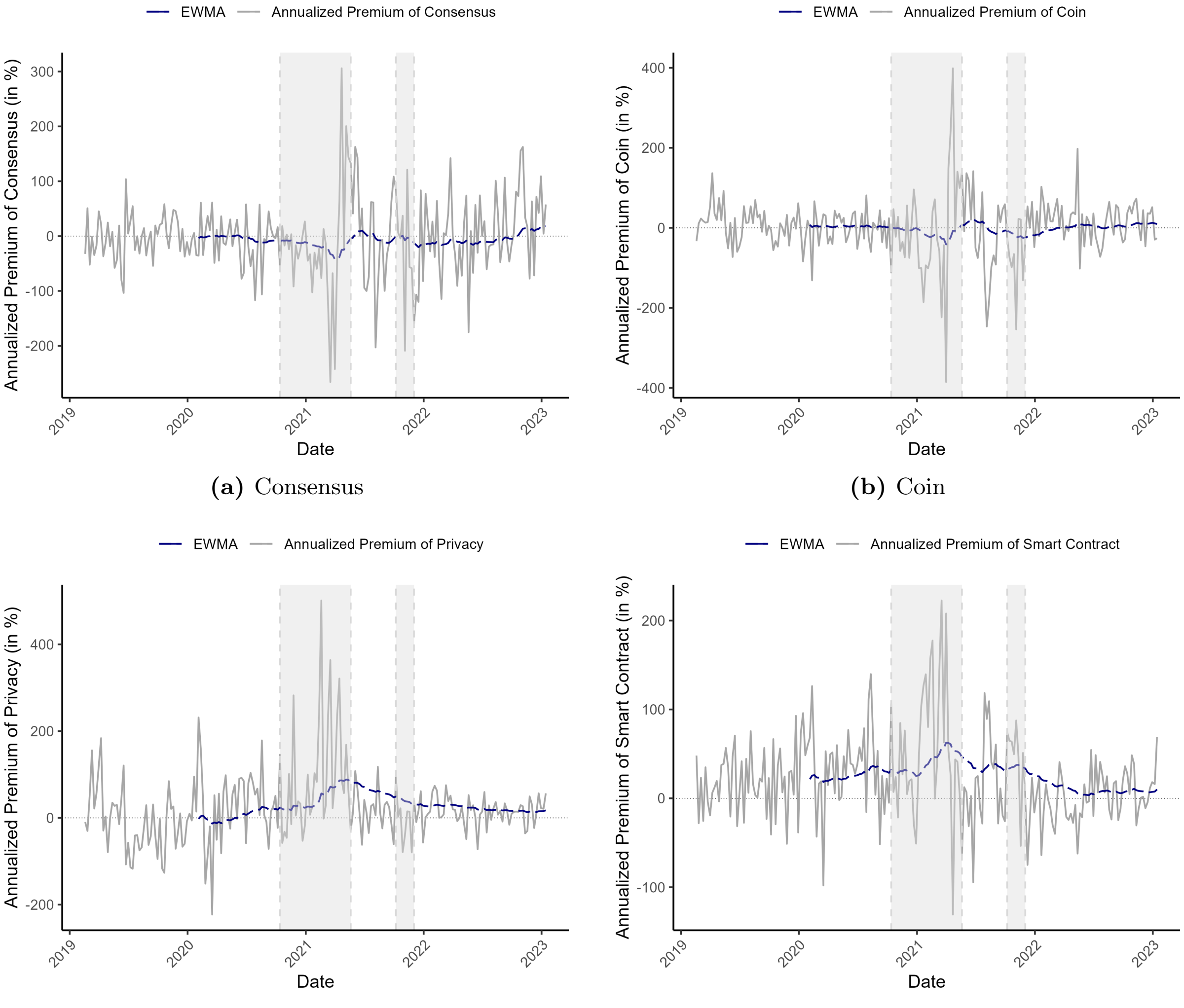
D.5.1 Design-Related Risk Premiums

IPCA bases on several specifications. In particular, the number of principal components have a key role and potentially evince inconsistent results from the corresponding models. A higher number of latent factors in the IPCA models can reveal additional effects that cannot be captured by fewer latent factors (Fieberg et al., 2020), although at the cost of potentially omitting an anomaly intercept. Against this background, we show the robustness of our results with respect to a higher number of principal components in the this section.

Exemplary, Table D.7 presents the average weekly risk premiums for the restricted IPCA model with $K = 7$ principal components. Figure D.3 graphically shows the corresponding trajectories of the design-related risk premiums. Comparing the systematic risk premiums with those obtained from our main analyses in Subsections 5.3.3 and 5.3.4, one finds that our results remain similar. Regarding the *Consensus* risk premium, we find consistency in the signs of the average risk premiums for the pre- and post-PEIAs periods. The total magnitudes are somewhat less pronounced when K is higher and the time series are not significantly different from zero. The positive risk premiums of *Coin* are observed constantly over the course of time in the $K = 7$ IPCA model, again. While the economic magnitude is estimated to be a little lower compared to the baseline results, the risk structure itself, however, remains untouched. The circumstance that *Privacy* recently earns a risk premium compensating for regulatory intervention risk persist for $K = 7$ principal components. Moreover, crypto assets featuring smart contracts again exhibit a positive risk premium over their respective peers in the pre-PEIAs period. Summarized, the robustness analysis with $K = 7$ principal components validate the results from Chapter 5.

Figure D.3: Robustness of design-related risk premiums

This figure shows weekly risk premiums of the long-short portfolios managed by the design-related characteristics *Consensus*, *Coin*, *Privacy*, and *Smart Contract*. For *Consensus*, the portfolio is long in PoW-based crypto assets and short in PoS networks. For the further characteristics, these portfolios are long in the crypto assets that have the specific characteristic and short in the ones without this characteristic. Baseline model is the restricted IPCA model with $K = 7$ latent factors. EWMA is the exponentially weighted moving average using the observations of the current week and the preceding 51 weeks. Gray-shaded areas belong to PEIA periods.



