

Association for Information Systems

AIS Electronic Library (AISeL)

ICIS 2022 Proceedings

Blockchain, DLT, and FinTech

Dec 12th, 12:00 AM

The Impact of Layer 2 Technologies on the Adoption and Security of Blockchain

Leonardo Maria De Rossi

Sda Bocconi School of Management, leonardo.derossi@sdabocconi.it

Michel Avital

Copenhagen Business School, michel@avital.net

Rob Gleasure

Copenhagen Business School, rg.digi@cbs.dk

Rebecca Solcia

Università Bocconi, rebecca.solcia@studbocconi.it

Follow this and additional works at: <https://aisel.aisnet.org/icis2022>

Recommended Citation

De Rossi, Leonardo Maria; Avital, Michel; Gleasure, Rob; and Solcia, Rebecca, "The Impact of Layer 2 Technologies on the Adoption and Security of Blockchain" (2022). *ICIS 2022 Proceedings*. 6.
<https://aisel.aisnet.org/icis2022/blockchain/blockchain/6>

This material is brought to you by the International Conference on Information Systems (ICIS) at AIS Electronic Library (AISeL). It has been accepted for inclusion in ICIS 2022 Proceedings by an authorized administrator of AIS Electronic Library (AISeL). For more information, please contact elibrary@aisnet.org.

The Impact of Layer 2 Technologies on the Adoption and Security of Blockchain

Completed Research Paper

Leonardo Maria De Rossi
Copenhagen Business School
Copenhagen, Denmark
lmdr.digi@cbs.dk

Michel Avital
Copenhagen Business School
Copenhagen, Denmark
michel@avital.net

Rob Gleasure
Copenhagen Business School
Copenhagen, Denmark
rg.digi@cbs.dk

Rebecca Solcia
Bocconi University
Milan, Italy
rebecca.solcia@studbocconi.it

Abstract

Numerous studies have raised concerns over the limited scalability of blockchain technologies and, in particular, Bitcoin. Layer 2 technologies have emerged as an advanced array of complementary innovations designed to solve this problem. Despite the growing optimism around layer 2 technologies, however, there is little evidence to show how they impact blockchain's long-term success. This paper argues that the use and expansion of layer 2 technologies have a positive impact on the adoption and security levels of the underlying blockchain systems. Building on the Bitcoin and Lightning Network case, we use a time-series model based on 1,494 daily observations to demonstrate that the growing activity on the Lightning Network precipitates increased use and better security for Bitcoin. These results highlight the importance of layer 2 technologies for blockchain systems and suggest several further research avenues in this nascent domain of inquiry.

Keywords: Blockchain, Layer 2 technologies, Bitcoin, Lightning Network, Adoption, Security

Introduction

Bitcoin has been a resilient cryptocurrency and network since it was envisioned in 2008 as a protocol to enable the peer-to-peer exchange of money without financial intermediaries (Nakamoto 2008). Bitcoin is also the first and most well-known application of blockchain. The growth of Bitcoin has been extraordinarily successful and has inspired thousands of developers since its appearance. Nonetheless, Bitcoin and blockchain remain heavily scrutinized by scholars of Information Systems, Computer Science, Economics, Finance, Law, and Sociology (Holub and Johnson 2018).

Many of the perceived problems with Bitcoin, and with blockchain in general, relate to scalability – that is, the number of transactions the network can handle per second. Studies have proposed a range of solutions, including new consensus mechanisms for validating transactions, such as Proof-of-Stake (Bartoletti et al. 2017), Proof-of-Space (Ateniese et al. 2014), and Proof-of-Activity (Bentov et al. 2014), as well as optimized block space, aimed at enhancing its 1 megabyte capacity (Gao et al. 2020), and alternative cryptographic algorithms (Courtois et al. 2014).

Bitcoin also has other problems relating to its geometrically decreasing coin release policy, which raises concerns about the anticipated security challenges once the 21,000,000 bitcoin limit is reached (Carlsten et al. 2016). Given that miners will not be able to receive new Bitcoins as a reward, they will have to rely on transaction fees as the main source of payment for validating transactions (Kaskaloglu 2014). This means that unless the mining costs could be drastically reduced, the transaction fees could become prohibitively high or the security prohibitively weak.

Against the backdrop of these concerns, the so-called “layer 2 technologies” have emerged as an advanced array of complementary blockchain innovations (Sguanci et al. 2021). This new generation of technologies can interface with the first-layer infrastructure without modifying the core blockchain protocol. Specifically, they use the underlying blockchain to cryptographically validate entire bundles of transactions as a single settlement, thereby unloading the blockchain from intermediate exchanges of money between parties (Sguanci et al. 2021). Some have argued these layer 2 technologies can improve scalability without corroding the positive aspects related to blockchain security (Del Monte et al. 2020).

In the context of Bitcoin, a central protocol belonging to the layer 2 solutions is the Lightning Network. This protocol was proposed by Poon and Dryja (2016) with the core objective of making Bitcoin a scalable and secure medium of exchange. In the original paper, the authors envisioned a new network on top of the first Bitcoin layer, in which parties could charge payment channels with bitcoins and proceed to transact until transmission of the final settlement to the blockchain, thereby saving block space by recording just one entry, instead of multiple entries, over the Bitcoin blockchain (Poon and Dryja 2016). Use-cases of this layer 2 solution include the government-driven El Salvador experiment in 2021 (Gorjón Rivas 2021) and the Lugano Plan B project by Luxochain. Both of these examples allow citizens to use Bitcoin as a legal currency to buy physical products, pay taxes and receive subsidies. Despite the growing optimism around layer 2 technologies, there is little evidence to show how they impact blockchain’s success in terms of popularity and network security. Such evidence is important because there are reasons to believe layer 2 technologies may not be as successful as first envisioned.

For example, two of the central ideological pillars of Bitcoin are its decentralization and its non-discrimination between individuals or groups. The Lightning Network arguably challenges these principles (Lee and Kim 2020), as benefits mostly accrue to those users making payments often and forming lasting payment sub-networks with other participants. This means that regular users may experience lower costs and more secure transactions than new or casual users. In other words, the Lightning Network creates a two-tier system that some users may find ideologically unappealing. Thus, this study aims to empirically explore the early effects of layer 2 technologies upon blockchain. Specifically, we ask: *What is the effect of layer 2 technologies on the adoption and security of blockchain?*

This research question is not only of empirical interest but also of theoretical and practical significance. One of the major developments in the open-source software field – arguably the largest decentralization-focused sociotechnical movement before blockchain – was that a formative ideological fixation on decentralization gradually gave way to pragmatic concessions in the interest of the common good (Fitzgerald 2006). As a technology, blockchain has followed a similar tendency, with businesses developing hybrid distributed ledger systems for a wide range of commercial settings that limit decentralization (Labazova 2019). However, there is evidence that decentralization remains a major aspect of interest for many cryptocurrency users (Cohen 2017; Fisch et al. 2021; Renwick and Gleasure 2021), raising doubts about whether the same pattern of pragmatic concessions is likely.

Subsequently, to explore this question, we rely on an econometric analysis of time-series data for Bitcoin and the Lightning Network. We selected Bitcoin and the Lightning Network for two major reasons. First, Bitcoin is the cryptocurrency market leader, accounting for 42% of the entire market in May 2022 (Coinmarketcap, 2022). Second, a fundamental prerequisite for the development of significant time-series analysis is the availability of large amounts of data. As the oldest cryptocurrency, Bitcoin offers a longer timeline to study than any other blockchain. The same reasoning also applies to the Lightning Network, the oldest and most diffused of Bitcoin’s layer 2 technologies (De Rossi et al. 2022). The next section provides the theoretical background, describing Bitcoin together with its bottlenecks, and culminates in two hypotheses that link the growing expansion of the Lightning Network with improved use and security in the Bitcoin network. We then present the method for the study, including how we gathered data and operationalized variables. Following this, we present the results of the analysis, which show support for

both hypotheses. Finally, we provide concluding remarks on the contributions to both literature and practice, starting from these new insights.