(a) Consensus

(b) Coin

(c) Anonymity (Privacy)

(d) Smart Contract

Table D.7: Robustness of risk premiums

This table shows the average risk premiums of the design-related characteristics resulting from the restricted IPCA model with $K = 7$ latent factors. The values in columns (1) to (3) are obtained by taking the time series average from the risk premiums of the portfolios that are long in the respective characteristic and short in the inverse of the characteristic. All values are reported in % on an annualized basis. For (1), we consider the time prior to the first PEIA period, i.e., from week 7, 2019 until week 41, 2020. (2) refers to the sample after the second PEIA period, i.e., from week 48, 2021, until week 2, 2023. (3) includes the whole time horizon, i.e., from week 7, 2019 until week 2, 2023. Newey and West (1987) adjusted t-statistics for the null hypothesis that the given value is equal to zero are given in parentheses. Column (4) reports the test statistics t of Welch's t-tests under the null hypothesis that the sample means of (1) and (2) are equal. * and ** indicate statistical significance at the 5% and 1% level, respectively.

Characteristic	Weekly risk premium in %			(4) Welch's
	(1) Pre-PEIAs	(2) Post-PEIAs	(3) Whole sample	t-test
Consensus	-5.28 (-1.28)	7.60 (0.82)	-3.67 (-0.54)	-1.25
Coin	3.00 (0.57)	16.55 (2.60)*	0.94 (0.13)	-1.69
Privacy	8.76 (0.76)	15.21 (4.02)**	24.05 (2.39)*	-0.68
Smart Contract	26.45 (5.46)**	0.94 (0.21)	22.97 (4.10)**	4.33**

D.5.2 Climate Change, Energy Prices, and Consensus Risk

Table D.8 shows robustness results for the multivariate regression relating the risk premium of *Consensus* to environmental sustainability awareness, energy prices, and staking popularity. We restrict some βs of regression (5.4) to zero and thereby only allow one proxy to account for energy cost, environmental sustainability awareness, or staking popularity at a time. Such, we control for our results' robustness accounting for a potential dependency among these independent variables. The results confirm the conclusions drawn within Subsection 5.3.3.

Table D.8: Robustness of multivariate regression results

This table reports the results from multivariate regression as in Equation (5.4). Besides the "control variables" $r^{PoW Basekt}$, $r^{Hashrate}$, $r^{PoS\ Basket}$, and the constant, we include only one proxy. Columns (1), (6), and (11), further include r^{Coal}. Columns (2), (7), and (12) further include r^{Gas}. Columns (3), (8), and (13) further include r^{Oil}. Columns (4), (9), and (14) further include r^{MCCC}. Columns (5), (10), and (15) further include $r^{GT\ Staking\ Crypto}$. For (1)-(5), we consider the time prior to the first PEIA period, i.e., from week 7, 2019 until week 41, 2020. (6)-(10) refer to the sample after the second PEIA period, i.e., from week 48, 2021, until week 2, 2023. (11)-(15) include the whole time horizon, i.e., from week 7, 2019 until week 2, 2023. Newey and West (1987) adjusted t-statistics are given in parentheses. * and ** indicate statistical significance at the 5% and 1% level, respectively.

	Pre-PEIAs					Post-PEIAs					Whole sample				
	(1)	(2)	(3)	(4)	(5)	(6)	(7)	(8)	(9)	(10)	(11)	(12)	(13)	(14)	(15)
r^{MCCC}	0.03					0.23*					0.10*				
	(0.99)					(2.59)					(2.23)				
r^{Coal}		0.14					0.01					0.05			
		(1.64)					(0.10)					(0.87)			
r^{Gas}			0.02					0.03					0.002		
			(0.66)					(0.61)					(0.03)		
r^{Oil}				0.03					0.05**					0.01	
				(1.55)					(2.92)					(0.32)	
$r^{GT\ Staking\ Crypto}$					0.05**					0.35					0.10**
					(2.65)					(1.64)					(3.48)
$r^{Hashrate}$	0.03	0.02	0.03	0.03	0.02	0.04	0.03	0.02	0.02	0.03	0.06	0.07	0.07	0.07	0.07
	(0.95)	(0.72)	(0.92)	(0.86)	(0.74)	(1.75)	(0.48)	(0.40)	(1.31)	(0.95)	(1.15)	(1.24)	(1.04)	(1.23)	(1.37)
$r^{PoW\ Basket}$	0.26**	0.28**	0.27**	0.28**	0.26*	0.08	0.03	0.03	0.03	0.02	0.18	0.18	0.18	0.18	0.17
	(2.70)	(2.71)	(3.03)	(3.06)	(2.38)	(0.63)	(0.18)	(0.24)	(0.68)	(0.22)	(1.21)	(1.89)	(1.86)	(1.63)	(1.51)
$r^{PoS\ Basket}$	0.23*	0.21*	0.22**	0.23**	0.23*	0.23	0.16	0.16	0.16**	0.12	0.27	0.26*	0.26*	0.26*	0.25
	(2.63)	(2.26)	(2.70)	(2.71)	(2.31)	(1.79)	(1.32)	(1.32)	(3.08)	(1.19)	(1.84)	(2.16)	(2.07)	(1.97)	(1.90)
Constant	0.15**	0.16**	0.16**	0.16**	0.14**	0.61**	0.57**	0.57**	0.57**	0.58**	0.14	0.11	0.11	0.11	0.13
	(3.24)	(3.86)	(3.04)	(3.23)	(3.34)	(8.71)	(8.86)	(9.23)	(13.35)	(9.42)	(1.84)	(0.88)	(0.89)	(0.98)	(1.15)
Obs.	85	85	85	85	85	58	58	58	58	58	203	203	203	203	203
Adj. R^2	0.55	0.56	0.55	0.55	0.56	0.11	0.03	0.03	0.03	0.06	0.18	0.17	0.17	0.17	0.18

Bibliography

Abadi, Joseph and Markus Brunnermeier (2018). Blockchain Economics. NBER Working Paper No. 25407.