Theoretical Background

The Bitcoin Protocol

The Bitcoin protocol was proposed by Satoshi Nakamoto as a “*purely peer-to-peer version of electronic cash*” that “*would allow online payments to be sent directly from one party to another without going through a financial institution*” Nakamoto (2008, p1). Bitcoin built on concepts that were already present decades before its creation, such as encryption tools, digital signatures, timestamping, synchronicity of broadcast, and fault tolerance, ultimately creating an immutable distributed ledger of transactions. Specifically, Bitcoin proposed a system of electronic coins, using chains of digital signatures to confirm the exit and the receipt of the transactions via hash-based verification mechanisms (Ramaswamy 2020). Each coin, therefore, carries the whole timeline of its owners, and, in order to be exchanged via a transaction, the network must adhere to a single, validated version of the timeline for all coins in the network. The Proof-of-Work (PoW) mechanism is used to regularly validate the transactions and append the block to the chain, at which point it is broadcasted to all participants on the network.

New coins are awarded to the miners, i.e., the users who make the effort to validate transactions. This means there is a gradual increase in the supply of bitcoins in the network. The number of coins awarded to miners is reduced over time, halving every 210,000 blocks or roughly four years to account for the greater computational capabilities available to miners. This process will continue until the network hits its hard-coded limit of 21 million bitcoins that can be produced.

Miners also receive transaction fees as an incentive. Transaction fees are fees that users may pay when making a payment over Bitcoin. Payments that pay higher transaction fees are more likely to be processed quickly, as miners tend to prefer blocks composed of higher fees. After 2140, the year in which Bitcoin is expected to reach the 21 million supply limit, transaction fees will play a crucial role in the participation levels of the users in the blockchain environment (Easley et al. 2019).

The Popularity and Security of Bitcoin

Since its creation, Bitcoin has been able to draw the public’s attention, with a current average of 1 million users actively transacting over the network daily. During August 2022, Bitcoin reached 500,000 daily Twitter mentions; almost double the number of mentions of any other cryptocurrency (The Block, 2022). Bitcoin has been praised as a sustainable asset class with mean reverting returns (Uddin et al. 2020) and as a form of money that can enhance the performance of time, security, and decentralization at the same time (Tanner 2020). Hence, Bitcoin users often include both ideological supporters and investors trying to gain from pure speculation, for many of whom the first cryptocurrency is seen as one of the biggest wealth generation opportunities of the century (Hackett and Wieczner 2018).

A wide range of solutions has been proposed to enhance Bitcoin’s potential as a trading platform and a medium of exchange (Hafid et al. 2020). In fact, if we operationalize scalability as the capacity of a system to handle greater amounts of work, it becomes clear that Bitcoin’s high congestion is a major problem in the network. With an average processing capacity of between 3.3 and 7 transactions per second and long confirmation times, Bitcoin loses the possibility of functioning as a method of trade (Poon and Dryja 2016). As fees are positively correlated, and congestion is negatively correlated, with Bitcoin returns, the negative relation between the level of congestion and Bitcoin’s price level confirms the idea that the possibility of working as a medium of trade is hindered by the increasing transaction fees (Kim 2020).

The Lightning Network

To enable improvements in Bitcoin’s processing capacity, the mere increase in block size is not a viable solution, as it could lead Bitcoin towards greater levels of centralization in the mining ecosystem and lower security, thereby disrupting two of the three elements of the blockchain scalability trilemma (Altarawneh et al. 2020). Other solutions, including looking for higher throughput, greater storage, lower cost, and shorter latency, all refer to enhancements that can take place at an upper level with respect to the

blockchain. Effective blockchain scalability solutions can be implemented either on the first layer, such as sharding and Proof-of-Stake, or on the second layer, such as the Lightning Network, which is theoretically capable of handling billions of transactions per second (Hafid et al. 2020).

With regards to the Lightning Network, the layer 2 solution was created as a reaction to the scalability problem of Bitcoin in 2016, and its main implementations were developed starting from the BOLT protocol and Bitcoin's SegWit upgrade, rendering it the most viable solution for Bitcoin's problems to the present day. Through the creation of a layer composed of payment channels on top of the blockchain, the Lightning Network was intended to free Bitcoin's mempool, where idle transactions waited for confirmation, by processing most of the activities off-chain and recording just the final output over the main blockchain. Even with the criticism related to the risk of Lightning leading to more centralization of the Bitcoin network (Lin et al. 2020) and the potential hackability of the systems in terms of the public information it provides (Kappos et al. 2021), there are predictions that the Lightning Network could become a crucial element, if Bitcoin is to become a well-established currency and an accepted medium of exchange (NYDIG 2022).

The theoretical ground for the Lightning Network was first laid in the whitepaper titled *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, published in 2016. Born as a decentralized system able to deal with micropayments transacted off-chain over an upper-level network, it was the first layer 2 solution proposed for Bitcoin (Poon and Dryja 2016). Having observed that a simple increment in block size for Bitcoin would not have been a viable solution, the authors proposed to offload the transactions by creating a network of micropayment channels between couples of parties that, upon loading money over the channel, have to broadcast the transactions on the Bitcoin blockchain, used as a timestamping system. The micropayment channels are created when two parties agree to open a 2-of-2 multisignature address and start using it as a parallel solution to the normal blockchain. The two participants create an unsigned funding transaction, charging the channel with money, and both parties need to agree to spend from the initial transaction, also called the "Funding Transaction". Having created the unbroadcasted Funding Transaction, the parties sign and exchange an initial "Commitment Transaction". Such Commitment Transactions spend money from the output of the Funding Transaction. The Funding Transaction is broadcasted to the network, but the next Commitment Transactions are not recorded onto the blockchain until the closing of the micropayment channel and the payment of the updated balance to each party.

The initial problem with the simple system of updated Commitment Transactions is that, when both parties agree to sign a new Commitment Transaction, any of the previous Commitment Transactions could potentially be broadcasted because they are all validly signed by both parties during the exchange process. This setting gives the incentive to the party with the lowest balance to claim that the true, valid, transaction is a transaction giving that party more money than it could actually claim.

To cope with the problem of asynchronous and false broadcasts, the parties involved establish a system of commitments and penalties (enforcing the original commitments). If one party decides to deviate, that party loses all the money initially funded to the channel. Penalties are enforceable via a mechanism of unique identification of the Commitment Transaction: each party has a version of the Commitment Transaction that is signed by the other party, and one party can just broadcast its own version of the Commitment Transaction, thereby making it easier to identify the faulty node. Additionally, as this partial solution is able to apportion blame, the possibility of revoking a Commitment Transaction is also included. The main element used for the Revocable Transactions (i.e., the revocable version of the Commitment Transactions) is the so-called "Revocable Sequence Maturity Contract" (RSMC), a Bitcoin script used to express the present balance of a channel without having to broadcast transactions to the Bitcoin blockchain and without having to trust the counterparty. By allowing the aggrieved party to sign a superseding Breach Remedy Transaction that gives them all the funds in case of contract breach, RSMCs are a disincentive for either party from broadcasting the wrong, old, transactions. If instead, both parties agree on the final transaction, the RSMC is needed to deliver the Revocable Delivery Transaction, to claim their share of Bitcoins.

If both parties decide jointly to close a channel, they take the balances in the most recent Commitment Transaction and spend from the Funding Transaction with another type of transaction called Exercise Settlement Transaction, which is recorded onto the Bitcoin blockchain. Finally, the Hashed Timelock Contract (HTLC) enables the secure transfer of funds across two parties that are not directly linked via a channel but whose connection is characterized by multiple hops across the network. Though the use of

cryptographically secured time-based escrows, funds are ensured to reach the final destination: if the claiming party is not the owner of the right private key associated with the linking hashed public key, or does not claim the funds within the timeframe, the funds are sent back to the origin.

The Impact of the Lightning Network on Bitcoin's Popularity and Security

The reasons why users adopt Bitcoin are varied. In principle, the different types of users can be ideologically divided into two main groups: the “hodlers”, setting limits and floors, and the “speculators”, creating upsides and attracting new users (Loi 2017). While both groups are able to generate a virtuous circle in terms of involvement, the first keeps their Bitcoins irrespective of the price due to either a strong belief in Bitcoin's ability to function as a store of value or trust in the underlying principles and technology, while the latter try to gain from the volatile behavior that has been characterizing the currency up to the present (Loi 2017). Moreover, there are users who actually perceive the potential of Bitcoin as an alternative method of payment, although the latency of the network is considered a major problem in this sense (Baur et al. 2015). More recently, Bitcoin's adoption has acquired an additional, more bureaucratic dimension related to its introduction as a form of legal tender. The example provided by El Salvador is foreseen to be followed by other emerging economies, thereby bringing the layer 2 technology (or, its unit of account) closer to its realization in everyday life (Arcane Research 2021).