Abdi, Farshid and Angelo Ranaldo (2017). A Simple Estimation of Bid-Ask Spreads from Daily Close, High, and Low Prices. *The Review of Financial Studies* 30 (12), 4437–4480.

Aggarwal, Reena, Carla Inclan, and Ricaro Leal (1999). Volatility in Emerging Stock Markets. *Journal of Financial and Quantitative Analysis* 34 (1), 33–55.

Ahmed, Shaker, Niranjan Sapkota, and Klaus Grobys (2020). Profitability of Technical Trading Rules among Cryptocurrencies with Privacy Function. *Finance Research Letters* 35, 101495.

Alabi, Ken (2017). Digital Blockchain Networks Appear to Be Following Metcalfe's Law. *Electronic Commerce Research and Applications* 24, 23–29.

Alexander, Carol and Michael Dakos (2020). A Critical Investigation of Cryptocurrency Data and Analysis. *Quantitative Finance* 20 (2), 173–188.

Amihud, Yakov (2002). Illiquidity and Stock Returns: Cross-Section and Time-Series Effects. *Journal of Financial Markets* 5 (1), 31–56.

Amirshahi, Bahareh and Salim Lahmiri (2023). Hybrid Deep Learning and GARCH-Family Models for Forecasting Volatility of Cryptocurrencies. *Machine Learning with Applications* 12, 100465.

Aoyagi, Jun and Daisuke Adachi (2018). Fundamental Values of Cryptocurrencies and Blockchain Technology. Working Paper.

Ardia, David, Keven Bluteau, Kris Boudt, and Koen Inghelbrecht (2023). Climate Change Concerns and the Performance of Green vs. Brown Stocks. *Management Science* 69 (12), 7607–7632.

Ardia, David, Keven Bluteau, and Maxime Rüede (2019). Regime Changes in Bitcoin GARCH Volatility Dynamics. *Fianance Research Letters* 29, 266–271.

Aslanidis, Nektarios, Aurelio F. Bariviera, and Alejandro Perez-Laborda (2021). Are Cryptocurrencies Becoming more Interconnected? *Economics Letters* 199, 109725.

Athey, Susan, Ivo Parashkevov, Vishnu Sarukkai, and Jing Xia (2016). Bitcoin Pricing, Adoption, and Usage: Theory and Evidence. Stanford University Graduate School of Business Research Paper No. 16-42.

Atzei, Nicola, Massimo Bartoletti, and Tiziana Cimoli (2017). A Survey of Attacks on Ethereum Smart Contracts (SoK). In: *Principles of Security and Trust: 6th International Conference, POST 2017.* Ed. by Matteo Maffei and Mark Ryan. Vol. 10204. Berlin, Heidelberg: Springer, pp. 164–186.

Auer, Raphael A. and Stijn Claessens (2021). Cryptocurrency Market Reactions to Regulatory News. In: *The Routledge Handbook of FinTech.* Ed. by K. Thomas Liaw. 1st ed. Abingdon: Routledge, pp. 455–468.

Babiak, Mykola and Daniele Bianchi (2021). A Risk-Based Explanation of Cryptocurrency Returns. Working Paper.

Basu, Soumya, David Easley, Maureen O'Hara, and Emin Sirer (2023). StableFees: A Predictable Fee Market for Cryptocurrencies. *Management Science* 69 (11), 6508–6524.

Baur, Dirk G. and Thomas Dimpfl (2018). Asymmetric Volatility in Cryptocurrencies. *Economics Letters* 173, 148–151.

— (2021). The Volatility of Bitcoin and its Role as a Medium of Exchange and a Store of Value. *Empirical Economics* 61, 2663—2683.

Bekaert, Geert and Campbell R. Harvey (1997). Emerging Equity Market Volatility. *Journal of Financial Economics* 43 (1), 29–77.

Berentsen, Aleksander and Fabian Schär (2017). *Bitcoin, Blockchain und Kryptoassets.* Erste Auflage. Norderstedt: BoD - Books on Demand.

Bhambhwani, Siddharth M., Stefanos Delikouras, and George M. Korniotis (2023). Blockchain Characteristics and Cryptocurrency Returns. *Journal of International Financial Markets, Institutions and Money* 86 (12), 101788.

Biais, Bruno, Christophe Bisière, Matthieu Bouvard, and Catherine Casamatta (2019). The Blockchain Folk Theorem. *The Review of Financial Studies* 32 (5), 1662–1715.

Biais, Bruno, Christophe Bisiere, Matthieu Bouvard, Catherine Casamatta, and Albert J. Menkveld (2023). Equilibrium Bitcoin Pricing. *The Journal of Finance* 78 (2), 967–1014.

Bianchi, Daniele (2020). Cryptocurrencies as an Asset Class? An Empirical Assessment. *The Journal of Alternative Investments* 23 (2), 162–179.

Bianchi, Daniele, Mykola Babiak, and Alexander Dickerson (2022). Trading Volume and Liquidity Provision in Cryptocurrency Markets. *Journal of Banking and Finance* 142, 106547.

Bolt, Wilko and Maarten R. C. van Oordt (2020). On the Value of Virtual Currencies. *Journal of Money, Credit and Banking* 52 (4), 835–862.

Borri, Nicola (2019). Conditional Tail-Risk in Cryptocurrency Markets. *Journal of Empirical Finance* 50, 1–19.

Borri, Nicola, Daniele Massacci, Mirco Rubin, and Dario Ruzzi (2022). Crypto Risk Premia. Working Paper.

Bouri, Elie, Chi K. M. Lau, Brian Lucey, and David Roubaud (2019a). Trading Volume and the Predictability of Return and Volatility in the Cryptocurrency Market. *Finance Research Letters* 29, 340–346.

Bouri, Elie, Syed J. H. Shahzad, and David Roubaud (2019b). Co-Explosivity in the Cryptocurrency Market. *Finance Research Letters* 29, 178–183.