This setting has provided motivation for the design and implementation of the Lightning Network. This layer 2 technology allows the Bitcoin system to scale to a point at which it can be widely applicable as a medium of exchange (Hoogendoorn 2019). Bitcoin can presently process about 3.3–7 transactions per second (Nakamoto 2008). In contrast, Visa can process around 2,000 transactions per second and reached a peak of 47,000 during the holiday period in 2013 (Poon and Dryja 2016). PayPal achieves a more modest average of 193, while Ethereum, the direct competitor of Bitcoin, can process about 20 transactions per second (Mechkaroska et al. 2018). This has led some to conclude that Bitcoin simply cannot compete in the domain of payment platforms with its current capacity limitations (Misra 2018).

Thus, despite the aforementioned criticisms of the Lightning Network protocol potentially causing higher centralization of the network (Lee and Kim 2020), the Lightning Network addresses Bitcoin's seemingly critical issue of low capacity, which appears to be a serious concern for potential users (Hinzen et al. 2022). With Lightning Network's fees remaining negligible (Khan and State 2019) and, eventually, proportional to the square root of channel capacity, an improved balance may be reached between paths, fees, and capacity, allowing for higher sustainability of the Lightning off-chain operations (Jun Ren et al. 2019). Based on these practical benefits of the Lightning Network, we hypothesize that more users will be attracted to the Bitcoin network than repelled by it.

H1: The expansion of the Lightning Network has a positive impact on the adoption of Bitcoin.

Transaction fees are, together with block rewards, the unique source of revenue for the miners in the PoW distributed consensus mechanism, which, by definition, requires intensive computational resources to solve (Nakamoto 2008). The presence of a satisfactory recompense for miners is crucial to the network, making it economically unprofitable for the security providers to append a fallacious block to the chain (Ciaian et al. 2021). Empirical research has demonstrated that, given a fixed block capacity (i.e., a limited number of transactions to be included in the next space on the chain), fees should remain essentially high to keep the levels of security stable (Houy 2014).

The Lightning Network can perform secure instant payments without actually relying on the Bitcoin blockchain (Poon and Dryja 2016). For this reason, the Lightning Network appears to reduce the number of blocks mined on the Bitcoin blockchain, with estimated reductions of 25 blocks in January 2019 growing to reductions of 332 blocks in July 2021 (Arcane Research 2021). The effect this could have on security is not clear. It is conceivable that the reduction in actual mining could diminish security, as the act of mining is essential to the security of decentralized blockchains. However, there is evidence that the Lightning Network should not lose funds to malicious players and can be run side by side with other protocols (such as the Bitcoin layer 1) without compromising security requirements (Kiayias and Litos 2020). This could mean a net improvement in security, as the more transactions that can be bundled in mining tasks, the more value is created, and thus the higher is the acceptability of growing transaction fees. Thus, we hypothesize that the growing use of the Lightning Network will maintain the level of security of Bitcoin.

H2: The expansion of the Lightning Network has a positive impact on the security of Bitcoin.

Data Collection

Data Gathering

We retrieved online data using Python 3.8 and the Requests and Selenium libraries, combined with simple ‘GET requests’ and other advanced web-scraping techniques. These techniques were adopted to efficiently automate the process of data retrieval from the publicly available datasets for Bitcoin and the Lightning Network. We retrieved data for the number of active addresses using the Crypto Compare website, which offers an API service with historical data. We retrieved data for the Lightning Network via web-scraping of the Bitcoin Visuals website. Finally, we retrieved data for the Fee Ratio Multiple (FRM) from Glassnode, a website that provides subscribers with detailed on-chain and financial metrics. For the analysis, we used E-Views 12. Complete daily data were available for the entire time period from the 26th of January 2018 to the 28th of February 2022.

Measurement

Variable	Measures	Description	Source
Expansion of the Lightning Network	Number of Public Channels	Total number of visible public channels over the Lightning Network	Bitcoin Visuals
	Channel Capacity	Total balance in USD made available for a certain channel in the Lightning Network	Bitcoin Visuals
Adoption of Bitcoin	Number of Active Addresses	Number of addresses with at least one transaction per day	Crypto-compare
Security of Bitcoin	FRM	Distance to cover in order to sustain current security levels through transaction fee revenue	Glassnode
Table 1. Overview of Measures			

Expansion of the Lightning Network. This variable relies on two measures. The first is the total number of visible public channels over the Lightning Network. Users that open a Lightning Network channel first finance the channel with money, thereby committing to the usage of the channel, and then proceed to send and receive money via a series of Commitment Transactions. The second measure is the average Lightning Network channel capacity. Differing from the number of channels opened, the capacity of a channel can be an effective measure to understand how many channels are actually used to exchange money. Channel capacity indicates the total balance made available for a certain channel. The total amount of satoshis deposited (and, therefore, locked) in the channel is the sum of the balance associated with every user participating in the channel and remains the same for the whole lifespan of the channel. Note that opening a lightning channel or changing its capacity does not mean an inactive account is considered ‘active’ for the purposes of measuring Bitcoin use. Rather, the use of the Lightning Network constitutes a structural change among active users, which may or may not encourage subsequent use.

Adoption of Bitcoin. The use of Bitcoin is measured by the total number of active end users. In Bitcoin, end users are represented by a specific cryptographic fingerprint, called an address, used in the same way as the beneficiary’s name on a check. The distinction between dormant and active addresses is based on the number of transactions made per day: active addresses correspond to users who have completed at least one transaction per day (De Rossi et al. 2022).

Security of Bitcoin. This variable is measured with the Fee Ratio Multiple (FRM), an index that measures the distance PoW chains have to cover to sustain current security levels solely through transaction fee revenue (Leibowitz 2018). The FRM index builds on the concept of a ‘Fee Ratio’ statistic (Carter 2020) that represents the level of block rewards and transaction fees paid to miners that are necessary to secure the chain. Leibowitz (2018) proposed FRM to calculate the multiple of existing transaction fee revenue that would be required to reach the Fee Ratio statistic. Low levels of FRM mean that an asset can maintain its current security budget without relying on inflationary subsidies, while high levels of FRM suggest that an asset will require heavy inflation via block reward subsidies to maintain its security budget (Leibowitz 2018). Thus, the FRM indicates the health of the network in terms of security (Easley et al. 2019).

Data Analysis

We performed the analysis following three main steps. The first step in the analysis applied the Vector Autoregressive analysis (VAR) model (Asteriou and Hall 2007; Guidolin and Pedio 2018), which is used to define and explore the relations between our variables, assuming they are endogenous (Guidolin and Pedio 2018).

The second step applied the Granger Causality Test (GCT) (Granger 1969; Granger and Newbold 1974), which allows us to identify directed Granger-causal relationships. Note that Granger causality does not necessarily imply ‘true’ causality (Maziarz 2015). Hence, we use the term ‘Granger-causes’, rather than ‘causes’ in this study. This is because Granger causality belongs to the branch of causal discovery, rather than causal inference (also known as treatment effect estimation) (Moraffah et al. 2021). As such, the GCT allows common causes to be ruled out in favor of ‘faithful’ temporal sequences, allowing for causal prediction without necessarily ruling out other causal paths or accommodating factors (Granger 1969; Holland 1986).

Finally, following the recommended practice (Enders 1995; Stock and Watson 2001), we complemented our time series analysis with Impulse Response Functions (IRFs) (Guidolin and Pedio 2018). IRFs act over the error term that is already included in the simultaneous equation. IRFs can thus simulate how the system may respond when one of its variables is shocked. Note that we do not speculate on the cause of the shock, only that such shocks are possible due to external events.