Brauneis, Alexander, Roland Mestel, Ryan Riordan, and Erik Theissen (2021). How to Measure the Liquidity of Cryptocurrency Markets? *Journal of Banking and Finance* 124, 106041.

Budish, Eric (2018). The Economic Limits of Bitcoin and the Blockchain. NBER Working Paper No. 24717.

Byström, Hans and Dominika Krygier (2018). What Drives Bitcoin Volatility? Working Paper.

Cai, Charlie X. and Ran Zhao (2024). Salience Theory and Cryptocurrency Returns. *Journal of Banking and Finance* 159, 107052.

Caporale, Guglielmo M. and Timur Zekokh (2019). Modelling Volatility of Cryptocurrencies Using Markov-Switching GARCH Models. *Research in International Business and Finance* 48, 143–155.

Carpentier, Cécile and Jean-Marc Suret (2015). Stock Market and Deterrence Effect: A Mid-Run Analysis of Major Environmental and Non-Environmental Accidents. *Journal of Environmental Economics and Management* 71, 1–18.

Catania, Leopoldo and Stefano Grassi (2022). Forecasting Cryptocurrency Volatility. *International Journal of Forecasting* 38 (3), 878–894.

Charfeddine, Lanouar, Noureddine Benlagha, and Karim B. Khediri (2022). An Intra-Cryptocurrency Analysis of Volatility Connectedness and its Determinants: Evidence from Mining Coins, Non-Mining Coins and Tokens. *Research in International Business and Finance* 62, 101699.

Cheikh, Nidhaleddine B., Younes B. Zaied, and Julien Chevallier (2020). Asymmetric Volatility in Cryptocurrency Markets: New Evidence from Smooth Transition GARCH Models. *Finance Research Letters* 35, 101293.

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

Choi, Michael and Guillaume Rocheteau (2021). Money Mining and Price Dynamics. *American Economic Journal: Macroeconomics* 13 (4), 246–294.

Chu, Jeffrey, Stephen Chan, Saralees Nadarajah, and Joerg Osterrieder (2017). GARCH Modelling of Cryptocurrencies. *Journal of Risk and Financial Management* 10 (4), 17.

Ciner, Cetin, Brian Lucey, and Larisa Yarovaya (2022). Determinants of Cryptocurrency Returns: A LASSO Quantile Regression Approach. *Finance Research Letters* 49, 102990.

Clark, Ephraim, Amine Lahiani, and Salma Mefteh-Wali (2023). Cryptocurrency Return Predictability: What Is the Role of the Environment? *Technological Forecasting and Social Change* 189, 122350.

Cong, Lin W. and Zhiguo He (2019). Blockchain Disruption and Smart Contracts. *The Review of Financial Studies* 32 (5), 1754–1797.

Cong, Lin W., Zhiheng He, and Ke Tang (2022). The Tokenomics of Staking. Working Paper.

Cong, Lin W., G. Andrew Karolyi, Ke Tang, and Weiyi Zhao (2021a). Value Premium, Network Adoption, and Factor Pricing of Crypto Assets. Working Paper.

Cong, Lin W., Ye Li, and Neng Wang (2021b). Tokenomics: Dynamic Adoption and Valuation. *The Review of Financial Studies* 34 (3), 1105–1155.

Cong, Lin W. and Simon Mayer (2021). The Coming Battle of Digital Currencies. The SC Johnson College of Business Applied Economics and Policy Working Paper Series No. 2022-04.

Conrad, Christian, Anessa Custovic, and Eric Ghysels (2018). Long-and Short-Term Cryptocurrency Volatility Components: A GARCH-MIDAS Analysis. *Journal of Risk and Financial Management* 11 (2), 23.

Corbet, Shaen, Charles Larkin, and Brian Lucey (2020). The Contagion Effects of the COVID-19 Pandemic: Evidence from Gold and Cryptocurrencies. *Finance Research Letters* 35, 101554.

Corbet, Shaen, Brian Lucey, and Larisa Yarovaya (2018). Datestamping the Bitcoin and Ethereum Bubbles. *Finance Research Letters* 26, 81–88.

— (2021). Bitcoin-Energy Markets Interrelationships – New Evidence. *Resources Policy* 70, 101916.

Cousins, Karlene, Hemang Subramanian, and Pouyan Esmaeilzadeh (2019). A Value-Sensitive Design Perspective of Cryptocurrencies: A Research Agenda. *Communications of the Association for Information Systems* 45 (27), 511–547.

D'Amato, Valeria, Susanna Levantesi, and Gabriella Piscopo (2022). Deep Learning in Predicting Cryptocurrency Volatility. *Physica A: Statistical Mechanics and its Applications* 596, 127158.

Dittmar, Robert F., Christian Schlag, and Julian Thimme (2020). Non-Substitutable Consumption Growth Risk. SAFE Working Paper No. 408.

Dunbar, Kwamie and Johnson Owusu-Amoako (2022). Cryptocurrency Returns under Empirical Asset Pricing. *International Review of Financial Analysis* 82, 102216.

Dupuis, Daniel and Kimberly Gleason (2020). Money Laundering with Cryptocurrency: Open Doors and the Regulatory Dialectic. *Journal of Financial Crime* 28 (1), 60–74.

Dwyer, Gerald P. (2015). The Economics of Bitcoin and Similar Private Digital Currencies. *Journal of Financial Stability* 17, 81–91.

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

El Ouadghiri, Imane, Khaled Guesmi, Jonathan Peillex, and Andreas Ziegler (2021). Public Attention to Environmental Issues and Stock Market Returns. *Ecological Economics* 180, 106836.

Elkan, Charles and Keith Noto (2008). Learning Classifiers from Only Positive and Unlabeled Data. In: *Proceedings of the 14th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Las Vegas, NV*, pp. 213–220.

Elton, Edwin J. (1999). Presidential Address: Expected Return, Realized Return, and Asset Pricing Tests. *The Journal of Finance* 54 (4), 1199–1220.

Eska, Fabian E., Steffen Hitzemann, and Marliese Uhrig-Homburg (2022a). After *the Merge*: Network Fragility and Robust Design of PoS Cryptocurrencies. Working Paper.

Eska, Fabian E. and Marcel Müller (2024). Climate Change, Energy Prices, and the Returns of Proof-of-Work vs. Proof-of-Stake Crypto Assets. Working Paper.

Eska, Fabian E., Yanghua Shi, Erik Theissen, and Marliese Uhrig-Homburg (2022b). Design and Valuation of Cryptocurrencies. Working Paper.

— (2024). Do Design Features Explain the Volatility of Cryptocurrencies? *Finance Research Letters* 66, 105536.

Europol (2017). Internet Organised Crime Threat Assessment (IOCTA) 2017. Online, https://www.europol.europa.eu/cms/sites/default/files/documents/iocta2017.pdf [Accessed: April 15, 2024].

Fama, Eugene F. and James D. MacBeth (1973). Risk, Return, and Equilibrium: Empirical Tests. *Journal of Political Economy* 81 (3), 607–636.

Fanti, Giulia, Leonid Kogan, Sewoong Oh, Kathleen Ruan, Pramod Viswanath, and Gerui Wang (2019). Compounding of Wealth in Proof-of-Stake Cryptocurrencies. In: *Financial Cryptography and Data Security. FC 2019. Lecture Notes in Computer Science*. Ed. by Ian Goldberg and Tyler Moore. Vol. 11598. Cham: Springer, pp. 42–61.

Feller, William (1968). *An Introduction to Probability Theory and its Applications, Volume 1*. 3rd ed. New York, NY: John Wiley & Sons.

Fernández-Villaverde, Jesús and Daniel Sanches (2019). Can Currency Competition Work? *Journal of Monetary Economics* 106, 1–15.

Fieberg, Christian, Lars Hornuf, Gerrit Liedtke, and Thorsten Poddig (2020). Are Characteristics Covariances? A Comment on Instrumented Principal Component Analysis. CESifo Working Paper No. 8377.

Finck, Michèle (2018). Blockchains: Regulating the Unknown. *German Law Journal* 19 (4), 665–692.

Gallersdörfer, Ulrich, Lena Klaaßen, and Christian Stoll (2020). Energy Consumption of Cryptocurrencies Beyond Bitcoin. *Joule* 4 (9), 1843–1846.

Gandal, Neil and Hanna Halaburda (2016). Can we Predict the Winner in a Market with Network Effects? Competition in Cryptocurrency Market. *Games* 7 (16), 23–29.

Gandal, Neil, J.T. Hamrick, Tyler Morre, and Marie Vasek (2021). The Rise and Fall of Cryptocurrency Coins and Tokens. *Decisions in Economics and Finance* 44, 981–1014.

Garriga, Martin, Stefano Dalla Palma, Maxmiliano Arias, Alan Renzis, Remo Pareschi, and Damian A. Tamburri (2020). Blockchain and Cryptocurrencies: A Classification and Comparison of Architecture Drivers. *Concurrency and Computation: Practice and Experience* 33 (8), e5992.

Geuder, Julian, Harald Kinateder, and Niklas F. Wagner (2019). Cryptocurrencies as Financial Bubbles: The Case of Bitcoin. *Finance Research Letters* 31, 179–184.

Gradojevic, Nikola and Ilias Tsiakas (2021). Volatility Cascades in Cryptocurrency Trading. *Journal of Empirical Finance* 62, 252–265.

Gutsche, Gunnar and Andreas Ziegler (2019). Which Private Investors Are Willing to Pay for Sustainable Investments? Empirical Evidence from Stated Choice Experiments. *Journal of Banking and Finance* 102, 193–214.

Haddad, Valentin and Tyler Muir (2021). Do Intermediaries Matter for Aggregate Asset Prices? *The Journal of Finance* 76 (6), 2719–2761.

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

Harvey, Campbell R., Ashwin Ramachandran, and Joey Santoro (2021). *DeFi and the Future of Finance*. Hoboken, NJ: John Wiley & Sons University Press.

Harvey, John and Ines Branco-Illodo (2020). Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in "Privacy Coin" Whitepapers. *Journal of Political Marketing* 19 (1–2), 107–136.

Hayes, Adam S. (2017). Cryptocurrency Value Formation: An Empirical Study Leading to a Cost of Production Model for Valuing Bitcoin. *Telematics and Informatics* 34 (7), 1308–1321.

He, Zhiguo, Bryan T. Kelly, and Asaf Manela (2017). Intermediary Asset Pricing: New Evidence from many Asset Classes. *Journal of Financial Economics* 126 (1), 1–35.

Hinzen, Franz J., Kose John, and Fahad Saleh (2022). Bitcoin's Limited Adoption Problem. *Journal of Financial Economics* 144 (2), 347–369.

Houben, Robby and Alexander Snyers (2018). Cryptocurrencies and Blockchain: Legal Context and Implications for Financial Crime, Money Laundering, and Tax Evasion. *Manuscript for Policy Department for Economic, Scientific and Quality of Life Policies, European Parliament*. Online, https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on %20cryptocurrencies%20and%20blockchain.pdf [Accessed: April 15, 2024].

Hu, Albert S., Christine A. Parlour, and Uday Rajan (2019). Cryptocurrencies: Stylized Facts on a New Investible Instrument. *Financial Management* 48 (4), 1049–1068.

Hu, Grace X., Jun Pan, and Jiang Wang (2013). Noise as Information for Illiquidity. *The Journal of Finance* 68 (6), 2341–2382.

Huberman, Gur, Jacob D. Leshno, and Ciamac C. Moallemi (2021). Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies* 88 (6), 3011–3040.

Härdle, Wolfgang K., Campbell R. Harvey, and Raphael C. G. Reule (2020). Understanding Cryptocurrencies. *Journal of Financial Econometrics* 18 (2), 181–208.