Vector Autoregressive Analysis

The VAR model is intended to deal with variables that are not only explanatory variables for a certain other variable but are influenced, and explained, by that same variable. For example, assuming a simple bivariate model, with the variables y_1 and y_2 influencing one another, the mathematical representation of the equations composing the co-dependent system are as follows:

$$y_{1,t} = \beta_{1,0} - \beta_{1,2}y_{2,t} + \gamma_{1,1}y_{1,t-1} + \gamma_{1,2}y_{2,t-1} + u_{1,t} \quad (1)$$

$$y_{2,t} = \beta_{2,0} - \beta_{2,1}y_{1,t} + \gamma_{2,1}y_{1,t-1} + \gamma_{2,2}y_{2,t-1} + u_{2,t} \quad (2)$$

This illustrative bivariate VAR(1) includes two equations, one for each variable, whose regressors are the variables included in the system lagged by the number of periods indicated for the VAR (in this case, one). Additionally, the assumptions behind the system of variables represented in Equations (1) and (2) are that both $y_{1,t}$ and $y_{2,t}$ are stationary processes and that $u_{1,t}$ and $u_{2,t}$ are uncorrelated white-noise errors. The same reasoning applies for multivariate VAR(p) models, where a number of different simultaneous variables can be included, lagged by a number p of periods.

The simultaneous dependent variables of the VAR system constructed starting from our theoretical model are the Number of Public Channels, the Channel Capacity, the Number of Active Addresses and the FRM, which could be seen as $y_{1,t}$, $y_{2,t}$, $y_{3,t}$ and $y_{4,t}$ in light of the previous specification.

The lag order selection criteria suggest a different number of lags for the VAR, with the AIC and the FPE criterion pointing at a value of 21 lags and the SC indicating 7 lags. For parsimony and consistency, the number of lags selected for the model is 7, leading to the final estimation of a VAR(7) containing four endogenous variables and an exogenous constant C . As the number of included lags is chosen to be 7, the right-hand side of each equation will contain the equation-specific constant, its white noise error, and the lags from 1 to 7 of each of the four variables. In total, the final estimation of the VAR will contain 116 parameters: four sets of 28 coefficients each, and four constants. The sample for this VAR(7) considers the 1,494 daily observations from the 26th of January 2018 to the 28th of February 2022.

Before applying VAR and GCT, some preliminary analyses of the data are required. In fact, Engle and Granger (Engle and Granger 2015) demonstrated that using these models in the presence of non-stationary variables can lead to spurious results. Therefore, the first step in the analysis was to determine whether the four series were stationary. We tested for the presence of a unit root through the Augmented Dickey-Fuller (ADF) test. The results suggest that all the variables present non-stationary time-series. In the case of non-stationarity, a typical approach used to obtain stationarity is called differencing (Granger and Joyeux 1980).

Thus, we calculated the first difference of the variables and re-examined the outcome using the ADF stationarity test. The results suggested these transformed variables were stationary.

Table 2 presents the results of the VAR(7) estimation. In this case, all the variables are treated as endogenous, and no ordering is assumed for the estimation step. The Number of Public Channels is deemed to be influenced by its past values, except for its fourth, sixth and seventh lags; by the Channel Capacity, by its second lag; and by the FRM by its first lag. The regression for the Number of Public Channels does not display any passive effects from the Number of Active Addresses over the Bitcoin main network, as the coefficients are not significant at this confidence level. Moreover, as shown by the other variables, the effects they have over the Number of Public Channels have a rather synchronous effect, with lags greater than three having a reduced impact over the dependent variable. Despite the significance of a great part of the regressors included, the model is well-behaved, with an adjusted R^2 of 0.19.

			Expansion of the Lightning Network		Adoption of Bitcoin	Security of Bitcoin
Variable	Measures	Lags	Number of Public Channels	Channel Capacity	Number of Active Address	FRM
Expansion of the Lightning Network	Number of Public Channels	1	0.13***	0.28***	-0.17	0.85*
		2	0.06**	-0.02	-0.01	-0.37
		3	0.16***	-0.11	0.24	0.16
		4	0.05	0.07	-0.12	0.11
		5	0.05*	-0.04	-0.02	-0.24
		6	0.04	-0.04	0.09	-0.93**
		7	0.00	-0.17**	0.05	0.77*
	Channel Capacity	1	0.02	-0.01	0.17***	-0.27*
		2	0.02*	0.01	0.15***	-0.36***
		3	0.00	-0.02	0.19***	-0.08
		4	-0.01	0.03	0.07	-0.01
		5	0.00	0.02	0.07	-0.16
		6	0.00	0.04	0.06	-0.10
		7	0.00	-0.02	0.02	-0.17
Adoption of Bitcoin	Number of Active Address	1	0.00	0.02	-0.61***	0.15*
		2	0.00	0.01	-0.57***	0.32***
		3	0.00	0.03	-0.48***	0.48***
		4	0.00	0.03	-0.40***	0.51***
		5	0.00	0.03	-0.41***	0.70***
		6	0.00	0.02	-0.33***	0.38***
		7	0.00	0.00	0.08***	-0.37***
Security of Bitcoin	FRM	1	0.01***	0.00	-0.05***	-0.17***
		2	0.00	0.00	0.01	-0.26***
		3	0.00	0.00	0.01	-0.10***
		4	0.00	0.01	0.02	-0.10***
		5	0.00	0.00	0.04***	-0.09***
		6	0.00	0.01	0.02*	-0.01
		7	0.00	-0.01	-0.07***	0.17***
Adjusted R²			0.19	0.01	0.55	0.39
Confidence levels: *95%, **97.5%, ***99%						
Table 2. Vector Autoregressive Analysis, Results						

Channel Capacity is not sufficiently explained by the other endogenous variables, even when considering their past values. With an adjusted R^2 of 0.01, the significant model coefficients are the first and seventh lags of Channel Capacity itself and the intercept.

The third result is the OLS-estimated equation for the Number of Active Address, the measure for the adoption of Bitcoin. Although the Number of Public Channels does not have a strong impact on the Number of Active Addresses, the coefficients for the present and past values of Channel Capacity (from lag 1 to 3), together with past values of the Number of Active Addresses itself (from lag 1 to 7), are able to direct and explain the continuously compounded growth of the dependent variable. The FRM shapes such growth when accounting for the fifth, sixth, and seventh lags, increasing the growth in the number of Number of Active Addresses in an asynchronous way, impacting it with its past values rather than the most recent ones. With an adjusted R^2 of about 0.55, the regression variance is well explained by past values of the endogenous variables belonging to the theoretical model envisioned.

Finally, the last endogenous dependent variable included in the VAR(7) model is the FRM. With an adjusted R^2 of 0.39, the model is influenced by past and present values of all endogenous variables in different fashions. While the coefficients representing the values of both the Number of Active Addresses and the FRM itself are significant in all the periods considered, the Number of Public Channels has significant coefficients at lags 1, 6 and 7, and Channel Capacity has significant coefficients for lags 1 and 2.

Granger Causality Test

An interesting feature of the VAR model is that it enables testing for the direction and the presence, if any, of causality between the different endogenous variables of the simultaneous equation system. The concept of “causality” has been introduced by Granger (1969) in the context of time series econometrics to represent the idea that the cause must happen before its effect in time. A variable $y_{2,t}$ is said to Granger-cause another variable $y_{1,t}$ if past values of $y_{2,t}$ help in predicting $y_{1,t}$, given the past values of $y_{1,t}$.

	Variables	Measures	Chi-sq	df	p-value
Expansion of the Lightning Network	Number of Public Channels	Channel Capacity	8.53	7	0.29
		Number of Active Addresses	2.66	7	0.91
		FRM	20.29	7	0.00***
	Channel Capacity	Number of Public Channels	22.73	7	0.00***
		Number of Active Addresses	7.36	7	0.39
		FRM	7.06	7	0.42
Adoption of Bitcoin	Number of Active Addresses	Number of Public Channels	5.41	7	0.61
		Channel Capacity	47.70	7	0.00***
		FRM	142.01	7	0.00***
Security of Bitcoin	FRM	Number of Public Channels	14.46	7	0.04*
		Channel Capacity	19.27	7	0.01**
		Number of Active Addresses	225.13	7	0.00***
* p < .05, ** p < .01, *** p < .001					
Table 3. Granger Causality/Block Exogeneity Wald Test					

Table 3 contains the results of the tests performed on the dataset used to estimate the VAR(7) model presented before. The null hypothesis of the test is that lagged values of a given excluded variable do not explain (or, more precisely, do not Granger-cause) the variation of the dependent variable. Table 3 is composed of four sub-tables, each having a dependent variable of interest and the remaining three endogenous variables as regressors. Given the dependent variable, each of the three excluded variables occupies a row, in which the p-value of the Granger Causality test is provided.