Irresberger, Felix, Kose John, Peter Mueller, and Fahad Saleh (2020). The Public Blockchain Ecosystem: An Empirical Analysis. NYU Stern School of Business Working Paper.

Jermann, Urban J. (2023). A Macro Finance Model for Proof-of-Stake Ethereum. Working Paper.

Ji, Qiang, Elie Bouri, Chi K. M. Lau, and David Roubaud (2019). Dynamic Connectedness and Integration in Cryptocurrency Markets. *International Review of Financial Analysis* 63, 257–272.

Jo, Hoje, Haehean Park, and Hersh Shefrin (2020). Bitcoin and Sentiment. *Journal of Futures Markets* 40 (12), 1861–1879.

John, Kose, Thomas Rivera, and Fahad Saleh (2021a). Economic Implications of Scaling Blockchains: Why the Consensus Protocol Matters. Working Paper.

— (2021b). Equilibrium Staking Levels in a Proof-of-Stake Blockchain. Working Paper.

Jones, Charles M. and Paul J. Seguin (1997). Transaction Costs and Price Volatility: Evidence from Commission Deregulation. *The American Economic Review* 87 (4), 728–737.

Karnaukh, Nina, Angelo Ranaldo, and Paul Söderlind (2015). Understanding FX Liquidity. *The Review of Financial Studies* 28 (11), 3073–3108.

Katsiampa, Paraskevi (2019). An Empirical Investigation of Volatility Dynamics in the Cryptocurrency Market. *Research in International Business and Finance* 50, 322–335.

Katsiampa, Paraskevi, Shaen Corbet, and Brian Lucey (2019). Volatility Spillover Effects in Leading Cryptocurrencies: A BEKK-MGARCH Analysis. *Finance Research Letters* 29, 68–74.

Kelly, Bryan T., Diogo Palhares, and Seth Pruitt (2023). Modeling Corporate Bond Returns. *The Journal of Finance* 78 (4), 1967–2008.

Kelly, Bryan T., Seth Pruitt, and Yinan Su (2019). Characteristics Are Covariances: A Unified Model of Risk and Return. *Journal of Financial Economics* 134 (3), 501–524.

Kilian, Lutz and Cheolbeom Park (2009). The Impact of Oil Price Shocks on the U.S. Stock Market. *International Economic Review* 50 (4), 1267–1287.

Kim, Thomas (2015). The Predecessors of Bitcoin and their Implications for the Prospect of Virtual Currencies. *PLOS ONE* 10 (4), e0123071.

Kocherlakota, Narayana R. (1998). Money Is Memory. *Journal of Economic Theory* 81 (2), 232–251.

Koenraadt, Jeroen and Edith Leung (2024). Investor Reactions to Crypto Token Regulation. *European Accounting Review* 33 (2), 367–397.

Kolbert, Elizabeth (2024). The Obscene Energy Demands of A.I. *The New Yorker*. Online, https://www.newyorker.com/news/daily-comment/the-obscene-energy-demands-of-ai [Accessed: April 15, 2024].

Koutmos, Dimitrios (2018). Return and Volatility Spillovers among Cryptocurrencies. *Economics Letter* 173, 122–127.

Krause, Max J. and Thabet Tolaymat (2018). Quantification of Energy and Carbon Costs for Mining Cryptocurrencies. *Nature Sustainability* 1 (11), 711–718.

Kristoufek, Ladislav (2020). Bitcoin and its Mining on the Equilibrium Path. *Energy Economics* 85, 104588.

Kristoufek, Ladislav and Miloslav Vosvrda (2019). Cryptocurrencies Market Efficiency Ranking: Not so Straightforward. *Physica A: Statistical Mechanics and its Applications* 531, 120853.

Kyriazis, Nikolaos, Stephanos Papadamou, and Shaen Corbet (2020). A Systematic Review of the Bubble Dynamics of Cryptocurrency Prices. *Research in International Business and Finance* 54, 101254.

Köchling, Gerrit, Janis Müller, and Peter N. Posch (2019). Does the Introduction of Futures Improve the Efficiency of Bitcoin? *Finance Research Letters* 30, 367–370.

Lagos, Ricardo and Randall Wright (2005). A Unified Framework for Monetary Theory and Policy Analysis. *Journal of Political Economy* 113 (3), 463–484.

Leong, Minhao and Simon Kwok (2023). The Pricing of Jump and Diffusive Risks in the Cross-Section of Cryptocurrency Returns. *Journal of Empirical Finance* 74, 101420.

Li, Leon and Peter Miu (2023). Are Cryptocurrencies a Safe Haven for Stock Investors? A Regime-Switching Approach. *Journal of Empirical Finance* 70, 367–385.

Li, Yannan, Willy Susilo, Guomin Yang, Yong Yu, Xiaojiang Du, Dongxi Liu, and Nadra Guizani (2019). Toward Privacy and Regulation in Blockchain-Based Cryptocurrencies. *IEEE Network* 33 (5), 111–117.

Liebi, Luca J. (2022). Is There a Value Premium in Cryptoasset Markets? *Economic Modelling* 109, 105777.

Liu, Weiyi, Xuan Liang, and Guowei Cui (2020). Common Risk Factors in the Returns on Cryptocurrencies. *Economic Modelling* 86, 299–305.

Liu, Yukun and Aleh Tsyvinski (2021). Risks and Returns of Cryptocurrency. *The Review of Financial Studies* 34 (6), 2689–2727.

Liu, Yukun, Aleh Tsyvinski, and Xi Wu (2022). Common Risk Factors in Cryptocurrency. *The Journal of Finance* 77 (2), 1133–1177.

Long, Huaigang, Ender Demir, Barbara Bedowska-Sojka, Adam Zaremba, and Syed J. H. Shahzad (2022). Is Geopolitical Risk Priced in the Cross-Section of Cryptocurrency Returns? *Finance Research Letters* 49, 103131.

Makarov, Igor and Antoinette Schoar (2020). Trading and Arbitrage in Cryptocurrency Markets. *Journal of Financial Economics* 135 (2), 293–319.

— (2022). Cryptocurrencies and Decentralized Finance (DeFi). NBER Working Paper No. 30006.

Metcalfe, Bob (2013). Metcalfe's Law after 40 Years of Ethernet. *Computer* 46 (12), 26–31.

Milkau, Udo (2023). Smart Contract Risk. In: *Decentralized Finance und Tokenisierung: Zukunftsweisende Trends zwischen Smart Contracts und Gamification.* Stuttgart: Schäffer-Poeschel, pp. 273–278.

Mora, Camilo, Randi L. Rollins, Katie Taladay, Michael B. Kantar, Mason K. Chock, Mio Shimada, and Erik C. Franklin (2018). Bitcoin Emissions Alone Could Push Global Warming Above 2°C. *Nature Climate Change* 8 (11), 931–933.

Müller, Marcel, Michael Reichenbacher, Philipp Schuster, and Marliese Uhrig-Homburg (2023). Expected Bond Liquidity. Working Paper.

Nabilou, Hossein and André Prüm (2019). Ignorance, Debt and Cryptocurrencies: The Old and the New in the Law and Economics of Concurrent Currencies. *Journal of Financial Regulation* 5 (1), 29–63.

Nadler, Philip and Yike Guo (2020). The Fair Value of a Token: How Do Markets Price Cryptocurrencies? *Research in International Business and Finance* 52, 101108.

Naeem, Muhammad A. and Sitara Karim (2021). Tail Dependence between Bitcoin and Green Financial Assets. *Economics Letters* 208, 110068.

Næs, Randi, Johannes A. Skjeltorp, and Bernt A. Ødegaard (2011). Stock Market Liquidity and the Business Cycle. *The Journal of Finance* 66 (1), 139–176.

Nakamoto, Satoshi (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Online, available from https://bitcoin.org/bitcoin.pdf [Accessed: April 15, 2024].

Narayanan, Arvind, Joseph Bonneau, Edward Felten, Andrew Miller, and Steven Goldfeder (2016). *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction.* Princeton, NJ: Princeton University Press.

NASA (2024). Global Climate Change - Vital Signs of the Planet. Online, https://climate.nasa.gov [Accessed: April 15, 2024].

Newey, Whitney K. and Kenneth D. West (1987). A Simple, Positive Semi-Definite, Heteroskedasticity and Autocorrelation Consistent Covariance Matrix. *Econometrica* 55 (3), 703–708.

Noda, Akihiko (2021). On the Evolution of Cryptocurrency Market Efficiency. *Applied Economics Letters* 28 (6), 433–439.

Novy, Robert (2018). Prepared Testimony before the United States House of Representatives Committee on Financial Services Subcommittee on Terrorism and Illicit Finance. Online, https://web.archive.org/web/20181129072304/https://financialservices.house.gov/uploadedfiles/hhrg-115-ba01-wstate-rnovy-20180620.pdf [Accessed: April 15, 2024].

Office of Science and Technology Policy (OSTP) (2022). Climate and Energy Implications of Crypto-Assets in the United States. *The White House*. Online, https://www.whitehouse.gov/wp-content/uploads/2022/09/09-2022-Crypto-Assets-and-Climate-Report.pdf [Accessed: April 15, 2024].

Pagnotta, Emiliano S. (2022). Decentralizing Money: Bitcoin Prices and Blockchain Security. *The Review of Financial Studies* 35 (2), 866–907.

Pagnotta, Emiliano S. and Andrea Buraschi (2018). An Equilibrium Valuation of Bitcoin and Decentralized Network Assets. Working Paper.

Panagiotidis, Theodore, Georgios Papapanagiotou, and Thanasis Stengos (2022). On the Volatility of Cryptocurrencies. *Research in International Business and Finance* 62, 101724.

Pástor, Luboš, Robert F. Stambaugh, and Lucian A. Taylor (2015). Scale and Skill in Active Management. *Journal of Financial Economics* 116 (1), 23–45.

— (2022). Dissecting Green Returns. *Journal of Financial Economics* 146 (2), 403–424.

Pessa, Arthur A. B., Matjaž Perc, and Haroldo V. Ribeiro (2023). Age and Market Capitalization Drive Large Price Variations of Cryptocurrencies. *Scientific Reports* 13 (1), 3351.

Pfautsch, Frederik, Nils Schubert, Conrad Orglmeister, Maximilian Gebhart, Philipp Habermann, and Ben Juurlink (2020). The Evolution of Secure Hash Algorithms. *PARS-Mitteilungen* 35 (1), 5–15.

Phillips, Peter C. B., Shuping Shi, and Jun Yu (2015). Testing for Multiple Bubbles: Historical Episodes of Exuberance and Collapse in the S& P 500. *Journal of Financial Economics* 56 (4), 1043–1078.

Phillips, Peter C. B., Yangru Wu, and Jun Yu (2011). Explosive Behavior in the 1990s Nasdaq: When Did Exuberance Escalate Asset Values? *International Economic Review* 52 (1), 201–226.

Polasik, Michal, Anna I. Piotrowska, Tomasz P. Wisniewski, Radoslaw Kotkowski, and Geoffrey Lightfoot (2015). Price Fluctuations and the Use of Bitcoin: An Empirical Inquiry. *International Journal of Electronic Commerce* 20 (1), 9–49.

Ready, Robert C. (2018). Oil Prices and the Stock Market. *Review of Finance* 22 (1), 155–176.

Rocheteau, Guillaume and Randall Wright (2005). Money in Search Equilibrium, in Competitive Equilibrium, and in Competitive Search Equilibrium. *Econometrica* 73 (1), 175–202.

Saleh, Fahad (2018). Volatility and Welfare in a Crypto Economy. Working Paper.

— (2021). Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies* 34 (3), 1156–1190.