According to the output of the Granger Causality tests performed over the VAR(7), Number of Public Channels Granger-causes FRM, and Channel Capacity Granger-causes Number of Active Addresses and FRM. Moreover, we identified two other interesting relationships. First, FRM Granger-causes both Number of Public Channels and Number of Active Addresses; second, Number of Active Addresses, in turn, Granger-causes FRM, together with Channel Capacity.

Impulse Response Functions (IRFs)

IRFs to Cholesky one standard deviation innovations are used to understand how the previously tested Granger-causal relationships shape the interaction between the variables in a more applied setting. IRFs simulate the response to a standard deviation shock in the error term of a given equation of the estimated structural VAR. Using the Cholesky transformation to enable the identification of the model, the relationships between the endogenous variables are transformed following a transformation of the matrix of contemporaneous effects of the estimated model into its lower-triangular version. As a consequence, the ordering of the variables is of crucial importance, together with the related assumption that some shocks might hit certain variables in a synchronous way, while impacting the remaining variables in subsequent time periods.

Given the necessity to order the variables from the most exogenous to the most endogenous, the sequence assumed for the channel-level IRFs specification is first the Number of Public Channels, second the Channel Capacity, third the Number of Active Addresses and, lastly, the FRM. This assumption is formed based on both the theoretical background and the GCT results. The Number of Public Channels affects the average channel capacity. The Lightning environment influences, in turn, the activity over Bitcoin, as transactions over the blockchain are needed to open and close Lightning payment channels (Poon and Dryja 2016). Finally, the levels of the FRM depend on the health of the Bitcoin network, which is causally influenced by and algorithmically tied to the Lightning protocol. For this reason, the ordering assumed for the channel-level IRFs specification is first the Number of Public Channels, second the Channel Capacity, third the Number of Active Addresses and, lastly, the FRM.

Figure 1 represents the accumulated response of the Number of Active Addresses to a one standard deviation shock in the Channel Capacity.

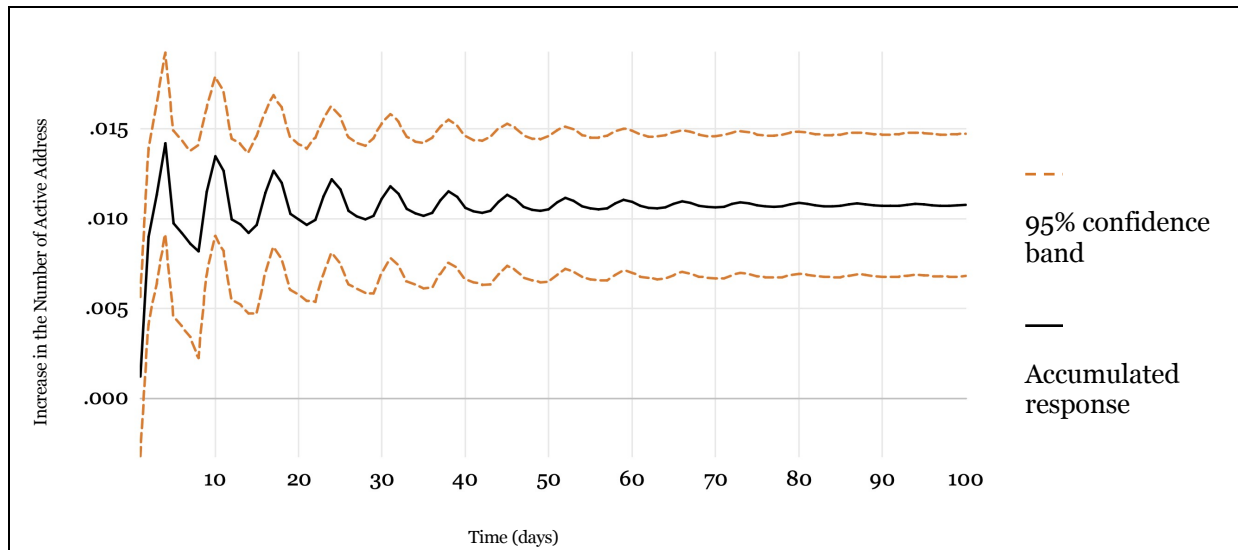


Figure 1. Accumulated Response of Number of Active Address to Cholesky One Standard Deviation Shock in the Channel Capacity

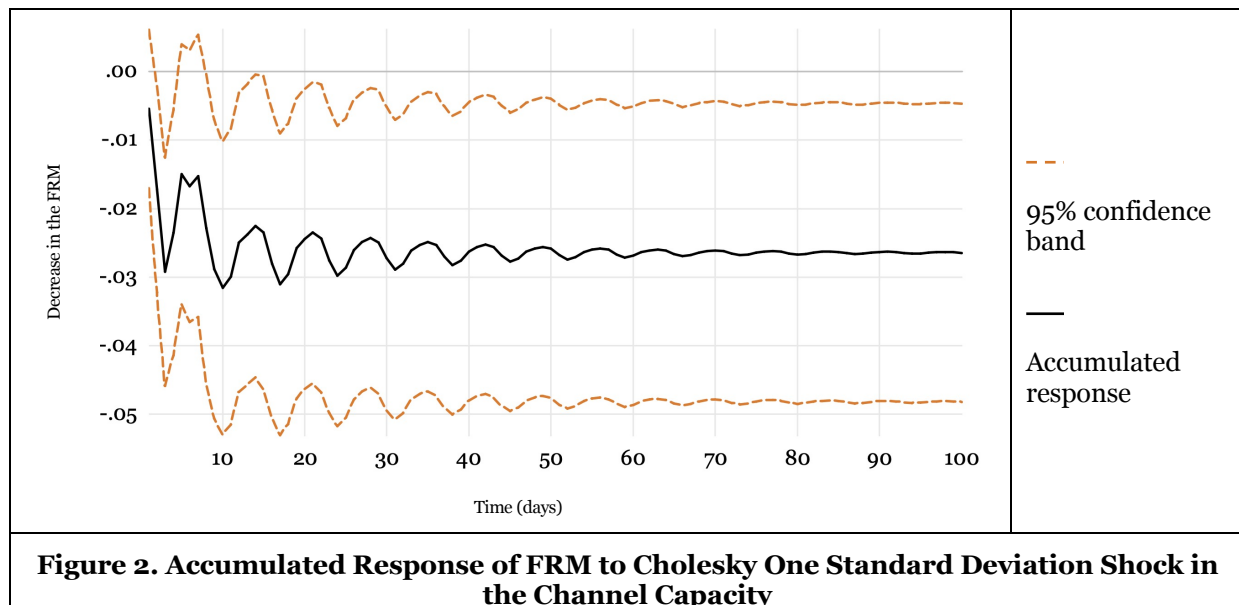
The accumulated response of the Number of Active Addresses to a one standard deviation shock in the Channel Capacity is strictly positive and significant. With an oscillatory behavior, the response peaks within the first few days, reaching a level of 0.014, and then remains around an average of 0.011 for the following

periods. The reduced numbers are a consequence of using the differencing of the variables, which also means that the results can be read in terms of the continuously compounded growth rate of the Number of Active Addresses following a one standard deviation shock in the continuously compounded growth rate in the Channel Capacity. This finding can be translated into the simple affirmation that, following the increasing growth in adoption of the Lightning Network, continuously positive growth can also be expected in the future for the adoption of Bitcoin.

Figure 2 represents the accumulated response of the FRM to a one standard deviation shock in the Average Channel Capacity.

A similar situation, with opposite consequences, can be found when analyzing the accumulated response of the FRM to a one standard deviation increase in the Channel Capacity. With the actual levels of the impact being interpreted in terms of continuously compounded growth rate, an increase in the growth of the usage of the Lightning Network results in sustained decreasing growth of the FRM. The long-term level of convergence of growth can be identified at -0.028 . The first periods are characterized by oscillatory trends, with the impacts for periods 5 to 8 not being significant yet remaining consistently negative in the projection.

These results suggest that an increase in the growth rate of the Number of Active Addresses results in an initial decrease in the FRM, followed by an increase. The activity over the main network first increases the demand for transactions, creating general positive feedback of the mining network (proxied by the fees), improving the network security and resiliency in turn. The relationship between the FRM and the Number of Active Addresses is due to the hard-coded rules of the protocol: fees increase when demand for transactions is high, leading to a decrease in demand when the fee level reaches a threshold that is not deemed acceptable for the demand side of the fee market.