Sapkota, Niranjan and Klaus Grobys (2021a). Asset Market Equilibria in Cryptocurrency Markets: Evidence from a Study of Privacy and Non-Privacy Coins. *Journal of International Financial Markets, Institutions and Money* 74 (12), 101402.

— (2021b). Blockchain Consensus Protocols, Energy Consumption and Cryptocurrency Prices. *Journal of Energy Markets* 13 (4), 117–139.

Schestag, Raphael, Philipp Schuster, and Marliese Uhrig-Homburg (2016). Measuring Liquidity in Bond Markets. *The Review of Financial Studies* 29 (5), 1170–1219.

Schilling, Linda and Harald Uhlig (2019). Some Simple Bitcoin Economics. *Journal of Monetary Economics* 106, 16–26.

Schuster, Philipp, Erik Theissen, and Marliese Uhrig-Homburg (2020). Finanzwirtschaftliche Anwendungen der Blockchain-Technologie. *Schmalenbachs Zeitschrift für betriebswirtschaftliche Forschung* 72 (2), 125–147.

Schär, Fabian (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Federal Reserve Bank of St. Louis Review* 103 (2), 153–174.

Shams, Amin (2020). The Structure of Cryptocurrency Returns. Fisher College of Business Working Paper No. 2020-03-011.

Sigalos, MacKenzie (2022). These 23-Year-Old Texans Made $4 Million Last Year Mining Bitcoin Off Flare Gas from Oil Drilling. *CNBC*. Online, https://www.cnbc.com/2022/02/12/23-year-old-texans-made-4-million-mining-bitcoin-off-flared-natural-gas.html [Accessed: April 15, 2024].

Sockin, Michael and Wei Xiong (2023). A Model of Cryptocurrencies. *Management Science* 69 (11), 6684–6707.

Temzelides, Ted and Jialin Yu (2004). Lack-of-Recall and Centralized Monetary Trade. *International Economic Review* 45 (4), 1221–1227.

Tibshirani, Robert (1996). Regression Shrinkage and Selection via the Lasso. *Journal of the Royal Statistical Society: Series B (Methodological)* 58 (1), 267—288.

Trimborn, Simon and Wolfgang K. Härdle (2018). CRIX – An Index for Cryptocurrencies. *Journal of Empirical Finance* 49, 107–122.

Umlauf, Steven R. (1993). Transaction Taxes and the Behavior of the Swedish Stock Market. *Journal of Financial Economics* 33 (2), 227–240.

Urquhart, Andrew (2017). The Volatility of Bitcoin. Working Paper.

U.S. Energy Information Administration (EIA) (2024). Tracking Electricity Consumption from U.S. Cryptocurrency Mining Operations. Online, https://www.eia.gov/todayinenergy/detail.php?id=61364 [Accessed: April 15, 2024].

Vashchuk, Oleksandr and Roman Shuwar (2018). Pros and Cons of Consensus Algorithm Proof of Stake. Difference in the Network Safety in Proof of Work and Proof of Stake. *Electronics and Information Technologies* 9 (9), 106–112.

Viglione, Robert (2018). Japan's Ban Is a Wake-Up Call to Defend Privacy Coins. *CoinDesk*. Online, https://www.coindesk.com/markets/2018/05/29/japans-ban-is-a-wake-up-call-to-defend-privacy-coins/ [Accessed: April 15, 2024].

Wang, Jiqian, Feng Ma, Elie Bouri, and Yangli Guo (2023a). Which Factors Drive Bitcoin Volatility: Macroeconomic, Technical, or Both? *Journal of Forecasting* 42 (4), 970–988.

Wang, Sha and Jean-Philippe Vergne (2017). Buzz Factor or Innovation Potential: What Explains Cryptocurrencies' Returns? *PLOS ONE* 12 (5), e0169556.

Wang, Yijun, Galina Andreeva, and Belen Martin-Barragan (2023b). Machine Learning Approaches to Forecasting Cryptocurrency Volatility: Considering Internal and External Determinants. *International Review of Financial Analysis* 90, 102914.

Wang, Yizhi, Biran Lucey, Samuel A. Vigne, and Larisa Yarovaya (2022). An Index of Cryptocurrency Environmental Attention (ICEA). *China Finance Review International* 12 (3), 378–414.

Wei, Wang C. (2018). Liquidity and Market Efficiency in Cryptocurrencies. *Economics Letters* 168 (1), 21–24.

Wilmoth, Josiah (2018). Japan Wants Cryptocurrency Exchanges to De-List Anonymous Altcoins: Report. *CCN.com.* Online, https://www.ccn.com/japan-is-pressuring-cryptocurrency-exchanges-to-de-list-anonymous-altcoins-report/ [Accessed: April 15, 2024].

Wu, Ke, Spencer Wheatley, and Didier Sornette (2018). Classification of Cryptocurrency Coins and Tokens by the Dynamics of their Market Capitalizations. *Royal Society Open Science* 5 (9), 180381.

Yen, Kuang-Chieh and Hui-Pei Cheng (2021). Economic Policy Uncertainty and Cryptocurrency Volatility. *Finance Research Letters* 38, 101428.

Yi, Shuyue, Zishuang Xu, and Gang-Jin Wang (2018). Volatility Connectedness in the Cryptocurrency Market: Is Bitcoin a Dominant Cryptocurrency? *International Review of Financial Analysis* 60, 98–114.

Zhang, Rong and Wai K. V. Chan (2020). Evaluation of Energy Consumption in Block-Chains with Proof of Work and Proof of Stake. *Journal of Physics: Conference Series* 1584 (1), 012023.

Zhang, Wei, Yi Li, Xiong Xiong, and Pengfei Wang (2021). Downside Risk and the Cross-Section of Cryptocurrency Returns. *Journal of Banking and Finance* 133, 106246.

Zimmerman, Peter (2020). Blockchain Structure and Cryptocurrency Prices. Bank of England Working Paper No. 855.