Discussion

Research about blockchain has intensified in recent years, and a central area of concern has been how blockchains will adapt to address issues with scalability (Zhou et al. 2020). Moreover, regarding Bitcoin, there are concerns that miners will require higher transaction fees as their main source of revenue (Kaskaloglu 2014), and this could mean that fees could become prohibitively high. The Lightning Network has been proposed as a complementary technology that should be able to address these cost and scalability issues of Bitcoin without compromising on security. While there are numerous theoretical arguments in

support of these benefits, this paper presents what we believe to be the first empirical study of Bitcoin that scrutinizes these claims.

The results are encouraging for proponents of the Lightning Network. First, the analysis suggests that when we see an increase in the use of the Lightning Network as a platform for exchange, we should expect a subsequent increase in the number of active users across the Bitcoin main network. Second, the analysis suggests that when we see an increase in the use of the Lightning Network as a platform for exchange, we should expect a decrease in FRM growth. This implies that when the Lightning Network is used more intensively, the main network becomes both more popular and more secure.

Relating these results to other general technology trends, we argue that the observed patterns are consistent with the classic theory of complementary externalities, which predicts that the adoption of one technology depends on the adoption of its complementary technologies (Dewan et al. 2010). The value of complementary externalities is one of the reasons why digital platforms have become such an important part of the digital landscape, as they provide a compelling socio-technical foundation where the value of the system increases with each new participant and each new functionality (Cusumano et al. 2020). Nonetheless, it is here that emerging systems with a strong ideological element, such as Bitcoin, face a dilemma, assuming they wish to enact systemic change and become one of these influential digital platforms.

When describing revolutionary systemic changes, Lyytinen and Newman (2008) argue that the presence of distinct, non-mainstream values allows experimental “building systems” to find new configurations of technologies, structures, actors, and tasks. For Bitcoin, this means the desire for absolute decentralization provided the impetus for a range of related innovations, such as ways to validate transactions and ways to maintain pseudoanonymity.

As a building system becomes more mainstream, it starts to challenge the status quo for dominance. Such a challenge is based on the building system’s ability to address gaps and tensions among system components in the status quo and/or gaps and tensions with the deeper structures supporting the system. For Bitcoin, this may conceivably include concerns regarding fees for international payments or frustrations with perceived corruption in large financial institutions, for example. However, the building system will inevitably create new tensions and gaps if it reaches mainstream adoption, given that it evolved within a set of deep structures and socio-technical elements that were necessarily distinct from the mainstream system. Some of the obvious examples for Bitcoin include its inability to process transactions sufficiently quickly for general commerce and its high energy consumption of mining protocols (Cousins et al. 2019). The key to addressing these gaps and tensions appears to be for Bitcoin to compromise the degree of decentralization demanded by complementary technologies – in this case, the Lightning Network.

These findings resonate with observations regarding the evolution of open-source software. That movement also began within a community dedicated to open participation and a non-consumerist attitude to systems development, before later becoming more permissive and pragmatic, as open source tools and projects became mainstream and commercial institutions and entrepreneurs became active and useful participants (Fitzgerald 2006; Medappa and Srivastava 2020). The result was a movement away from a single archetypical open-source license to a range of licenses, many of which facilitate restrictions on participation and dissemination activities (Sen et al., 2008).

Despite these similarities with other technological trends, the willingness of Bitcoin users to accept a less-decentralized layer 2 technology like the Lightning Network is nonetheless a significant observation, given that issues related to blockchain decentralization have produced polarized views in the past (Beck et al. 2017) and that Bitcoin is often seen as the standard bearer for maintaining decentralization (Mattke et al. 2021). We have limited basis from our study design to explain why this concession appears to be effective. This is because our focus in this study was to perform causal discovery related to prediction, rather than explanation (cf. Gregor 2006); that is, we wanted to explore *whether* rather than *why* the adoption of layer 2 technologies is likely to increase the adoption and security of Bitcoin. We argue that the next step is therefore to theorize more substantively around the causal mechanisms that would explain why the Lightning Network, and perhaps layer 2 technologies in general, appear to have a positive impact on these variables.

For example, perhaps long-term users and new users alike are encouraged by the ability of system developers to react to technological concerns. This could be explained by theories of “signaling”, in which

information recipients look for signs of unobservable qualities in others (Connelly et al. 2011), such as innovativeness or technology competence in this instance. Alternatively, perhaps the Lightning Network is alienating long-term users of Bitcoin who are committed to system decentralization, but this number is lost in the shadow of a larger number of new performance or sustainability-driven users drawn to Bitcoin by the Lightning Network. This could represent a form of “mavenism”, where products or services both attract and lose users, due to associated changes in status consumption and creative choice counterconformity (Goldsmith et al. 2006). Whatever the explanation, more explicit theorization and measurement are needed to expand on the results in this study. This may require methods more amenable to causal inference, such as natural experiments, quasi-experiments, and instrumental variables (Angrist and Pischke 2009).

Practical Implications

First, the role of layer 2 technology suggests that the success of a blockchain is likely to rely heavily on the inclusion of new additions to the technological stack. This conclusion is important because it mitigates concerns that the blockchain trilemma cannot be solved. This multi-layer approach is similar to the one adopted to develop the technological protocol of the so-called “Internet” (Loshin 2003). Nowadays, most people understand the potential of the Internet and take it for granted. Indeed, for many people and organizations, the Internet has become a necessary infrastructure as the electricity grid and telecommunication network. But even the most basic Internet operations require a number of layers of infrastructure, protocols, and APIs that have been developed over more than forty years. From a technical perspective, the Internet is known as the Transmission Control Protocol/Internet Protocol (TCP/IP), i.e., a stack of protocols. This stack includes (i) the Link layer, (ii) the Network layer, (iii) the Transport layer, and (iv) the Application layer—each layer responsible for a different facet of the communication (Stevens and Wright 1996). The future development of blockchain is likely to rely on a similar stack-based architecture. Undoubtedly, there are still numerous standards, protocols, and services needed for the smooth functioning of blockchain infrastructure.

Second, the role of Bitcoin within the blockchain field may change in the next few years. Most of today’s classes of decentralized applications (DApps) – such as Decentralized Finance (DeFi), Non-Fungible-Tokens (NFT), and Self-Sovereign Identity (SSI) – were developed on top of other blockchain protocols, especially the Ethereum blockchain (Stockburger et al. 2021). Moreover, most cryptocurrencies have been developed to overcome some of Bitcoin’s technical limitations, especially in terms of scalability. The Lightning Network may boost the diffusion of Bitcoin through the Lightning Applications (LApps) that can enable services, such as micropayments, decentralized securities transfers, and token exchanges, to name a few (Miraz and Donald 2019). The Lightning Network is especially promising for developers, given that the growing use of the Lightning Network appears to precipitate Bitcoin becoming faster, cheaper, and more private without entailing its security levels.

The findings also suggest that layer 2 technologies generate positive network effects. To date, most of the efforts analyzing layer 2 technologies have taken a technical perspective, focusing on specific features such as scalability, security, decentralization, privacy and fees (Gudgeon et al. 2020; Sguanci et al. 2021). While it is widely accepted that layer 2 technologies have the potential to enable blockchains scalability in a private and secure way, the findings of this study suggest that layer 2 technologies can improve blockchain’s utility and enhance the overall network’s value, which in turn may have a positive impact on the general adoption of blockchain. These results suggest that there are positive network effects enabled by layer 2 technologies (Luther 2016; Stylianou et al. 2021). The network effects and complementary externalities of layer 2 technologies should be studied in further detail.

From a research perspective, the aforementioned time-series model could represent a starting point for further investigating the role of layer 2 technologies in the cryptocurrency field and in blockchain in general.

Challenges and limitations

Blockchain is an accelerating force of innovation that offers radical openness of dynamic repositories on a global scale (Avital et al. 2016). This analysis shows the value in considering the longevity of blockchain technologies according to the capacity for complementary developments, rather than just the technologies themselves. Executives interested in long-term investments in cryptocurrencies may wish to prioritize those

blockchain projects complemented by promising layer 2 technologies or more active development communities.

The findings from this study also raise interesting questions about whether blockchain will eventually be subject to a winner-take-all dynamic, whereby a small number of cryptocurrencies will eventually become the dominant players due to the high network externalities involved (De Rossi et al. 2022). The prevailing assumption regarding most maturing systems is that over time they become increasingly rigid and, in turn, obsolete, because new and better socio-technical systems replace them (Christensen 1997; Lyytinen and Newman 2008). The act of facilitating such novel technology stacks arguably transforms Bitcoin from a technology to a platform, and such platforms tend to follow different trajectories, in which the incumbent tends to benefit from both longevity and monopoly (Cusumano 2022).

This study has some limitations. First, other variables could be used as proxies: node-level data rather than channel-level series and hash rate as a general measure for the security of the network, among others. Future research may also consider the expression of sums of money in terms of Bitcoin rather than US Dollars. Second, the model has not been applied nor generalized to other cryptocurrencies or other layer 2 technologies, thus making it infeasible to provide general implications for other prominent crypto ecosystems, such as Ethereum. We call for future research to make these comparisons and add more nuance to our collective understanding of layer 2 technologies and their implications.

Conclusion

We began this paper by highlighting the need to understand how layer 2 technologies impact the long-term prospects of blockchain. Subsequently, we created an original database of 1,494 daily observations on Bitcoin and the Lightning Network. Based on this data pool, we developed a time-series model to observe relationships between the expansion of the Lightning Network, the adoption of Bitcoin and its overall security levels. In view of the scarce IS research on the Lightning Network, this study demonstrates the relevance of this research topic and how it may be instrumental to determine the future of Bitcoin. Finally, we demonstrate that growing activity on the Lightning Network precipitates increased use of and security for Bitcoin. We hope that future related research will focus on developing robust consolations of layer 2 technologies that take into consideration high-impact everyday life use-case scenarios.

References

- Altarawneh, A., Herschberg, T., Medury, S., Kandah, F., and Skjellum, A. 2020. "Buterin's Scalability Trilemma Viewed through a State-Change-Based Classification for Common Consensus Algorithms," in 2020 10th Annual Computing and Communication Workshop and Conference (CCWC), Las Vegas, pp. 727–736.
- Angrist, J. D., and Pischke, J.-S. 2009. *Mostly Harmless Econometrics: An Empiricist's Companion*.
- Arcane Research. 2021. "The State of Lightning," Oslo, October. (<https://www.research.arcane.no/the-state-of-lightning>).
- Asteriou, D., and Hall, S. G. 2007. *Applied Econometrics: A Modern Approach Using EViews and Microfit*, (Ed. riv.), Basingstoke.
- Ateniese, G., Bonacina, I., Faonio, A., and Galesi, N. 2014. "Proofs of Space: When Space Is of the Essence," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (8642), pp. 538–557.
- Avital, M., Beck, R., King, J. L., Rossi, M., & Teigland, R. 2016. "Jumping on the blockchain bandwagon: Lessons of the past and outlook to the future," *Proceedings of the 37th International Conference on Information Systems*, Dublin, Ireland.
- Bartoletti, M., Lande, S., and Podda, A. S. 2017. "A Proof-of-Stake Protocol for Consensus on Bitcoin Subchains," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (10323), pp. 568–584.
- Baur, A. W., Bühler, J., Bick, M., and Bonorden, C. S. 2015. "Cryptocurrencies as a Disruption? Empirical Findings on User Adoption and Future Potential of Bitcoin and Co," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (9373), pp. 63–80.
- Beck, R., Avital, M., Rossi, M., and Thatcher, J. B. 2017. "Blockchain Technology in Business and

- Information Systems Research,” *Business & Information Systems Engineering*, pp. 381–384.
- Bentov, I., Lee, C., Mizrahi, A., and Rosenfeld, M. 2014. “Proof of Activity,” *ACM SIGMETRICS Performance Evaluation Review* (42:3), pp. 34–37.
- Carlsten, M., Kalodner, H., Narayanan, A., and Weinberg, S. M. 2016. “On the Instability of Bitcoin without the Block Reward,” in *Proceedings of the ACM Conference on Computer and Communications Security* (Vol. 24-28-Octo), Vienna, October 24, pp. 154–167.
- Carter, N. 2020. Bitcoin as a Novel Economic Institution. (<https://www.docdroid.net/FbgH1WS/bitcoin-institution-riga-pdf>).
- Christensen, C. M. 1997. *The Innovator’s Dilemma: When New Technologies Cause Great Firms to Fail*, Boston.
- Ciaian, P., Kancs, D., and Rajcaniova, M. 2021. “The Economic Dependency of Bitcoin Security,” *Applied Economics* (53:49), pp. 5738–5755.
- Cohen, B. 2017. “The Rise of Alternative Currencies in Post-Capitalism,” *Journal of Management Studies* (54:5), pp. 739–746.
- Coinmarketcap. (2022, August). Today's Cryptocurrency Prices by Market Cap. <https://coinmarketcap.com>.
- Connelly, B. L., Certo, S. T., Ireland, R. D., and Reutzel, C. R. 2011. “Signaling Theory: A Review and Assessment,” *Journal of Management* (37:1), pp. 39–67.
- Courtois, N. T., Grajek, M., and Naik, R. 2014. “Optimizing SHA256 in Bitcoin Mining,” *Communications in Computer and Information Science* (448), pp. 131–144.
- Cousins, K., Subramanian, H., and Esmaeilzadeh, P. 2019. “A Value-Sensitive Design Perspective of Cryptocurrencies: A Research Agenda,” *Communications of the Association for Information Systems* (45:1), p. 27.
- Cusumano, M. 2022. “The Evolution of Research on Industry Platforms,” *Academy of Management Discoveries* (8:1).
- Cusumano, M., Yoffie, D., and Gawer, A. 2020. *The Future of Platforms*, MIT Sloan Management Review.
- Del Monte, G., Pennino, D., and Pizzonia, M. 2020. “Scaling Blockchains Without Giving up Decentralization and Security: A Solution to the Blockchain Scalability Trilemma,” in *CryBlock ’20: Proceedings of the 3rd Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, New York: Association for Computing Machinery (ACM), September 21, pp. 71–76.
- Dewan, S., Ganley, D., and Kraemer, K. L. 2010. “Complementarities in the Diffusion of Personal Computers and the Internet: Implications for the Global Digital Divide,” *Information Systems Research* (21:4), pp. 925–940.
- De Rossi, L. M., Avital, M., and Gleasure, R. 2022. “The Proliferation of End Users as a Success Metric for Cryptocurrencies,” in *Proceedings of the 55th Hawaii International Conference on System Sciences*, Hawaii: Hawaii International Conference on System Sciences (HICSS), pp. 6083–6092.
- Easley, D., O’Hara, M., and Basu, S. 2019. “From Mining to Markets: The Evolution of Bitcoin Transaction Fees,” *Journal of Financial Economics* (134:1), pp. 91–109.
- Enders, W. 1995. *Applied Econometric Time Series*, New York.
- Engle, R. F., and Granger, C. W. J. 2015. “Co-Integration and Error Correction: Representation, Estimation, and Testing,” *Applied Econometrics* (39:3)..
- Fisch, C., Masiak, C., Vismara, S., and Block, J. 2021. “Motives and Profiles of ICO Investors,” *Journal of Business Research* (125), pp. 564–576.
- Fitzgerald, B. 2006. “The Transformation of Open-Source Software,” *MIS Quarterly: Management Information Systems* (30:3), Management Information Systems Research Center, pp. 587–598.
- Gao, J., Li, B., and Li, Z. 2020. “Blockchain Storage Analysis and Optimization of Bitcoin Miner Node,” *Lecture Notes in Electrical Engineering* (517), pp. 922–932.
- Goldsmith, R. E., Clark, R. A., and Goldsmith, E. B. 2006. “Extending the Psychological Profile of Market Mavenism,” *Journal of Consumer Behaviour: An International Research Review* (5:5), pp. 411–419.
- Gorjón Rivas, S. 2021. “The Role of Cryptoassets as Legal Tender: The Example of El Salvador,” *Economic Bulletin - Banco de España* (2021:4).
- Granger, C. W. J. 1969. “Investigating Causal Relations by Econometric Models and Cross-Spectral Methods,” *Econometrica* (37:3), p. 424.
- Granger, C. W. J., and Joyeux, R. 1980. “An Introduction to Long-Memory Time Series Models and Fractional Differencing,” *Journal of Time Series Analysis* (1:1).
- Granger, C. W. J., and Newbold, P. 1974. “Spurious Regressions in Econometrics,” *Journal of Econometrics* (2:2), pp. 111–120.

- Gregor, S. 2006. "The Nature of Theory in Information Systems," *MIS Quarterly*, pp. 611–642.
- Gudgeon, L., Moreno-Sanchez, P., Roos, S., McCorry, P., and Gervais, A. 2020. "Sok: Layer-Two Blockchain Protocols," in *International Conference on Financial Cryptography and Data Security*, pp. 201–226.
- Guidolin, M., and Pedio, M. 2018. "Essentials of Time Series for Financial Applications," *Essentials of Time Series for Financial Applications*, London: United Kingdom: Academic Press.
- Hackett, R., and Wieczner, J. 2018. "How High Will Bitcoin Go?," *Fortune* (177:1), pp. 36–44.
- Hafid, A., Hafid, A. S., and Samih, M. 2020. "Scaling Blockchains: A Comprehensive Survey," *IEEE Access* (8), Institute of Electrical and Electronics Engineers Inc., pp. 125244–125262.
- Hinzen, F. J., John, K., and Saleh, F. 2022. "Bitcoin's Limited Adoption Problem," *Journal of Financial Economics* (144:2), pp. 347–369.
- Holland, P. W. 1986. "Statistics and Causal Inference," *Journal of the American Statistical Association* (81:396), pp. 945–960.
- Holub, M., and Johnson, J. 2018. "Bitcoin Research across Disciplines," *Information Society* (34:2).
- Hoogendoorn, R. 2019. "The Lightning Network as Bitcoin's Rocket to the Moon," *The Startup*, , November 13.
- Houy, N. 2014. "The Economics of Bitcoin Transaction Fees," No. 1407, Working Papers, Lyon: Elsevier BV.
- Jun Ren, A. H., Feng, L., Cheong, S. A., and Goh, R. S. M. 2019. "Optimal Fee Structure for Efficient Lightning Networks," in *Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, Singapore, February 19, pp. 980–985.
- Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., Miller, A., and Meiklejohn, S. 2021. "An Empirical Analysis of Privacy in the Lightning Network," *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)* (12674), pp. 167–186.
- Kaskaloglu, K. 2014. "Near Zero Bitcoin Transaction Fees Cannot Last Forever," in *The International Conference on Digital Security and Forensics (DigitalSec2014)*, Ostrava, pp. 93–101.
- Khan, N., and State, R. 2019. "Lightning Network: A Comparative Review of Transaction Fees and Data Analysis," in *Blockchain and Applications, Advances in Intelligent Systems and Computing*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado (eds.), pp. 11–18.
- Kiayias, A., and Litos, O. S. T. 2020. "A Composable Security Treatment of the Lightning Network," *Proceedings - IEEE Computer Security Foundations Symposium (2020-June)*, Boston, June 22–26, pp. 334–349.
- Kim, S. T. 2020. "Bitcoin Dilemma: Is Popularity Destroying Value?," *Finance Research Letters* (33), p. 101228.
- Labazova, O. 2019. "Towards a Framework for Evaluation of Blockchain Implementations," *Proceedings of the 40th International Conference on Information Systems*, Munich, Germany.
- Lee, S., and Kim, H. 2020. "On the Robustness of Lightning Network in Bitcoin," *Pervasive and Mobile Computing* (61), p. 101108.
- Leibowitz, M. 2018. "Introducing: Fee Ratio Multiple (FRM)," *Medium*, , October 1.
- Lin, J. H., Primicerio, K., Squartini, T., Decker, C., and Tessone, C. J. 2020. "Lightning Network: A Second Path towards Centralisation of the Bitcoin Economy," *New Journal of Physics* (22:8).
- Loi, H. 2017. "The Liquidity of Bitcoin," *International Journal of Economics and Finance* (10:1), Canadian Center of Science and Education, p. 13.
- Loshin, P. 2003. *TCP/IP Clearly Explained*.
- Luther, W. J. 2016. "Cryptocurrencies, Network Effects, And Switching Costs," *Contemporary Economic Policy* (34:3).
- Lyytinen, K., and Newman, M. 2008. "Explaining Information Systems Change: A Punctuated Socio-Technical Change Model," *European Journal of Information Systems* (17:6), pp. 589–613.
- Mattke, J., Maier, C., Reis, L., and Weitzel, T. 2021. "Bitcoin Investment: A Mixed Methods Study of Investment Motivations," *European Journal of Information Systems* (30:3), pp. 261–285.
- Maziarz, M. 2015. "A Review of the Granger-Causality Fallacy," *The Journal of Philosophical Economics: Reflections on Economic and Social Issues* (8:2), Rosetti International Publishing House, pp. 86–105.
- Mechkaroska, D., Dimitrova, V., and Popovska-Mitrovikj, A. 2018. "Analysis of the Possibilities for Improvement of BlockChain Technology," 2018 26th Telecommunications Forum, TELFOR 2018 - Proceedings, Institute of Electrical and Electronics Engineers Inc.
- Medappa, P. K., and Srivastava, S. C. 2020. "Ideological Shifts in Open Source Orchestration: Examining the Influence of Licence Choice and Organisational Participation on Open Source Project Outcomes,"

- European Journal of Information Systems (29:5), Taylor & Francis, pp. 500–520.
- Miraz, M. H., and Donald, D. C. 2019. “Lapps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications,” ACM International Conference Proceeding Series, Association for Computing Machinery, pp. 185–189.
- Misra, S. 2018. “What Is the Lightning Network?,” Medium, , May 20..
- Moraffah, R., Sheth, P., Karami, M., Bhattacharya, A., Wang, Q., Tahir, A., Raglin, A., and Liu, H. 2021. “Causal Inference for Time Series Analysis: Problems, Methods, and Evaluation,” Knowledge and Information Systems (63:12), pp. 3041–3085.
- Nakamoto, S. 2008. “Bitcoin: A Peer-to-Peer Electronic Cash System,” Cryptography Mailing List, pp. 1–9.
- NYDIG. 2022. “The Bitcoin Lightning Network,” NYDIG Research.
- Poon, J., and Dryja, T. 2016. “The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments,” , January. (<https://lightning.network/lightning-network-paper.pdf>).
- Ramaswamy, B. 2020. “The Bitcoin Whitepaper,” Medium, , June 3. (<https://medium.com/@bhavishramaswamy/the-bitcoin-whitepaper-summary-1038c8e5c36>, accessed March 31, 2022).
- Renwick, R., and Gleasure, R. 2021. “Those Who Control the Code Control the Rules: How Different Perspectives of Privacy Are Being Written into the Code of Blockchain Systems,” Journal of Information Technology (36:1).
- Sen, R., Subramaniam, C., and Nelson, M. L. 2008. “Determinants of the Choice of Open Source Software License,” Journal of Management Information Systems (25:3), pp. 207–240.
- Sguanci, C., Spatafora, R., and Vergani, A. M. 2021. “Layer 2 Blockchain Scaling: A Survey,” ArXiv Preprint ArXiv:2107.10881.
- Stevens, W. R., and Wright, G. R. 1996. TCP/IP Illustrated: Volume 2, Addison-wesley.
- Stock, J. H., and Watson, M. W. 2001. “Vector Autoregressions,” Journal of Economic Perspectives (15:4), American Economic Association, pp. 101–115.
- Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., and Avital, M. 2021. “Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation,” Blockchain Research and Applications (2:2), pp. 1-18.
- Stylianou, K., Spiegelberg, L., Herlihy, M., and Carter, N. 2021. “Cryptocurrency Competition and Market Concentration in the Presence of Network Effects,” Ledger (6), University Library System, University of Pittsburgh, pp. 81–101.
- Tanner, J. 2020. “The Biggest Problems of Bitcoin That People Are Not Speaking About,” Medium, , March 10.
- The Block. (2022, August). Alternative Crypto Metrics Social. <https://www.theblock.co/data/alternative-crypto-metrics/social>
- Uddin, M. A., Ali, M. H., and Masih, M. 2020. “Bitcoin - A Hype or Digital Gold? Global Evidence,” Australian Economic Papers (59:3), pp. 215–231.
- Zhou, Q., Huang, H., Zheng, Z., and Bian, J. 2020. “Solutions to Scalability of Blockchain: A Survey,” IEEE Access (8), pp. 16440-16455.